International Journal of Cryptology Research X(Y): (20ZZ)

Survey and New Idea for Attribute-Based Identification Scheme Secure against Reset Attacks

[1]Ji-Jian Chin, [2]Hiroaki Anada, [3]Seiko Arita, [2,4]Kouichi Sakurai, [5]Swee-Huay Heng and [1]Raphael Phan

[1]Faculty of Engineering, Multimedia University
[2]Institute of Systems, Information Technologies and Nanotechnologies, Japan
[3]Institute of Information Security, Japan.
[4]Faculty of Information Science and Electrical Engineering, Kyushu University
[5]Faculty of Information Science and Technology, Multimedia University
Email: [1]jjchin@mmu.edu.my, [2]anada@isit.or.jp

ABSTRACT

Identification schemes are a common one-way authentication technique for a user to prove himself securely to a verifier. However, it is known that identification schemes based on the sigma-protocol are basically insecure against reset attacks. On the other-hand, attribute-based cryptography is a technique which allows for the secure implementation of access policies within a cryptosystem. In this paper, we report on the developments in the area of reset attacks for identification schemes as well as for attribute-based identification schemes. Then we put together a new idea to construct attribute-based identification schemes secure against reset attacks.

SECTION 1: INTRODUCTION

An identification scheme is a cryptographic primitive that allows one party, the prover, to prove himself convincingly to another party, the verifier, without revealing any knowledge about his private key. First proposed by Fiat and Shamir (1983), this primitive is usually used to facilitate access control to allow legitimate users to access resources upon being able to prove themselves securely to a verifying mechanism.

Identification schemes are generally categorized into two-move challenge-response and three-move sigma protocols. Two-move challenge-response protocols basically revolve around the capability of the prover to decrypt a challenge ciphertext or sign a verifiable message, given that he has a valid private key. However, in general, two-move protocols are more expensive operationally.

For three-move sigma protocols the prover and verifier engage in a three-step canonical interaction every time a prover wishes to prove itself. The prover begins by sending a commitment. The verifier follows by selecting a random challenge from a predefined challenge set. Then the prover provides a response using a combination of his private key,

commitment as well as the challenge. The verifier will then decide to accept or reject a prover's session based on the response.

Sigma-protocols have the following properties:

i) Completeness – provers with valid private keys should be given an "accept" except with negligible probability.

ii) Soundness – provers with invalid private keys should be given a reject decision except with negligible probability.

iii) Zero-knowledge – certain sigma protocols have a zero-knowledge property, where the verifier upon completing the interaction with the prover learns nothing about the user's private key. This is proven by a simulator that is able to produce a valid interaction transcript with or without a prover's participation. However, since it is hard to prove security against concurrent-active attacks for protocols with zero-knowledge properties, sometimes the requirement is relaxed to just satisfying a witness indistinguishability requirement (Fiege and Shamir, 1990), where a verifier cannot distinguish between the two witnesses used in the protocol.

1.1 Reset Attacks

While generally two-move challenge-response protocols are secure against reset attacks, unfortunately sigma protocols have an inherent weakness against reset attacks, where an adversary is allowed to reset the prover to where he first sent the commitment. Then due to the soundness property, with two different challenges, the adversary is able to extract a user's private key from the different responses and challenges but using the same commitment.

Reset attacks can be performed if an adversary has access to the verifying machine, for example a smart card reader that is able to tamper with the internal state of the smart card. Thus the adversary with access to this smart card reader will be able to extract an honest user's private key if the user interacts with it.

The reset attack was first addressed for identification schemes by Bellare et al. (2001). In their seminal paper, they tackled the problem of adversaries with the resetting capability and proposed several methods of overcoming this problem. We provide a more comprehensive review of these methods in a later section of this paper.

The power of reset attacks can be seen by the following scenarios given by Bellare et al. (2001), describing how a reset-attack can be mounted practically. Firstly, if an adversary captures a prover device such as a smart

card, the adversary can disconnect and reinsert the battery to reset the card's secret internal state to its initial state. This can be done multiple times.

Secondly if an adversary is able to crash the prover device, such as by causing a stack/heap overflow, upon reinitializing the device will resume computation after the crash, forcing the device to reset itself.

Thus, reset-secure identification schemes are desirable due to the existence of these threats.

1.2 Identification Schemes without Certificates

In traditional public key cryptography, certificates are required to bind a user to his public key, which could otherwise be replaced by a malicious party. These certificates are issued by certificate authorities, and include a wide-array of information ranging from the public key to validity period. Any doubtful parties can verify that a user's public key actually belongs to a particular user by checking the Certificate Authority's digital signature on the certificate.

The certificate management issue occurs when the users of the cryptosystem grow large and a large overhead is required to issue, validate, manage and revoke these certificates. To circumvent this issue, Adi Shamir first proposed identity-based cryptography (Shamir, 1984), where users can implicitly certify themselves using a publicly known identity-string. Identity-based cryptography only kicked off in 2001 when Boneh and Franklin (2001) proposed the first identity-based encryption scheme. In 2004, the first identity-based identification schemes were proposed by Bellare et al. (2004) and Kurosawa and Heng (2004) independently.

Since then, many identity-based identification schemes have been proposed, but none of them are secure against reset attacks. The first identity-based identification scheme that is secure against reset attacks was first proposed by Thorncharoensri et al. (2009).

In addition to identity-based cryptography, other extensions for identification schemes that operate without the requirement of certificates have surfaced in the recent decade. Certificateless cryptography was proposed by Alriyami and Paterson (2001) to resolve the key escrow issue, where the central key generation center has access to every user's private key. In certificateless cryptography, the key generation center creates a partial private key, which the user combines with his component of the private key to create the full private key. Thus without the user's component the key generation center does not have complete access to the full private key. For the identification primitive, certificateless identification was first defined and proposed by Dehkordi and Alimoradi (2013) and Chin et al. (2013) independently. However, subsequently Chin et al. (2014) pointed out flaws

in Dehkordi and Alimoradi (2013)'s design, therefore it is insecure against impersonation attacks.

Another new area of identification schemes without certificates is the attribute-based identification (ABID) scheme. Attribute-based identification was introduced by Anada et al. (2013). In an ABID scheme, each entity has credentials called attributes. An access policy is written as a boolean formula over these attributes. Thus, a verifier can identify that a prover possesses a certain set of attributes that satisfies the verifier's access policy. Hence, ABID schemes can be considered as an expansion of the usual ID schemes. In Anada et al. (2013)'s seminal paper, a two-move generic (and concrete) construction was presented. That is, by employing an attribute-based key encapsulation mechanism (Sahai and Waters 2005, Waters 2011), a challenge-and-response protocol was proposed. Their scheme was proven to be secure against reset attacks. After their two-move construction, a three-move construction was presented by Anada et al. (2014a). This three-move construction was captured as a canonical ABID scheme and it was transformed into an attribute-based signature scheme by using the Fiat-Shamir transform (Anada et al. 2014b).

In contrast to the earlier construction by Anada et al. (2013), the three-move construction was based on the (traditional) sigma protocol (Cramer et al., 2001). Enhancing the technique of OR-proof (Damgard, 2004), they succeeded to provide a three-move generic ABID scheme that can be concretely realized without pairings. Hence Anada et al. (2014a)'s three-move protocol can be said to be more efficient than the two-move protocol (Anada et al., 2013). But their three-move protocol is not secure against reset attacks because its security is based on the Reset-Lemma (Bellare and Palacio, 2002). That is, under the condition that an adversary is allowed to reset an honest prover, the adversary can extract the prover's witness in polynomial-time.

1.3 Motivations and Contributions

Since its conception in 2004, identification schemes without certificates have received much attention, particularly attribute-based identification schemes. Secondly, the notion of reset attacks has not yet been examined in depth, particularly with regards for identification schemes without certificates.

In this paper, we introduce the reader to the security notions of reset-secure identification as well as attribute-based identification (ABID) schemes. After that, we provide the first generic construction to modify a three-move attribute-based identification scheme to be secure against reset attacks.

It is worthwhile to note that the security against reset attacks discussed in this paper is Concurrent-Reset-1 (CR1) security defined by Bellare et al. (2001). CR1 security is, even if we ignore concurrency, different from the security of resettable zero-knowledge and the security of resettable soundness (see Arita 2012 for definitions).

The rest of the paper is organized as follows: In Section 2 we begin by reviewing the definitions and security model of reset-secure identification schemes and ABID schemes. In Section 3, we introduce the first generic construction to modify three-move ABID schemes to be reset-secure. We conclude in Section 4 with some closing remarks.

SECTION 2: PRELIMINARIES AND DEFINITIONS

In this section, we review the formal definitions and security notions for reset-secure identification schemes as well as ABID schemes.

2.1 Reset-Secure Identification Schemes

An identification scheme consists of three probabilistic polynomial-time algorithms: Keygen, Prover and Verifier.

Keygen takes in the security parameter 1^k and generates a public/private key pair for the user $\langle pk, sk \rangle$.

Prover takes in the private key sk while Verifier takes in the public key pk. Together they run the sigma protocol as such:

1) Prover sends the commitment CMT.
2) Verifier selects and sends a random challenge CHA from a set of predefined challenges.
3) Prover calculates his response RSP based on the challenge and returns it to Verifier. Verifier will then choose to accept/reject based on the response given.

An adversary towards an identification scheme is an impersonator. For normal identification schemes an impersonator can be a passive one, where he only eavesdrops on conversations, or an active one where he can play a cheating verifier to learn information by interacting with honest users before attempting impersonation.

For reset-secure identification schemes, an additional concurrent reset-attacker is defined. This attacker is more powerful than the conventional passive/active attacker and is able to run several instances of the prover interactions concurrently, interleaving executions and performing reset actions on the prover states. Bellare et al. first formalized these two types of concurrent reset attackers as CR1 and CR2 respectively.

For the CR1 attacker, the adversary may interact with the honest user's Prover algorithm as a verifier and in addition to identification queries, be able to perform a reset action for the Prover algorithm to any state. Later the adversary performs the impersonation attempt.

For the CR2 attacker, the adversary may do all the actions described for the CR1 attacker, but may attempt impersonation whenever it wishes to. Therefore, the CR1 attacker is a special case of CR2 attacker.

We describe the security for the reset-secure identification scheme using the following game played between a challenger C and an impersonator I.

Keygen: C takes in the security parameter 1^k, generates $\langle pk, sk \rangle$ and passes pk to I.

Phase 1: I is able to make the following queries:

i) Identification queries: I interacts as a cheating verifier with a prover simulated by C to learn information.

ii) Reset queries: I resets the prover simulated by C to any state that it wishes within the three-step sigma protocol.

Phase 2: I changes mode into a cheating prover trying to convince C. For CR2 impersonators, I can still continue to make any of the queries from Phase 1. I wins if it manages to convince C to accept its interaction with non-negligible probability.

We say an identification scheme is $(t, q_I, q_r, \varepsilon)$ -secure under concurrent reset attacks if any reset concurrent impersonator I that runs in time t, $Pr[I \text{ can impersonate}] < \varepsilon$ where I can make at most q_I identification queries and q_r reset queries.

Bellare et al. (2001) also proposed four techniques in order to secure identification schemes that are constructed using the sigma protocol against reset attackers, which are naturally insecure against reset attacks. We briefly describe the four techniques here:

1) Stateless digital signatures: a prover can authenticate himself to a verifier by showing the capability of signing random documents the verifier chooses. Here the message becomes the challenge while the signature is used as the response. Statelessness is required so that the reset attacker cannot reset the state of the signer. However, this is generally a two-move protocol.
2) Encryption schemes: a prover can authenticate himself to a verifier by showing the capability to decrypt random ciphertexts the verifier chooses. Here the ciphertext becomes the challenge while the message becomes the response. However, reset-security requires that an encryption scheme secure against chosen-ciphertext attacks be used.

3) Trapdoor commitments: this technique uses a trapdoor commitment scheme to 'commit' a verifier's challenge. This commitment is used as the generator for the prover's salt using a pseudorandom function. One can therefore verify that upon revealing the verifier's challenge, the salt can be regenerated in order to create the proper response for the verifier. If the prover was reset, the regeneration of the salt would yield a different (and invalid) response.
4) Zero-knowledge proof of membership: a prover proves membership in a hard language rather than proving that it has a witness for the language. This is done by using a resettable zero-knowledge proof of language membership, as defined by Canetti et al. (2000).

In this work, we utilize the third technique as a generic way to construct reset-secure ABID schemes.

2.2 ABID Schemes

Let $U = \{1, \ldots, u\}$ be an attribute Universe. An access structure A, which means an access policy, is defined as a subset of $2^U \backslash \phi$. We only treat monotone access structures.

An ABID scheme consists of four PPT algorithms: Setup, KeyGen, Prover and Verifier.

Setup(1^k , U) → (PK, MSK). Setup takes as input the security parameter λ and the attribute universe U. It outputs a public key PK and a master secret key MSK.

KeyGen(PK, MSK, S) →SK_S . A key-generation algorithm KeyGen takes as input the public key PK, the master secret key MSK and an attribute set S. It outputs a secret key SK_S corresponding to S.

Prover(PK, SK_S) and Verifier(PK, A). Prover and Verifier are interactive algorithms. Prover takes as input the public key PK and the secret key K_S . Here the secret key SK_S is given to Prover by an authority that runs KeyGen(PK, MSK, S). Verifier takes as input the public key PK and an attribute set S. Prover is provided Verifier's access structure A by the first round. Prover and Verifier interact with each other for some rounds. Then, Verifier finally returns its decision bit b. When $b = 1$ it means that Verifier $accepts$ Prover in the sense Prover has a secret key SK_S such that S satisfies A. When $b = 0$ it means that Verifier $rejects$ Prover.

We require correctness of an ABID scheme that for any 1^k and U, and if $S \in A$, then the probability of Verifier outputting an $accept$ will always be true, namely

$$\Pr[(PK, MSK) \leftarrow Setup(1^k, U);$$

$$SK_S \leftarrow KeyGen(PK, MSK, S);$$
$$b \leftarrow \langle P(PK, SK_S), V(PK, A)\rangle : b = 1] = 1.$$

SECTION 3: GENERIC CONSTRUCTION OF 3-MOVE RESET-SECURE ABID SCHEME

In this section, we present a new and generic idea for modifying three-move ABID schemes to be secure against reset attacks. We utilize Bellare et al. (2001)'s third paradigm, which is to use a trapdoor commitment scheme, and embed this scheme within the three-move ABID scheme. The resulting scheme consists of four-moves.

The construction of the scheme is described in Table 1.

Table 1: Generic Construction of 3-move Reset-Secure ABID Scheme

<table>
<tr><td colspan="3">Setup($1^k, U$)$\rightarrow (\boldsymbol{PK} \coloneqq (\boldsymbol{PK_{ABID}}, \boldsymbol{PK_{TDC}}), \boldsymbol{MSK})$:

Setup takes in the security parameter 1^k and the space of the attribute universe U and outputs the public key and master secret key $\langle PK = (PK_{ABID}, PK_{TDC}), MSK\rangle$. However, the public key consists of two components, one for the ABID scheme PK_{ABID} and the other for the trapdoor commitment scheme PK_{TDC}.</td></tr>
<tr><td colspan="3">KG($\boldsymbol{PK_{ABID}}, \boldsymbol{MSK}, \boldsymbol{S}$)$\rightarrow \boldsymbol{SK_S}$:

Keygen KG takes in the public key for the ABID scheme, PK_{ABID}, the master secret key MSK and the set of attributes S and outputs the secret key SK_S corresponding to S.</td></tr>
<tr><td>Prover($\boldsymbol{PK_{ABID}}, \boldsymbol{PK_{TDC}}, \boldsymbol{SK_S}$):

$R_{ABID} \leftarrow PRF(R_P, TDCMT)$
$CMT \leftarrow ABID_{CMT}(SK_S, R_{ABID}, A)$

IF
$TDC_{VF}(PK_{TDC}, TDCMT, CHA_V || R_C) = accept$
THEN
$RSP \leftarrow ABID_{RSP}(SK_S, CMT, CHA_V; R_{ABID})$
ELSE $RSP = \perp$</td><td>$\xleftarrow{TDCMT, A}$
$\xrightarrow{CMT}$
$\xleftarrow{CHA_V || R_C}$

$\xrightarrow{RSP}$</td><td>Verifier($\boldsymbol{PK}, \boldsymbol{A}$)
$CHA_V \leftarrow ABID_{CHA}(1^k)$
$TDCMT \leftarrow TDC_{CMT}(PK_{TDC}, CHA_V; R_C)$

$dec \leftarrow ABID_{VF}(PK_{ABID}, A, CMT, CHA_V RSP)$</td></tr>
</table>

Prover and Verifier engage in the identification protocol as follows:

1) Upon receiving an initialization message from Prover, Verifier first generates a commitment $TDCMT$ for his random challenge CH_V using the trapdoor commitment scheme's commit algorithm TDC_{CMT} and sends it to Prover along with the access policy A.
2) Prover evaluates $TDCMT$ and his own internal coins R_P with a pseudorandom function PRF and generates the salt R_{ABID}. This salt is used to generate his commitment CMT and is sent to Verifier.
3) Verifier then sends his random challenge CH_V and random coins R_C to Prover.
4) The Prover uses the trapdoor commitment scheme's public key PK_{TDC}, the Verifier's trapdoor commitment $TDCMT$, as well as the newly received challenge CHA_V and random coins from the Verifier R_C to reveal the commitment for verification.
5) If verification of the commitment is an $accept$, Prover will then calculate the response RSP for the ABID scheme and send it to the Verifier. Otherwise it aborts.
6) Verifier then outputs the decision on whether to accept the Prover's response or not.

Informally, the trapdoor commitment generated using a pre-determined challenge by the Verifier serves to fix the commitment value to be used by the Prover. Later on, when this pre-determined challenge is revealed as the challenge from the Verifier, the Prover then verifies that it was indeed the committed value by the Verifier before continuing with its response. If the Prover is reset to the commitment state, it cannot continue with a different challenge from the Verifier (which normally exposes the user secret key) due to the fact that the trapdoor commitment verification stage will fail.

The construction and provable security of a concrete scheme is currently a work-in-progress.

SECTION 4: CONCLUSION

In this paper, we provided a review of the security notions of reset-secure identification as well as ABID schemes. We also provided a brief survey of all the work currently done in both reset-secure identification schemes as well as attribute-based identification schemes. Then, we gave a generic construction to modify three-move ABID schemes to be reset secure. Future work would include providing detailed proof of security as well as a concrete construction as a case study for the transformation work.

ACKNOWLEDGEMENTS

This research is partially supported by Grants-in-Aid for Scientific Research (Research Project Number:25540004) by the Japan Society for the Promotion of Science and The Fundamental Research Project Scheme (No.: FRGS/2/2013/ICT07/MMU/03/5) by the Ministry of Education of the Government of Malaysia.

REFERENCES

1. Amos Fiat, Adi Shamir: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. CRYPTO 1986: 186-194
2. Uriel Feige, Adi Shamir: Witness Indistinguishable and Witness Hiding Protocols. STOC 1990: 416-426
3. Mihir Bellare, Marc Fischlin, Shafi Goldwasser, Silvio Micali: Identification Protocols Secure against Reset Attacks. EUROCRYPT 2001: 495-511
4. Adi Shamir: Identity-Based Cryptosystems and Signature Schemes. CRYPTO 1984: 47-53
5. Dan Boneh, Matthew K. Franklin: Identity-Based Encryption from the Weil Pairing. CRYPTO 2001: 213-229
6. Mihir Bellare, Chanathip Namprempre, Gregory Neven: Security Proofs for Identity-Based Identification and Signature Schemes. EUROCRYPT 2004: 268-286
7. Kaoru Kurosawa, Swee-Huay Heng: From Digital Signature to ID-based Identification/Signature. Public Key Cryptography 2004: 248-261
8. Pairat Thorncharoensri, Willy Susilo, Yi Mu: Identity-Based Identification Scheme Secure against Concurrent-Reset Attacks without Random Oracles. WISA 2009: 94-108
9. Sattam S. Al-Riyami, Kenneth G. Paterson: Certificateless Public Key Cryptography. ASIACRYPT 2003: 452-473
10. Massoud Hadian Dehkordi and Reza Alimoradi: Certificateless Identification Protocols from Super Singular Elliptic Curve. Security and Communication Networks, 2013.
11. Ji-Jian Chin, Raphael C.-W. Phan, Rouzbeh Behnia, Swee-Huay Heng: An Efficient and Provably Secure Certificateless Identification Scheme. SECRYPT 2013: 371-378

12. Ji-Jian Chin, Rouzbeh Behnia, Swee-Huay Heng, Raphael C-W. Phan: Cryptanalysis of a Certificateless Identification Scheme. Security and Communication Networks, 2014, 7, 4
13. Hiroaki Anada, Seiko Arita, Sari Handa, and Yousuke Iwabuchi: Attribute-based Identification: Definitions and Efficient Constructions. ACISP 2013, 168-186.
14. Hiroaki Anada, Seiko Arita, Kouichi Sakurai (a): Attribute-Based Identification Schemes of Proofs of Knowledge. SCIS2014, 3E3-3.
15. Hiroaki Anada, Seiko Arita, Kouichi Sakurai (b): Attribute-Based Signatures without Pairings via the Fiat-Shamir Paradigm. To appear in ASIAPKC2014.
16. Amit Sahai and Brent Waters: Fuzzy Identity-based Encryption. EUROCRYPT 2005, 457-473.
17. Brent Waters: Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient and Provably Secure Realization. PKC 2011, 53-70.
18. Ronald Cramer, Ivan Damgard, Jesper Buus Nielsen: Multiparty computation from threshold homomorphic encryption. EUROCRYPT 2001, 280-300.
19. Ran Canetti, Shafi Goldwasser, Oded Goldriech and Silvio Micali: Resettable zero-knowledge. Proceedings of the 32nd Annual Symposium on the Theory of Computing, ACM 2000.
20. Seiko Arita: A Constant-Round Resettably-Sound Resettable Zero-Knowledge Argument in the BPK Model. IEICE Transactions 2012, 95-A (8): pp. 1390-1401.