論文の内容の要旨

論文題目 Efficient Constructions of Cryptographic Schemes and Generic Techniques for Security Enhancement
(効率的な暗号方式の設計と，安全性を高めるための汎用的技術の研究)

氏　　名 山田翔太

暗号理論において，より効率的で，より安全な暗号方式を設計することは，中心的な研究課題である．本研究では，既存方式の効率性を改良し，また，既存方式の安全性を向上する方法を提案した．

効率的な暗号技術の研究

まず，前者に関して得られた結果について説明する．本研究では，特に，安全で効率的な電子署名方式に焦点をあてて研究を行った．電子署名は，物理的な印鑑の電子的な類似で，文書の統合性を保証する．電子署名の効率は，公開鍵長，署名長，秘密鍵長，署名アルゴリズムと検証アルゴリズムの計算効率で測られる．特に，通信におけるデータサイズの制約が厳しい状況でも用いることができることから，署名長の短い電子署名方式は非常に有用であり，そのような方式の実現に向けて多くの研究がなされてきた．Hofheinz らによる近年の研究(Asiacrypt2011)では，楕円曲線を用いた場合，わずか 200 ビット程度，RSA 合成数を用いた場合も 1074 ビット程度の署名長の安全な電子署名方式の設計が可能であることが示されている．一方，彼らの提案方式は，全て公開鍵長が非常に長い．例えば，楕円曲線を用いた場合には，３メガバイトもの公開鍵長が必要である．これほど公開鍵が長いと，公開鍵をダウンロードするだけでも長い時間が必要になってしまい，非効率的な場合があると考えられる．彼らの方式の中では，カバーフリーファミリー(cover free family)と呼ばれる組み合わせ論的な技術が用いられている．カバーフリーファミリーは，有用な性質を持つため，暗号理論の様々な文脈で利用されてきた．彼らの研究では，カバーフリーファミリーを用いて，プログラム可能ハッシュ関数（programmable hash function）

という暗号学的要素技術を構成し, さらにそれを用いて電子署名方式を設計するという手順で方式が設計されている．彼らの方式において，非常に長い公開鍵が必要となる原因は，このプログラム可能ハッシュ関数が，非常に長い公開パラメータを必要とするためである．

本研究では，プログラム可能ハッシュ関数を用いる代わりに，q 回使い捨て署名(q-times signature)と，弱安全署名(weakly secure signature)を組み合わせることによって，従来よりも効率的で，実用に十分な安全性と考えられている存在的偽造不可能性(Existential unforgeability)を達成しているような電子署名方式を構成できる可能性があることを考察した．また, 以下に説明するように, この設計方針にしたがって, 新しい電子署名方式を複数提案した．これは, 従来の一回使い捨て署名(one-time signature)と, 弱安全署名(weakly secure signature)を組み合わせることで, 存在的偽造不可能な電子署名方式を構成できるという既存の結果の拡張と考えることができる．Hofheinz らは，楕円曲線を用いた場合，RSA 合成数群を用いた場合に関して，電子署名方式を提案しているが，我々はそれぞれに関して，対応する改良方式を提案している．

まず，楕円曲線を用いた場合に関しては，楕円曲線上の双線型写像の性質と，カバーフリーファミリーの二次元的利用法という本研究で新しく開発した技法を組み合わせることにより q-耐性を持つ ID ベース暗号(q-resilient identity-based encryption)という要素技術で，暗号文長，公開鍵長がともに短いような方式を設計することができることを示した．また，この q-耐性を持つ ID ベース暗号に，Canetti-Halevi-Katz 変換と呼ばれる変換を適用することで，q-制限付き選択暗号文攻撃(bounded chosen ciphertext attack)の下で安全な公開鍵暗号方式を得ることができる．この方式は，従来の同じ安全性を達成している Cramer らの方式(Asiacrypt 2007)と比較すると，暗号文長を保ったまま，公開鍵長を大幅に削減している．また，上記の q-耐性を持つ ID ベース暗号に対して，Naor 変換と呼ばれる変換を適用すると，新しい q 回使い捨て署名(q-times signature)を得ることができ，この方式もまた，同様の安全性を達成している電子署名方式に比べ，公開鍵長が短くなっている．さらに，この q 回使い捨て署名を，既存の弱安全署名と，代数的な性質を利用して組み合わせることによって，Hofheinz らの方式に比べ，署名長は同じで, 公開鍵長を 1/100 以下に削減したような, 新しい電子署名方式を得ることに成功した．

上記で開発した手法は，双線型写像の性質に強く依存しており，RSA 合成数群を用いた場合には簡単に適用できない．RSA 合成数群を使った場合に関しては，疑似ランダム関数の性質を利用して，公開鍵長が非常に短い q 回使い捨て署名を設計し，これを既存の弱安全な電子署名方式と組み合わせるこという方法で，新しい電子署名方式を提案した．我々の提案方式は，上記の Hofheinz らの方式に比べ，公開鍵長を典型的なパラメータの下で，1/20000 程度にまで削減することに成功している．一方，我々の提案方式も，彼らの方式も，署名アルゴリズムの中で，複数回の素数生成が必要であり，このステップにはかなりの計算量が必要であるため，未だに十分

に実用的であるとは言えない．十分に実用的な，RSA 問題に基づくような電子署名方式の設計は今後の課題である．（なお，我々の研究成果の発表後に発表された Böhl らによる結果(Eurocrypt2013)は，この方向への著しい進展である．）

より安全な暗号技術の研究

ここまで，効率的な暗号方式の設計に関して得られた結果について述べてきたが，次に，もう一つの非常に重要な研究の方向性である，より安全な暗号方式の設計に関して，得られた結果に関して述べる．特に，本研究では，選択暗号文攻撃に対して安全な述語暗号の研究に焦点をあてた．選択暗号文攻撃とは，攻撃目標とする暗号文以外の任意の暗号文を復号する神託機械へのアクセスが許されている状況での攻撃を指している．そのような攻撃は，現実には実行不可能であると考えられていたが，Bleichenbacher (Crypto1998)が，暗号方式の標準規格である PKCS ＃1 に対して，類似の攻撃が可能であることを示して以来，選択暗号文攻撃に対する耐性は，公開鍵暗号の安全性要件として，必須であると考えられるようになった．一方，述語暗号とは，公開鍵暗号や，ID ベース暗号の拡張であり，暗号文に対応する平文へのきめ細かいアクセス制御を可能にする技術である．過去の研究では，放送型暗号，属性ベース暗号，内積述語暗号などの述語暗号が提案されてきた．

既存研究では，よりきめ細かいアクセス制御を達成した述語暗号の研究が重視されており，選択暗号文攻撃のようなより高い安全性を達成した述語暗号の提案は少ない．つまり，従来研究で提案された多くの方式は，一部を除いて，より弱い安全性である選択平文攻撃に対する安全性しか示されていない．本研究では，検証可能性という性質と，いくつかの自然な性質を持つような，選択平文攻撃に対して安全な述語暗号を，選択暗号文攻撃に対して安全な述語暗号に汎用的に変換する手法を提案した．また，従来研究で提案された多くの述語暗号が，検証可能性を持っているか，あるいは持つように変形できることも示した．これらの結果によって，新しい選択暗号文攻撃に対して安全な述語暗号を複数得ることができる．類似の既存研究として，山田らによる，選択暗号文攻撃に対して安全な属性ベース暗号の一般的構成法(PKC2011)と花岡らによる，選択暗号文攻撃に対して安全な放送型暗号(Asiacrypt2008)の一般的構成法が知られているが，これらの成果は，本研究よりも適用範囲が狭いものである．

さらに，我々は，匿名否認可能述語認証という新しい要素技術を定義し，上記の変換により得られた述語暗号を利用することでこれを構成することが可能であることを示した．匿名否認可能述語認証方式は，検証者が，証明者の属性がある条件を満たすこと以外の情報は一切得られないという性質をもつ認証方式である．さらに，証明者は，検証者と過去に通信した事実を否認することができるという特徴を持つ．この方式は，内部告発などを安全に行うために有用であると考えられる．