# 博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

**論文題目**　：　A Study on Efficient Identification Schemes Secure against Concurrent Man-in-the-Middle Attacks

**申請者**　：　穴田 啓晃

**審査委員会**　：　主査　教授　有田 正剛
副査　教授　松尾 和人
副査　教授　佐藤 直
副査　准教授　國廣 昇　（東京大）

## Ⅰ．論文内容の要旨

博士後期課程学生、穴田啓晃君の博士請求論文は“A Study on Efficient Identification Schemes Secure against Concurrent Man-in-the-Middle Attacks（同時発生的中間者攻撃に対し安全な効率的認証スキームの研究）”と題し、８章から成っている。

第１章“Introduction”では、本論文の研究の背景や動機を述べている。まず背景として、システムやサービスへのログインにおいて、パスワード（秘密鍵）に基づくユーザ認証が広く行われているが、盗聴やフィッシングの脅威の下では、なりすましの危険が実際にあることを述べ、公開鍵の枠組みに基づくユーザ認証（認証スキーム）が必要であることを説明している。更に、昨今のネットワーク環境においては、このような認証スキームに対し、同時発生的中間者攻撃と呼ばれる攻撃、すなわち、同一秘密鍵をもつ複数のアプリケーションが同時に認証サーバにアクセスする状況における中間者攻撃が、脅威となっていることを指摘し、本研究の動機を説明している。続いて、認証スキームの先行研究においては、基本的ツールとしてΣプロトコル（知識証明の一種）を用いてきたが、このアプローチでは効率性を維持しつつ同時発生的中間者攻撃に対する耐性を持たせることは困難であることを指摘している。以上を踏まえて、本研究においては、チャレンジ＆レスポンス型方式によるアプローチを採用し、特に、鍵カプセル化機構 KEM（Key Encapsulation Mechanism）をチャレンジ＆レスポンス型方式で利用することによって、同時発生的中間者攻撃に対して安全でかつ効率性の高い認証スキームを具体的に構成することに成功したことを説明している。

第２章“Preliminaries”では、認証スキームの数学的な記述に必要となる事項を準備し、続いて、提案認証スキームの安全性の根拠となる、Computational Diffie-Hellman 問題等の、計算量的な数論的難問を記述している。

第３章“The Models of ID Schemes, Attacks and Security Proofs”では、認証スキームを数学的に定式化した上で、認証スキームに対する、同時発生的中間者攻撃等の攻撃シナリオを数学的にモデル化し、認証スキームの安全性を厳密に定義している。

第４章“A Survey of Previous works on ID Schemes”では、先行研究の調査を行い、それらにおいてはもっぱらΣプロトコルに基づく認証スキームが対象とされてきたことを、複数の代表的スキームの具体的記述を通して、確認している。そして、同時発生的中間者攻撃に耐性を持たせるために、それらΣプロトコルに基づく認証スキームはその効率性をおおきく損なってしまっている状況を説明している。

第 5 章“A Generic Conversion from KEM to ID Scheme”では、鍵カプセル化機構 KEM を数学的に定式化した上で、KEM を認証スキームに変換する一般的変換方法を提案している。更に、その変換において、KEM の安全性が認証スキームの安全性にどのように反映されるかを考察し、注目すべき成果として、従来研究で KEM に対する目標とされてきた「選択暗号文攻撃における識別不可能性」は、認証スキームを構築する上では過剰であって、より弱い安全性である「選択暗号文攻撃における一方向性」が認証スキームを構築する上では必要十分であることを示し、これが第 6 章に示す、認証スキームの具体的構成の鍵となることを示唆している。

第 6 章“A Series of Concrete ID Schemes from KEMs”では、前章の一般的変換を活用し、「選択暗号文攻撃における一方向性」の安全性を持つ KEM を構成することにより、同時発生的中間者攻撃に対して安全でかつ効率性の高い認証スキームを具体的に構成している。まず出発点として、従来よりよく知られていた ElGamal KEM に注目し、それが実は、非常に強い仮定を必要とするものの、同時発生的攻撃に対し安全であること、しかしながら、中間者攻撃には脆弱であることを示している。そこで、本研究は ID ベース暗号等で用いられる tag フレームワークに注目し、それを KEM に導入し、tag を用いて複数セッションを分離することで、ElGamal KEM を同時発生的中間者攻撃に対しても安全な KEM へと変換できることを示している（定理 6.2)。さらに、CHK 変換、Target Collision Resistant ハッシュ関数、双子 Diffie-Hellman といった先行技術を応用することによって tag フレームワークからの自立を図り、ついには、tag に依存しない一般的フレームワークにおいて効率性を損なうことなく同時発生的中間者攻撃に対し安全な認証スキームの構築に成功している（定理 6.3 から定理 6.5)。このような一連の変換の成功は、目標とする安全性が選択暗号文攻撃における識別不可能性ではなく、より弱い、選択暗号文攻撃における一方向性であることに強く負っているとしている。

第 7 章“Efficiency Comparison”では、先行研究の認証スキームの効率と、本論文の提案する認証スキームの効率とを、具体的にそれらの演算コストやメッセージコストを数え上げることによって比較し、同時発生的中間者攻撃に対する安全性を達成する認証スキームの中では、本研究の提案する認証スキーム群が最も高い効率性をもつことを示している。

第 8 章“Conclusions”では、本論文の研究成果を要約し、第 1 章で説明した問題を解決したことを述べている。

## Ⅱ. 論文審査結果の要旨

本論文は、昨今のネットワーク環境において脅威となっている同時発生的中間者攻撃に注目し、選択暗号文攻撃における一方向性をもつ KEM を構成した上でそれを認証スキームに変換するという新たなアプローチにもとづいて同時発生的中間者攻撃に対し安全でかつ効率性の高い認証スキームの構築に成功したものであって、情報学並びに情報社会の発展に貢献するところが大きい。よって、本論文は情報学における博士論文として十分価値のあるものと認める。

## Ⅲ. 審査経過

本審査委員会は、平成 24 年 1 月 24 日に論文内容とこれに関連する事項について口述試問を行い、その後、平成 24 年 2 月 22 日にこれに関連する事項の最終試験審査を実施し、申請者が学位取得にふさわしい知見を持つものと判断した。