修 士 論 文 の 和 文 要 旨

大学院　電気通信　学研究科　　博士前期課程　情報通信工学　　専攻		
氏　　名	ｻﾝﾄｿ　ﾊﾞｸﾞｽ SANTOSO BAGUS	学籍番号 0330022
論　文　題　目	Comprehensive Optimal Security Proof for Probabilistic Full Domain Hash under Strong Existential Unforgeability	

要　　旨

Goldwasser らはデジタル署名の安全性を段階的に分類し定式化した．デジタル署名の最も高い安全性の定義として「適応的選択文書攻撃に対して存在偽造すら不可能」(*existential unforgeability under adaptive chosen message attack (eUF-ACMA)*) が提案された．現在，使用されているデジタル署名方式は確定的署名方式(*Unique Signature Scheme*) と確率的署名方式(*Probabilistic Signature Scheme*) の二つの方式に分類できる．従来の研究結果によって確率的署名方式が満たすべき安全性レベルはeUF-ACMA よりも厳しいということが明らかになった．その安全性モデルは「適応的選択文書攻撃に対して強存在的偽造すら不可能」(*strong existential unforgeability under adaptive chosen message attack*(sUF-ACMA)) と呼ばれている．現在まで，eUF-ACMA で安全性証明が付いた確率的署名方式がsUF-ACMA を満たすかどうかはまだ知られていない．
本研究では，基本的な確率的署名方式であるPFDH (Probabilistic Full Domain Hash) において,eUF-ACMA での最適な安全性証明とsUF-ACMA での最適な安全性証明の関係についての厳密な評価を行った．両方の安全性モデル(eUF-ACMA とsUF-ACMA) における最適安全性証明の関係を明らかにするには我々は最適な安全性証明を再定義した．また，効率的にsF-ACMA(sUF-ACMA の攻撃モデル) 攻撃者をeF-ACMA(eUF-ACMA の攻撃モデル) 攻撃者に変換する新技法を開発した．その結果，次の定理を証明できた．

■**定理**　eUF-ACMA (弱い安全性) において帰着率上界関数h に対して最適な帰着アルゴリズムが存在するならば，sUF-ACMA (強い安全性) において帰着率上界関数h に対して最適な帰着アルゴリズムが存在する．但し,h はどの安全性パラメータにおいても必ず計算可能な最大値を持つような関数とする．

発表論文

[1] B. Santoso and K. Ohta. Concrete Argument on the Optimal Security Proof for PFDH. In *Symposium on Cryptography and Information Security*, 2005.
[2] B. Santoso, K. Ohta, and N. Kunihiro. Optimal Security Proof of PFDH under Existential Unforgeability against Strong Adaptive Chosen Message Attack. Technical report, Technical Group on Information Security (ISEC), July 2004.