博士論文

Sybil-Resistant Self-Sovereign Identity Based-on Attested Execution Secure Processors

Koichi Moriyama
森山 光一

情報セキュリティ大学院大学
情報セキュリティ研究科
情報セキュリティ専攻

2025年3月

Sybil-Resistant Self-Sovereign Identity Based-on Attested Execution Secure Processors

Koichi Moriyama

Submitted in partial fulfillment of the requirements
for the Degree of Doctor of Philosophy in Informatics
at the Graduate School of Information Security

INSTITUTE OF INFORMATION SECURITY, JAPAN

March 2025

List of Publications

This thesis is based on the below publications.

Peer-Reviewed Journal Articles

[**MO24**] Koichi Moriyama and Akira Otsuka, "Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors," In *IEICE Transactions on Information and Systems – Special Section on Blockchain and Security, VOL.E107-D, NO.9*, pages 1112-1122, September 1, 2024. IEICE. doi: 10.1587/transinf.2023BCI0001

[**MO25**] Koichi Moriyama and Akira Otsuka. "Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors and Zero-Knowledge Membership Proofs," In *IEEE Access, Vol.13*, pages 17919-17944, January 24, 2025. IEEE. doi: 10.1109/ACCESS.2025.3533877

A Peer-Reviewed Paper in Proceedings of International Conference

[**MO22**] Koichi Moriyama and Akira Otsuka. "Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors." In *IEEE Blockchain 2022*, pages 1–10, Espoo, Finland, August 2022. IEEE. doi: 10.1109/Blockchain55522.2022.00012 [1]

[1]

Preprint (Bulletin at Institute of Information Security)

[**MO23**] Koichi Moriyama and Akira Otsuka. "Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors." In「情報セキュリティ総合科学」, Vol.14, 2023年2月. 情報セキュリティ大学院大学. https://www.iisec.ac.jp/proc/vol0014/moriyama-otsuka23.pdf

Abstract

The current circumstances that require people to be more online has encouraged me to address digital identity, preserving privacy. There is a momentum of research addressing self-sovereign identity (SSI); many research approaches credential systems and blockchain technology as a foundation. SSI brings various benefits to natural persons, such as owning controls; conversely, digital identity systems in the real world require Sybil-resistance as a critical requirement to comply with anti-money laundering (AML) and other needs such as metaverse services. I will propose two core ideas in this thesis: one is a new architecture and a set of system protocols for building a secure Sybil-resistant SSI system over permissionless blockchains utilizing attested execution secure processors (AESPs), and the other is a novel scheme that enables unlinkability among credentials with commitment-based identifiers in secure and anonymous Sybil-resistant SSI systems by utilizing zero-knowledge membership proofs and other techniques.

AESP-Based Sybil-Resistant SSI Architecture and System Protocols. This thesis first proposes an architecture and a set of system protocols for building a secure Sybil-resistant SSI system by utilizing permissionless blockchain technology and Rafael Pass, Elaine Shi, and Florian Tramèr's contribution of the formal abstraction of AESPs. The proposal of Sybil-resistant SSI architecture and system protocols utilizing AESPs, $\Pi^{\mathcal{G}_{\mathtt{att}}}$, demonstrates the powerfulness of hardware-assisted security and the formal abstraction of AESPs, fitting into building a proper SSI system that satisfies Sybil-resistance. Assuming AESPs and $\mathcal{G}_{\mathtt{att}}$, the protocols may eliminate a distributed committee of trusted nodes assumed in other research such as CanDID proposed by Deepak Maram *et al.*; thus, $\Pi^{\mathcal{G}_{\mathtt{att}}}$ allows not to rely on multi-party computation (MPC), and it brings drastic flexibility and efficiency compared to existing SSI systems.

Anonymous Sybil-Resistant SSI Utilizing Zero-Knowledge Membership Proofs. In addition, this thesis proposes a novel scheme that enables users (holders) to request verifiers to verify their credentials without AESPs, and it further achieves unlinkability among derived credentials created for public verification. In the scheme, as a set of the extended secure, anonymous and Sybil-resistant SSI system protocols $\Pi^{\mathcal{G}_{\text{att}}+}$, I propose a simplified format of computed claims in Boolean, commitment-based anonymous identifiers incorporating Pedersen commitments, so-called *perfectly anonymous identifiers*, and a technique to utilize zero-knowledge membership proofs, in particular, Jens Groth and Markulf Kohlweiss' "One-Out-of-Many Proofs" Σ-protocol that can prove the existence of an expected credential among anonymous credentials in Sybil-resistant SSI systems in logarithmic order in the population. Along with other techniques to make the best use of the BBS+ signature scheme and proofs of equality about discrete logarithms for verifying such anonymous credentials, I demonstrate how the proposed scheme can resolve the conflicting requirements, preserving privacy and dealing with AML, with having a higher level of assurance for Sybil-resistance and pragmatic performance for identifying and verifying an expected credential than the other existing research. Entitling unlinkability among credentials in the anonymous Sybil-resistant SSI results in proper privacy preservation.

Acknowledgment

First, I sincerely thank my supervisor, Prof. Akira Otsuka, for supporting my work while studying at the Institute of Information Security, Japan. I was very fortunate to have the chance to meet with him online during the pandemic for a project led by a governmental agency in January 2021. I immediately decided to join his laboratory for research addressing preserving the privacy of digital identities through modern cryptographic approaches. In the early days of this project, he introduced me to one of the papers by David Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete" (1985). This paper deeply inspired me to get involved in such cryptographic approaches, which also utilized a device (a card computer in his case) based on my experiences in the tech industry. He guided me to this domain's frontier; I enjoyed working on the project and cannot sufficiently express my appreciation for his dedication in words alone.

I am very thankful to the Doctoral Dissertation Review Committee of Prof. Kazue Sako at Waseda University, Prof. Kazumasa Omote at the University of Tsukuba, and Prof. Seigo Arita at the Institute of Information Security, Japan. Their insightful feedback at the preliminary examination held in August 2023 and the subsequent examination held in February 2024 was pivotal in shaping and advancing my research. Their constructive, valuable, and profound suggestions have helped me to proceed with and accomplish the research accordingly.

I thank former Prof. Mario Tokoro at Keio University and Dr. Yasuhiko Yokote at Sony Computer Science Laboratories, Inc. (in those days), and Prof. Calton Pu at the College of Computing, Georgia Institute of Technology, who guided my development as a researcher while I was a student at Prof. Tokoro's laboratory, Computer Science, Keio University from 1991–1994 and a research scholar at Georgia Tech from 1999–

2000, respectively. I appreciate their dedicated support; it's been a foundation for my research work.

I want to thank the anonymous reviewers of my papers as well as many contributors in the tech industry's digital identity domain, including my colleagues at FIDO Alliance and the World Wide Web Consortium (W3C), Mr. Nat Sakimura, chairman of OpenID Foundation, and other practitioners who helped me learn about digital identity and contribute my efforts to the industry. While working as a colleague on the Board of Directors at W3C, Inc., Prof. Jun Murai at Keio University encouraged my parallel works of business, the tech industry, and this research with considerable suggestions.

I am also thankful to my executive management and colleagues at NTT DOCOMO, INC. They have kindly assisted me with the research project while I am employed as that company's Chief Security Architect, a Corporate Evangelist.

Lastly, I extend my deepest gratitude to my family: wife (Chikako), daughter (Momoko), son (Tomohiro), parents (Teruhiko and Setsuko), and parents-in-law (The Komakine). Their unwavering support and understanding have been the cornerstone of my research journey, and their encouragement to balance my research with other responsibilities in life has been invaluable.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Our lives have changed throughout the pandemic and require more online activities than before. Identifying who I am and who you are has become critical. Conversely, people have retained their privacy concerns much more than ever before. Digital identity must be a valuable domain for cryptographers and practitioners utilizing modern cryptography to address and resolve problems from various perspectives, such as digital cash and electric voting systems. I want to solve the problem of conflict by preserving privacy and verifying identification in digital identity with modern cryptographic approaches.

Self-sovereign identity (SSI) [PR21] is gaining momentum in academia and the tech industry. Christoper Allen wrote a blog article regarding the ideas of SSI with the ten principles in his definition [All16], followed by numerous research and industry implementations [DA18, FCO19, NJ20a, Boy21]. The terminology "Self-Sovereign" inspires many people to think about how SSI can protect privacy and resolve reliance on authorities that may control personal data. These efforts are not limited to technology, government, and human beings. One of these studies addressed the relationship between SSI and GDPR [KE20], whereas some initiatives already exist to utilize SSI in Europe [Gom19, Seu19] and Canada [Boy21].

Many studies in this domain have addressed SSI systems architecture utilizing blockchain technology [Müh+18, SP18]. Some researchers have discussed the necessity of blockchain technology and concluded that it is not necessary; however, they still recognize that it is a good foundation [Bok+19]. All the well-known existing implemen-

tations utilize blockchain, such as uPort on Ethereum [NJ20b] and Sovrin on the Sovrin ledger [Win21].

Digital identity systems in the real world now require a crucial requirement of Sybil-resistance [Dou02] to comply with anti-money laundering (AML) and other needs. It is a critical and conflicting requirement from the perspective of preserving privacy. Deepak Maram *et al.* addressed the requirement in their research of CanDID [Mar+21]; however, they assume a distributed committee of trusted nodes, not a permissionless blockchain, in their scheme.

I address the problem of conflict by preserving privacy and verifying identification for SSI (permissionless) while meeting with the Sybil-resistance requirement in this thesis, and have achieved two significant contributions with proposals for each; one is the attested execution secure processors (AESPs)-based Sybil-resistant SSI systems architecture and protocols, and the other is *anonymous* Sybil-resistant SSI systems utilizing zero-knowledge membership proofs and other techniques.

1.1 AESP-Based Sybil-Resistant SSI Architecture and System Protocols

One of the papers by David Chaum [Cha85] and his approach to avoid unexpected tracing by someone else like Big Brother[1] utilizing pseudonyms, digital signatures, and card computers inspired me to consider using mobile devices with recent hardware-assisted secure modules such as the Global Platform-supported Secure Elements (GP-SE)[2] when I got started this research addressing the conflicting requirement of preserving privacy in the real world today with modern cryptographic approaches.

I surveyed research papers, tech-industry implementations, and others, including a book on SSI [PR21]. Figure 1.1 illustrates my interpretation of typical SSI architecture, where a verifiable credential (VC) issued by an issuer is passed to a verifier as a derived credential (DC) or a verifiable credential for presentation controlling their attributes

[1]See the novel by George Orwell, *"Nineteen Eighty-Four(1984) – Big Brother Is Watching You,"* published in 1948.

[2]`https://globalplatform.org/resource-publication/introduction-to-secure-elements/`

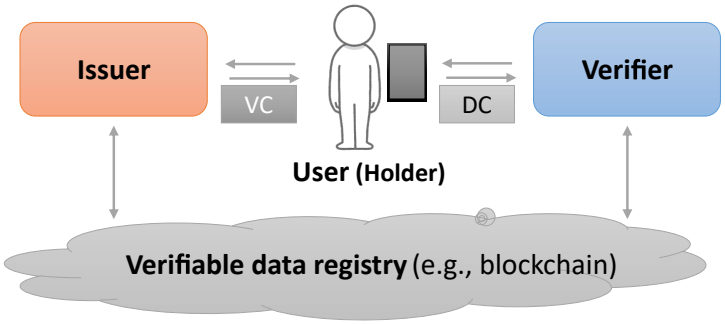


Figure 1.1: Proposed Self-Sovereign Identity Systems in the Tech Industry

disclosure. A blockchain is assumed to work as a verifiable data registry.

However, surprisingly, to the best of our knowledge, no study has addressed the opportunity to utilize hardware-assisted security [CLD16, Shi+17] implemented within mobile devices that people own in their daily lives. Several studies and implementations have addressed mobile apps for SSI systems, but these mobile apps focus on user experiences and have never addressed security feature perspectives. This result reminds me of the approach by David Chaum. The card computer expressed in 1985 was a dream written as a vision; however, it has become real, and secure processors are also becoming the norm in such mobile devices as a mandatory requirement today. Why do we not utilize such capabilities to build SSI systems and resolve the problem of conflict?

This thesis, firstly, proposes a permissionless blockchain-based SSI systems architecture that utilizes the formal abstraction of AESPs [PST17] equipped in mobile devices.

Contributions (1/2)

- Demonstrate the powerfulness of hardware-assisted security and the formal abstraction of AESPs that fit to build a secure SSI system satisfying the Sybil-resistance requirement.

- In concrete, propose the AESP-based SSI systems architecture and protocols $\Pi^{\mathcal{G}_{\mathtt{att}}}$ by a theorem, with its construction, security properties such as Sybil-resistance, and proof of the theorem through addressing each security property.

- Assuming AESPs and $\mathcal{G}_{\mathtt{att}}$, the AESP-based SSI system protocols $\Pi^{\mathcal{G}_{\mathtt{att}}}$ eliminates the online distributed committee of trusted nodes assumed in CanDID [Mar+21].

Thus, $\Pi^{\mathcal{G}_{\text{att}}}$ allows not to rely on multi-party computation (MPC) that requires such a distributed committee of trusted nodes, and it brings more flexibility and efficiency than the existing systems.

1.2 Anonymous Sybil-Resistant SSI Utilizing Zero-Knowledge Membership Proofs

I will further address the remaining open items in the first proposal. One is the stronger assumption that requires AESPs for all entities in the protocol; thus, not only a natural person who owns their mobile device equipped with an AESP but all verifiers require AESPs. In addition, linkability among credentials appears as long as pseudonyms are used as identifiers for credentials once those credentials become public. To solve these problems, I propose a novel scheme utilizing zero-knowledge membership proofs to realize unlinkability in managing verifiable credentials while meeting the Sybil-resistance requirement in SSI systems.

The World Wide Web Consortium (W3C)[3] has been contributing to this domain by defining some specifications, one of which is Verifiable Credentials Data Model [W3C22b, W3C24], already being utilized in decentralized digital identity and SSI system implementations. The W3C specifications refer to the signature scheme proposed by Jan Camenisch and Anna Lysyanskaya [CL02a] for implementers who want to extend verifiable credentials and verifiable presentations to support zero-knowledge proof systems. The recent revisions touch upon the BBS+ signature scheme [BBS04, CL04, ASM06] without references; it does not address details, but standardization bodies in the tech industry, such as the Internet Engineering Task Force (IETF)[4] and the Decentralized Identity Foundation (DIF)[5], have recently been focusing on it very proactively in order, for instance, to enable verifiers to prove possession of a signature [Kal22, Loo+23]. They call it unlinkable proofs via a zero-knowledge proof protocol utilizing the BBS+ signature scheme.

[3] `https://www.w3.org`

[4] `https://www.ietf.org`

[5] `https://identity.foundation`

Thanks to those recent and rapid efforts to address unlinkability; however, those credentials are identifiable by pseudonyms, such as Decentralized Identifiers (DIDs) [W3C22a], so that they are still linkable. In addition, we cannot forget the very important requirement of Sybil-resistance. The first proposal in this thesis addressed the problem in SSI under a permissionless blockchain while meeting the Sybil-resistance requirement, and the protocol $\Pi^{\mathcal{G}_{\mathtt{att}}}$ provides functions of issuing and verifying credentials utilizing AESPs [PST17] for both; however, ideally, verifiers would prefer to verify derived credentials under weaker assumptions, namely without AESPs.

Secondly, this thesis proposes a novel scheme for realizing unlinkability in managing verifiable credentials with computed claims in Sybil-resistant digital identity systems, primarily focusing on SSI. A verifier may still resolve a derived credential by verifying its existence utilizing zero-knowledge membership proofs and other techniques. In particular, I focused on the one-out-of-many proofs Σ-protocol by Jens Groth and Markulf Kohlweiss [GK15] as a building block, and proposed secure and anonymous Sybil-resistant SSI system architecture and the extended set of system protocols $\Pi^{\mathcal{G}_{\mathtt{att}}+}$, including commitment-based identifiers incorporating Pedersen commitments, so-called *perfectly anonymous identifiers*.

Contributions (2/2)

- Introduced a new notion of *computed claims*, a predicate ρ in Boolean form, computed from multiple claims certified by multiple issuers but cannot be claimed fraudulently only under the standard cryptologic assumptions. This concept is first implicitly introduced in CanDID, assuming a distributed committee of trusted nodes with multi-party secure computation (MPC). I followed, assuming a trusted hardware assumption, and this work first formally defines the concept.

- Also introduced *perfectly anonymous identifier* that utilizes Pedersen commitments for blinding identifiers, making verifiable credentials perfectly anonymous, among other credentials. In addition, I proposed a technique to utilize zero-knowledge membership proofs, "One-Out-of-Many Proofs" Σ-protocol in particular, enabling only the verifier to identify and verify the expected anonymous credential. Thanks to the efficiency of the one-out-of-many proofs, it brings loga-

rithm order for proving the existence of the anonymous Sybil-resistant credential among N those credentials.

- This thesis provides a set of protocols $\Pi^{\mathcal{G}_{\text{att}}+}$, definitions, and the main theorem and lemma with proofs that describe how the proposals combined with the Sybil-resistant SSI based on AESPs can resolve the conflicting requirements of anonymity and Sybil-resistance. Additionally, the construction incorporates generating a BBS+ signature for verifiers not to require AESPs for compatibility; thus, the novel scheme that achieves unlinkability among credentials successfully in secure and anonymous Sybil-resistant SSI has been demonstrated.

In Summary

In this thesis, I proposed the AESP-basd Sybil-resistant SSI architecture over a permissionless blockchain and a set of protocols $\Pi^{\mathcal{G}_{\text{att}}}$ that enable to build a secure SSI system meeting the Sybil-resistance requirement without MPC and requiring a distributed committee of trusted nodes. In addition, I addressed remaining issues under weaker assumptions, and proposed a novel scheme that utilizes zero-knowledge of membership proofs, in particular "One-Out-of-Many Proofs" Σ-protocol, and other techniques such as modern signature schemes (BBS+ signature scheme) and proof of knowledge about discrete logarithms to eliminate linkability among credentials. The scheme is also demonstrated as the extended set of system protocols $\Pi^{\mathcal{G}_{\text{att}}+}$ with *perfectly anonymous identifier* and other definitions; thus, it also enables public verifiers to verify credentials without AESPs. As a result, this thesis has demonstrated to a path to the future decentralized identity systems that resolve a conflicting problem of providing anonymity for preserving privacy and the real-world requirement of Sybil-resistance.

1.3 Structure of the Thesis

Chapter 2 describes some backgrounds of this thesis: digital identity, decentralized digital identity, and self-sovereign identity (SSI). In addition to the comprehensive survey regarding SSI in Section 2.4, Section 2.2.2 illustrates Deepak Maram *et al.*'s CanDID,

which addresses Sybil-resistance as a significant contribution of decentralized digital identity that influenced this thesis.

Chapter 3 provides some detailed description regarding Rafael Pass, Elaine Shi, and Florian Tramèr's formal abstraction of AESPs, Jan Camenisch and Anna Lysyanskaya's signature scheme and efficient protocols and related schemes and protocols, including the BBS+ signature scheme, and Jens Groth and Markulf Kohlweiss' "One-Out-of-Many Proofs" Σ-protocol.

In **Chapter 4**, I will propose one of the two core ideas, an architecture and a set of system protocols $\Pi^{\mathcal{G}_{\text{att}}}$ for building a secure Sybil-resistant SSI system by utilizing permissionless blockchain technology and the formal abstraction of AESPs. It includes an overview of the architecture and system protocols in detail, as well as security properties and proof of the theorem through addressing each security property.

Chapter 5 then will demonstrate a novel scheme and a set of system protocols $\Pi^{\mathcal{G}_{\text{att}}+}$ to realize unlinkability among credentials in AESP-based secure SSI systems and potentially other SSI systems by utilizing zero-knowledge membership proofs, in particular "One-Out-of-Many Proofs" Σ-protocol, and other techniques, including *perfectly anonymous identifiers*, and adopting and other signature schemes.

Chapter 6 addresses applications, limitations, and further directions for future research, and **Chapter 7** will conclude this thesis.

Chapter 2

Backgrounds

2.1 Digital Identity

The importance of "digital identity" is rapidly increasing under the current circumstances. Many people feel that many things have changed after the pandemic. People would need to do much more things online than before. Service providers, companies, and governmental organizations must provide services online for customers, employees, and citizens to deal with the circumstances. Ideas and past efforts on digital identity are not only for the occasion today, but accumulated contributions have helped society survive the pandemic.

Researchers and influencers in the tech industry in this domain refer to Kim Cameron's blog article, "The Laws of Identity" [Cam05]. Beyond the contribution, researchers and the industry have made significant efforts, including standardization bodies resolving many problems from various perspectives, such as identity proofing, authentication, and federation. Overall, recent digital identity efforts are mainly about how to verify their identity while preserving their privacy.

In digital identity approaches, managing claims and credentials is one of the essential elements of representing who I am or who you are. Identity is a set of attributes or claims by definitions, e.g., ISO/IEC 24760-1:2019/Amd 1:2023(en) [ISO23b], and a credential represents an identity for authentication. There are also many activities

at standardization bodies such as W3C[1], OpenID Foundation[2], and FIDO Alliance[3]. The NIST's Digital Identity Guidelines [GGF17] is a set of guidelines, NIST Special Publication 800-63-3 and its family, that address various perspectives through its digital identity model. Very recently, the NIST's Digital Identity Guidelines are being revised toward revision 4 of the guidelines[4], the first public draft issued in December 2023 and the second public draft issued on August 2024.

Digital identity management started from the Isolated User Identity (SILO) model by definition of Md Sadek Ferdous *et al.*'s work [Fer+15]. It then moved to the Federated User Identity (FED) model. They define a mathematical model of digital identity and its management. The (total) identity representing a natural person is a union of partial identities, each set of claims consisting of each attribute and its value pair. In the SILO model, each service provider maintains its identity domain with its IdP (Identity Provider). The FED model, on the other side, enables some previously agreed-upon service providers to share the unified identity domain, the federated domain. The FED model offers interoperability among different SILO domains, allowing users to utilize single-sign-on and other benefits. A limitation in their approach did not deal with privacy properties; however, they demonstrated that digital identity and identity management are moving from the most straightforward model toward federated models in a decentralized fashion.

One of the standards recently defines Attribute-based Unlinkable Entity Authentication (ABUEA) determined in ISO/IEC 27551:2021(en) [ISO21b]. Regarding digital identity for human beings, it is well-recognized that the importance of following OECD's privacy principles[5], the eleven privacy principles determined in ISO/IEC 29100:2011(en), and other privacy principles. ABUEA addresses a form of trust between two unfamiliar parties that share trust in a common third-party entity. Also, it approaches to define unlinkability among entities such as AP (Attribute Provider) and RP (Relying Party). Providing mechanisms to eliminate linkability for resolving

[1] `https://www.w3.org`

[2] `https://openid.net/foundation/`

[3] `https://fidoalliance.org`

[4] `https://pages.nist.gov/800-63-4/`

[5] `https://www.oecd.org/digital/privacy/`

privacy concerns has become more important than before in the tech industry and the real world.

2.2 Decentralized Digital Identity

In the tech industry, several initiatives are addressing decentralized digital identity. Microsoft has been driving an initiative[6] and announced ION[7] on behalf of the Decentralized Identity Foundation (DIF)[8] in May 2021. The approach utilizes W3C's contributions, Verifiable Credentials Data Model [W3C22b] and Decentralized Identifiers (DIDs) [W3C22a], decentralized systems such as blockchains and ledgers, and DIF's standards. There is another industry consortium addressing decentralized identity, DID Alliance[9].

There are also many pieces of research addressing decentralized identity in academia. I want to focus on cryptographic approaches for preserving privacy because of my motivations and fundamental requirements from identity management. Thus, I will address Deepak Maram *et al.*'s work [Mar+21] and Christina Garman *et al.*'s work [GGM14] among decentralized digital identity research in the following sections.

2.2.1 W3C's Contributions and Tech Industries Efforts

Microsoft proposes their design of decentralized identity systems utilizing industry standards such as W3C's and DIF's standards to provide users and organizations with control over their data, which is possibly owned and controlled by other parties. They do not explicitly demonstrate that their approach is for self-sovereign identity (SSI), but the ideas behind it are close.

The approach is assumed to utilize W3C's Verifiable Credentials Data Model [W3C22b] and DIDs [W3C22a], decentralized systems such as blockchains and ledgers, DIF's Universal Resolver, Identity Hubs, their offerings of DID User Agents, Attestations, and

[6] `https://www.microsoft.com/en-us/security/business/identity-access-management/decentralized-identity-blockchain`

[7] `https://identity.foundation/ion/`

[8] `https://identity.foundation`

[9] `https://www.didalliance.or.kr`

decentralized apps and services. A user can have one or more DIDs, DIDs can be resolved across chains and ledgers, DID permission is managed via keys accessible only to the user, their identity attributes or claims are stored in off-chain DIF Identity Hub personal data stores, and users can have one or more Identity Hub instances across devices and clouds.

Their approach intentionally relies on existing standards such as OAuth 2.0[10] and OpenID Connect[11], but it successfully demonstrates the importance of data controls over decentralized systems for users and organizations.

2.2.2 CanDID and Sybil-Resistance

Deepak Maram *et al.* proposed CanDID [Mar+21], which can do decentralized identity with legacy compatibility, Sybil-resistance [Dou02], and accountability. They identify remaining problems for building a decentralized identity system, legacy compatibility, Sybil-resistance, and accountability as entitled. In order to solve the problems, they propose system protocols with a trusted committee of nodes-based architecture. Figure 2.1 illustrates the overview of CanDID's approach. In the figure, VC stands for a Verifiable Credential, and DC stands for a Derived Credential, $\mathsf{DC}_{\mathsf{master}}$ means a master credential, and $\mathsf{DC}_{\mathsf{context}}$ means a context-based credential in their work.

CanDID supports the deduplication of identities that may ensure the existence of at most one pseudonym with a unique identifier such as Social Security Number (SSN) in the U.S. This scheme enables the system to issue credentials in a unique manner per user and meets Sybil-resistance. For this, the CanDID system protocols provide three APIs for issuing credentials, `issuePreCred`(), `issueMasterCred`(), and `issueCtxCred`().

Credentials retrieved from legacy providers with `issuePreCred`() are not yet deduplicated, but `issueMasterCred`() deduplicates a master credential with a special attribute `dedupOver` to ensure the uniqueness. `issueCtxCred`() is designed to create various derived credentials associated with the master credential for different contexts. For these credentials, the CanDID committee manages users' attributes in a table within the committee. They utilize multi-party computation (MPC) to prevent committee mem-

[10] `https://datatracker.ietf.org/doc/html/rfc6749`

[11] `https://openid.net/connect/`

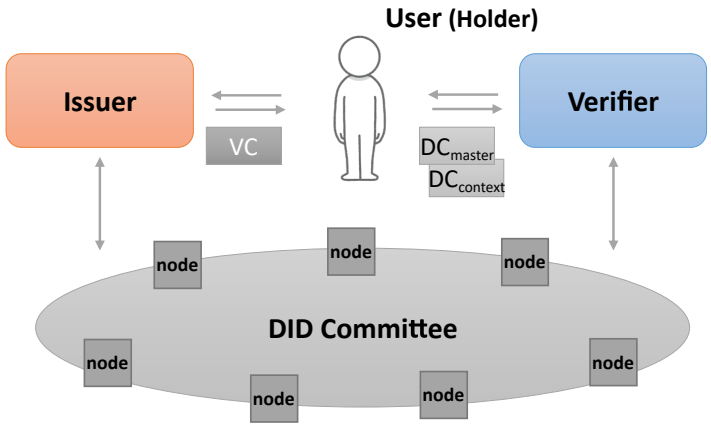


Figure 2.1: CanDID – A State-of-the-Art Approach for Decentralized Digital Identity

bers from learning any unnecessarily private information. They also utilize SNARK proofs for registration-time screening and other various purposes of privacy-preserving.

Deepak Maram *et al.* successfully demonstrated that the committee-based architecture achieves its goals with some special purpose MPC protocols for privacy-preserving deduplication and fuzzy matching for scanning sanction lists for AML.

Sybil-Resistance

"Sybil" is a book by Flora Rheta Schreiber in 1973 and a pseudonym for Shirley Ardell Mason, who was in dissociative identity disorder with 16 multiple personalities in the book. Brian Zill, a researcher at Microsoft, suggested in 2002 to name a type of attack by creating a large number of pseudonymous identities and using them to gain a disproportionately large influence, according to John. R. Douceur's contribution entitled "The Sybil Attack" [Dou02]. Sybil-resistance has been recognized as a critical requirement to deal with impersonation by preventing Sybil-attack.

2.3 Hardware-Assisted Security for Mobile Devices

Hardware-assisted security may provide tamper-resistant features, also supporting the attested execution capability. Hardware-assisted security has recently become the norm in mobile devices.

Apple iPhone implements Secure Enclave[12], which is a dedicated secure subsystem that is isolated from the app execution environment on the main processor. Android devices support KeyStore[13] and other security-related functionalities utilizing hardware-assisted implementations, such as Trusted Execution Environment (TEE) solutions, including Arm TrustZone. Google announced the Android Ready SE program[14], which will support hardware-backed security applets for various use cases such as digital keys and identity credentials on Global Platform-supported Secure Elements (GP-SE)[15]. Microsoft announced Windows 11 with new hardware requirements in which the Trusted Platform Module (TPM) 2.0 is mandated[16]. There are also other design choices among implementations in the industry, such as Intel SGX[17], in addition to TrustZone, GP-SE, and TPM 2.0. Hardware-assisted security implementations are now used for various purposes in the real world, such as biometrics, secure lock screen, FIDO authentication[18], NFC-based secure payments, and eSIM, but are not limited to these examples.

Among numerous implementations and studies addressing hardware-assisted security, Rafael Pass *et al.* formally addressed attested execution for hardware-assisted secure processors [PST17]. In their words, trusted hardware is commonly believed to provide a powerful abstraction for building secure systems. They formalized the attested execution abstraction and retrieved the formal modeling of a broad class of attested execution secure processors (AESPs) from the common belief. The abstraction formulated by Rafael Pass *et al.* is relatively close to TPM and SGX among the listed examples and sufficiently feasible for deployment in the real world. I was inspired and encouraged to utilize the formal abstraction of AESPs to formulate and demonstrate the proposed scheme.

---

[12] `https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff`

[13] `https://developer.android.com/privacy-and-security/keystore`

[14] `https://developers.google.com/android/security/android-ready-se`

[15] `https://globalplatform.org/resource-publication/introduction-to-secure-elements/`

[16] `https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview`

[17] `https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html`

[18] `https://fidoalliance.org`

2.3.1 Direct Anonymous Attestation (DAA) and Enhanced Privacy ID (EPID)

Ernie Brickell *et al.* contributed a series of direct anonymous attestation scheme (DAA) and its enhancement as a scheme that enables the remote authentication of hardware-assisted security, particularly for a Trusted Platform Module (TPM), while preserving users' privacy [BCC04, BL07, BL09, BL10]. The notion of Enhanced Privacy ID (EPID) gets around the problem of the limited revocation properties of early stages of DAA, and the revision of the EPID scheme is efficient and provably secure in the random oracle model under the strong Diffie-Hellman assumption and the decisional Diffie-Hellman assumption [BL10].

Figure 2.2 illustrates the overall structure of EPID that is capable of revocation with whichever private key or signature, and very interestingly, it utilizes the BBS+ signature scheme [BL09], which is described for other reasons in Section 3.2.

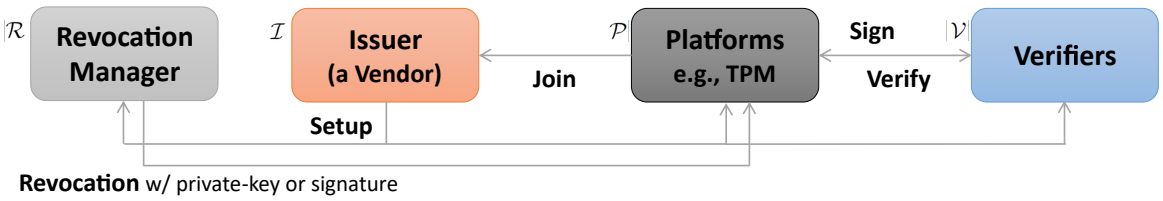


Figure 2.2: Overview: Enhanced Privacy ID (EPID)

2.3.2 Decentralized Direct Anonymous Attestation (dDAA)

Christina Garman, Matthew Green, and Ian Miers addressed anonymous credentials that David Chaum originally introduced [Cha85, GGM14]. They focused on the existing fundamental limitation within anonymous credentials, such as the DAA portion of the TPM specification [BCC04]. It means that the anonymous credential systems still require, in almost all cases, a central trusted party, such as a platform system-on-chip (SoC) manufacturer, to issue the attestations. Therefore, such a trusted party is potentially a single point of failure and an obvious target for compromise, both of which can seriously damage the reliability of the credential systems.

To address this limitation, they proposed a protocol for building a fully decentralized anonymous credential system utilizing a distributed public append-only ledger (a permissionless blockchain) and modern cryptography techniques such as zero-knowledge proofs, Pedersen commitments [Ped91], and accumulators [CL02b] under the Strong RSA assumption. In their proposed protocol, MintCred() "mints" a credential among the ledger, and the generated credentials no longer rely on a single point trusted party; thus, it eliminates the limitation. Their approach is sophisticated from a mathematical perspective; however, it has performance limitations [Ros+23].

They also addressed mitigating Sybil-attack as an application utilizing their approach. The idea is to use k-show anonymous credentials and allow an entity to obtain them only a limited number of times within a given period. Thus, unexpected cloned credentials can be identified and revoked when the k-use threshold is exceeded. This threshold approach works for some scenarios but is limited, unlike the other approach by CanDID [Mar+21], which introduced a master credential that each user can obtain only one and associates with the existing real identity for making the system Sybil-resistant.

2.4 Self-Sovereign Digital Identity (SSI)

Christopher Allen published his blog article entitled "The Path to Self-Sovereign Identity" in 2016 [All16]. It presented the evolution of digital identity from Phase 1: Centralized Identity, Phase 2: Federated Identity, Phase 3: User-Centric Identity through Phase 4: Self-Sovereign Identity, followed by his definition of SSI with the ten principles:

1. **Existence**. *Users must have an independent existence.*
2. **Control**. *Users must control their identities.*
3. **Access**. *Users must have access to their own data.*
4. **Transparency**. *Systems and algorithms must be transparent.*
5. **Persistence**. *Identities must be long-lived.*
6. **Portability**. *Information and services about identity must be transportable.*
7. **Interoperability**. *Identities should be as widely usable as possible.*
8. **Consent**. *Users must agree to the use of their identity.*
9. **Minimalization**. *Disclosure of claims must be minimized.*

10. **Protection**. *The rights of users must be protected.*

As David Chaum proposed in 1985, the motivation toward Self-Sovereign Identity (SSI) described by Christopher Allen has been encouraging many researchers to create and establish proper SSI systems preserving privacy from various perspectives [DA18, DGP18, TA19, FCO19, KE20]. Some research addressed if the ten principles express all the principles that may describe the essentials of SSI [SP18, SNE19]; however, they have still been treated as foundational principles.

Figure 1.1 illustrates an SSI solution architecture in my interpretation. In the figure, VC is a verifiable credential, and DC is a derived credential. There are several SSI implementations, such as uPort and Sovrin [PFS20, Win21]. In addition, some experimental research and prototypes in the tech industry support governmental agencies' interests [Gom19, Seu19]. Through such activities, including the efforts on verifiable credentials [W3C22b, W3C24] and DIDs [W3C22a] by W3C, there has been becoming a common structure and primary role involved in exchanging verifiable credentials among an issuer, a holder (a natural person – a prover), and a verifier.

Frederico Schardong *et al.* [SC22], Yirui Bai *et al.* [Bai+22], and Evan Krul *et al.* [Kru+24] independently surveyed research addressing SSI. Their papers, especially the SoK paper by Evan Krul *et al.*, are comprehensive, and the SoK paper provides a framework for future SSI research and development [Kru+24]. Further, there are a few more interesting research papers that approach SSI. Let me explain those in the following subsections.

2.4.1 Extended Principles

Some research addressed whether the ten principles express all principles that may describe the essentials of SSI. Quinten Stokkink *et al.* proposed to add another principle **Provable** [SP18]. Md Sadek Ferdous *et al.* presented five taxonomies and 17 principles under the taxonomies of classes derived from the ten principles in his comprehensive survey [FCO19]. Abylay Satybaldy *et al.* proposed to add **Usability** in their SSI evaluation framework, which also refers to the ten principles as a comprehensive spectrum of SSI requirements [SNE19].

Špela Čučko *et al.* reached all other such papers that addressed SSI and its properties

[Čuč+22]. They classified the 18 SSI properties in their definition into the final set of (i) Controllability, (ii) Privacy, (iii) Security, (iv) Usability and User Experience (UX), and (v) Adoption and Sustainability. In their analysis, Security and Protection, Verifiability and Authenticity, Privacy and Minimal Disclosure, and Ownership and Control among the 18 SSI properties are considered as being mandatory.

2.4.2 Building Blocks and Blockchain Technology

Many pieces of research addressed how to build SSI systems; essential components [Müh+18], design patterns [Liu+20], and needs of, how to utilize, or if it requires blockchain technology [SP18, GMM18, Bok+19, HK19, PFS20, KE20, MTC21]. Two of these researches concluded that a blockchain was not mandated. However, they still recognize that blockchain technology is a good foundation to build an SSI system and indicated that some specific requirements would require further extra efforts to fill in gaps.

2.4.3 SSI Systems with Mobile Devices

There are several SSI implementations such as uPort and Sovrin [PFS20, Win21]. Also, some experimental research and prototypes in the tech industry support governmental agencies' interests [Seu19, Boy21]. Through such activities, including W3C's efforts on verifiable credentials and DIDs [W3C22b, W3C22a], there has been becoming a common structure and primary roles involved in exchanging verifiable credentials among an issuer, a holder (a natural person), and a verifier.

Figure 1.1 illustrates the proposed SSI solution architecture in my interpretation. An issuer issues a verifiable credential (VC in the figure) for the holder. To minimize disclosure, they may have a derived credential (DC in the figure) for presentation. A verifier may verify with the received derived credential per a request. Blockchain technology can be a verifiable data registry in the proposed structure.

I put a mobile phone next to the user in the figure because some SSI implementations provide a mobile app, such as a wallet app, for the use with their SSI systems. To the best of our knowledge, however, such mobile apps never play their roles in utilizing hardware-assisted security features of the mobile device. Kalman C. Torh and Alan

Anderson-Priddy addressed using users' mobile devices as a digital identity for each of them [TA19]; however, they have not mentioned opportunities for hardware-backed attestations. The survey papers place less emphasis on SSI research utilizing mobile devices and hardware-assisted security.

2.4.4 SSI Systems Utilizing Zero-Knowledge Proofs

The SoK paper covers some SSI research that utilizes zero-knowledge proofs (ZKP) of knowledge for signature [Kru+24]. The recent effort by Mohameden Dieye *et al.* [Die+23] demonstrated an interesting approach utilizing ZKP and automorphism in their SSI. These SSI research do not address Sybil-resistant.

Michael Rosenberg *et al.* addressed anonymous credentials [Ros+23] inspired by their previous work [GGM14]. They uniquely proposed `zk–creds` utilizing zero-knowledge succinct non-interactive argument of knowledge (zk-SNARKs) to improve their earlier works from various perspectives. They approached Sybil-resistance and proposed to use email address and Domain Keys Identified Mail (DKIM) Signatures[19]; however, people may have multiple email addresses, and their approach does not meet a high assurance level for Sybil-resistance.

2.4.5 Recent Related Work Addressing Sybil-Resistant SSI

There have recently been current and independent works that address Sybil-resistant SSI [Cri+24, Rab+24]. Table 2.1 compares related works addressing Sybil-resistant SSI.

Elizabeth Crites *et al.* propose Sybil-Resilient Anonymous (SyRA) signatures [Cri+24]. They also address the conflicting requirements of Sybil-resilience (resistance) vs. anonymity and propose a novel scheme utilizing verifiable random functions (VRFs) in the Universal Composition (UC) setting. It must also be a state-of-the-art approach, and their definition of Sybil-resistance is identical to mine: the pair of real identity and context is unique. Their construction, however, forces each signature (identity proof) to leak a unique pseudonym so that the person cannot change their pseudonym within the same context, hence "linkable" by the pseudonym.

[19] https://datatracker.ietf.org/doc/html/rfc6376

Reyhaneh Rabaninejad *et al.* propose attribute-based threshold issuance anonymous counting tokens (tACT) and its application to Sybil-resistant SSI [Rab+24]. They refer to CanDID [Mar+21], where unlinkability breaks in the presence of a single malicious issuer, and it achieves better performance with tACT to avoid resource-intensive MPC in their description. They keep assuming the distributed committee of trusted nodes.

Compared to the other research [GGM14, Mar+21, Ros+23, Cri+24, Rab+24], the proposed scheme in this thesis achieves a higher level of assurance for Sybil-resistance, pragmatic performance in logarithmic order for identifying and verifying an expected credential, and under weaker assumptions and no-requiring distributed committee of trusted nodes nor AESPs for verifiers, in decentralized anonymous credential systems satisfying Sybil-resistance and unlinkability across programs and credentials (Table 2.1).

Table 2.1: Comparison of Related Works Addressing Sybil-Resistant SSI

	Moriyama and Otsuka	Garman *et al.* [GGM14]	Maram *et al.* [Mar+21]	Rosenberg *et al.* [Ros+23]	Crites *et al.* [Cri+24]	Rabaninejad *et al.* [Rab+24]
Appearance	August 2022 and this thesis	October 2013*1 and February 2014	July 2020*1 and May 2021	July 2022*1 and May 2023	February and June 2024*1	June 2024*1
Assumptions	Tamper-resistant AESP for holders, permissionless blockchain, q-SDH, discrete logarithm	Strong RSA and discrete logarithm	Distributed committee of trusted nodes	Standard assumptions, including discrete logarithm	Decisional Diffie-Hellman and q-DBDHI*2	Distributed committee of trusted nodes, k-OMDL*3, and discrete logarithm
Assurance level for Sybil-resistance	High	Low (threshold-base)	High	Middle (email address-base)	High	High
Unlinkability	Achieved (across programs and credentials)	Not addressed	Achieved (across programs)*4	Addressed but not focused*5	Limited because of using pseudonym	Achieved (across programs and credentials)
Performance	$O(\lambda(\log N))$ among N in global population for verification	Limited according to [Ros+23]	Measured (in case of 4 nodes)	Improved than [GGM14] drastically and measured (show and verify)	Measured (for single signature generation and verification)	Measured (comparable than Candid in 128 nodes)
Note	Proposing to utilize tamper-resistant AESPs, BBS+, and ZKP (OOoM)	Decentralized Direct Anonymous Attestations (DAA)	Proposing MPC-based protocols	Proposing to utilize zk-SNARKs	Utilizing Verifiable Random Functions (VRFs)	Proposing tACT (attribute-based threshold issuance anonymous tokens)

*1 Appeared as preprints

*2 q-Decisional Bilinear Diffie-Hellman Inversion

*3 the one more-discrete logarithm assumption (OMDL)

*4 Rabaninejad *et al.* indicate that it could be broken in the presence of a single malicious issuer [Rab+24]

*5 Addressed unlinkability across programs and must be anonymous across credentials but not explicit.

Chapter 3

Preliminaries

3.1 Attested Execution Secure Processors (AESPs)

Among numerous implementations and researches addressing hardware-assisted security, including how to realize [CLD16] and how to utilize [San+14], Rafael Pass, Elaine Shi, and Florian Tramèr uniquely addressed hardware-assisted security, secure processors, in a formal fashion [PST17]. In their words, trusted hardware is commonly believed to provide a very powerful abstraction for building secure systems. They approached formalizing the attested execution abstraction and retrieved the formal modeling of a broad class of attested execution secure processors (AESPs), $\mathcal{G}_{\mathtt{att}}$ from the common belief. Also, they successfully demonstrated an additional observation regarding composable two-party computation with attested execution processors.

3.1.1 The Formal Modeling of AESPs: $\mathcal{G}_{\mathtt{att}}$

According to their efforts, the attested execution abstraction enables the following:

- A platform equipped with an attested execution processor can send a program and inputs, denoted $(\mathtt{prog}, \mathtt{inp})$, to its local secure processor. The secure processor executes the program over the inputs and computes $\mathtt{outp} := \mathtt{prog}(\mathtt{inp})$. The secure processor then signs the tuple $(\mathtt{prog}, \mathtt{outp})$ with a secret signing key to obtain a digital signature σ_M, which is commonly referred to as an "attestation," and this entire execution is referred to as an "attested execution."

- The program's execution is conducted in a sandboxed environment, an enclave, in other words, in the sense that a software adversary and/or a physical adversary cannot tamper with the execution or inspect data that lives inside the enclave. This is important for realizing privacy-preserving applications[1].

They had some options to choose at the abstraction level, such as whether the secure processor provides a trusted clock and/or implements anonymous or non-anonymous attestation. In their consideration, they first described a basis, namely anonymous attestation without trusted clocks, and I follow that abstraction called $\mathcal{G}_{\mathtt{att}}$.

The ideal functionality $\mathcal{G}_{\mathtt{att}}$ captures the core abstraction a broad class of AESPs, such as Intel SGX[2], intend to provide. $\mathcal{G}_{\mathtt{att}}$ is parametrized with a signature scheme Σ and also a registry $\mathtt{reg}$ that is meant to capture all the platforms equipped with an AESP. Here, the signature scheme Σ assumes EUF-CMA (Existential Unforgeability under Chosen Message Attack), and the registry $\mathtt{reg}$ is treated as a static registry for simplicity in the research. $\mathcal{G}_{\mathtt{att}}$ consists of the initialization function to generate a manufacturer public key and secret key pair denoted $(\mathtt{mpk}, \mathtt{msk})$, public query interface $\mathsf{getpk}()$, and stateful enclave operations of $\mathsf{Install}()$ and $\mathsf{Resume}()$, which realize the anonymous attestation capability. A platform $\mathcal{P}$ that is in the registry $\mathtt{reg}$ may invoke those enclave operations.

- *initialization:* $\Sigma.\mathsf{KeyGen}(1^\lambda) \rightarrow (\mathtt{mpk}, \mathtt{msk})$, $T = \emptyset$.
- *public query interface:* $\mathsf{getpk}()$ from some $\mathcal{P}$: send $\mathtt{mpk}$ to $\mathcal{P}$.
- *local interface – install an enclave:* $\mathsf{Install}(idx, \mathtt{prog})$ from some $\mathcal{P} \in \mathtt{reg}$: if $\mathcal{P}$ is honest, assert $idx = sid$, $\mathcal{G}_{\mathtt{att}}$ generate a nonce for a fresh enclave identifier $eid \in \{0,1\}^\lambda$, store $T[eid, \mathcal{P}] := (idx, \mathtt{prog}, \mathbf{0})$, and send eid to $\mathcal{P}$.
- *local interface – resume an enclave:* $\mathsf{Resume}(eid, \mathtt{inp})$ from $\mathcal{P} \in \mathtt{reg}$: resuming the execution of an existing enclave with inputs $\mathtt{inp}$. First, let $(idx, \mathtt{prog}, \mathtt{mem}) :=$

[1] In their example about this capability, a secure channel with a secure processor residing on a remote server can be established with a public key of the secure processor by a remote client, and the server cannot eavesdrop on the contents, nor can it tamper with the communication while messages are passed through the intermediary server.

[2] `https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html`

$T[eid, \mathcal{P}]$, and abort if not found. Second, $\mathcal{G}_{\mathtt{att}}$ executes the `prog` over the inputs `inp`, namely let $(\mathtt{outp}, \mathtt{mem}) := \mathtt{prog}(\mathtt{inp}, \mathtt{mem})$ and obtains an output `outp`, and update $T[eid, \mathcal{P}] := (idx, \mathtt{prog}, \mathtt{mem})$. $\mathcal{G}_{\mathtt{att}}$ would then sign the `prog` together with `outp` as well as additional metadata, namely let $\sigma_M := \Sigma.\mathrm{Sig}_{\mathtt{msk}}(idx, eid, \mathtt{prog}, \mathtt{outp})$, and return both `outp` and the resulting anonymous attestation σ_M to $\mathcal{P}$.

The initialization function is executed at most once, while other functions, getpk(), Install(), and Resume() are denoted as reentrant activation points. That means different programs $\{\mathtt{prog}\}_{i=1,\ldots,n}$ can be installed and resumed independently in theory (e.g., Figure 4.1). Here, the limits of how many programs are not determined. The enclave program `prog` may be probabilistic and this is important for privacy-preserving applications. Enclave program outputs are included in an anonymous attestation σ_M. For honest parties, the functionality verifies that installed enclaves are parametrized by the session id *sid* of the protocol issuance.

There are some notable characteristics that I need to describe here as a part of the preliminaries as follows:

Registry. $\mathcal{G}_{\mathtt{att}}$ is parameterized with a registry `reg` that is meant to capture all the platforms equipped with an AESP. For simplicity, this thesis considers a static registry `reg` the same as their original paper.

Stateful enclave operations. A platform $\mathcal{P}$ that is in the registry `reg` may invoke enclave operations of Install() and Resume(). Each installed enclave program can be resumed multiple times, and the enclave operations store state as a result across multiple invocations. This stateful property is related to the description above about the characteristics of the reentrant activation points.

Anonymous attestation. Hardware-assisted secure processors such as SGX rely on group signatures and other anonymous credential techniques to offer "anonymous attestation," allowing a user to verify that the attestation is produced by some attested execution processors without identifying which one. $\mathcal{G}_{\mathtt{att}}$ functionality has a manufacturer public key and secret key pair denoted $(\mathtt{mpk}, \mathtt{msk})$, and is parametrized by the signature scheme Σ. When an enclave operation is invoked, $\mathcal{G}_{\mathtt{att}}$ signs any output to be attested with `msk`, say σ_M, using the signature scheme

Σ. At the same time, $\mathcal{G}_{\mathtt{att}}$ provides the manufacture public key `mpk` to any party upon query. Let us assume that a secret key distribution channel exists to distribute `msk` in this model, and any party can verify an anonymous attestation signed by $\mathcal{G}_{\mathtt{att}}$.

Globally shared functionality. $\mathcal{G}_{\mathtt{att}}$ functionality essentially captures all attested execution processors in the world by definition. Further, let us note that $\mathcal{G}_{\mathtt{att}}$ is globally shared by all users, all applications, and all protocols. In particular, rather than generating a different (`mpk`, `msk`) pair for each different protocol instance, the same (`mpk`, `msk`) pair is globally shared.

The characteristics described above show that the global sharing of the key pair can be an attack target as a potential vulnerability. I will address a plan for resolution as the future direction in Section 6.2.1.

3.2 Signature Scheme and Efficient Protocols

Jan Camenisch and Anna Lysyanskaya proposed a signature scheme with efficient protocols (CL signature scheme) [CL02a]. They intended to create a pragmatic signature scheme for real-world applications such as credential systems and proposed a basic signature scheme, the scheme for blocks of messages, and protocols for the signature scheme, including one for signing a committed value and one for on blocks of messages.

They provided a zero-knowledge proof of knowledge protocol for showing that a committed value is a signature on another committed value. These characteristics are well designed for signing and verifying credentials for presentations derived from the original credentials without unveiling claims, namely with zero knowledge. The CL signature scheme was referred to by the W3C specification [W3C22b] since v1.0 for implementers who want to extend verifiable credentials and verifiable presentations to support zero-knowledge proof systems; although, details are omitted.

Jan Camenisch and Anna Lysyanskaya also approached utilizing bilinear maps for efficiency (CL+ signature scheme) [CL04] and addressed in their paper that Dan Boneh, Xavier Boyen, and Hovav Shacham made another effort independently under the strong Diffie-Hellman (q-SDH) assumption (BBS signature scheme) [BBS04], unlike the CL

signature scheme is under the Strong RSA assumption. Man Ho Au, Willy Susilo, and Yi Mu then presented the detailed construction to adopt the ideas of CL/CL+ signature schemes over the effort by Dan Boneh, Xavier Boyen, and Hovav Shacham, called BBS+ signature scheme [ASM06].

The recent W3C revisions such as v1.1 and the candidate recommendation draft for v2.0 [W3C24] touch upon the BBS+ signature scheme still without details, but as mentioned earlier, standardization bodies such as IETF and DIF have recently focused on it very proactively to enable verifiers to verify derived credentials without knowing the origin and claims inside by utilizing proof of knowledge of signatures on those derived credentials [Kal22, Loo+23]. Dan Yamamoto, Yuji Suga, and Kazue Sako successfully formalized linked-data based verifiable credentials for selective disclosure [YSS22].

3.2.1 Verifiable Credentials and CL / BBS+ Signature Scheme

Verifiable credentials consist of metadata, claims, and proof by definition in the specifications. Both metadata and claims can be treated as a collection of messages, and they can be described if the CL signature scheme is utilized for proof: choosing a special RSA modulus with safe primes[3]. Their basic signature scheme consists of key generation, signing, and verification algorithms under the determined message space range. On input 1^k, a chosen special RSA modulus $n = pq$ where both p and q are safe primes, and chosen $a, b, c \in QR_n$, output $PK = (n, a, b, c)$, and $SK = p$, where $QR_n \subseteq \mathbb{Z}_n^*$ is denoted that the set of quadratic residues modulo n, i.e., elements $a \in \mathbb{Z}_n^*$ such that $\exists b \in \mathbb{Z}_n^*$ such that $b^2 \equiv a \bmod n$. Then, on input m, the *signing algorithm* computes the value v of a signature (e, s, v) such that

$$v^e \equiv a^m b^s c \bmod n \tag{3.1}$$

where e is a prime number of length $\ell_e \geq \ell_m + 2$, and s is a random number of length $\ell_s = \ell_n + \ell_m + l$. ($l$ is a security parameter.) The *verification algorithm* verifies that the tuple (e, s, v) is a signature on message m in the message space, check that $v^e \equiv a^m b^s c \bmod n$, and check if e is within the message space range. The CL signature

[3]A prime number p is called a safe prime if $p = 2p' + 1$ such that p' is also a prime number. The corresponding number p' is known as a Sophie Germain prime [CL02a].

scheme includes a straightforward extension to support signing a block of messages, and it is represented below

$$v^e \equiv a_1^{m_1} a_2^{m_2} \dots a_L^{m_L} b^s c \bmod n \tag{3.2}$$

where $a_1, a_2, \dots, a_L, b, c \in QR_n$, output $PK = (n, a_1, a_2, \dots, a_L, b, c)$ on input of a block of messages $(m_1, m_2, \dots, m_L)$, and the tuple (e, s, v) is a signature.

The BBS+ signature scheme also consists of key generation, signing, and verification algorithms supporting signing a block of messages as well as efficient protocols for signing a committed block of messages and for proof of knowledge of a signature. Let $(\mathbb{G}_1, \mathbb{G}_2)$ be a bilinear group pair of some prime order p. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a computable bilinear paring function. Selected $g_0, g_1, \dots, g_{L+1} \in \mathbb{G}_1$ and $h_0 \in \mathbb{G}_2$ are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. A secret key $\gamma \in_R \mathbb{Z}_p^*$ is randomly chosen, and the corresponding public key is $w = h_0^\gamma$. Then, on input $(m_1, m_2, \dots, m_L) \in \mathbb{Z}_p^L$, the *signing algorithm* chooses t, a random number s, and computes

$$A = \left[g_0 g_1^s g_2^{m_1} g_3^{m_2} \dots g_{L+1}^{m_L} \right]^{\frac{1}{t+\gamma}} \tag{3.3}$$

where (A, t, s) is a signature on the input block message. To verify a signature (A, t, s) on the message block, the *signature verification algorithm* checks if

$$\mathrm{e}(A, w h_0^t) = \mathrm{e}\big(g_0 g_1^s g_2^{m_1} g_3^{m_2} \dots g_{L+1}^{m_L}, h_0\big). \tag{3.4}$$

Because of flexibility, efficiency, and recent many use in the tech industry, I am going to utilize the BBS+ signature scheme in this thesis.

3.2.2 Proof of Knowledge of a Signature

In both the CL signature scheme and the BBS+ signature scheme, one of the most efficient and useful protocols is the protocol for "Proof of Knowledge (PoK) of a Signature," so-called SPK. They both define a protocol of signing committed block of messages as described. By utilizing it, SPK enables various use cases for credential systems such as for Enhanced Privacy ID [BL09] as well as the recently focused scenario

of selective disclosure in digital identity systems [YSS22, Loo+23] for proof possession of the original signature without disclosing value of each attribute.

In case of the BBS+ signature scheme, a user possessing a signature (A, t, s) with the block of messages $(m_1, \ldots, m_L)$ can be proven as

$$SPK\{(A, t, s, m_1, \ldots, m_L) : A^{t+\gamma} = g_0 g_1^s g_2^{m_1} g_3^{m_2} \ldots g_{L+1}^{m_L}\}(M) \tag{3.5}$$

by first computing the following quantities: $A_1 = g_1^{r_1} g_2^{r_2}$, and $A_2 = A g_2^{r_1}$ for some randomly generated $r_1, r_2 \in_R \mathbb{Z}_p^*$, where $M \in \{0,1\}^*$ (any text string). In the following computation described in [ASM06],

$$\begin{aligned} \Pi_5 : SPK\Big\{(r_1, r_2, \delta_1, \delta_2, t, s, m_1, \ldots, m_L) : \\ A_1 = g_1^{r_1} g_2^{r_2} \wedge A_1^t = g_1^{\delta_1} g_2^{\delta_2} \wedge \frac{\mathrm{e}(A_2, w)}{\mathrm{e}(g_1, h_0)} = \\ \mathrm{e}(A_2, h_0)^{-t}\, \mathrm{e}(g_2, w)^{r_1}\, \mathrm{e}(g_2, h_0)^{\delta_1}\, \mathrm{e}(g_1, h_0)^{s}\, \mathrm{e}(g_2, h_0)^{m_1} \cdots \mathrm{e}(g_{L+1}, h_0)^{m_L} \Big\}(M) \end{aligned} \tag{3.6}$$

where $\delta_1 = r_1 t$ and $\delta_2 = r_2 t$. It indicates that a signature does not have to be disclosed and only a message consisting of public parameters is disclosed, then SPK enables proving possession of the signature by a non-interactive honest-verifier zero-knowledge proof-of-knowledge protocol with special soundness.

3.2.3 Proofs of Equality about Discrete Logarithms

The similarity of such proof of knowledge of a signature encourages the use of "Proof of Knowledge of Discrete Logarithms" and "Proof of Knowledge of Equality" [CM99, CS03, BL07]. A proof of equality of discrete logarithms of two group elements $y_1, y_2 \in G$ to the bases $z_1, z_2 \in G$, respectively, is denoted $PK\{(a) : y_1 = z_1^a \wedge y_2 = z_2^a\}$. Such protocol can also be used to prove that the discrete logarithms of two group elements $y_1 \in G_1$ and $y_2 \in G_2$ to the bases $z_1 \in G_1$ and $z_2 \in G_2$, respectively in two different groups G_1 and G_2 are equal. In nature, Pedersen commitments [Ped91] can also be adapted to the proof of equality.

3.2.4 Notation to Represent a Transcript

Lastly, as a part of the preliminaries in this section, let us denote

$$\pi_{SPK}(\sigma; \widetilde{\sigma}) \tag{3.7}$$

to represent a transcript that a user possessing signatures of σ and $\widetilde{\sigma}$ with the same block of a message, where $\widetilde{\sigma} = (A_2, t, s)$ is randomly represented differently from $\sigma = (A, t, s)$ based on the scheme as described in Section 3.2.2.

Also, let us denote a proof of equality about discrete logarithms if the same witness appears in equations,

$$\pi_{eq}(a; \widehat{a} = \widehat{a}') \tag{3.8}$$

to represent a transcript, $PK\{(a) : \widehat{a} = g_1^a \wedge \widehat{a}' = g_2^a\}$, the result of a proof of equality about discrete logarithms as described in Section 3.2.3.

3.3 "One-Out-of-Many Proofs" Σ-Protocol

Jens Groth and Markulf Kohlweiss proposed a 3-move public coin special honest verifier zero-knowledge proof, a Sigma-protocol, for a list of commitments having at least one commitment that opens to 0 [GK15]. It is not required for a prover to know openings of the other commitments. They propose an application to utilize their Sigma-protocol as a (linkable) ad-hoc group identification scheme where the users have public keys that are commitments and demonstrate knowledge of an opening for one of the commitments to *unlinkably* identify themselves (once) as belonging to the group. They also propose to utilize the Sigma-protocol for an efficient proof of membership of a secret committed value u belonging to a public list $\mathcal{L} = \{\lambda_1, \ldots, \lambda_N\}$, not limited for a prover to find a commitment that opens to 0.

Jens Groth and Markulf Kohlweiss described that a Σ-protocol should be **complete**, **sound**, and **zero-knowledge**. Σ-protocols are widely used, especially in the construction of non-interactive zero-knowledge proofs in nature. I will utilize the one-out-of-many proofs Σ-protocol in my proposal; thus, let me further describe the foundation of their contributions as a part of the preliminaries.

They consider statements consisting of N commitments $c_0, \ldots, c_{N-1}$, and the prover's claim is that they know an opening of one of the commitments c_ℓ to the value 0. They demonstrated as one of their main contributions that such a statement has logarithmic communication complexity. Their construction works for any additively homomorphic non-interactive commitment schemes such as Pedersen commitments [Ped91] over $\mathbb{Z}_q$, where q is a large prime. Those commitment schemes specify a commitment key ck, which in the case of Pedersen commitments specifies a prime-order group $\mathbb{G}$ and two group elements g, h. Given a value $m \in \mathbb{Z}_q$ and a randomness $r \in \mathbb{Z}_q$, a Pedersen commitment is computed as $c = g^m h^r$. Given a commitment key ck and a statement of the form $(c_0, \ldots, c_{N-1})$, the prover who knows an opening $(0, r)$ of one of the commitments $c_\ell = \mathrm{Com}_{ck}(m; r)$ with $m = 0$ can use the one-out-of-many proofs Σ-Protocol to convince the verifier of having this knowledge. It has *perfect completeness*, $(\log N + 1)$-*special soundness*, and *special honest verifier zero-knowledge* such that given a challenge x from the verifier, it is possible to simulate a transcript without knowing an opening of any of the commitments.

I plan to utilize the characteristics of the one-out-of-many proofs Σ-protocol for a holder (user) and a verifier to communicate and for the verifier to identify and accept the user's derived credentials without sharing any secrets in SSI under a permissionless blockchain. To utilize their Σ-protocol, I also assume to use Pedersen commitments for identifiers anonymity. In the following subsection, I describe some key definitions and a theorem for my proposals as preliminaries.

3.3.1 Definitions and the Theorem

In their notation, and I will follow[4], a non-interactive commitment scheme is a pair of probabilistic polynomial time algorithm $(\mathcal{K}, \mathrm{Com})$. The setup algorithm $ck \leftarrow \mathcal{K}(1^\lambda)$ generates a commitment key ck. The commitment key specifies a message space $\mathcal{M}_{ck}$, a randomness space $\mathcal{R}_{ck}$, and a commitment space $\mathcal{C}_{ck}$. The commitment algorithm combined with the commitment key specifies a function $\mathrm{Com}_{ck} : \mathcal{M}_{ck} \times \mathcal{R}_{ck} \to \mathcal{C}_{ck}$. Given a message $m \in \mathcal{M}_{ck}$ the sender picks uniformly at random $r \leftarrow \mathcal{R}_{ck}$ and computes

[4]The key generator is specified as $\mathcal{G}$ in the original paper by Jens Groth and Markulf Kohlweiss, but this thesis describes it as $\mathcal{K}$ because of a conflict with a notation in the other paper by Rafael Pass *et al.* which is also refereed to by this thesis.

the commitment $c = \mathrm{Com}_{ck}(m : r)$.

Definition 3.1 (Hiding)**.** *A non-interactive commitment scheme* $(\mathcal{K}, \mathrm{Com})$ *is hiding if a commitment does not reveal the value. For all probabilistic polynomial time stateful adversaries* $\mathcal{A}$*,*

$$\left|\Pr\Big[\mathcal{A}(c) = b \;\Big|\; ck \leftarrow \mathcal{K}(1^\lambda);\ (m_0, m_1) \leftarrow \mathcal{A}(ck);\ b \leftarrow \{0,1\}; c \leftarrow \mathrm{Com}_{ck}(m_b)\Big] - \frac{1}{2}\right| \leq \mathrm{negl}(\lambda) \tag{3.9}$$

where $\mathcal{A}$ *outputs* $m_0, m_1 \in \mathcal{M}_{ck}$*. If the probability is exactly* $\frac{1}{2}$*, they say the commitment scheme is* perfectly *hiding.*

Definition 3.2 (Binding)**.** *A non-interactive commitment scheme* $(\mathcal{K}, \mathrm{Com})$ *is binding if a commitment can only be opened to one value. For all probabilistic polynomial time adversaries* $\mathcal{A}$*,*

$$\Pr\Big[m_0 \neq m_1 \wedge \mathrm{Com}_{ck}(m_0; r_0) = \mathrm{Com}_{ck}(m_1; r_1) \;\Big|\; ck \leftarrow \mathcal{K}(1^\lambda);\ (m_0, r_0, m_1, r_1) \leftarrow \mathcal{A}(ck)\Big] \leq \mathrm{negl}(\lambda) \tag{3.10}$$

where $\mathcal{A}$ *outputs* $m_0, m_1 \in \mathcal{M}_{ck}$ *and* $r_0, r_1 \in \mathcal{R}_{ck}$*. If the probability is exactly* 0*, they say the commitment scheme is* perfectly *binding.*

They assume the existence of a probabilistic polynomial time setup algorithm $\mathcal{K}$ that generates a common reference string ck for a homomorphic non-interactive commitment scheme. They call w a witness for a statement u if $(ck, u, w) \in R$, a polynomial time decidable ternary relation. Then, they define the CRS-dependent language

$$\mathcal{L}_{ck} = \big\{u \mid \exists w : (ck, u, w) \in R\big\} \tag{3.11}$$

as the set of statements u that have a witness w in the relation R.

A Σ-protocol for R is a triple of probabilistic polynomial time stateful interactive algorithms $(\mathcal{K}, \mathcal{P}, \mathcal{V})$. The following run of a Σ-protocol describes the interaction of the algorithms

$ck \leftarrow \mathcal{K}(1^\lambda)$: Generate the common reference string.

$a \leftarrow \mathcal{P}(ck, u, w)$: The prover generates an initial message a.

$x \leftarrow \{0,1\}^\lambda$: A challenge x is chosen uniformly at random by the verifier.

$z \leftarrow \mathcal{P}(x)$: The prover responds to the challenge x.

$b \leftarrow \mathcal{V}(ck, u, a, x, z)$: The verifier returns 1 if accepting; otherwise, returns 0.

The triple $(\mathcal{K}, \mathcal{P}, \mathcal{V})$ is called a Σ-protocol for R if it is *complete*, *special sound*, and *special honest verifier zero-knowledge* as defined below:

Definition 3.3 (Completeness)**.** $(\mathcal{K}, \mathcal{P}, \mathcal{V})$ *is complete if for all probabilistic polynomial time adversaries* $\mathcal{A}$*,*

$$\left|\Pr\Big[\mathcal{V}(ck,u,a,x,z)=1 \;\Big|\; ck \leftarrow \mathcal{K}(1^\lambda);\ (u,w) \leftarrow \mathcal{A}(ck);\ a \leftarrow \mathcal{P}(ck,u,w);\ x \leftarrow \{0,1\}^\lambda;\ z \leftarrow \mathcal{P}(x)\Big] - 1\right| \leq \mathrm{negl}(\lambda) \tag{3.12}$$

where $\mathcal{A}$ *outputs* (u, w) *such that* $(ck, u, w) \in R$*. If the probability is exactly* 0*, they say the commitment scheme is* perfectly *complete.*

Definition 3.4 (n-Special soundness)**.** $(\mathcal{K}, \mathcal{P}, \mathcal{V})$ *is* n*-special sound if there is an efficient extraction algorithm* $\mathcal{X}$ *that can compute the witness given* n *accepting transcripts with the same initial message. Formally, for all probabilistic polynomial time adversaries* $\mathcal{A}$*,*

$$\left|\Pr\Big[(ck,u,w)\in R \;\Big|\; ck \leftarrow \mathcal{K}(1^\lambda);\ (u,a,x_1,z_1,\ldots,x_n,z_n) \leftarrow \mathcal{A}(ck);\ w \leftarrow \mathcal{X}\left(ck,u,a,x_1,z_1,\ldots,x_n,z_n\right)\Big] - 1\right| \leq \mathrm{negl}(\lambda) \tag{3.13}$$

where $\mathcal{A}$ *outputs distinct* $x_1, \ldots, x_n \in \{0,1\}^\lambda$ *and for all* $i \in \{1, \ldots, n\}$ *the transcript is accepting, i.e.,* $\mathcal{V}(ck, u, a, a_i, z_i) = 1$*.*

Definition 3.5 (Special honest verifier zero-knowledge (SHVZK))**.** $(\mathcal{K}, \mathcal{P}, \mathcal{V})$ *is special honest verifier zero-knowledge if there exists a probabilistic polynomial time simulator*

$\mathcal{S}$ such that for all interactive probabilistic polynomial time adversaries $\mathcal{A}$,

$$\Big|\Pr\Big[\mathcal{A}(a,z)=1 \;\Big|\; ck\leftarrow\mathcal{K}(1^\lambda);(u,w,x)\leftarrow\mathcal{A}(ck);a\leftarrow\mathcal{P}(ck,u,w);z\leftarrow\mathcal{P}(x)\Big] - \Pr\Big[\mathcal{A}(a,z)=1 \;\Big|\; ck\leftarrow\mathcal{K}(1^\lambda);(u,w,x)\leftarrow\mathcal{A}(ck);(a,z)\leftarrow\mathcal{S}(ck,u,x)\Big]\Big| \leq \mathrm{negl}(\lambda) \tag{3.14}$$

where $\mathcal{A}$ outputs (u,w,x) such that $(ck,u,w)\in R$ and $x\in\{0,1\}^\lambda$. The Σ-protocol is said to be perfect *special honest verifier zero-knowledge if the two probabilities are exactly equal to each other.*

Definition 3.6 (Witness-indistinguishability)**.** *$(\mathcal{K},\mathcal{P},\mathcal{V})$ is witness indistinguishable if for all interactive polynomial adversaries $\mathcal{A}$,*

$$\Big|\Pr\Big[\mathcal{A}(z)=b \;\Big|\; ck\leftarrow\mathcal{K}(1^\lambda);\,(u,w_0,w_1)\leftarrow\mathcal{A}(ck);\,b\leftarrow\{0,1\}; \\ a\leftarrow\mathcal{P}(ck,u,w_b);x\leftarrow\mathcal{A}(a);z\leftarrow\mathcal{P}(x)\Big]-\frac{1}{2}\Big| \leq \mathrm{negl}(\lambda) \tag{3.15}$$

where $\mathcal{A}$ outputs (u,w_0,w_1) such that $(ck,u,w_0)\in R$ and $(ck,u,w_1)\in R$ and $x\in\{0,1\}^\lambda$. The Σ-protocol is perfectly *witness-indistinguishable if the probability is exactly half.*

A well-known example of a Σ-protocol for knowledge of a committed value being 0 or 1 supposes that ck is a commitment key for a homomorphic commitment scheme and R is the relation consisting of commitments to 0 or 1, with the witnesses being opening of the commitment, i.e.,

$$R=\big\{(ck,c,(m,r))\,\big|\,c=\mathrm{Com}_{ck}(m;r)\text{ where }m\in\{0,1\}\text{ and }r\in\mathbb{Z}_q\big\}. \tag{3.16}$$

It can be extended for the one-out-of-many proofs Σ-protocol for knowledge of one out of N commitments $c_0,\ldots,c_{N-1}$ being a commitment to 0 with the relation,

$$R=\big\{\,(ck,(c_0,\ldots,c_{N-1}),(\ell,r))\;\big|\; \\ \forall i: c_i\in\mathcal{L}_{ck}\wedge\exists\ell\in\{0,\ldots,N-1\}\wedge r\in\mathbb{Z}_q\wedge c_\ell=\mathrm{Com}_{ck}(0;r)\big\}. \tag{3.17}$$

The one-out-of-many proofs Σ-Protocol $(\mathcal{K},\mathcal{P},\mathcal{V})$ for R with $\mathcal{K}$ being the key generation

algorithm for the commitment scheme, $\mathcal{P}(ck, (c_0, \ldots, c_{N-1}), (\ell, r))$, and $\mathcal{V}(ck, (c_0, \ldots, c_{N-1}))$, running on $ck \leftarrow \mathcal{K}(1^\lambda)$, $c_0, \ldots, c_{N-1} \in \mathcal{L}_{ck}$, $\exists \ell \in \{0, \ldots, N-1\}$ and $r \in \mathbb{Z}_q$ such that $c_\ell = \mathrm{Com}_{ck}(0; r)$.

Theorem 3.1 (Theorem 3 originally proposed by Jens Groth and Markulf Kohlweiss [GK15])**.** *The Jens Groth and Markulf Kohlweiss Σ-protocol for "One-Out-of-Many Proofs" for knowledge of one out of N commitments opening to* 0 *is perfectly* ***complete****. It is* $(n+1)$*-****special sound*** *if the commitment scheme is* binding*. It is perfect* ***special honest verifier zero-knowledge*** *if the commitment scheme is perfectly* hiding*.*

3.3.2 One-Out-of-Many Proofs for Commitments Containing a Value

The one-out-of-many proofs Σ-protocol can be used for membership proof. Given a commitment c and a set of values $\lambda_0, \ldots, \lambda_{N-1}$, they wanted to prove that they know an opening of the commitment c to a value u, one of the values λ_ℓ. This can be done based on the characteristics of additively homomorphic encryption by defining $c_0 = c \cdot \mathrm{Com}_{ck}(\lambda_0 - \lambda_\ell; r_0), \ldots, c_{N-1} = c \cdot \mathrm{Com}_{ck}(\lambda_{N-1} - \lambda_\ell; r_{N-1})$ and proving there is a c_ℓ with an opening to 0.

3.3.3 Notation to Represent a Transcript

Lastly, as a part of the preliminaries in this section, let us denote

$$\pi_{OOoM}(\lambda_\ell \in \mathcal{C}_{ck}) \tag{3.18}$$

to represent a transcript, the result of the zero-knowledge membership proof utilizing "One-Out-of-Many Proofs" Σ-protocol of the triple $(\mathcal{K}, \mathcal{P}, \mathcal{V})$, where the commitment algorithm combined with the commitment key specifies a function $\mathrm{Com}_{ck} : \mathcal{M}_{ck} \times \mathcal{R}_{ck} \to \mathcal{C}_{ck}$, the witness relation

$$R = \big\{(ck, c, (m, r)) \,\big|\, c = \mathrm{Com}_{ck}(m; r) \text{ where } m \in \mathcal{M}_{ck} \text{ and } r \in \mathbb{Z}_q\big\}, \tag{3.19}$$

$m \in \mathcal{M}_{ck} = \{\lambda_0, \ldots, \lambda_{N-1}\}$, the sender picks uniformly at random $r \leftarrow \mathcal{R}_{ck}$, and computes the commitment $c = \mathrm{Com}_{ck}(m : r)$.

Chapter 4

AESP-Based Sybil-Resistant SSI Architecture and System Protocols

4.1 Architecture and Protocols Overview

I propose an architecture and system protocols to build a flexible, efficient, and secure self-sovereign identity (SSI) system by utilizing the formal abstraction of attested execution secure processors (AESPs) along with permissionless blockchain technology. Also, I propose a design and construction for realizing a secure SSI to support Sybil-resistance based on the AESP-based SSI architecture.

4.1.1 Architecture

Figure 4.1 illustrates an overview of the architecture and how the basic AESP enclave operations of Install() and Resume() are integrated into the proposed architecture.

Overview of the main ideas are below:

- A person has a mobile device equipped with an AESP, complying with the proposed AESP-based SSI architecture, which needs to be set up to make their device a self-sovereign identity holder. This setup operation includes a device key pair $(\texttt{mpk}, \texttt{msk})$ generation.

- The person may install programs, $\texttt{prog}_{i=1,\ldots,n}$, by Install() for enabling the device

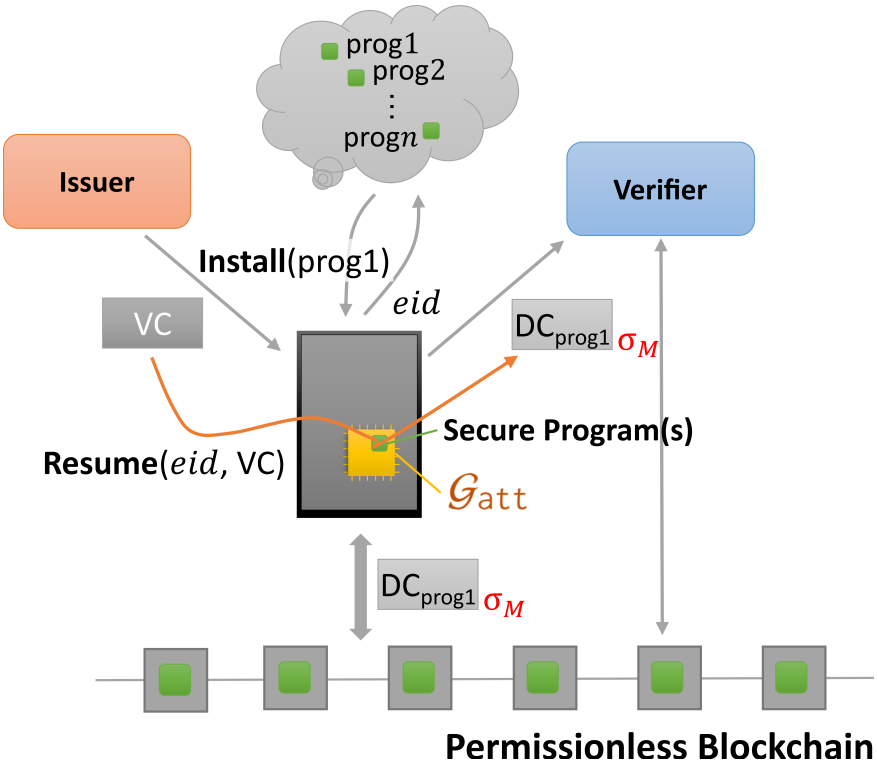


Figure 4.1: Overview: The Proposed Architecture and the AESP Enclave Operations

SSI-operations capable such as creating derived credentials. For example, a `prog` is designed and implemented for minimizing disclosure of their original, verifiable credentials, less than 18 years old in particular. Once installed, `eid` is assigned for identifying the program `prog` to be executed by Resume().

- The person may ask authorities (Issuer) such as a governmental agency, a university, or other service providers to issue a verifiable credential consisting of claims and proof π for each claim.

- Once the installed program is executed by Resume(), and the AESP digitally signs an output `outp` to prove that the program has been executed on the specific AESP, and signed signature is attached with the output as a proof, σ_M. Before generating a derived credential, they should be allowed to produce a pairwise pseudonym for each entity E; thus, their identity is to be represented with a key pair $(\mathtt{pk}_U^E, \mathtt{sk}_U^E)$. For simplicity, I will describe such a key pair like $(\mathtt{pk}_U, \mathtt{sk}_U)$ in this thesis.

- Such verifiable credentials or derived credentials signed by the AESP with each proof are registered to a permissionless blockchain system as a repository.
- Verifiers may utilize the signed credentials with a corresponding proof for each credential to verify whether the person is requesting to subscribe and use services provided by the verifiers.

In this proposal, the owner of a mobile device equipped with an AESP is the person who may represent their self-sovereign identity. Because of utilizing AESPs, computation for preserving privacy can securely be executed within a device. In addition, verifiers may identify if the holder is the same person or not since the proof is attested by the holder's device equipped with an AESP. It means that MPC requiring a committee of trusted parties is not required, and permissionless blockchains can efficiently be utilized for openness.

4.1.2 Derived Credentials and Sybil-Resistance

Because of various needs, the proposed SSI architecture allows people to create programs for issuing derived credentials to meet different requirements. For example, some service providers need to verify if customers are not younger than 18 years old but do not need to know their birthdays. Some agencies need to verify if applicants are formally registered as residents in the city but do not need any other claims. For infinite varieties of needs to utilize derived credentials for presentation, which allows minimizing disclosure, and the programmable architecture allows users to choose appropriate `prog` for their needs. Those programs for the proposed SSI architecture must be public and open source for anyone to verify.

Sybil-Resistant Derived Credentials

Unlike CanDID, the AESP-based SSI architecture does not assume generating the master credential, an interim credential designed to support the deduplication of identities for satisfying Sybil-resistance. An AESP is a unique entity capable of secure computation within a local processor. The equipped AESP may embed an encrypted link for derived credentials with a natural person by their key pair $(\mathtt{pk}_U, \mathtt{sk}_U)$. Figure 4.2

illustrates the relationship among real identities $\mathcal{I}$, Sybil-resistant credentials $\mathcal{C}$, and derived credentials some of which are Sybil-resistant; let us call Sybil-resistant derived credentials $\mathcal{D}$.

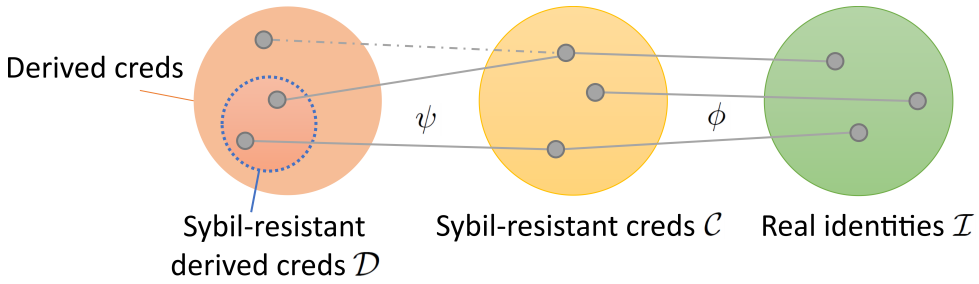


Figure 4.2: Sybil-resistant derived credentials and the injective map $\psi : \mathcal{D} \rightarrow \mathcal{C}$

Programs requiring to manage credentials that meet the Sybil-resistance requirement should implement a function *identification mapper* ψ that creates and maintains the injective map: $\mathcal{D} \rightarrow \mathcal{C}$. AESPs may install and execute programs capable of treating the functionality of ψ securely. Section 4.2 with Figure 4.5 will describe the detailed protocol for creating Sybil-resistant derived credentials.

4.2 Protocols in Detail

The proposed SSI architecture defines and provides some primitive protocols as described in Figure 4.3, 4.4, 4.5, and 4.6. The scheme assumes EUF-CMA (Existential Unforgeability under Chosen Message Attack) signature scheme Σ and IND-CCA (Indistinguishability under Chosen Ciphertext Attack) encryption algorithm $\{\text{Gen}, \text{Enc}, \text{Dec}\}$. Further, the scheme assumes all AESP-equipped devices share `mpk` and `msk` as determined in the Rafael Pass, Elaine Shi, and Florian Tramèr's works [PST17].

Definition 4.1 (A mobile device equipped with $\mathcal{G}_{\texttt{att}}$)**.** *The ideal functionality of attested execution secure processors (AESPs) is denoted by* $\mathcal{G}_{\texttt{att}}$*, and let us assume that every natural person's mobile device who needs a secure SSI is equipped with* $\mathcal{G}_{\texttt{att}}$*.*

Definition 4.2 (A set of secure SSI system protocols)**.** *A set of protocols* Π *is said to be secure SSI system protocols if and only if it satisfies Sybil-resistance, Unforgeability, Privacy – credential-issuance and verification, and Unlinkability.*

Theorem 4.1 (The AESP-based secure SSI system protocols)**.** *Assuming that natural persons own their mobile devices equipped with* $\mathcal{G}_{\mathtt{att}}$ *and standard computational assumptions, a set of protocols* $\Pi^{\mathcal{G}_{\mathtt{att}}}$ *shown in* Figure 4.3, 4.4, 4.5, and 4.6 *realizes a secure SSI system protocols.*

The protocol $\Pi^{\mathcal{G}_{\mathtt{att}}}$ consists of three types of functionality: foundation (Figure 4.3), issuance (Figure 4.4 and 4.5), and verification (Figure 4.6). The functionality for foundation mainly consists of the ideal abstraction of AESPs – the ideal functionality $\mathcal{G}_{\mathtt{att}}$. Namely, $\Pi^{\mathcal{G}_{\mathtt{att}}}$ includes the enclave operations of $\mathcal{G}_{\mathtt{att}}$, such as $\mathsf{Install}()$ and $\mathsf{Resume}()$ as well as for set-up, in addition to Π specific primitives such as for setup, and credentials issuance and verification.

AESP-based secure SSI system protocols – $\Pi^{\mathcal{G}_{\mathtt{att}}}$: Foundation

The core abstraction of AESPs – the ideal functionality $\mathcal{G}_{\mathtt{att}}$:

- $\mathsf{Setup}(1^\lambda) \rightarrow (\mathtt{mpk}, \mathtt{msk})$.
  1: $\mathcal{G}_{\mathtt{att}}.\mathsf{KeyGen}(1^\lambda)$; // for generating a key pair.
  2: $\mathcal{G}_{\mathtt{att}}.\mathsf{getpk}()$. // for receiving the key pair from some platform $\mathcal{P}$.
- $\mathsf{Install}(\mathtt{prog}) \rightarrow eid$. // for installing a program to enclave.
  1: $\mathcal{G}_{\mathtt{att}}$ asserts if $\mathcal{P}$ is honest;
  2: $\mathcal{G}_{\mathtt{att}}$ generates a nonce $eid \in \{0,1\}^\lambda$, stores the program $\mathtt{prog}$, and sends eid to $\mathcal{P}$.
- $\mathsf{Resume}(eid, \mathtt{inp}) \rightarrow (\mathtt{outp}, \sigma_M)$.
  1: $\mathcal{G}_{\mathtt{att}}$ checks if the program $\mathtt{prog}$ associated eid exists, abort if not found;
  2: $\mathcal{G}_{\mathtt{att}}$ executes $\mathtt{prog}$ and generates output $\mathtt{outp}$;
  3: $\mathcal{G}_{\mathtt{att}}$ generates a signature σ_M by $\Sigma.\mathsf{Sig}_{\mathtt{msk}}(eid, \mathtt{prog}, \mathtt{outp})$, and sends $(\mathtt{outp}, \sigma_M)$ to $\mathcal{P}$.
- $\mathsf{KeyGen}(1^\lambda) \rightarrow (\mathtt{pk}_U^E, \mathtt{sk}_U^E)$.
  1: An AESP generates a user's key pair $(\mathtt{pk}_U^E, \mathtt{sk}_U^E)$, a pseudonym for each Entity. For simplicity, let us omit E in the following descriptions.

Figure 4.3: AESP-based SSI System Protocols $\Pi^{\mathcal{G}_{\mathtt{att}}}$: Foundation

Figure 4.4 illustrate two issuance function in $\Pi^{\mathcal{G}_{\mathtt{att}}}$. One of the issuance functions is for legacy compatibility followed by the same functionality defined by CanDID [Mar+21], and the other is the main proposal to support creating derived credentials by AESPs, accessing the oracle $\mathcal{G}_{\mathtt{att}}$. $\Pi^{\mathcal{G}_{\mathtt{att}}}$ provides flexibility by allowing a natural person to choose and install programs `prog` for various needs.

AESP-based secure SSI system protocols – $\Pi^{\mathcal{G}_{\mathtt{att}}}$: Issuance

$\Pi^{\mathcal{G}_{\mathtt{att}}}$ Secure SSI-featured basic functions accessing the oracle $\mathcal{G}_{\mathtt{att}}$: Issuance

- $\mathsf{IssueCred}(\mathtt{sk}_U, \mathtt{pk}_U, \mathit{Stmt}) \rightarrow \mathtt{cred}$. // for legacy compatibility.
  1: An AESP requests a legacy authority to issue their verifiable credential consisting of claims regarding Stmt;
  2: An AESP retrieves a verifiable credential from the authority and treats $\{\mathtt{pk}_U, (\mathtt{claim}_i)_{j=1,\ldots,m}, \pi\}$ as `cred`, where π is a proof for a set of the claims by the authority.
- $\mathsf{IssueDCred}\,(\mathtt{msk}, \mathtt{sk}_U, \mathtt{pk}_U^{\mathtt{new}}, \mathtt{ctx}, \mathtt{cred}) \rightarrow \mathtt{derivedCred}$.
  This function, $\mathsf{IssueDCred}()$, is a program `prog`, which can be vary for different context `ctx`. To install and execute `prog`,
  1: $\mathcal{G}_{\mathtt{att}}.\mathsf{Install}(\mathtt{prog}) \rightarrow \mathit{eid}$; // only once for install.
  2: $\mathcal{G}_{\mathtt{att}}.\mathsf{Resume}(\mathit{eid}, \mathtt{inp}) \rightarrow (\mathtt{outp}, \sigma_M)$.

  Inputs `inp` of `ctx` and `cred` are depend on various context specified by `ctx`, outputs `outp` are $(\mathtt{claim}_j)_{j=1,\ldots,m}$ as a part of `derivedCred`, where σ_M is $\Sigma.\mathsf{Sig}_{\mathtt{msk}}(\mathit{eid}, \mathtt{prog}, \mathtt{outp})$, and `prog` is an open-source program satisfying the following transformation:

$$\mathtt{prog} : \{\mathtt{cred}_k\}_{k=1,\ldots,n} \mapsto \{\mathtt{claim}_j\}_{j=1,\ldots,m} \tag{4.1}$$

  For creating a Sybil-resistant credential, the program `prog` should satisfy the construction defined in Figure 4.5.

Figure 4.4: AESP-based SSI System Protocols $\Pi^{\mathcal{G}_{\mathtt{att}}}$: Issuance

As described in Section 4.1.2, the AESP-based SSI architecture and primitive protocols can be extended to adopt various requirements, including Sybil-resistance – this is one of the most important perspectives in this thesis. Below, Figure 4.5 describes how the AESP-based Sybil-resistant SSI architecture creates derive credentials that meet the Sybil-resistance requirement.

Construction for creating Sybil-resistant credentials in $\Pi^{\mathcal{G}_{\mathtt{att}}}$

For creating a Sybil-resistant derived credential, the program `prog` should satisfy the following construction: the program `prog` treats $(\mathtt{pk}_U, \widehat{\psi})$ as inputs `inp`, where $\widehat{\psi}$ is Sybil-resistant pseudonymizer to transform verifiable credentials to a set of claims satisfying the injective map with *identification mapper*

$$\psi : \mathcal{D} \rightarrow \mathcal{C} \tag{4.2}$$

in encrypted form. The construction requires at least one verifiable credential, say $\mathtt{cred}_k$, which is a Sybil-resistant credential. It embeds encrypted links using IND-CCA encryption algorithm $\mathcal{E}$:

$$\widehat{\psi} = \mathcal{E}.\,\mathrm{Enc}_{\mathtt{mpk}}(\mathtt{cred}_k) \tag{4.3}$$

The program `prog` decrypts $\widehat{\psi}$ to get ψ and checks if $\psi(\mathtt{cred}_k) \in \mathcal{C}$.
The generated derived credential consists of $\mathtt{pk}_U$, $\widehat{\psi}$ as `prog`, claims transformed by the Sybil-resistant pseudonymizer, together with the attestation signature σ_M from $\mathcal{G}_{\mathtt{att}}$ as follows:

$$\mathtt{derivedCred} \leftarrow (\mathtt{pk}_U, \widehat{\psi}, \{\mathtt{claim}_j\}_{j=1,\ldots,m}, \sigma_M) \tag{4.4}$$

To generate and treat derived credentials that are Sybil-resistant, the construction needs to satisfy both **Definition 4.4** and the definitions for privacy at the same time. These requirements contradict each other. However, only the AESP can decrypt and verify links between the derived and Sybil-resistant credentials. Thus, the construction requires all derived credentials to embed an encrypted link to one of those Sybil-resistant credentials in encrypted form.

Figure 4.5: Construction of `prog` for creating Sybil-resistant credentials in $\Pi^{\mathcal{G}_{\mathtt{att}}}$

Lastly, let me describe the verification function of $\Pi^{\mathcal{G}_{\mathtt{att}}}$ in Figure 4.6.

AESP-based secure SSI system protocols – $\Pi^{\mathcal{G}_{\mathtt{att}}}$: Verification

$\Pi^{\mathcal{G}_{\mathtt{att}}}$ Secure SSI-featured basic functions accessing the oracle $\mathcal{G}_{\mathtt{att}}$: Verification

- $\mathsf{VerifyDCred}(\mathtt{sk}_U, \mathtt{cred}) \to \{\mathtt{true}, \mathtt{false}\}$.

  Two-party protocol between U and V with common input $\mathtt{mpk}$. User U inputs $\mathtt{sk}_U$ and $\mathtt{cred}$, verifying party V authenticates U if U knows $\mathtt{sk}_U$ whose public key $\mathtt{pk}_U$ is on $\mathtt{cred}$ as follows,

  1: User U sends $(\mathtt{cred}, \sigma)$ to V where $\sigma = \mathsf{Sig}_{\mathtt{sk}_U}(c)$;
  2: Verifying party V checks if

$$\mathcal{V}_{\mathtt{mpk}}(\mathtt{cred.body}, \mathtt{cred}.\sigma_M) = \mathtt{true} \wedge \mathcal{V}_{\mathtt{pk}_U}(c, \sigma) = \mathtt{true}, \tag{4.5}$$

  where $\mathcal{V}_{\mathtt{mpk}}$ is a verifying program that verifies using $\mathtt{mpk}$ if $\mathtt{cred}$ is valid with the attested signature σ_M issued by $\mathcal{G}_{\mathtt{att}}$, and $\mathcal{V}_{\mathtt{pk}_U}$ is a verifying program that verifies using $\mathtt{pk}_U$ if a challenge c is signed by the corresponding $\mathtt{sk}_U$.

Figure 4.6: AESP-based SSI System Protocols $\Pi^{\mathcal{G}_{\mathtt{att}}}$: Verification

4.3 Security Analysis and Attacker Models

With respect to the contributions by Deepak Maram *et al.* [Mar+21], I will follow how CanDID demonstrates that their protocols of decentralized identity systems are designed securely as much as possible. In particular, they define CanDID API; in some of their definitions, adversaries have unlimited access to the entire CanDID API, which they model for conciseness as an oracle $\mathcal{O}^*$. Also, in their security definitions, the adversaries may have access to an external account oracle $\mathcal{O}^*_{\text{ext}}$ that models the legacy providers called by CanDID.

The proposal will reuse the same oracle models[1] for the AESP-based SSI system

[1]Following the conventions in CanDID [Mar+21], $\mathcal{O}^*$ has the same functions (APIs) as Figure 4.3,

protocols $\Pi^{\mathcal{G}_{\text{att}}}$. We assume that all issuers and AESPs are honest; however, a holder (a natural person) who can be recognized as a prover or a verifier could be malicious. When a holder is malicious, the holder may attack their AESP to issue a wrong derived credential as an adversary $\mathcal{A}$ (*the malicious prover model*). Conversely, when a verifier is malicious, the verifier may violate holders' privacy (*the malicious verifier model*).

4.4 Security Properties

The set of protocols $\Pi^{\mathcal{G}_{\text{att}}}$ aims to satisfy the following security properties, for each of which adversary may access and try to corrupt, Sybil-resistance, Unforgeability, Privacy – credential-issuance and verification, and Unlinkability.

4.4.1 Sybil-Resistance

An adversary cannot obtain Sybil-resistant credentials, which we define as below:

Definition 4.3 (Sybil-resistant credential)**.** *Let $\mathcal{I}$ be a set of real identities and $\mathcal{C}$ be a set of credentials. The credentials $\mathcal{C}$ is said to be Sybil-resistant credentials if and only if there exists a bijective map $\phi : \mathcal{C} \to \mathcal{I}$; hence, $\phi^{-1} : \mathcal{I} \to \mathcal{C}$.*

In the real world, a national PKI system, e.g., JPKI (described in Section 6.1.4), is an example of authorities that can provide a unique identifier for creating Sybil-resistant credentials. A master credential in CanDID corresponds to a Sybil-resistant credential. We assume a single system of Sybil-resistant credentials for brevity in this thesis.

Definition 4.4 (Existence)**.** *Suppose $\mathcal{C}$ be a set of all Sybil-resistant credentials and $\mathcal{D}$ be a set of derived credentials. A derived credential* `cred` *within $\mathcal{D}$ is said to be Sybil-resistant with respect to $\mathcal{C}$ if and only if, for any PPT (Probabilistic Polynomial-Time)*

4.4, 4.5, and 4.6, but acts honestly as an ideal functionality. $\mathcal{O}^*_{\text{ext}}$ has its internal state L, where L is a set of tuples of the form $(\texttt{id}, a, v)$ where `id` is an user identifier (equivalent with $\texttt{pk}_U$ in the constructions), a an attribute, and v the corresponding value. $\mathcal{O}^*_{\text{ext}}$ has the following functions with initial state $L = \emptyset$:

1. $\mathsf{update}(\texttt{id}, a, v')$: if $\exists(\texttt{id}, a, v) \in L$, replace it with $(\texttt{id}, a, v')$.
2. $\mathsf{delete}(\texttt{id})$: Remove all $(\texttt{id}, \_, \_)$ from L if exist.
3. $\mathsf{getProof}(\texttt{id}, a) \to v, \pi$: If $\exists(\texttt{id}, a, v) \in L$, return v with a proof π, or $\perp$ otherwise.
4. $\mathsf{getOwnershipProof}(\texttt{id}) \to \pi$: If $\exists(\texttt{id}, \_, \_) \in L$, return a proof of account ownership, or $\perp$ otherwise.

adversary $\mathcal{A}$ *and security parameter* λ*, there exists an injective map* $\psi : \mathcal{D} \to \mathcal{C}$ *such that*

$$\Pr\left[\psi(\texttt{cred}) \in \mathcal{C} \;\middle|\; \begin{array}{c} \texttt{mpk}, \texttt{msk} \leftarrow \mathsf{KeyGen}(1^\lambda); \\ \texttt{cred} \leftarrow \mathcal{A}^{\mathcal{O}^*, \mathcal{O}^*_{\mathrm{ext}}}(\texttt{mpk}); \\ \mathcal{V}_{\texttt{mpk}}(\texttt{cred}) = \texttt{true} \end{array}\right] \geq 1 - \mathrm{negl}(\lambda) \tag{4.6}$$

where `cred` *consists of* $(\texttt{pk}_U, \texttt{prog} : \psi\{\texttt{claim}_j\}_{j=1,\ldots,m})$ *as its* `body`[2] *and its signature* σ_M*,* `prog` *is capable of functionality* ψ*, and* $\mathcal{V}_{\texttt{mpk}}$ *is a verification algorithm to verify* `cred` *using* `mpk` *in a simple form, which can be expressed if* `cred` *is valid with the attested signature* σ_M *issued by* $\mathcal{G}_{\texttt{att}}$ *as follows:*

$$\Sigma.\mathsf{Ver}_{\texttt{mpk}}\left(\texttt{cred.body}, \texttt{cred.}\sigma\right) = \texttt{true}. \tag{4.7}$$

Informally, this definition captures the infeasibility of an adversary to obtain a derived credential `cred` that is not in the set of all Sybil-resistant credentials such that $\psi(\texttt{cred}) \in \mathcal{C}$ as far as `cred` bears a valid attestation signature. Here, the *identification mapper* ψ is defined over all elements in derived credentials. Hence, ψ uniquely ***identifies*** the holders' real identity from derived credentials. The set of system protocols assumes that the map ψ is accessed only internally by the AESP. Thus, the link between derived credentials and Sybil-resistant credentials is hidden; it supports privacy preservation.

This game resides on *the malicious prover model* in the attacker models. An adversary $\mathcal{A}$ attacks the holder to create potentially a wrong derived credential under the assumption that $\mathcal{V}_{\texttt{mpk}}$ is honest.

4.4.2 Unforgeability

An adversary cannot forge the credentials of honest users or otherwise impersonate them.

Definition 4.5 (Unforgeability)**.** *Let* `chals` *denote a set of all challenges and their responses produced by* $\mathcal{A}$ *in oracle access with* $\mathcal{O}^*$ *and a special oracle* $\mathcal{O}^*_{\texttt{sk}_U}$ *that allows*

[2] $\texttt{pk}_U$ works as an identifier, `id`.

calling any $\Pi^{\mathcal{G}_{\text{att}}}$ *functions with the user key parameter set to* $\mathtt{sk}_U$. *The protocol* $\Pi^{\mathcal{G}_{\text{att}}}$ *offers unforgeability if, for any stateful PPT adversary* $\mathcal{A}$,

$$\Pr\left[\begin{array}{c}\mathsf{VerifyDCred}(\mathtt{sk}_U,\mathtt{cred})\\=\mathtt{true}\end{array}\;\middle|\;\begin{array}{c}\mathtt{mpk},\mathtt{msk}\leftarrow\mathsf{KeyGen}(1^\lambda);\\ \mathtt{pk}_U,\mathtt{sk}_U\leftarrow\mathsf{KeyGen}(1^\lambda);\\ \mathtt{cred}\leftarrow\mathcal{A}^{\mathcal{O}^*,\mathcal{O}^*_{\mathtt{sk}_U},\mathcal{O}^*_{\text{ext}}}(\mathtt{mpk},\mathtt{pk}_U)\\ s.t.\ \mathtt{cred.body}\notin\mathtt{chals};\end{array}\right]\leq\text{negl}(\lambda). \tag{4.8}$$

The definition captures that it must be infeasible for an adversary to impersonate users, that is, forge signatures with users' keys. This game also resides on *the malicious prover model* where an adversary $\mathcal{A}$ attacks the holder to potentially create a wrong credential under the assumption that the verifier is honest.

4.4.3 Privacy – Credential-Issuance

It is infeasible for an adversary to learn users' attributes from observing the derived credential-issuance protocol. Let us denote $\{c_1^0,...,c_n^0\}$ for $\{\mathtt{cred}_k^0\}_{k=1,...,n}$ and $\{c_1^1,...,c_n^1\}$ for $\{\mathtt{cred}_k^1\}_{k=1,...,n}$ as a set of claims for each $\{0,1\}$.

Definition 4.6 (Credential issuance privacy)**.** *The protocol* $\Pi^{\mathcal{G}_{\text{att}}}$ *offers derived credential issue privacy if, for any stateful PPT adversary* $\mathcal{A}$,

$$\left|\Pr\left[b=b'\;\middle|\;\begin{array}{c}\mathtt{mpk},\mathtt{msk}\leftarrow\mathsf{KeyGen}(1^\lambda);\\ \mathtt{pk}_U,\mathtt{sk}_U,\{c_1^0,...,c_n^0\},\{c_1^1,...,c_n^1\}\leftarrow\mathcal{A}^{\mathcal{O}^*,\mathcal{O}^*_{\text{ext}}}(\mathtt{mpk});\\ \mathtt{cred}^b\leftarrow\mathsf{IssueDCred}(\mathtt{msk},\mathtt{sk}_U,\mathtt{pk}_U,\{c_1^b,...,c_n^b\},\mathtt{prog}),\\ \textit{where }\mathtt{cred}^b=(\mathtt{pk}_U,\{\mathtt{claim}_j^b\}_{j=1,...,m},\widehat{\psi^b},\mathtt{prog},\sigma_M^b)\\ \textit{for } b=0,1;\\ \text{assert }\{\mathtt{claim}_j^0\}_{j=1,...,m}=\{\mathtt{claim}_j^1\}_{j=1,...,m}\textit{ as sets};\\ b\leftarrow\$\{0,1\};\\ b'\leftarrow\mathcal{A}^{\mathcal{O}^*,\mathcal{O}^*_{\text{ext}}}(\mathtt{cred}^b)\end{array}\right]-\frac{1}{2}\right|\leq\text{negl}(\lambda). \tag{4.9}$$

This game resides on *the malicious verifier model* in the attacker models. An adversary $\mathcal{A}$ tries to violate a holder's privacy by retrieving information from their new credential, assuming that the holder is honest.

4.4.4 Privacy – Credential-Verification

An adversary can learn about a user no more than the information that the user explicitly presents while using their credentials.

Definition 4.7 (Credential verification privacy)**.** *Given an open-source map* `prog` *that maps user data in verifiable credentials to derived credential claims, any PPT adversary* $\mathcal{A}$ *learns negligibly more about any given user than the output of* `prog`*.*

4.4.5 Unlinkability

The entities administering the protocol $\Pi^{\mathcal{G}_{\text{att}}}$ reliant programs cannot collude and link the respective transactions of any given user.

Definition 4.8 (Unlinkability across programs)**.** *The protocol* $\Pi^{\mathcal{G}_{\text{att}}}$ *offers unlinkability if, for any stateful PPT adversary* $\mathcal{A}$*,*

$$\left|\Pr\left[b=b' \;\middle|\; \begin{array}{c} \mathtt{mpk},\mathtt{msk}\leftarrow \mathsf{KeyGen}(1^\lambda);\\ \mathtt{cred}^0,\mathtt{cred}^1,\mathtt{pk}_U,\mathtt{sk}_U,\mathtt{ctx}\leftarrow \mathcal{A}^{\mathcal{O}^*,\mathcal{O}^*_{\text{ext}}}(\mathtt{mpk});\\ \text{assert } \mathcal{V}_{\mathtt{pk}_U}(\mathtt{cred}^b.\mathtt{body},\mathtt{cred}^b.\sigma)=\mathtt{true} \;\; \textit{for } b=0,1;\\ b\leftarrow \$\{0,1\};\\ \mathtt{cred}_{new}\leftarrow \mathsf{IssueDCred}(\mathtt{msk},\mathtt{sk}_U,\mathtt{pk}_U,\mathtt{cred}^b);\\ b'\leftarrow \mathcal{A}^{\mathcal{O}^*,\mathcal{O}^*_{\text{ext}}}(\mathtt{cred}_{new},\mathtt{ctx}) \end{array}\right] - \frac{1}{2}\right| \leq \text{negl}(\lambda). \tag{4.10}$$

This game also resides on *the malicious verifier model* in the attacker models. An adversary $\mathcal{A}$ tries to violate a holder's privacy by retrieving information from their credential, assuming that the holder is honest.

4.5 Proof of the Theorem

Proof of Theorem 4.1. We prove that the set of protocols $\Pi^{\mathcal{G}_{\text{att}}}$ defined in Figure 4.3, 4.4, 4.5, and 4.6, which is a set of secure self-sovereign identity (SSI) system protocols.

4.5.1 Sybil-Resistance

First, let us prove $\Pi^{\mathcal{G}_{\text{att}}}$ satisfies **Definition 4.4** for **Existence**. It is sufficient to prove that every derived credential `cred` has an injective map ψ by the *identification mapper*

such that $\psi(\texttt{cred}) \in \mathcal{C}$. In the protocol $\Pi^{\mathcal{G}_{\texttt{att}}}$, every $\texttt{cred}$ has the following form

$$(\texttt{pk}_U, \widehat{\psi}, \{\texttt{claim}_j\}_{j=1,\ldots,m}, \sigma_M) \tag{4.11}$$

where $\widehat{\psi}$ is a ciphertext of a verifiable and Sybil-resistant credential $\texttt{cred}$ encrypted with the public key of $\mathcal{G}_{\texttt{att}}$. Therefore, given

$$\begin{aligned} &\Sigma.\mathsf{Ver}_{\texttt{mpk}}(\texttt{cred.body}, \texttt{cred}.\sigma_M) = \texttt{true} \Rightarrow \\ &\Sigma.\mathsf{Ver}_{\texttt{mpk}}(\texttt{pk}_U, \widehat{\psi}, \{\texttt{claim}_j\}_{j=1,\ldots,m}, \sigma_M) = \texttt{true}, \end{aligned} \tag{4.12}$$

it implies that $\mathcal{G}_{\texttt{att}}$ can decrypt $\widehat{\psi}$ to get $\texttt{cred}$ as $\texttt{cred} = \mathcal{E}.\mathrm{Dec}_{\texttt{msk}}(\widehat{\psi})$ and verify the relation $\texttt{cred} \in \mathcal{C}$ unless the signature σ_M is forged. $\mathcal{E}$ denotes IND-CCA encryption algorithm, and the latter probability is negligible in λ given Σ is EUF-CMA signature scheme.

4.5.2 Unforgeability

In $\Pi^{\mathcal{G}_{\texttt{att}}}$ based SSI systems, users' key never leaves their device with an AESP. During the protocols, they use it only to sign challenges issued as part of $\mathsf{VerifyDCred}()$. Thus, unforgeability of the $\Pi^{\mathcal{G}_{\texttt{att}}}$ based SSI systems follows in a straightforward way.

Here, $\texttt{cred}$ has the following form:

$$\big(\texttt{pk}_U, \widehat{\psi}, \{\texttt{claim}_j\}_{j=1,\ldots,m}, \sigma_M\big). \tag{4.13}$$

Queries to $\mathcal{O}^*$ and $\mathcal{O}^*_{\texttt{sk}_U}$ must be a set of tuples

$$(\texttt{pk}_U, \{\texttt{cred}_k\}_{k=1,\ldots,\ell}, \texttt{prog}) \tag{4.14}$$

and the responses are $(\texttt{pk}_U, \widehat{\psi}, \{\texttt{claim}_j\}_{j=1,\ldots,m}, \sigma_M)$ where a set of claims $\{\texttt{claim}_j\}_{j=1,\ldots,m}$ is the image of $\texttt{prog}$ with inputs $\{\texttt{cred}_k\}_{k=1,\ldots,\ell}$. Thus, $\texttt{chals}$ contains all tuples appeared in the oracle access by $\mathcal{A}$ of the form $(\texttt{pk}_U, \widehat{\psi}, \{\texttt{claim}_j\}_{j=1,\ldots,m})$. For creating new $\texttt{cred}$ such that $\texttt{cred.body} \notin \texttt{chals}$, $\mathcal{A}$ must forge a signature $\texttt{cred}.\sigma$ on the message tuple $\texttt{cred.body}$. Given the underlying EUF-CMA signature scheme Σ, this probability

is bounded by negl(λ), that is negligible in the security parameter λ.

4.5.3 Privacy – Credential-Issuance

In the privacy game for privacy – credential-issuance, the adversary chooses a pseudonym of the user who initiates each query and which providers are used, but otherwise learns nothing else about users' identities or attributes during operations such as credentials issuance.

By **Definition 4.6**, the adversary chooses two identities of $\{0, 1\}$ and observes that derived credentials are created by executing IssueDCred() with inputs of claims for each identity and the program `prog` with the encrypted *identification mapper* $\widehat{\psi}$. The adversary tries to access and guess any attributes and/or values; however, they cannot guess from a derived credential selected randomly.

Let me explain the reason behind it more. Since two credentials, $\texttt{cred}^0$ and $\texttt{cred}^1$ only differ in $\widehat{\psi}^0$, $\widehat{\psi}^1$ and related signatures, σ_U^0 and σ_U^1. $\widehat{\psi}^0$ and $\widehat{\psi}^1$ are encrypted by the IND-CCA encryption algorithm $\mathcal{E}$. Probability to distinguish them is upper-bounded negl(λ). Therefore, I conclude that the adversary cannot win the game as it does not learn any information to distinguish the verifiable credentials.

4.5.4 Privacy – Credential-Verification

The scheme assumes that all privacy operations for issuing and treating credentials are executed within an AESP internally by `prog`, including IssueDCred() and VerifyDCred(). The scheme also expects that only `prog` will be accepted by both users and providers that reach the consensus. Such `prog` only leaks required privacy information described as a set of claims $\{\texttt{claim}_j\}_{j=1,\ldots,m}$. This process is expected to leak any more information as defined in **Definition 4.7**.

4.5.5 Unlinkability

As the same as the other privacy game for privacy – credential issuance, the adversary needs to try an input but randomly selected, and a credential $\texttt{cred}^0$ or $\texttt{cred}^1$ in this case as defined in **Definition 4.8**. It cannot guess any information to distinguish which

provider from a credential selected randomly. Therefore, I conclude that the adversary cannot win the game for unlinkability in the scheme. □

Chapter 5

Anonymous Sybil-Resistant SSI Utilizing Zero-Knowledge Membership Proofs

Furthermore, I propose a novel scheme with constructions that make credentials blind from others utilizing Pedersen commitments [Ped91] and zero-knowledge membership proofs, "One-Out-of-Many Proofs" Σ-protocol [GK15] in particular, with other techniques such as the BBS+ signature scheme [ASM06].

The proposal described in the previous section demonstrated the powerfulness of hardware-assisted security and the formal abstraction of AESPs, and it brings drastic flexibility and efficiency to Sybil-resistant decentralized identity systems. However, it assumes the stronger assumption requiring AESPs for all entities in the protocol; thus, not only a natural person who owns their mobile device equipped with an AESP but all verifiers require AESPs. To eliminate AESPs from verifiers, I needed to consider various perspectives such as how an attested signature can be converted to another one that does not require an AESP.

It is a challenge in general how to treat strings publicly verifiable under permissionless blockchains because any personal information, including identifiers, should not be stored as linkable as they were. Linkability could remain among identifiers and credentials as long as pseudonyms, even public keys, are used as identifiers of credentials. Particularly, we need to revisit how to realize unlinkability among credentials for pub-

lic verification under weaker assumptions to make the AESP-based Sybil-resistant SSI more efficient and useful.

To solve these problems, my proposal includes predicates for claims, *computed claims in Boolean* from multiple issuers, and commitment-based identifiers, *perfectly anonymous identifiers*. I will call verifiable credentials with these two new notions *Anonymous Verifiable Credentials*. I also propose a technique that adopts the one-out-of-many proofs Σ-protocol enabling users (holders) to prove a list of commitments (list of anonymous identifiers) having the expected commitment corresponding to the witness (associated with the credential) for verifiers with zero-knowledge.

5.1 The Scheme Overview

Figure 5.1 illustrates the relationship among a set of real identities $\mathcal{I}$, a set of all the Sybil-resistant credentials $\mathcal{C}$ that associates with the real identities $\mathcal{I}$, and various derived credentials, some of which are Sybil-resistant. As the same as the proposal described in Chapter 4, $\mathcal{C}$ is a set of (the master) Sybil-resistant credentials if and only if there exists a bijective map $\phi : \mathcal{C} \to \mathcal{I}$, real identities. $\mathcal{D}_\ell$ is a set of Sybil-resistant *derived* credentials for service numbered ℓ, and there exists a Sybil-resistant derived credential if it sustains an *identification mapper* $\psi_\ell : \mathcal{D}_\ell \to \mathcal{C}$. Let us omit ℓ for brevity unless it is explicitly required in the following descriptions.

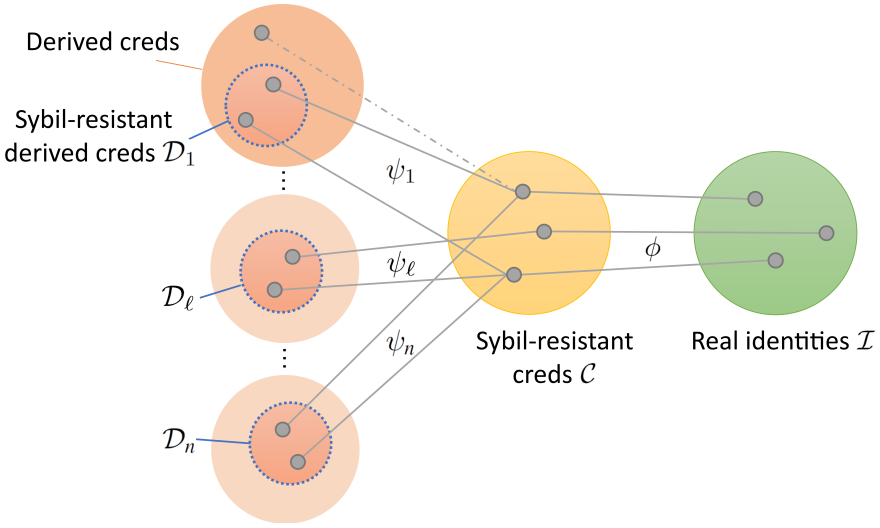


Figure 5.1: Sybil-resistant derived credentials and the injective maps $\psi_\ell : \mathcal{D}_\ell \to \mathcal{C}$

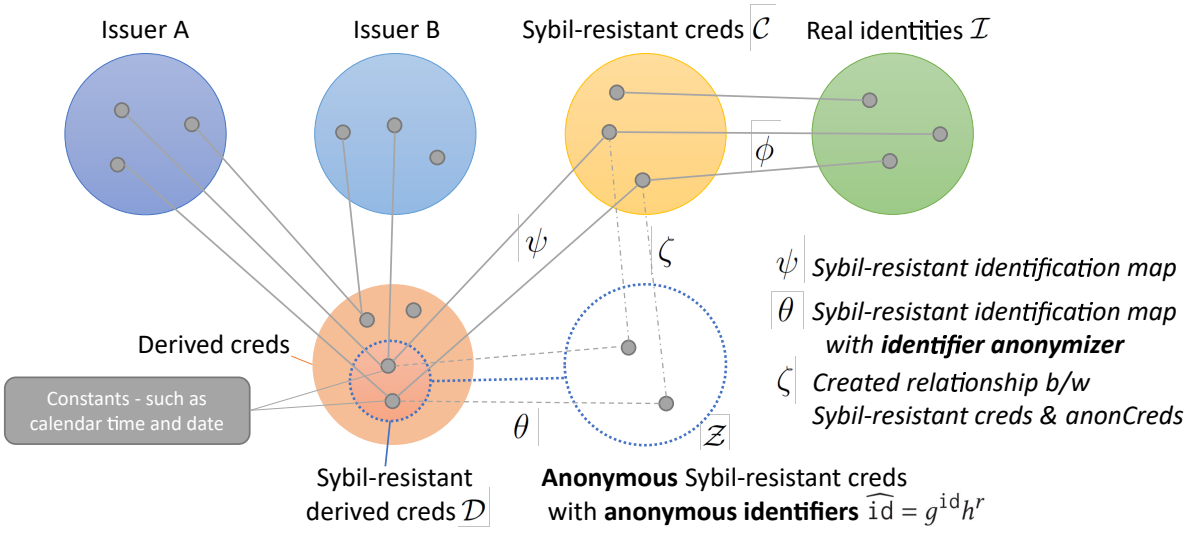


Figure 5.2: Sybil-Resistant SSI with Anonymous Credentials

Figure 5.2 illustrates the proposed architecture of anonymous Sybil-resistant credentials with perfectly anonymous identifiers, working with the one-out-of-many proofs Σ-protocol. Sybil-resistant credentials consist of computed claims from Issuer A and Issuer B, as illustrated. I propose ***identifier anonymizer*** θ that generates ***anonymous*** *Sybil-resistant credentials* with ***perfectly anonymous identifiers***, all of which are defined and described in the following subsections.

5.1.1 Computed Claims in Boolean

This thesis will define *computed claims* and its simplified form in Boolean, predicates ρ. I already addressed such a computed claim in Chapter 4 in the following notation:

$$\mathtt{prog} : \{\mathtt{cred}_k\}_{k=1,\ldots,n} \mapsto \{\mathtt{claim}_j\}_{j=1,\ldots,m} \tag{5.1}$$

where `prog` should be an open-source program satisfying an expected transformation for service providers that verify generated derived credentials of computed claims, $\{\mathtt{claim}_j\}_{j=1,\ldots,m}$, and $\mathtt{cred}_k$ are verifiable credentials issued by multiple issuers, $k = 1, \ldots, n$.

A straightforward example of such a computed claim is to represent if they are over 20 years old at a particular time computed from their identification cards, including the

date of birth. On the other side, some Vaccination Certificates for COVID-19 do not include the date of birth, but they might need to be present as vaccinated over enough times for their age. More importantly, derived credentials for presentation for some services may be required if they are securely issued to deal with the Sybil-resistance requirement, for which those credentials must be computed to ensure the injective *identification mapper* ψ to a set of Sybil-resistant real identities.

Definition 5.1 (Computed Claims in a Verifiable Credential)**.** *Let* `prog` *be a stateful program to be installed in AESPs, which securely stores secret keys in its local storage, denoted by* κ*.* `prog` *is said to* ***possess*** *a* `cred` *if and only if* `prog` *stores the corresponding secret key* `sk` *with the public key* `pk` *claimed in* `cred`*. Then, a computed claim is a claim generated by computation from multiple claims and also other sources* τ *(e.g., time and date) if required. More formally,* `prog` *takes a set of input credentials with auxiliary data* τ *and its internal key store* κ *as inputs and outputs a set of claims:*

$$\texttt{prog} : (\{\texttt{cred}_k\}_{k=1,\ldots,n}, \tau) \mapsto \{\texttt{claim}_j\}_{j=1,\ldots,m} \text{ or } \perp \tag{5.2}$$

where `prog` *outputs* $\{\texttt{claim}_j\}_{j=1,\ldots,m}$ *if and only if* `prog` *posesses all secret keys corresponding to* $\{\texttt{cred}_k\}_{k=1,\ldots,n}$ *or outputs* $\perp$ *otherwise. The thesis assumes all secret keys generated by* `prog` *are stored in* κ *and never go out of* `prog`*.*

Ultimately, the purpose of having verifiable credentials is for a user (holder) as a prover to ask a service provider (verifier) to verify whether they have the right, are privileged, or are qualified to receive appropriate services. From this perspective, computed derived credentials for presentation can be simplified and treated in Boolean. Therefore, the thesis proposes a simplified form of computed claims as a predicate in Boolean as below:

$$\rho : \{0,1\}^* \rightarrow \{0,1\} \tag{5.3}$$

where ρ is a program that predicates a value $\in \{0,1\}$ from computed claims.

Definition 5.2 (Computed Claims in Boolean, a Predicate)**.** *A computed claim in Boolean is a computed claim that is predicated to a value* $\{0,1\}$ *in a message from computed claims.*

5.1.2 Perfectly Anonymous Identifiers

In the existing decentralized identity systems, pseudonyms are often used to identify various subjects or entities, such as credentials. W3C's DIDs are a type of identifier designed for such purposes based on a form of URI (Universal Resource Identifier). Pseudonyms could be a hint to trace subjects and/or entities as long as such pseudonyms remain. Therefore, it is required for credential systems, especially SSI, to dedicate a scheme to blind pseudonymous identifiers randomly from all others.

For those needs, I propose *perfectly anonymous identifiers* utilizing Pedersen commitments [Ped91]. The thesis assumes an identifier `id`, which is a typical pseudonym. Here, the main idea of the proposal of *perfectly anonymous identifiers* is represented as follows:

$$\widehat{\texttt{id}} = g^{\texttt{id}} h^r \tag{5.4}$$

where the Pedersen commitments scheme specifies a prime-order group $\mathbb{G}$ and two group elements g, h, some randomness $r \in \mathbb{Z}_q$. In this novel notion, since r is random, the generated $\widehat{\texttt{id}} = g^{\texttt{id}} h^r$ can also be uniformly random in information theory perspectives. The reason for using $\widehat{\ }$ over `id` in the above notation is to express something hidden, `id` in this case, by an umbrella in a cryptographic manner.

Definition 5.3 (Perfectly Anonymous Identifiers)**.** *A perfectly anonymous identifier is an identifier that is normalized in Pedersen commitment form with randomness.*

A significant advantage of this notion of *perfectly anonymous identifiers* can flexibly be utilized by proofs of equality and other zero-knowledge proofs, including the one-out-of-many proofs because of Pedersen commitments in nature. However, it is practically applicable only for Sybil-resistant identity systems because it is uniformly randomized and it requires the characteristics of the *identification mapper* ψ, defined in **Lemma 5.1**. Details will be described in the following Section 5.1.4.

5.1.3 Anonymous Verifiable Credentials

With those definitions of **Definition 5.2** and **5.3**, the thesis defines *Anonymous Verifiable Credentials* as follows:

Definition 5.4 (Anonymous Verifiable Credentials)**.** *Anonymous verifiable credentials are anonymized with an Anonymous Identifier, a simplified credential in Boolean, and a proof. Such an anonymous verifiable credential can be represented as below:*

$$\texttt{anonCred} : \left(\widehat{\texttt{id}}, \widehat{\rho}, \sigma\right). \tag{5.5}$$

This form of simplified anonymous verifiable credentials, including anonymous *Sybil-resistant* verifiable credentials defined below, can be treated over a permissionless blockchain more privately than today in an efficient enough manner with another proposal in this thesis by myself – a novel scheme to utilize the one-out-of-many proofs Σ-protocol [GK15].

Definition 5.5 (Anonymous Sybil-Resistant Credential)**.** *Anonymous Sybil-resistant (verifiable and derived) credentials are based on Sybil-resistant credentials defined as* **Definition 4.3** *in an anonymous verifiable (and derived) credentials form with a perfectly anonymous identifier.*

Here, a program `prog` that computes and creates *Anonymous Sybil-resistant* credentials is a stateful program to be installed in AESPs and securely manages its data in its local storage κ defined as **Definition 5.1**. The program must maintain **only the first time** a natural person requests to associate their identity with a service by the characteristics of the *identification mapper* ψ, and it enables the set of Sybil-resistant credentials **distinct** as long as the local storage κ is securely controlled by, for instance, its tamper-resistant capability.

5.1.4 Adopting "One-Out-of-Many Proofs" Σ-Protocol

As described in Section 3.3, the one-out-of-many proofs Σ-protocol has a notable capability to verify the existence of at least one among commitments in logarithm order. The idea is that users (holders) and verifiers assume to use anonymous verifiable credentials, which would be recorded over a permissionless blockchain. We call a set of anonymous verifiable credentials for a verifier as a pool $\mathcal{Z}$, as illustrated in Figure 5.2.

I now introduce ***identifier anonymizer*** θ that generates anonymous Sybil-resistant credentials corresponding to the set of illustrated Sybil-resistant derived credentials, and

such generated credentials having a *perfectly anonymous identifier* are registered in the $\mathcal{Z}$ pool under a permissionless blockchain. Those anonymous Sybil-resistant credentials are not able to be retrieved by anyone unless one may know a witness because its identifier is uniformly randomized by an anonymous identifier perfectly, $\widehat{\mathtt{id}} = g^{\mathtt{id}}h^r$, but only users (holders) and verifiers may identify if there exists in the $\mathcal{Z}$ pool with the construction, which will also be described in the following Section 5.3, based on the one-out-of-many proofs Σ-protocol.

Since the scheme is designed to comply with the Sybil-resistance requirement, an anonymous verifiable credential corresponding to a real identity uniquely exists, as indicated by the relationship ζ in Figure 5.2. In other words, since the one-out-of-many proofs Σ-protocol have a notable capability to verify the existence of, but *at least one* among commitments, the scheme works accordingly with the Sybil-resistance requirement. Under the scheme with the assumption, a Pedersen commitment-based *perfectly anonymous identifier*, even which is randomized by a different random value r', can be found by the one-out-of-many proofs in logarithm order among N commitments, namely numerous numbers of credentials.

With the notation determined in Section 3.3.2, adoption of the one-out-of-many proofs to prove the existence of an anonymous Sybil-resistant credential consisting of the corresponding anonymous identifier in the $\mathcal{Z}$ pool is said to be

$$\pi_{OOoM}(\widehat{\mathtt{id}} \in \mathcal{Z}); \tag{5.6}$$

otherwise, the expected anonymous Sybil-resistant credential does not exist in the $\mathcal{Z}$ pool, which is a subspace where only the distinctly generated commitments are registered because of meeting with the Sybil-resistance requirement.

5.2 The Scheme in Detail

Figure 5.3 illustrates how an AESP works with the idea of utilizing the one-out-of-many proofs, as well as utilizing the Proof of Knowledge of a Signature (SPK), the selective disclosure, and proofs of equality about discrete logarithms. One of the critical points is that utilizing all of these ideas enables verifiers to verify a credential created by an

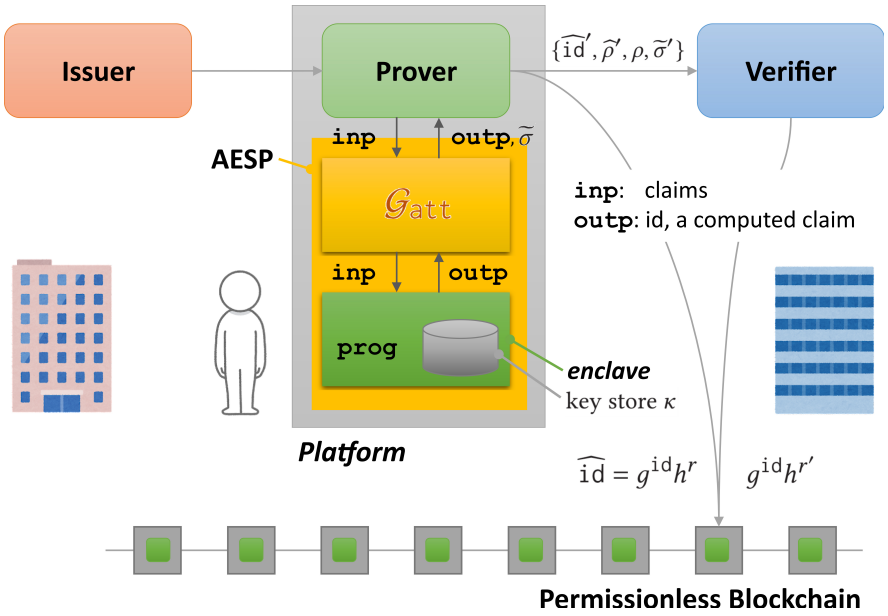


Figure 5.3: How AESP Works with Anonymous Identifiers

AESP without AESPs in the scheme proposed in this thesis.

A prover initiates an action to create a credential and then asks a verifier to verify it. The AESP handles inputs `inp`, and the secure and anonymous Sybil-resistant SSI system protocols work with `prog` for each purpose to generate an anonymous Sybil-resistant credential. Because `id` as the witness of perfectly anonymous identifiers, such as $\widehat{\texttt{id}}$ or $\widehat{\texttt{id}}'$, is equal even if such anonymous identifiers for the credential are randomly shifted for perfect anonymity, the verifier may resolve if the provided credential is the credential for them to verify.

5.2.1 Utilizing BBS+ Signature Scheme and SPK

I will use the BBS+ signature scheme to utilize the selective disclosure capability in the construction for efficiency, legacy compatibility, and constracting the scheme, keeping anonymity. As described in previous sections, the BBS+ signature scheme allows verifying the possession of the original signature, but the use is not limited to. A block message $(\texttt{id}, \rho)$ for verifiable credentials may have a signature (A, t, s) where a secret key $\gamma \in_R \mathbb{Z}_p^*$ is randomly chosen, (the corresponding public key is $w = h_0^{\gamma},$) the *signing*

algorithm chooses t, a random number s, and computes

$$A = \left[g_0 g_1^s g_2^{\mathtt{id}} g_3^{\rho}\right]^{\frac{1}{t+\gamma}} \tag{5.7}$$

in the BBS+ signature scheme. To verify a signature (A, t, s) on the block message $(\mathtt{id}, \rho)$, the scheme may check if

$$\mathrm{e}(A, \mathtt{mpk} h_0^t) = \mathrm{e}\big(g_0 g_1^s g_2^{\mathtt{id}} g_3^{\rho}, h_0\big) \tag{5.8}$$

where the scheme assumes $\mathtt{msk}$ as a secret key (instead of $\gamma \in_R \mathbb{Z}_p^*$), and the corresponding public key is $\mathtt{mpk} = h_0^{\mathtt{msk}}$.

I now ensure that the credentials are derived from the same origin (including multiple sources) by utilizing *SPK*, Proof of Knowledge of a Signature. I aim to allow provers owing an AESP to ask verifiers in public to verify their credentials without AESPs, but also strongly aim to eliminate linkability. If an attached signature σ is a fixed string as generated it was, it could be a cause of linkability. Therefore, I propose to make the best use of the BBS+ signature scheme based *SPK* of A_1 and A_2, which are randomly shifted like $A_1 = g_1^{r_1} g_2^{r_2}$ and $A_2 = A g_2^{r_1}$ as described in Section 3.2.2. Let us denote such a randomly shifted signature as $\widetilde{\sigma}$ with $\widetilde{\ }$ to represent (A_2, t, s), where $\sigma = (A, t, s)$ and $A_2 = A g_2^{r_1}$ explicitly, also as $\widetilde{\sigma}'$ if randomly shifted with r' if necessary.

In addition, I also utilize proofs of equality π_{eq} to confirm if the same witness, such as $\mathtt{id}$ and ρ, is shared in both the signature and gives uniformly randomized values, such as $\widehat{\mathtt{id}}$ and $\widehat{\rho}$. The idea behind is that a part of a BBS+ signature, A of (A, t, s), is expressed in Equation (5.7) includes discrete logarithms of the same group elements in both $\widehat{\mathtt{id}} = g^{\mathtt{id}} h^{r_{\mathtt{id}}}$ and $\widehat{\rho} = g^{\rho} h^{r_{\rho}}$ with a chosen random number, $r_{\mathtt{id}}$ and r_{ρ}, for each. In more concrete, $\pi_{SPK}(\sigma; \widetilde{\sigma}')$ can be expressed as follows:

$$\begin{aligned} SPK\Big\{(r_1, r_2, \delta_1, \delta_2, t, s, \mathtt{id}, \rho) : A_1 = g_1^{r_1} g_2^{r_2} \wedge A_1^t = g_1^{\delta_1} g_2^{\delta_2} \wedge \frac{e(A_2, w)}{\mathrm{e}(g_1, h_0)} = \\ \mathrm{e}(A_2, h_0)^{-t}\, \mathrm{e}(g_2, w)^{r_1}\, \mathrm{e}(g_2, h_0)^{\delta_1}\, \mathrm{e}(g_1, h_0)^{s}\, \mathrm{e}(g_2, h_0)^{\mathtt{id}}\, \mathrm{e}(g_3, h_0)^{\rho}\Big\}(M) \end{aligned} \tag{5.9}$$

where $\delta_1 = r_1 t$, $\delta_2 = r_2 t$, and $A_2 = g_2^{r_1} \left[g_0 g_1^s g_2^{\mathtt{id}} g_3^{\rho}\right]^{\frac{1}{t+\mathtt{msk}}}$ for the particular use case.

5.2.2 Utilizing Proofs of Logarithm Equality

Once the possession of the signature is verified, a technique of proofs of equality about discrete logarithms may bring a transcript to express if the same $\mathtt{id}$ and ρ are initially included in the randomly shifted signature. Let us denote them as follows:

$$\pi_{eq}(\mathtt{id}; \widehat{\mathtt{id}} \in \widetilde{\sigma}) \stackrel{\text{def}}{=} PK\{(\mathtt{id}, r_{\mathtt{id}}) : \widehat{\mathtt{id}} = g_2^{\mathtt{id}} h^{r_{\mathtt{id}}} \wedge C_{\mathtt{id}} = \mathrm{e}(g_2, h_0)^{\mathtt{id}}\} \tag{5.10}$$

$$\pi_{eq}(\rho; \widehat{\rho} \in \widetilde{\sigma}) \stackrel{\text{def}}{=} PK\{(\rho, r_\rho) : \widehat{\rho} = g_3^{\rho} h^{r_\rho} \wedge C_\rho = \mathrm{e}(g_3, h_0)^{\rho}\} \tag{5.11}$$

where

$$C_{\mathtt{id}} = \mathrm{e}(A_2, w)\mathrm{e}(g_1, h_0)^{-1}\,\mathrm{e}(A_2, h_0)^{t}\,\mathrm{e}(g_2, w)^{-r_1}\,\mathrm{e}(g_2, h_0)^{-\delta_1}\,\mathrm{e}(g_1, h_0)^{-s}\,\mathrm{e}(g_3, h_0)^{-\rho}, \text{ and}$$
$$C_\rho = \mathrm{e}(A_2, w)\mathrm{e}(g_1, h_0)^{-1}\,\mathrm{e}(A_2, h_0)^{t}\,\mathrm{e}(g_2, w)^{-r_1}\,\mathrm{e}(g_2, h_0)^{-\delta_1}\,\mathrm{e}(g_1, h_0)^{-s}\,\mathrm{e}(g_2, h_0)^{-\mathtt{id}},$$

respectively. Note that those constants $C_{\mathtt{id}}$ and C_ρ are retrieved from Equation (5.9), and all other witnesses, r_1, δ_1, t, s, and ρ or $\mathtt{id}$ for each, have to be proven separately.

In summary, the novel scheme of using selective disclosure, *SPK*, and proofs of equality about discrete logarithms, along with adopting "One-Out-of-Many Proofs," enables a credential system to treat created derived credentials anonymously.

5.3 Constructions

I aim to construct a set of system protocols $\Pi^{\mathcal{G}_{\mathtt{att}}+}$ that is extended from $\mathcal{G}_{\mathtt{att}}$to support *anonymous Sybil-resistant verifiable credentials* consisting of *perfectly anonymous identifiers* and *computed claims in Boolean* with other techniques as described in the previous sections.

Here, let me describe a detailed construction: Figure 5.4, 5.5, 5.6, and 5.7 illustrate the set of protocols $\Pi^{\mathcal{G}_{\mathtt{att}}+}$ in detail. Figure 5.4, 5.5, and 5.6 illustrate the protocols that work with AESPs, while Figure 5.7 illustrates the protocol for verifiers in public. It means the protocol for verification does not require AESPs for various opportunities.

Once a user (holder) has a chance to create an anonymous Sybil-resistant credential, they utilize their own AESP to use IssueCred() derived from $\Pi^{\mathcal{G}_{\mathtt{att}}}$ and followed by IssueASDCred() newly defined for $\Pi^{\mathcal{G}_{\mathtt{att}}+}$, which

i. computes a predicate as a computed claim in Boolean $\rho : \{0, 1\}$ from multiple issuers,

ii. ensures if it is Sybil-resistant while forming it as a derived verifiable credential, namely an anonymous Sybil-resistant verifiable credential,

iii. produces an $\mathtt{id}$ and creates an anonymous identifier $g^{\mathtt{id}}h^{r}$ with a random value r, and

iv. adds an attested signature in the BBS+ signature form.

Regarding step-2 (ii.) in the above, it is critical if a set of Sybil-resistant derived credentials and associated anonymous credentials satisfy the Sybil-resistant *identification mapper* ψ and *identifier anonymizer* θ while those credentials are maintained. To secure this, as described in Section 5.1.3 with **Definition 5.5**, the protocol determines a procedure that such a credential can be created **only the first time** a natural person requests to associate their identity with a service by $\mathtt{prog} : (\widehat{\psi}, \widehat{\theta})$ in Figure 5.4. It enables the maintenance of the set ***distinct***; thus, the one-out-of-many proofs Σ-protocol works accordingly. The user (holder) may keep the $\mathtt{id}$ without disclosing it to anyone. During the above process, the anonymous Sybil-resistant verifiable credential is registered in the $\mathcal{Z}$ pool under a permissionless blockchain.

5.3.1 Public Verification without AESPs

$\Pi^{\mathcal{G}_{\mathtt{att}}+}$ defines another function, $\mathsf{VerifyASDCred}()$ in addition, which allows a prover to ask a verifier to verify such an anonymous Sybil-resistant verifiable credential without an AESP (Figure 5.7). To achieve this, the user (holder) may now pass a created anonymous Sybil-resistant verifiable credential to a verifier; however, they need to

v. create another anonymous identifier with a different random value r', the new $\widehat{\mathtt{id}}' = g^{\mathtt{id}}h^{r'}$ for passing the credential to a verifier.

Since the newly created identifier $\widehat{\mathtt{id}}' = g^{\mathtt{id}}h^{r'}$ is also uniformly random, it is perfect hiding. The verifier requires access to the permissionless blockchain with the one-out-of-many proofs Σ-protocol to determine if the expected credential exists in the $\mathcal{Z}$ pool. Once the existence is confirmed, the verifier can verify the credential with the predicate

Anonymous Sybil-Resistant SSI with an AESP – $\Pi^{\mathcal{G}_{\mathtt{att}}+}$: Issuance

$\Pi^{\mathcal{G}_{\mathtt{att}}+}$ anonymous and secure SSI-featured function (issuance) :

- $\mathsf{IssueASDCred}(\mathtt{msk}, \mathtt{sk}_U, \mathtt{pk}_U, \mathtt{prog}\colon (\widehat{\psi}, \widehat{\theta}), \mathtt{cred}_{k=1,\ldots,\ell}, \tau)$
  $\rightarrow \mathtt{anonymousDCred} : \{\widehat{\mathtt{id}}, \widehat{\rho}, \rho, \widetilde{\sigma}\}$

  This function, $\mathsf{IssueASDCred}()$, utilizes $\mathcal{G}_{\mathtt{att}}$ to install and execute a specified program $\mathtt{prog}$, which must be capable for Sybil-resistant *identification mapper* ψ and also *identifier anonymizer* θ, using IND-CCA encryption algorithm $\mathcal{E}$ for both. To install and execute $\mathtt{prog}$,

  1: $\mathcal{G}_{\mathtt{att}}.\mathsf{Install}(\mathtt{prog}) \rightarrow eid$;
  2: $\mathcal{G}_{\mathtt{att}}.\mathsf{Resume}(eid, \mathtt{inp}) \rightarrow (\mathtt{outp}, \widetilde{\sigma})$;

  At the end, $\mathcal{G}_{\mathtt{att}}$ requires EUF-CMA (Existential Unforgeability under Chosen Message Attack) signature scheme Σ for generating a signature, and the BBS+ signature scheme.

  3: Receives a block of messages $(\mathtt{id}, \rho)$, uses $\mathtt{msk}$ as a secret key and the corresponding public key is $\mathtt{mpk}$, chooses e, a random number s, and computes

  $$A = \left[g_0 g_1^s g_2^{\mathtt{id}} g_3^{\rho}\right]^{\frac{1}{t+\mathtt{msk}}}; \tag{5.12}$$

  thus, (A, t, s) is a signature on the block of messages[a]. To eliminate linkability, $\Pi^{\mathcal{G}_{\mathtt{att}}+}$ randomly shifts the value of the signature through computing A_2 of (A, t, s) to represent $\widetilde{\sigma}$.

  4: Stores the created anonymous Sybil-resistant credential of $\widehat{\mathtt{id}}, \widehat{\rho}$, and the signature $\widetilde{\sigma}$ in the $\mathcal{Z}$ pool in a permissionless blockchain.

[a] As described in Equation (5.12), the platform accesses $\mathtt{msk}$ that is basically stored and securely managed within an AESP, namely $\mathcal{G}_{\mathtt{att}}$. Therefore, it is preferable to define the extension of $\mathcal{G}_{\mathtt{att}}$ ideally; however, let me omit a detailed description because it is very straightforward.

Figure 5.4: Construction of Anonymous Secure SSI – $\Pi^{\mathcal{G}_{\mathtt{att}}+}$: Issuance

Construction of prog for Anonymous Sybil-Resistant SSI with an AESP – $\Pi^{\mathcal{G}_{\mathtt{att}}+}$

$\mathtt{prog}$: $(\widehat{\psi}, \widehat{\theta})$ for creating anonymous Sybil-resistant credentials :

1: Retrieves inputs ($\mathtt{inp}$), keys, $\mathtt{cred}_{k=1,\ldots,n}$ and τ;

2: Ensures if the specified $\mathtt{prog}$ creates the expected derived credential for a natural person $(\mathtt{sk}_U, \mathtt{pk}_U)$ at the first time with $\widehat{\psi}$, then may keep Sybil-resistant; otherwise, error. *Note that this process enables the $\mathcal{Z}$ pool* a distinct set *of credentials for Sybil-resistance.*

3: Generates a predicate $\rho(\{0,1\}^*) = \{0,1\}$ in Boolean through computing $\mathtt{claim}_{j=1,\ldots,m}$;

4: Produces $\mathtt{id}$ from $\mathtt{pk}_U$. With $\widehat{\theta}$, chooses a random number r and creates an anonymous identifier $\widehat{\mathtt{id}} = g^{\mathtt{id}} h^r$;

5: Creates $\widehat{\rho}$ in the same fashion;

6: Generates outputs ($\mathtt{outp}$) as a set of those above, $(\widehat{\mathtt{id}}, \widehat{\rho}, \rho)$; and lastly,

7: Makes a block of messages $(\mathtt{id}, \rho)$ just for $\mathcal{G}_{\mathtt{att}}$ to create a BBS+ signature, shifts it randomly, and passes it as $\widetilde{\sigma}$ to them.

Figure 5.5: Construction of $\mathtt{prog}$ for Anonymous Secure SSI – $\Pi^{\mathcal{G}_{\mathtt{att}}+}$

Anonymous Sybil-Resistant SSI with an AESP – $\Pi^{\mathcal{G}_{\mathtt{att}}+}$: Verification

$\Pi^{\mathcal{G}_{\mathtt{att}}+}$ anonymous and secure SSI-featured function (verification) :

- $\mathsf{VerifyASDCred}(\mathtt{msk}, \mathtt{sk}_U, \mathtt{anonymousDCred}) \rightarrow \{\mathtt{true}, \mathtt{false}\}$

  This function, $\mathsf{VerifyASDCred}()$, utilizes $\widehat{\theta}$,

  1: Chooses a random number r' and creates another anonymous identifier $\widehat{\mathtt{id}}' = g^{\mathtt{id}} h^{r'}$; and creates $\widehat{\rho}'$ in the same fashion;

  2: Sends the anonymous Sybil-resistant credential of $\widehat{\mathtt{id}}', \widehat{\rho}', \rho$, and the signature (A, t, s) to a verifier.

Figure 5.6: Construction of Anonymous Secure SSI – $\Pi^{\mathcal{G}_{\mathtt{att}}+}$: Verification

Construction for Public Verification for $\Pi^{\mathcal{G}_{\text{att}}+}$

Verifiers in public proceeds the following construction for verification :

1: Retrieves a message of $\widehat{\texttt{id}}', \widehat{\rho}', \rho$ and the randomly shifted signature $\widetilde{\sigma}'$ as an anonymous Sybil-resistant verifiable credential `anonCred` from the prover;

2: Calls the one-out-of-many proofs Σ-protocol with the input $\widehat{\texttt{id}}'$ to check if there exists the expected credential in the $\mathcal{Z}$ pool;

> *Note: If exists, it means that only the credential associated with the prover exists, and the verifier must receive a valid anonymous Sybil-resistant verifiable credential.*

3: Verifies $\pi_{SPK}(\sigma, \widetilde{\sigma}')$ to ensure if the passed `anonCred` is signed as expected.

4: Verifies $\pi_{eq}(\texttt{id}; \widehat{\texttt{id}}' \in \widetilde{\sigma}')$ and $\pi_{eq}(\rho; \widehat{\rho}' \in \widetilde{\sigma}')$, and goes to the final step if true; otherwise, error.

5: Checks ρ in Boolean once the verifier may accept the prover's verifiable credential, if it is privileged or not.

Figure 5.7: Construction for $\Pi^{\mathcal{G}_{\text{att}}+}$ – Public Verification

in Boolean. Figure 5.7 illustrates the protocol for a verifier to verify an anonymous Sybil-resistant verifiable credential without an AESP.

5.4 Security Analysis and Proofs

The set of system protocols $\Pi^{\mathcal{G}_{\text{att}}+}$, implementing the proposed novel scheme, is extended from $\Pi^{\mathcal{G}_{\text{att}}}$ that realizes the set of secure SSI system protocols Π (**Definition 4.2**) and satisfies the security properties, including *Existence* meeting with the Sybil-resistance requirement (**Definition 4.4**). $\Pi^{\mathcal{G}_{\text{att}}+}$ must satisfy the same security properties, and we need to revisit if they are affected by the anonymous setting:

- *Existence* is obvious that I will need to revisit how it is affected and if it is satisfied by the anonymous setting.
- *Unforgeability* is not affected because users (holders) still own their AESPs, and settings are unchanged.

- *Unlinkability across programs* is not affected because the scheme creates derived credentials still within their AESPs, and the environment for programs is unchanged.

- *Privacy – credential-issuance and verification* is critical because created credentials are stored in $\mathcal{Z}$ pools. I will need to investigate *Unlinkability among derived credentials* and if these security properties are satisfied.

5.4.1 Existence

Lemma 5.1 (Existence)**.** *Suppose $\mathcal{C}$ be a set of all Sybil-resistant credentials, $\mathcal{D}_\ell$ be a set of derived credentials for a service numbered ℓ, and $\mathcal{Z}_\ell$ be a set of* anonymous *derived credentials for the same service numbered ℓ. For any stateful PPT adversary $\mathcal{A}$, the construction* $\mathsf{IssueASDCred}()$ *yields an element-wise relation that preserves the bijective map $\theta_\ell : \mathtt{cred} \mapsto \mathtt{anonCred}$ and an injective map $\zeta_\ell(\mathtt{anonCred}) \in \mathcal{C}$. Hence, $\psi_\ell = \theta_\ell \circ \zeta_\ell$; namely, the construction satisfies* **Definition 4.4** (Existence) *in the anonymous setting. That is equivalently redefined from the original setting in order to introduce $\mathcal{Z}_\ell$ as the anonymity set for the service numbered ℓ as follows:*

$$\Pr\left[\begin{array}{l|c} & \mathtt{mpk}, \mathtt{msk} \leftarrow \mathsf{KeyGen}(1^\lambda); \\ & \mathtt{cred}, \mathtt{pk}_U, \mathtt{sk}_U \leftarrow \mathcal{A}^{\mathcal{O}^*, \mathcal{O}^*_{\mathrm{ext}}}(\mathtt{mpk}); \\ & \text{assert } \Sigma.\mathsf{Ver}_{\mathtt{mpk}}(\mathtt{cred.body}, \mathtt{cred}.\sigma_M) = \mathtt{true}; \\ \exists \mathtt{anonCred}' \in \mathcal{Z}_\ell \ \textit{s.t.} & \mathtt{anonCred} \leftarrow \mathsf{IssueASDCred}(\mathtt{msk}, \mathtt{sk}_U, \mathtt{pk}_U, \mathtt{cred}) \\ \theta_\ell(\mathtt{cred}) = \mathtt{anonCred}' & \textit{s.t. } \mathtt{anonCred} \in \mathcal{Z}_\ell \textit{ and } \zeta_\ell(\mathtt{anonCred}) \in \mathcal{C}; \\ \wedge\, \zeta_\ell(\mathtt{anonCred}') \in \mathcal{C} & \pi_{OOoM}(\widehat{\mathtt{id}}^\circ \in \mathcal{Z}_\ell), \pi_{SPK}(\sigma; \widetilde{\sigma}^\circ), \\ & \qquad \pi_{eq}(\mathtt{id}; \widehat{\mathtt{id}}^\circ \in \widetilde{\sigma}^\circ) \leftarrow \mathcal{A}^{\mathcal{O}^*}(\mathtt{cred}); \\ & \pi_{OOoM}(\widehat{\mathtt{id}}^\circ \in \mathcal{Z}_\ell), \pi_{SPK}(\sigma; \widetilde{\sigma}^\circ), \textit{ and} \\ & \quad \pi_{eq}(\mathtt{id}; \widehat{\mathtt{id}}^\circ \in \widetilde{\sigma}^\circ) \textit{ are accepting transcripts.} \end{array}\right] \geq 1 - \mathrm{negl}(\lambda) \tag{5.13}$$

where $\widehat{\mathtt{id}}^\circ$ and $\widetilde{\sigma}^\circ$ are elements of $\mathtt{anonCred}^\circ$, and the probability is taken over the randomness of the probabilistic algorithms, $\mathsf{KeyGen}()$ *and* $\mathsf{IssueASDCred}()$.

$\mathtt{anonCred}'$ and $\mathtt{anonCred}^\circ$ in Equation (5.13) in the above statement could be identical if the adversary $\mathcal{A}$ may hit $\mathtt{anonCred}'$. Still, they should formally be different because the probability of the equation is not perfect.

The verification algorithm $\Sigma.\mathsf{Ver}_{\mathtt{mpk}}$ in Equation (5.13) is the same as Equation (4.7)

in **Definition 4.4**, while the objective of $\mathcal{V}_{\mathtt{mpk}}$ in **Definition 4.4** is represented by consisting of Equation (4.7) and three verification algorithms of Proof of Knowledge (PoK) transcripts: $\pi_{OOoM}(\widehat{\mathtt{id}}^{\circ} \in \mathcal{Z}_\ell)$, $\pi_{SPK}(\sigma; \widetilde{\sigma}^{\circ})$, and $\pi_{eq}(\mathtt{id}; \widehat{\mathtt{id}}^{\circ} \in \widetilde{\sigma}^{\circ})$ from the perspective of verifying authenticity of credentials produced by $\mathcal{A}$ in Equation (5.13). Note that verification of $\pi_{SPK}(\sigma; \widetilde{\sigma}^{\circ})$ requires $\mathtt{mpk}$ (See Equation (5.9)).

Proof. The lemma states that the verifier is convinced that the derived credential $\mathtt{cred} \in \mathcal{D}_\ell$ has an injective map into the set $\mathcal{C}$, namely $\mathtt{cred}$ is also a Sybil-resistant credential with with overwhelming probability no less than $1 - \mathrm{negl}(\lambda)$ when the verifier accepts the thee transcripts: $\pi_{OOoM}(\widehat{\mathtt{id}}^{\circ} \in \mathcal{Z}_\ell)$, $\pi_{SPK}(\sigma; \widetilde{\sigma}^{\circ})$, and $\pi_{eq}(\mathtt{id}; \widehat{\mathtt{id}}^{\circ} \in \widetilde{\sigma}^{\circ})$. Equivalently, let us restate Equation (5.13)[1] as follows:

$$\Pr\left[\begin{array}{c|c} \begin{array}{c} \pi_{OOoM}(\widehat{\mathtt{id}}^{\circ} \in \mathcal{Z}_\ell), \\ \pi_{SPK}(\sigma; \widetilde{\sigma}^{\circ}), \textit{ and} \\ \pi_{eq}(\mathtt{id}; \widehat{\mathtt{id}}^{\circ} \in \widetilde{\sigma}^{\circ}) \\ \textit{are accepting transcripts.} \end{array} & \begin{array}{c} \mathtt{mpk}, \mathtt{msk} \leftarrow \mathsf{KeyGen}(1^\lambda); \\ \mathtt{cred}, \mathtt{pk}_U, \mathtt{sk}_U \leftarrow \mathcal{A}^{\mathcal{O}^*, \mathcal{O}^*_{\mathrm{ext}}}(\mathtt{mpk}); \\ \text{assert } \Sigma.\mathsf{Ver}_{\mathtt{mpk}}(\mathtt{cred.body}, \mathtt{cred}.\sigma_M) = \mathtt{true}; \\ \mathtt{anonCred} \leftarrow \mathsf{IssueASDCred}(\mathtt{msk}, \mathtt{sk}_U, \mathtt{pk}_U, \mathtt{cred}) \\ \textit{s.t. } \mathtt{anonCred} \in \mathcal{Z}_\ell \text{ and } \zeta_\ell(\mathtt{anonCred}) \in \mathcal{C}; \\ \pi_{OOoM}(\widehat{\mathtt{id}}^{\circ} \in \mathcal{Z}_\ell), \pi_{SPK}(\sigma; \widetilde{\sigma}^{\circ}), \\ \pi_{eq}(\mathtt{id}; \widehat{\mathtt{id}}^{\circ} \in \widetilde{\sigma}^{\circ}) \leftarrow \mathcal{A}^{\mathcal{O}^*}(\mathtt{cred}); \\ \theta_\ell(\mathtt{cred}) \neq \mathtt{anonCred}' \vee \zeta_\ell(\mathtt{anonCred}') \notin \mathcal{C} \\ \textit{for all } \mathtt{anonCred}' \in \mathcal{Z}_\ell \end{array} \end{array}\right] < \mathrm{negl}(\lambda). \tag{5.14}$$

We prove Equation (5.14) by contradiction. Assume that the equation (5.14) holds with non-negligible probability, and this can be divided into the following two cases for all $\mathtt{anonCred}' \in \mathcal{Z}_\ell$ from the last line of the condition part,

Case 1.) $\theta_\ell(\mathtt{cred}) \neq \mathtt{anonCred}'$, and/or

Case 2.) $\zeta_\ell(\mathtt{anonCred}') \notin \mathcal{C}$,

then all three transcripts are accepted with non-negligible provability. We carefully investigate each case as follows:

Case 1.) $\theta_\ell(\mathtt{cred}) \neq \mathtt{anonCred}'$ This must be the case where a program capable of θ_ℓ or the corresponding AESP that executes the program capable of θ_ℓ is corrupted

[1]Based on the asymptotic argument regarding contrapositive probability. Given $\Pr(X \mid Y) > 1 - \mathrm{negl}(\lambda)$, we have $\Pr(Y \mid \overline{X}) < \mathrm{negl}(\lambda)$. As it is easy to see that $\Pr(\overline{X} \mid Y) = 1 - \Pr(X \mid Y) < \mathrm{negl}(\lambda)$, and from $\Pr(\overline{X} \mid Y) = \Pr(\overline{X}, Y)/\Pr(Y)$, it follows that $\Pr(\overline{X}, Y) < \mathrm{negl}(\lambda)$. Hence, $\Pr(Y \mid \overline{X}) < \mathrm{negl}(\lambda)$.

because `cred` is verified and asserted in Equation (5.14). We assume tamper-resistance to all AESPs[2] and also that any programs `prog` are correct as they are open source for anyone to verify as described in Section 4.1.2. Thus, these lead to a contradiction.

Case 2.) $\zeta_\ell(\texttt{anonCred}') \notin \mathcal{C}$ This must be the case where $\mathcal{A}$ produces all three accepting proof transcripts, $\pi_{OOoM}(\widehat{\texttt{id}}^\circ \in \mathcal{Z}_\ell)$, $\pi_{SPK}(\sigma; \widetilde{\sigma}^\circ)$, and $\pi_{eq}(\texttt{id}; \widehat{\texttt{id}}^\circ \in \widetilde{\sigma}^\circ)$, nevertheless $\zeta_\ell(\texttt{anonCred}') \notin \mathcal{C}$ *for all* $\texttt{anonCred}' \in \mathcal{Z}_\ell$. Whenever any AESPs register an `anonCred` to $\mathcal{Z}_\ell$, all honest AESPs are defined to maintain the injective relation from any $\texttt{anonCred} \in \mathcal{Z}_\ell$ to the corresponding master Sybil-resistant credential $\texttt{c} \in \mathcal{C}$, and neither

1. $^\exists\texttt{anonCred} \in \mathcal{Z}_\ell \wedge \zeta_\ell(\texttt{anonCred}) \notin \mathcal{C}$ (identity creation in $\mathcal{Z}_\ell$) , nor
2. $^\exists\texttt{anonCred} \neq \texttt{anonCred}' \in \mathcal{Z}_\ell \wedge \zeta_\ell(\texttt{anonCred}) = \zeta_\ell(\texttt{anonCred}') \in \mathcal{C}$ (duplicated identity in $\mathcal{Z}_\ell$)

can happen as long as all AESPs work accordingly. Therefore, in **Case 2.)**, at least one of AESPs must be corrupted, and the corrupted AESP registered an `anonCred` which bears a valid signature of the corrupted AESP in such a way that the resulted `anonCred` has no corresponding Sybil-resistant credential in $\mathcal{C}$, or the resulted `anonCred` in $\mathcal{Z}_\ell$ has overlapped correspondence to a single Sybil-resistant credential in $\mathcal{C}$ under the assumptions of tamper-resistance to all AESPs and the correctness of `prog`. Otherwise, $\mathcal{A}$ must break the soundness of $\pi_{OOoM}(\widehat{\texttt{id}}^\circ \in \mathcal{Z}_\ell)$, $\pi_{SPK}(\sigma; \widetilde{\sigma}^\circ)$, or $\pi_{eq}(\texttt{id}; \widehat{\texttt{id}}^\circ \in \widetilde{\sigma}^\circ)$. The soundness of $\pi_{OOoM}(\widehat{\texttt{id}}^\circ \in \mathcal{Z}_\ell)$ is negligible in λ (See **Definition 3.4** (n-Special soundness) and **Theorem 3.1** (Theorem 3 of Groth and Kohlweiss [GK15])), and the soundness of $\pi_{SPK}(\sigma; \widetilde{\sigma}^\circ)$ and $\pi_{eq}(\texttt{id}; \widehat{\texttt{id}}^\circ \in \widetilde{\sigma}^\circ)$ is also negligible in λ (See *Theorem 2* of Au, Susilo, and Mu in [ASM06]). Thus, these lead to a contradiction. □

5.4.2 Unlinkability

We retain **Definition 4.8** (Unlinkability across programs) as described. Instead, we need to revisit **Definition 4.6** and **4.7** for *Privacy – credential-issuance and verification*. Derived credentials are treated differently for public verification in the anonymous

[2]Possible mitigation to the compromise of AESPs is discussed later in Section 6.2.1.

setting; thus, the security properties need to address *Unlinkability* among derived credentials, *anonymous credentials*, in this case.

Lemma 5.2 (Unlinkability among *anonymous* credentials)**.** *Given the identifier anonymizer* $\theta_\ell : \mathcal{D}_\ell \to \mathcal{Z}_\ell$*, generated anonymous credentials with perfectly anonymous identifiers are uniformly randomized and indistinguishable if, for any stateful PPT adversary* $\mathcal{A}$*,*

$$\left| \Pr \left[b = b' \;\middle|\; \begin{array}{c} \mathtt{mpk}, \mathtt{msk} \leftarrow \mathsf{KeyGen}(1^\lambda); \\ \mathtt{cred}^0, \mathtt{cred}^1, \mathtt{pk}_U, \mathtt{sk}_U \leftarrow \mathcal{A}^{\mathcal{O}^*, \mathcal{O}^*_{\mathrm{ext}}}(\mathtt{mpk}); \\ \mathtt{anonCred}^b \leftarrow \mathsf{IssueASDCred}(\mathtt{msk}, \mathtt{sk}_U, \mathtt{pk}_U, \mathtt{cred}^b) \\ \textit{for } b = 0,1;\ b \leftarrow \$\{0,1\}; \\ b' \leftarrow \mathcal{A}^{\mathcal{O}^*, \mathcal{O}^*_{\mathrm{ext}}}(\mathtt{anonCred}^b) \end{array} \right] - \frac{1}{2} \right| \leq \mathrm{negl}(\lambda) \tag{5.15}$$

where IssueASDCred()*, illustrated in* Figure 5.4*, generates a commitment-based anonymous identifier* $\widehat{\mathtt{id}}^b = g^{\mathtt{id}^b} h^{r^b}$ *and assigns it to* $\mathtt{anonCred}^b$*. The construction in the anonymous setting satisfies* **Definition 4.6** *and* **4.7** (Privacy – credential-issuance and verification) *simultaneously.*

Proof of Lemma 5.2. Created credentials, $\mathtt{cred}^0$ and $\mathtt{cred}^1$, are supposed to be different, and both are passed to the function IssueASDCred() that creates an anonymous Sybil-resistant derived credential, which refers $b \leftarrow \$\{0,1\}$. The created $\mathtt{anonCred}^b$ consists of $\widehat{\mathtt{id}}^b$, which is uniformly randomized by a random value r^b when the function issues the anonymous Sybil-resistant derived credential. The witnesses ($\mathtt{id}^b$ and $\mathtt{id}^{b'}$ in this case) are indistinguishable in the proposed scheme as described by **Definition 3.6** (Witness-indistinguishability) in Section 3.3; therefore, the adversary cannot guess the value of b (or b'), and the probability $-\frac{1}{2}$ is negligible. □

Note that the game plan above is identical to that of **Definition 4.6** (Credential issuance privacy), and it results in that the extended construction satisfies *Credential issuance privacy.* Also, we may confirm that **Definition 4.7** (Credential verification privacy) is not affected by the anonymous setting. The proposed scheme maintains unlinkability among derived credentials for multiple verifiers because of the witness-indistinguishability described above, and also, no verifier can guess a chosen uniform randomness $r \in \mathbb{Z}_q$ each other, and the generated $\widehat{\mathtt{id}} = g^{\mathtt{id}} h^r$ is also uniformly random across verifiers.

It has been challenging to eliminate linkability among credentials as long as a pseudonym is used as the identifier. We may build a secure, anonymous, and Sybil-resistant SSI system that supports unlinkability among derived credentials designed for public verification by hiding credentials by introducing *perfectly anonymous identifiers* incorporating Pedersen commitments and utilizing zero-knowledge membership proofs as well as other techniques.

5.4.3 The Main Theorem

From **Lemma 5.1** and **5.2**, we can state the following theorem:

Theorem 5.1 (The AESP-based *anonymous* and Sybil-resistant SSI system protocols)**.** *Assuming that all provers of natural persons own their mobile devices equipped with an AESP and its ideal functionality* $\mathcal{G}_{\mathtt{att}}$ *and standard computational assumptions, there exists a set of system protocols* $\Pi^{\mathcal{G}_{\mathtt{att}}+}$ *extended from* $\Pi^{\mathcal{G}_{\mathtt{att}}}$ *to realize an anonymous and Sybil-resistant SSI system.*

I have been aiming to achieve *perfect anonymity* in building secure Sybil-resistant SSI systems. For this, what I have achieved with the protocol $\Pi^{\mathcal{G}_{\mathtt{att}}+}$ is to support unlinkability among credentials with *perfectly anonymous identifiers*. Also, a predicate, *computed claims in Boolean* form, brings anonymity for managing credentials over a permissionless blockchain. It is a binary and uniformly randomized, the same as perfectly anonymous identifiers; thus, it is indistinguishable.

One of the most notable points of our scheme is the proposal of Pedersen commitment-based, *perfectly anonymous identifiers*, with the one-out-of-many proofs Σ-protocol to prove the existence of the expected credential that meets the Sybil-resistance requirement. The zero-knowledge membership proof allows verification of the existence of at least one commitment opening to a specific value; therefore, it is still comparatively infeasible to determine the exact one. The Sybil-resistance requirement, however, ensures that the commitment opening to the particular value exists just one in the $\mathcal{Z}$ pool, efficiently in logarithmic order simultaneously. Let me emphasize that the anonymous identifier of the commitment opening to `id` as a witness uniquely exists because the $\mathcal{Z}$ pool is a distinct set of credentials.

5.5 Performance Consideration

At the end of this chapter, let us consider the performance perspective. Computation and communication costs must be considered, and for the latter, issuance and verification should be addressed.

5.5.1 Computation Cost

First, I want to consider computation power and cost. Computational power is increasing dramatically, even in mobile devices such as smartphones. Main processors equipped with recent smartphones are almost 3GHz for the "big" part of quad or octa cores in the big-little architecture[3]; over 2GHz processors are equipped as the "little" part of the cores within the same system-on-chip (SoC).

Hardware-assisted security is implemented within such smartphones in various ways; for instance, trusted execution environment (TEE) is built by utilizing a part of the main processors, while Global Platform-supported Secure Elements (GP-SE) is implemented as a separate chip to deal with tamper resistance. A certain GP-SE chip implements a 48MHz processor today. This is not faster than smartphones' main processors, but it works in the market for key generation and/or signing/verification processes for various applications.

In such circumstances, the computation cost in each operation proposed in this thesis can be treated as trivial for whatever issuance or verification.

5.5.2 Communication Cost

Second, let us address the communication cost. This should be considered more than the computation cost. According to various sources, the global population is now estimated at over 8 billion. Population in some countries has become over 1.4 billion; therefore, I should consider at least a few billion natural persons in the set of real identities $\mathcal{I}$ that may work as an authority, ideally 8 billion.

[3]Arm offers big.LITTLE architecture since 2012, the big processors are designed for performance, and the LITTLE part is designed for power consumption, and the total performance can be well-tuned by the combination. See `https://www.arm.com/ja/technologies/big-little`.

Table 5.1: Performance Consideration – Order of Communication Cost

Issuance	Verification
$O(\lambda N)$	$O(\lambda(\log N))$

For issuing a Sybil-resistant derived credential and an anonymous Sybil-resistant derived credential, an AESP must ensure managing the injective map by the *identification mapper* ψ, which requires only the first time to associate a credential and the real identity for Sybil-resistance. Therefore, the AESP must communicate with a server maximally N order. It is a huge number, but a one-time event.

For verification, it may affect more than the issuance because created derived credentials could be used more often than just the one-time event, issuance. Thanks to the efforts by Jens Groth and Markulf Kohlweiss, the zero-knowledge membership proofs, "One-Out-of-Many Proofs" Σ-protocol allows us to verify the existence of commitments opening to an expected value within logarithmic communication complexity, namely in logarithmic order as described in Table 5.1, where let us denote N be the number of users to estimate asymptotic communication cost and λ be a security parameter.

As a result of performance consideration, the order can be described as

$$\text{Computation cost} \ll \text{Verification (Communication)} < \text{Issuance (Communication)}.$$

Note that Christina Garman *et al.* proposed a decentralized anonymous credentials scheme utilizing Pedersen commitments and accumulators with a distributed public append-only ledger, and also addressed the Sybil-resistance requirement [GGM14], as described in Section 2.3.2. Their approach is sophisticated from a mathematical perspective; however, it has performance limitations [Ros+23]. Other research, such as [Cri+24, Rab+24], measured computation and communication time for each method while they have not addressed performance trends in the global population on the planet.

Chapter 6

Applications, Limitations, and Future Directions

6.1 Applications

The proposals in this thesis have many opportunities and applications in the real world because of the rapid increase of smartphones and other mobile devices equipped with a tamper-resistant secure processor in the market.

In this thesis, permissionless blockchains play the role of self-sovereign identity (SSI) systems as a foundation. Like previous research and implementations, it works for verifiable data registries. In addition, combining a permissionless blockchain and AESPs may extend the usage. For instance, secure programs for creating derived credentials by IssueDCred(), which allows for a user to choose a program `prog` depending on different context `ctx`, can and should probably be registered and maintained on the permissionless blockchain. Also, derived credentials created by the user's device with an AESP may represent the person on permissionless blockchain ecosystems, preserving privacy. Because of the recent rapid growth of blockchain-based business ecosystems, opportunities to utilize the overall architecture in this thesis to combine a permissionless blockchain and AESPs are unlimited.

6.1.1 Metaverse

There is an industrial moment of building services over an infrastructure combining physical and virtual on the Internet or the web, utilizing various devices such as head-mounted displays. From users' perspectives, anonymity and privacy preservation are essential requirements in such services. Simultaneously, such services may require payment or wiring from one to the other, and compliance with AML is a critical element.

Let us assume that we build and provide a metaverse service focusing on a flea market under a permissionless blockchain to openly invite people from all over the world. Users would like to retain their privacy and may utilize their mobile devices equipped with an AESP. Users must have a Sybil-resistant service account to subscribe to and use the service to avoid fraud and unexpected wiring of money to others, complying with AML-related requirements. The AESP and the proposed scheme in this thesis will be able to resolve the problem of dealing with the conflicting requirements of AML and preserving privacy.

Qiuyun Lyu *et al.* recently addressed the need for Sybil-resistance in SSI for the metaverse [Lyu+23]. Metaverse services are appropriate applications of the proposals in this study, and they may apply accordingly.

6.1.2 Vaccination Pass

The COVID-19 pandemic has had a profound impact on the world. The pandemic led us to take action for rapid testing and vaccination under various guidance, but people must consider privacy concerns. The concerns are not about things only in the physical environment but also online for tracking coronavirus spread and others.

Users would like to maintain their privacy and may utilize their mobile devices equipped with an AESP in this scenario. Mauricio Barros *et al.* addressed SSI, blockchain technology, and zero-knowledge proof for building a privacy-preserving vaccination pass [BSC22]. They implemented a prototype, but their credentials are linkable because of pseudonymous identifiers. There must be opportunities for the proposals described in this thesis, and they may apply accordingly in this domain.

6.1.3 Digital Identity Wallets and Related Initiatives

Recently, there have been ongoing initiatives regarding digital identity wallets in the tech industry. The European Commission proposed the European Digital Identity Wallet (EUDIW) through the European Digital Identity Framework discussion[1]. Another well-known initiative is mDL, a mobile driver's license[2], as a special case of an "mdoc" app [ISO21a, ISO23a].

It must be helpful, but people would not always be happy to show their driver's license or personal identification on their mobile device, even though it allows them to show only requested claims such as name and age. In addition, there are other initiatives regarding SSI and digital identity wallets, such as the Cardano Foundation[3]. Many of those initiatives refer to similar or almost the same architecture utilizing verifiable credentials of issuers, users (holders), and verifiers.

Service providers for digital identity wallets must deal with AML. The ideas proposed in this study are beneficial because of the importance of resolving conflicting requirements. The AESP-based SSI architecture and protocols will enable digital identity wallet service providers to create programs that meet their requirements.

6.1.4 My Number Individual Card and JPKI

As an invited consultant, I am involved in the Japanese government's initiative to enable JPKI and other My Number Individual Card capabilities on smartphones. This initiative utilizes GP-SE to achieve the goal of duplicating and protecting a digital certificate with key pairs in a secure manner[4].

To realize the goal of duplicating digital certificates with key pairs, the initiative utilizes Global Platform-supported Secure Elements (GP-SE). The goals of the initiative and the ideas of SSI are not identical; however, there are many analogies between them. For example, a mobile device may become a digital identity for a user once the registration process is completed. Duplicated certificates and key pairs are securely

[1] `https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/`

[2] `https://www.aamva.org/Mobile-Drivers-License/`

[3] `https://identity.cardanofoundation.org/`

[4] `https://www.digital.go.jp/policies/mynumber/smartphone-certification` (in Japanese)

stored in the device, and it may work for their identity proofing or verifying claims. These certificates and key pairs can also be utilized to create Sybil-resistant credentials. Future extensions of real-world identity-related initiatives toward self-sovereign are expected.

6.2 Limitations and Future Directions

This thesis has initially focused on utilizing the abstraction of AESPs with a permissionless blockchain to build a secure SSI system by defining the architecture and the system protocols, $\Pi^{\mathcal{G}_{\mathtt{att}}}$. In addition, to resolve the remaining issues of unlinkability among credentials and to resolve a relatively stronger assumption requiring an AESP to verifiers, I proposed the scheme with $\Pi^{\mathcal{G}_{\mathtt{att}}+}$. In this section, I describe four problems that will remain and need to be addressed in future works.

6.2.1 Potential Vulnerability of Hardware-Assisted Security

Some readers might be concerned about the vulnerability of tamper-resistant secure processors to compromise. One of the possible concerns is the globally shared key pair of `mpk` and `msk` in AESPs, which can be an obvious target for compromise; however, I believe that previous research addressing anonymous attestation may resolve the concern. As described in Section 2.3.1, Ernie Brickell *et al.* proposed direct anonymous attestation scheme (DAA) and Enhanced Privacy ID (EPID) to address the problem [BCC04, BL07, BL09, BL10], firstly adopted onto TPM.

Taisei Tahakashi, Taishi Higuchi, and Akira Otsuka addressed a similar problem through their use AESPs for digital cash, and proposed to enhance $\mathcal{G}_{\mathtt{att}}$ as $\mathcal{G}_{\mathtt{epid}}$ to utilize EPID [THO22]. This research may apply the same approach to resolve the concern.

I wanted to emphasize that the BBS+ signature scheme is very focused on applying selective disclosure in recent digital identity innovations in the tech industry; on the other side, it was addressed also for EPID by Ernie Brickell and Jiangtao Li [BL09]. With respect to their approach, I plan to propose a scheme to revoke a compromised AESP by modifying the EPID's revocation protocol. Each platform may choose a

unique membership key f, which is equivalent to `msk` in theory, and the issuer in the scheme computes a BBS+ signature (A, e, s) on f. In addition, each platform chooses a random base B and computes $K \coloneqq B^f$. This (B, K) pair serves the revocation check. e.g., let a private key-revocation list $\texttt{Priv-RL} = \{f_1, \ldots, f_n\}$ for $i = 1, \ldots, n$, it checks that $K \overset{?}{\neq} B^{f_i}$.

6.2.2 Addressing Further Complexity in the Real World

This thesis proposes incorporating Rafael Pass, Elaine Shi, and Florian Tramèr's contribution regarding the formal abstraction of AESPs [PST17] to build an SSI system. Also, I have demonstrated the ideas of protocols, security properties, and proofs; however, I made some assumptions for brevity, such as a single system of Sybil-resistant credentials. In concrete, there are about 150 countries and regions on the planet. No uniform fashion exists to prove the existence of a natural person in the sense of Self-Sovereign in the real world, even by any authorities. The idea originally proposed by CanDID was to ensure avoiding deduplication by maintaining an injective map with the real identities roughly represented in Social Security Number (SSN) in the U.S. in their case. Further research is expected to address more complexity existing in the real world.

6.2.3 Practice – Reference Implementation

In this thesis, I have not addressed implementation and evaluation in practice to utilize a permissionless blockchain and AESPs in alignment with the proposed architecture and the system protocols $\Pi^{\mathcal{G}_{\mathsf{att}}}$ / $\Pi^{\mathcal{G}_{\mathsf{att}}+}$. Since some existing SSI systems are already deployed utilizing permissionless blockchains [NJ20b, Nak08, Win21], I plan to design a prototype of the proposed architecture based on the existing permissionless blockchain systems such as Ethereum 2.0[5]. There are also several prototype implementations of the one-out-of-many proofs[6].

The further detailed design includes *a.*) interface between issuers/holders/verifiers and permissionless blockchains for a natural person who owns a mobile device equipped

[5] `https://ethereum.org/en/eth2/`

[6] e.g., `https://crates.io/crates/one-of-many-proofs`

with an AESP to control their credentials, *b.*) interface for such a natural person to access programs that can and should also be maintained on the permissionless blockchain, and *c.*) some applications, such as a scenario where a natural person purchases something with their digital identity wallet on the permissionless blockchain only when a shop there may verify if the person's age is over 18 years old, but other private information is not disclosed at all.

Performance evaluation is valuable, and the proposal described in Chapter 5 can be proven through the work in practice.

6.2.4 Theory – Universal Composability

For further study, one direction is to revisit the proposed scheme under universal composability (UC) setting [Can20, CDL16, Cri+24].

Chapter 7

Conclusion

In this thesis, I have, firstly, demonstrated the powerfulness of hardware-assisted security and the formal abstraction of attested execution secure processors (AESPs) over permissionless blockchain technology. Based on those techniques, this thesis proposed the AESP-based secure self-sovereign identity (SSI) architecture and system protocols $\Pi^{\mathcal{G}_{\mathtt{att}}}$ along with security properties, including Sybil-resistance, and the proof. Assuming AESPs and $\mathcal{G}_{\mathtt{att}}$, the AESP-based SSI system protocols $\Pi^{\mathcal{G}_{\mathtt{att}}}$ eliminates the online distributed committee of trusted nodes assumed in CanDID; thus, $\Pi^{\mathcal{G}_{\mathtt{att}}}$ allows not to rely on multi-party computation (MPC). It brings drastic flexibility and efficiency when compared with CanDID.

Second, this thesis described a novel scheme that enables unlinkability among derived credentials for public verification in secure, anonymous, and Sybil-resistant SSI systems. The scheme includes commitment-based *perfectly anonymous identifiers*, a simplified format for computed claims *in Boolean* from multiple issuers, anonymous Sybil-resistant derived credentials, and the construction that allows verifiers to prove the existence and verify such an anonymous Sybil-resistant credential in public without AESPs utilizing "One-Out-of-Many Proofs" Σ-protocol as a zero-knowledge membership proof. For this, the thesis also demonstrated the best use of *SPK* and Proof of Knowledge of a Signature with randomly shifted signatures. Thanks to the efficiency of the one-out-of-many proofs, $\Pi^{\mathcal{G}_{\mathtt{att}}+}$ brings logarithm order for verifying the existence of an anonymous Sybil-resistant credential among N credentials (commitments); thus, the scheme presented in this thesis is encouraging.

Lastly, I described this research's applications, limitations, and future directions. Compared to the other research, the proposed scheme achieves a higher level of assurance for Sybil-resistance, pragmatic performance in logarithmic order for identifying and verifying an expected credential, and under weaker assumptions, q-SDH and no-requiring distributed committee of trusted nodes nor AESPs for verifiers, in decentralized anonymous credential systems satisfying the Sybil-resistance requirement and unlinkability.

In conclusion, I have demonstrated the novel architecture and schemes of utilizing hardware-assisted security, permissionless blockchains, and modern cryptographic signature schemes, including zero-knowledge membership proofs, and how they resolve the conflicting requirements of having anonymity for preserving privacy and the Sybil-resistance requirement for dealing with anti-money laundering (AML) or other needs, which is a critical requirement in the real world, in mathematical approach. I expect that the achievement of this research will resolve remaining issues in digital identity for human beings.

Bibliography

[All16] Christopher Allen. *The Path to Self-Sovereign Identity*. Apr. 2016. URL: https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (visited on 12/10/2023).

[ASM06] Man Ho Au, Willy Susilo, and Yi Mu. "Constant-Size Dynamic k-TAA". In: *Proceedings of 5th International Conference on Security and Cryptography for Networks (SCN 2006)*. Vol. 4116. LNCS. Maiori, Italy: Springer, Sept. 2006, pp. 111–125. DOI: 10.1007/11832072.

[Bai+22] Yirui Bai, Hong Lei, Suozai Li, Haoyu Gao, Jun Li, and Leixiao Li. "Decentralized and Self-Sovereign Identity in the Era of Blockchain: A Survey". In: *Proceedings of 2022 IEEE International Conference on Blockchain (Blockchain 2022)*. Espoo, Finland: IEEE, Aug. 2022, pp. 500–507. ISBN: 978-1-6654-6104-7. DOI: 10.1109/Blockchain55522.2022.00077.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. "Short Group Signatures". In: *Proceedings of Advances in Cryptology – CRYPTO 2004*. Vol. 3152. LNCS. Santa Barbara, CA, USA: Springer, Aug. 2004, pp. 41–55. DOI: 10.1007/978-3-540-28628-8_3.

[BCC04] Ernie Brickell, Jan Camenisch, and Liqun Chen. "Direct Anonymous Attestation". In: *Proceedings of the 11th ACM Conference on Computer and Communications Security - CCS '04*. Washington DC, USA: ACM, Oct. 2004, pp. 132–145. DOI: 10.1145/1030083.1030103.

[BL07] Ernie Brickell and Jiangtao Li. "Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities". In: *Proceedings of the 2007 ACM workshop on Privacy in electronic society.*

Alexandria, VA, USA: ACM, Aug. 2007, pp. 21–30. DOI: 10.1145/1314333.1314337.

[BL09] Ernie Brickell and Jiangtao Li. *Enhanced Privacy ID from Bilinear Pairing*. Cryptographic protocols. Cryptology ePrint Archive, Paper 2009/095. Mar. 2009. URL: https://eprint.iacr.org/2009/095.

[BL10] Ernie Brickell and Jiangtao Li. "Enhanced Privacy ID from Bilinear Pairing for Hardware Authentication and Attestation". In: *Proceedings of 2010 IEEE Second International Conference on Social Computing (SocialCom)*. Minneapolis, MN, USA: IEEE, Aug. 2010, pp. 768–775. DOI: 10.1109/SocialCom.2010.118.

[Bok+19] Dirk van Bokkem, Rico Hageman, Gijs Koning, Luat Nguyen, and Naqib Zarin. *Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology*. preprint. arXiv:1904.12816. Apr. 2019. URL: https://arxiv.org/pdf/1904.12816.pdf.

[Boy21] Andrew Boysen. "Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada". In: *Frontiers in Blockchain*. Frontiers in Blockchain 4.624258 (Apr. 2021), pp. 1–8. DOI: 10.3389/fbloc.2021.624258.

[BSC22] Mauricio Barros, Frederico Schardong, and Ricardo Felipe Custódio. *Leveraging Self-Sovereign Identity, Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass*. preprint. arXiv:2202.09207. Feb. 2022. URL: http://arxiv.org/abs/2202.09207.

[Cam05] Kim Cameron. *The Laws of Identity*. May 2005. URL: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (visited on 12/10/2023).

[Can20] Ran Canetti. "Universally Composable Security". In: *Journal of the ACM* 67.5 (Oct. 2020), pp. 1–94. DOI: 10.1145/3402457.

[CDL16] Jan Camenisch, Manu Drijvers, and Anja Lehmann. "Universally Composable Direct Anonymous Attestation". In: *Proceedings of 19th IACR International Conference on Practice and Theory in Public-Key Cryptogra-*

phy (PKC 2016). Vol. 9615. LNCS. Taipei, Taiwan: Springer, Mar. 2016, pp. 234–264. DOI: 10.1007/978-3-662-49387-8_10.

[Cha85] David Chaum. "Security Without Identification: Transaction Systems to Make Big Brother Obsolete". In: *Communications of the ACM* 28.10 (Oct. 1985), pp. 1030–1044. DOI: 10.1145/4372.4373.

[CL02a] Jan Camenisch and Anna Lysyanskaya. "A Signature Scheme with Efficient Protocols". In: *Proceedings of Third International Conference on Security in Communication Networks (SCN 2002)*. Vol. 2576. LNCS. Amalfi, Italy: Springer, Sept. 2002, pp. 268–289. DOI: 10.1007/3-540-36413-7_20.

[CL02b] Jan Camenisch and Anna Lysyanskaya. "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials". In: *Proceedings of Advances in Cryptology — CRYPTO 2002*. Ed. by Gerhard Goos, Juris Hartmanis, Jan Van Leeuwen, and Moti Yung. Vol. 2442. LNCS. Santa Barbara, CA, USA: Springer, Aug. 2002, pp. 61–76. DOI: 10.1007/3-540-45708-9_5.

[CL04] Jan Camenisch and Anna Lysyanskaya. "Signature Schemes and Anonymous Credentials from Bilinear Maps". In: *Proceedings of Advances in Cryptology – CRYPTO 2004*. Vol. 3152. LNCS. Santa Barbara, CA, USA: Springer, Aug. 2004, pp. 56–72. DOI: 10.1007/978-3-540-28628-8_4.

[CLD16] Victor Costan, Ilia Lebedev, and Srinivas Devadas. "Sanctum: Minimal Hardware Extensions for Strong Software Isolation". In: *Proceedings of 25th USENIX Security Symposium (USENIX Security '16)*. Aug. 2016, pp. 857–874. ISBN: 978-1-931971-32-4.

[CM99] Jan Camenisch and Markus Michels. "Proving in Zero-Knowledge that a Number Is the Product of Two Safe Primes". In: *Proceedings of Advances in Cryptology — EUROCRYPT '99*. Vol. 1592. LNCS. Prague, Czech Republic: Springer, May 1999, pp. 107–122. DOI: 10.1007/3-540-48910-X_8.

[Cri+24] Elizabeth Crites, Aggelos Kiayias, Markulf Kohlweiss, and Amirreza Sarencheh. *SyRA: Sybil-Resilient Anonymous Signatures with Applications to Decen-*

tralized Identity. Cryptology ePrint Archive, Paper 2024/379. June 2024. URL: https://eprint.iacr.org/2024/379.

[CS03] Jan Camenisch and Victor Shoup. "Practical Verifiable Encryption and Decryption of Discrete Logarithms". In: *Proceedings of Advances in Cryptology - CRYPTO 2003*. Vol. 2729. Santa Barbara, CA, USA: Springer, Aug. 2003, pp. 126–144. DOI: 10.1007/978-3-540-45146-4_8.

[Čuč+22] Špela Čučko, Šeila Bećirović, Aida Kamišalić, Saša Mrdović, and Muhamed Turkanović. "Towards the Classification of Self-Sovereign Identity Properties". In: *IEEE Access* 10 (Aug. 2022), pp. 88306–88329. DOI: 10.1109/ACCESS.2022.3199414.

[DA18] Paul Dunphy and Fabien A. P. Petitcolas. "A First Look at Identity Management Schemes on the Blockchain". In: *IEEE Security & Privacy* 16.4 (Jan. 2018), pp. 20–29. DOI: 10.1109/MSP.2018.3111247.

[DGP18] Paul Dunphy, Luke Garratt, and Fabien Petitcolas. "Decentralizing Digital Identity: Open Challenges for Distributed Ledgers". In: *Proceedings of 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. London, UK: IEEE, Apr. 2018, pp. 75–78. DOI: 10.1109/EuroSPW.2018.00016.

[Die+23] Mohameden Dieye, Pierre Valiorgue, Jean-Patrick Gelas, El-Hacen Diallo, Parisa Ghodous, Frédérique Biennier, and Éric Peyrol. "A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain". In: *IEEE Access* 11 (Apr. 2023), pp. 49445–49455. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2023.3268768.

[Dou02] John R. Douceur. "The Sybil Attack". In: *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS 2002)*. Vol. 2429. LNCS. Cambridge, MA, USA: Springer, Mar. 2002, pp. 251–260. DOI: 10.1007/3-540-45748-8_24.

[FCO19] Md Sadek Ferdous, Farida Chowdhury, and Madini O. Alassafi. "In Search of Self-Sovereign Identity Leveraging Blockchain Technology". In: *IEEE*

Access 7 (Aug. 2019), pp. 103059–103079. DOI: 10.1109/ACCESS.2019.2931173.

[Fer+15] Md Sadek Ferdous, Gethin Norman, Audun Jøsang, and Ron Poet. "Mathematical Modelling of Trust Issues in Federated Identity Management". In: *Proceedings of 9th IFIP WG 11.11 International Conference, IFIPTM 2015: Trust Management IX*. Hamburg, Germany: Springer, May 2015, pp. 13–29. DOI: 10.1007/978-3-319-18491-3_2.

[GGF17] Paul A. Grassi, Michael E. Garcia, and James L. Fenton. *NIST Special Publication 800-63-3 Digital Identity Guidelines*. June 2017. URL: https://pages.nist.gov/800-63-3/ (visited on 11/12/2021).

[GGM14] Christina Garman, Matthew Green, and Ian Miers. "Decentralized Anonymous Credentials". In: *Proceedings of Network and Distributed System Security Symposium 2014 (NDSS' 2014)*. San Diego, CA, USA: Internet Society, Feb. 2014, pp. 1–15. DOI: 10.14722/ndss.2014.23253.

[GK15] Jens Groth and Markulf Kohlweiss. "One-Out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin". In: *Proceedings of Advances in Cryptology - EUROCRYPT 2015 Part II*. Vol. 9057. LNCS. Sofia, Bulgaria: Springer, Apr. 2015, pp. 253–280. DOI: 10.1007/978-3-662-46803-6_9.

[GMM18] Andreas Grüner, Alexander Mühle, and Christoph Meinel. *On the Relevance of Blockchain in Identity Management*. preprint. arXiv:1807.08136. July 2018. URL: http://arxiv.org/abs/1807.08136.

[Gom19] Carlos Gomez Munoz. *eIDAS Supported Self-Sovereign Identity*. Tech. rep. European Commission, May 2019. URL: https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf (visited on 09/23/2021).

[GYK21] Sandro Rodriguez Garzon, Hakan Yildiz, and Axel Küpper. *Decentralized Identifiers and Self-sovereign Identity in 6G*. preprint. arXiv:2112.09450. Dec. 2021. URL: http://arxiv.org/abs/2112.09450.

[HK19] Samia El Haddouti and Mohamed Dâfir Ech-Cherif El Kettani. "Analysis of Identity Management Systems Using Blockchain Technology". In: *Proceedings of 2019 International Conference on Advanced Communication Technologies and Networking (CommNet 2019)*. Rabat, Morocco: IEEE, Apr. 2019, pp. 1–7. DOI: 10.1109/COMMNET.2019.8742375.

[ISO21a] ISO/IEC. *ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application*. Sept. 2021. URL: https://www.iso.org/standard/69084.html.

[ISO21b] ISO/IEC. *ISO/IEC 27551:2021(en), Information security, cybersecurity and privacy protection — Requirements for attribute-based unlinkable entity authentication*. Sept. 2021. URL: https://www.iso.org/standard/72018.html.

[ISO23a] ISO/IEC. *ISO/IEC 23220-1:2023 Cards and security devices for personal identification — Building blocks for identity management via mobile devices Part 1: Generic system architectures of mobile eID systems*. Feb. 2023. URL: https://www.iso.org/standard/74910.html.

[ISO23b] ISO/IEC. *ISO/IEC 24760-1:2019/Amd 1:2023 (en), IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*. Jan. 2023. URL: https://www.iso.org/standard/84248.html.

[Kal22] Vasileios Kalos. *The BBS Signature Scheme (IETF BBS+)*. July 2022. URL: https://datatracker.ietf.org/meeting/114/materials/slides-114-cfrg-bbs-signature-scheme-pdf-00 (visited on 05/01/2023).

[KE20] Galia Kondova and Jörn Erbguth. "Self-sovereign identity on public blockchains and the GDPR". In: *Proceedings of the 35th Annual ACM Symposium on Applied Computing (SAC '20)*. New York, NY, USA: ACM, Mar. 2020, pp. 342–345. DOI: 10.1145/3341105.3374066.

[Kru+24] Evan Krul, Hye-young Paik, Sushmita Ruj, and Salil S. Kanhere. "SoK: Trusting Self-Sovereign Identity". In: *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2024.3 (July 2024), pp. 297–313. ISSN: 2299-0984.

DOI: 10.56553/popets-2024-0079. URL: https://petsymposium.org/popets/2024/popets-2024-0079.php.

[Liu+20] Yue Liu, Q. Lu, H. Paik, and Xiwei Xu. "Design Patterns for Blockchain-based Self-Sovereign Identity". In: *Proceedings of the European Conference on Pattern Languages of Programs 2020*. Virtual Event Germany, July 2020, pp. 1–14. DOI: 10.1145/3424771.3424802.

[Loo+23] Tobias Looker, Vasilis Kalos, Andrew Whitehead, and Mike Lodder. *The BBS Signature Scheme*. Apr. 2023. URL: https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html (visited on 05/01/2023).

[Lyu+23] Qiuyun Lyu, Mingya Zhao, Yanzhao Shen, Yizhi Ren, Shaopeng Chen, Zhen Wang, Junnan Bao, and Junliang Liu. *NSSIM: A Novel Self-Sovereign Identity Scheme For Metaverse with Sybil-Resistance, Full Lifecycle Synchronization and Joint Accountability*. preprint. Dec. 2023. DOI: 10.21203/rs.3.rs-3785871/v1. URL: https://www.researchsquare.com/article/rs-3785871/v1.

[Mar+21] Deepak Maram, Harjasleen Malvai, Fan Zhang, Nerla Jean-Louis, Alexander Frolov, Tyler Kell, Tyrone Lobban, Christine Moy, Ari Juels, and Andrew Miller. "CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability". In: *Proceedings of 2021 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA, USA: IEEE, May 2021, pp. 1348–1366. DOI: 10.1109/SP40001.2021.00038.

[MO22] Koichi Moriyama and Akira Otsuka. "Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors". In: *Proceedings of 2022 IEEE International Conference on Blockchain (Blockchain 2022)*. Espoo, Finland: IEEE, Aug. 2022, pp. 1–10. DOI: 10.1109/Blockchain55522.2022.00012.

[MO23] Koichi Moriyama and Akira Otsuka. *Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Pro-*

cessors. Bulletin at Institute of Information Security Vol.14. Feb. 2023. URL: https://www.iisec.ac.jp/proc/vol0014/moriyama-otsuka23.pdf.

[MO24] Koichi Moriyama and Akira Otsuka. "Permissionless Blockchain-Based Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors". In: *IEICE Transactions on Information and Systems - Special Section on Blockchain and Security* E107-D.9 (Sept. 2024), pp. 1112–1122. DOI: 10.1587/transinf.2023BCI0001.

[MO25] Koichi Moriyama and Akira Otsuka. "Sybil-Resistant Self-Sovereign Identity Utilizing Attested Execution Secure Processors and Zero-Knowledge Membership Proofs". In: *IEEE Access* 13 (Jan. 2025), pp. 17919–17944. DOI: 10.1109/ACCESS.2025.3533877.

[MTC21] Stanislav Mahula, Evrim Tan, and Joep Crompvoets. "With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case". In: *Proceedings of the 22nd Annual International Conference on Digital Government Research (DG.O '21)*. Omaha, NE, USA: ACM, June 2021, pp. 495–504. DOI: 10.1145/3463677.3463705.

[Müh+18] Alexander Mühle, Andreas Grüner, Taiana Gayvoronskaya, and Christoph Meinel. *A Survey on Essential Components of a Self-Sovereign Identity*. preprint. arXiv:1807.06346. July 2018. URL: https://arxiv.org/pdf/1807.06346.pdf.

[Nak08] Satoshi Nakamoto. *Bitcoin : A Peer-to-Peer Electronic Cash System*. 2008. URL: https://bitcoin.org/bitcoin.pdf.

[NJ20a] Nitin Naik and Paul Jenkins. "Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology". In: *Proceedings of 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. Oxford, UK: IEEE, Aug. 2020, pp. 90–95. DOI: 10.1109/MobileCloud48802.2020.00021.

[NJ20b] Nitin Naik and Paul Jenkins. "uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain". In: *Proceedings of 2020 IEEE International Symposium on Systems Engineering (ISSE)*. Vienna, Austria: IEEE, Nov. 2020, pp. 1–7. DOI: 10.1109/ISSE49799.2020.9272223.

[Ped91] Torben Pryds Pedersen. "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing". In: *Proceedings of Advances in Cryptology — CRYPTO '91*. Ed. by Joan Feigenbaum. Vol. 576. LNCS. Santa Barbara, CA, USA: Springer, Aug. 1991, pp. 129–140. DOI: 10.1007/3-540-46766-1_9.

[PFS20] Andreea-Elena Panait, Ruxandra F. Olimid, and Alin Stefanescu. "Analysis of uPort Open, an Identity Management Blockchain-Based Solution". In: *Proceedings of 17th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2020)*. Vol. 12395. LNCS. Bratislava, Slovakia: Springer, Sept. 2020, pp. 3–13. DOI: 10.1007/978-3-030-58986-8_1.

[PR21] Alex Preukschat and Drummond Reed. *Self-Sovereign Identity, Decentralized Digital Identity and Verifiable Credentials*. Shelter Island, NY, USA: Manning Publications Co., May 2021. ISBN: 978-1-61729-659-8.

[PST17] Rafael Pass, Elaine Shi, and Florian Tramèr. "Formal Abstractions for Attested Execution Secure Processors". In: *Proceedings of Advances in Cryptology – EUROCRYPT 2017*. Vol. 10210. LNCS. Paris, France: Springer, Apr. 2017, pp. 260–289. DOI: 10.1007/978-3-319-56620-7_10.

[Rab+24] Reyhaneh Rabaninejad, Behzad Abdolmaleki, Sebastian Ramacher, and Antonis Michalas. *Attribute-Based Threshold Issuance Anonymous Counting Tokens and Its Application to Sybil-Resistant Self-Sovereign Identity*. Cryptology ePrint Archive, Paper 2024/1024. June 2024. URL: https://eprint.iacr.org/2024/1024.

[Ros+23] Michael Rosenberg, Jacob White, Christina Garman, and Ian Miers. "zkcreds: Flexible Anonymous Credentials from zkSNARKs and Existing Iden-

tity Infrastructure". In: *Proceedings of 2023 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA, USA: IEEE, May 2023, pp. 790–808. DOI: 10.1109/SP46215.2023.10179430.

[San+14] Nuno Santos, Himanshu Raj, Stefan Saroiu, and Alec Wolman. "Using ARM trustzone to build a trusted language runtime for mobile applications". In: *Proceedings of the 19th international conference on Architectural support for programming languages and operating systems*. Salt Lake City, UT, USA: ACM, Feb. 2014, pp. 67–80. DOI: 10.1145/2541940.2541949.

[SC22] Frederico Schardong and Ricardo Custódio. *Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy*. arXiv:2108.08338. June 2022. DOI: 10.48550/arXiv.2108.08338. URL: http://arxiv.org/abs/2108.08338.

[Seu19] Daniël Du Seuil. *European Self Sovereign identity framework*. July 2019. URL: https://ssimeetup.org/understanding-european-self-sovereign-identity-framework-essif-daniel-du-seuil-carlos-pastor-webinar-32/ (visited on 09/23/2021).

[Shi+17] Elaine Shi, Fan Zhang, Rafael Pass, Srini Devadas, Dawn Song, and Chang Liu. *Trusted Hardware: Life, the Composable Universe, and Everything (2015 12 15 4 Elaine Shi, et el.)* May 2017. URL: https://www.youtube.com/watch?v=57KnieAVFkY (visited on 09/25/2021).

[SNE19] Abylay Satybaldy, Mariusz Nowostawski, and Jørgen Ellingsen. "Self-Sovereign Identity Systems". In: *14th IFIP International Summer School on Privacy and Identity Management (Privacy and Identity)*. Windisch, Switzerland, Aug. 2019, pp. 447–461. DOI: 10.1007/978-3-030-42504-3_28.

[SP18] Quinten Stokkink and Johan Pouwelse. "Deployment of a Blockchain-Based Self-Sovereign Identity". In: *Proceedings of 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. Halifax, NS, Canada:

IEEE, July 2018, pp. 1336–1342. DOI: 10.1109/Cybermatics_2018.2018.00230.

[Sto+21] Quinten Stokkink, Georgy Ishmaev, Dick Epema, and Johan Pouwelse. "A Truly Self-Sovereign Identity System". In: *Proceedings of IEEE 46th Conference on Local Computer Networks (LCN 2021)*. Edmonton, AB, Canada: IEEE, Oct. 2021, pp. 1–8. DOI: 10.1109/LCN52139.2021.9525011.

[TA19] Kalman C. Torh and Alan Anderson-Priddy. "Self-Sovereign Digital Identity: A Paradigm Shift for Identity". In: *IEEE Security & Privacy* 17.3 (May 2019), pp. 17–27. DOI: 10.1109/MSEC.2018.2888782.

[THO22] Taisei Takahashi, Taishi Higuchi, and Akira Otsuka. "VeloCash: Anonymous Decentralized Probabilistic Micropayments With Transferability". In: *IEEE Access* 10 (Sept. 2022), pp. 93701–93730. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2022.3201071.

[W3C22a] W3C. *Decentralized Identifiers (DIDs) v1.0 (W3C Recommendation)*. July 2022. URL: https://www.w3.org/TR/did-core/ (visited on 09/26/2021).

[W3C22b] W3C. *Verifiable Credentials Data Model 1.1 (W3C Recommendation)*. Mar. 2022. URL: https://www.w3.org/TR/vc-data-model/ (visited on 09/26/2021).

[W3C24] W3C. *Verifiable Credentials Data Model 2.0 (W3C Candidate Recommendation Draft)*. June 2024. URL: https://www.w3.org/TR/vc-data-model-2.0/ (visited on 06/09/2024).

[Win21] Phlllip J. Windley. "Sovrin: An Identity Metasystem for Self-Sovereign Identity". In: *Frontiers in Blockchain*. Frontiers in Blockchain 4.626726 (July 2021), pp. 1–14. DOI: 10.3389/fbloc.2021.626726.

[Yil+22] Hakan Yildiz, Axel Küpper, Dirk Thatmann, Sebastian Göndör, and Patrick Herbke. *A Tutorial on the Interoperability of Self-sovereign Identities*. preprint. arXiv:2208.04692. Aug. 2022. URL: http://arxiv.org/abs/2208.04692.

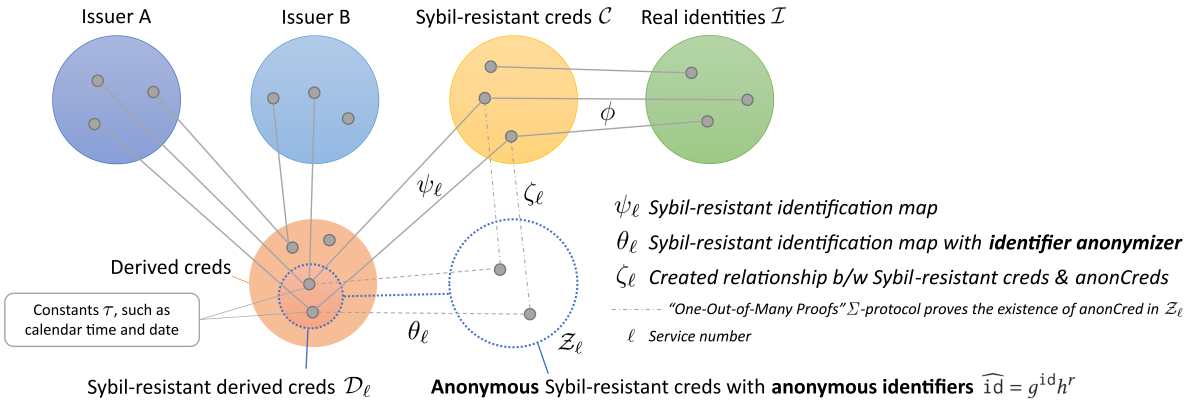
[YSS22] Dan Yamamoto, Yuji Suga, and Kazue Sako. “Formalising Linked-Data based Verifiable Credentials for Selective Disclosure”. In: *Proceedings of 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Genoa, Italy: IEEE, June 2022, pp. 52–65. DOI: 10.1109/EuroSPW55150.2022.00013.

[佐古 23] 佐古和恵. “分散型デジタルアイデンティティとは？～概念、仕組み、実現に資する技術と課題～”. ja. In: 日本銀行金融研究所 *Discussion Paper* 2023-J.8 (2023), p. 35.

[大塚 21] 大塚玲. “ブロックチェーンを利用した暗号資産の安全性と匿名性：原理と限界”. ja. In: 日本銀行金融研究所 *Discussion Paper* 2021-J.4 (2021), p. 47.

[大塚 22] 大塚玲. “耐タンパー性に基づくデジタル通貨ウォレットの研究動向－匿名性と透明性の両立に向けて－”. ja. In: 日本銀行金融研究所 *Discussion Paper* 2022-J.9 (2022), p. 39.

Appendix. Graphical Abstract



The novel scheme anonymizes credentials and achieves unlinkability among them by introducing commitment-based anonymous identifier $\widehat{\mathtt{id}} = g^{\mathtt{id}}h^r$ with θ_ℓ and a set of anonymous Sybil-resistant credentials $\mathcal{Z}_\ell$. Utilizing zero-knowledge membership proofs for ζ_ℓ enables to proof of the existence of anonymous Sybil-resistant credentials in $\mathcal{Z}_\ell$ to replace with ψ_ℓ; hence, $\psi_\ell = \theta_\ell \circ \zeta_\ell$.

Index