社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

公開鍵暗号研究の動向

岡本龍明
okamoto@sucaba.isl.ntt.jp
NTT 情報通信研究所
〒239 神奈川県横須賀市光の丘 1-1, NTT R&D センタ 609A

あらまし まず、認証実用化実験協議会暗号技術研究タスクフォースにおける公開鍵方式に関する研究内容の概略を紹介する。さらに、それに関連して、実用的でかつ安全性の証明のついた公開鍵暗号方式の研究動向について述べる。

和文キーワード 認証実用化実験協議会、公開鍵暗号、安全性の証明

On the Research of Public-key Cryptosystems

Tatsuaki Okamoto
okamoto@sucaba.isl.ntt.jp
NTT Laboratories
1-1 Hikarinooka, Yokosuka-shi, Kanagawa, 239 Japan

Abstract First, we briefly introduce the research activities of the crypto TF of ICAT, regarding public-key cryptosystems. We then describe provably secure and practical public-key cryptosystems, which are related to some cryptosystems of the crypto TF.

英文 key words ICAT, public-key cryptosystems, provably secure

1 ICAT 暗号技術研究 TF における公開鍵方式の研究

ICAT の暗号技術研究 TF における公開鍵方式の研究としては、独自の暗号・署名方式の提案ならびにその評価を行なうとともに、広域 TF に提供する暗号・署名ツールを作成する予定である。独自暗号方式の評価用には、PARIS を用いて評価用ソフトウェアを作成しそれら方式間の速度比較等を行なう。一方、広域 TF に提供する暗号・署名ツールとしては、gmp を用いて作成する。このツールで今回提供する方式は、楕円暗号・署名方式とするが、インターフェースは、将来の拡張を考慮してある程度一般性のあるものを定める予定である。以下、その内容を簡単にまとめる。（各提案方式の詳細については、本ワークショップの他講演でそれぞれ紹介される予定である。）

- 各種暗号・署名方式の開発ならびに評価用ソフトウェア（PARIS ベース）の作成を行なっている。
  - ナップザック問題などに基づく公開鍵暗号方式の提案・安全性評価
  - 変形 ElGamal 署名の提案・安全性評価
  - Message-Recovery 署名の提案・安全性評価
  - PSSS(Provably Secure Signature Scheme) 署名の提案・安全性評価
- 楕円暗号方式（ElGamal 暗号・DSA 署名）ソフトウェアの作成（gmp ベース）：広域タスクフォース提供用

2 安全性の証明のついた実用的公開鍵暗号方式の研究動向

1976 年の Diffie と Hellman による公開鍵暗号の発見以来、多くの方式の提案が行なわれてきた。その歴史は、提案と解読の繰り返しだけではなく、解読されそうにない（安全性が基本的な問題と同等であることが証明された）暗号をいかに作るかの試みも数多く行なわれてきた。その中でも、最近注目を集めている方式が、「実用性が高く」かつ安全性に保証のある方式である。ここでは、このような方式を簡単に紹介しよう。最初に暗号方式について、その後ディジタル署名方式について述べる。いずれにおいても、「仮想的なランダム関数」が重要な役割を果たす。

2.1 公開鍵暗号

2.1.1 安全性の定義

暗号は攻撃者（盗聴者）に通信内容を隠して送ることを目的とするためどの程度通信内容を隠しているかの度合いが重要である。

一方、攻撃者のタイプには単に暗号通信を受信しそれだけから解読を試みる受動的攻撃と、送信者に様々な質問をし（暗号文を送り）その回答（その復号結果）をもらうことが許され、そこで得られた情報を利用して目的とする暗号文の解読をするような能動的攻撃がある。能動的攻撃としては、適応選択暗号文攻撃 (adaptive chosen ciphertext attack) が最も強力な攻撃である。

さらに、暗号文から平文の内容を知ることはできないが、暗号文を操作することにより、対応する平文に意図的な変更を加えることができるかもしれない。（例えば、平文をビット反転させるなど）このようなことが一切できないことを頑強性（non-malleable 性）とよぶ。

以上の観点より、公開鍵暗号の安全性はつぎのように整理できる。

- 秘匿性
  - 完全解読：暗号文より平文が完全に求められること。
  - 部分解読：暗号文より平文の部分情報が求められること。例えば、平文のある 1 ビットが求められる。ここで、解読の対象となる 1 ビットは、平文の最上位ビットなどの特定の位置の 1 ビットの場合だけでなく、平文のヤコビ記号の値などの関数値の 1 ビットである場合もある。

    ここで、どのような部分解読も困難なとき、強秘匿 (semantically secure [6]) とよぶ。
- 攻撃法[1]
  - 暗号文攻撃 (ciphertext-only attack: 暗号文だけを利用する攻撃)
  - 選択暗号文攻撃 (chosen-ciphertext attack: 解読者が任意に選んだ暗号文を真の受信者に復号させた後に，そこで得た情報と公開情報を用いて，別の暗号文を復号する攻撃)

[1] 秘密鍵暗号の場合は、さらに既知平文攻撃と選択平文攻撃が存在するが、公開鍵暗号では、攻撃者が公開鍵より自ら多くの既知平文対ならびに選択平文に対する暗号文を作ることができるため、これらの攻撃は暗号文攻撃と等価である。

- 頑健性

  どのような関係 f に対しても、攻撃者が $c = E(m)$ から $m' = f(m)$ を満足するような $c' = E(m')$ を作成できなければ、頑健 (non-malleable) であるとよぶ。（ここで、E は公開の暗号化関数である。）

したがって，最も安全な公開鍵暗号は，攻撃者に選択暗号文攻撃を許したとしても，強秘匿でありかつ頑健性を保持した方式である．以下では、そのような公開鍵暗号を「安全な」公開鍵暗号と呼ぶ。

2.1.2 「安全な」公開鍵暗号方式

「安全な」公開鍵暗号としては、ゼロ知識証明を用いた方式が提案されているが決して実用的とは言えない [5, 4]。そこで、ある程度強い仮定を前提にしても、実用性の高い安全性の証明のついた「安全な」方式があればそのような方式は大変重要である。

このような要求に答えたものが、Bellare と Rogaway による OAEP (Optimal Asymmertric Encryption Padding)[2] である。彼らの方式は、仮想的なランダム関数の仮定を前提にして効率的で安全性の証明のついた「安全な」方式となっている。この方式は、仮想的なランダム関数を実用的なハッシュ関数に置き換えると実用的な構成が可能となる。このような実用的構成では、安全性は理論的に保証されないが、仮想的な場合での安全性の保証が一種の保険の役割を果たしている。このような構成法は、RSA 法に基づく OAEP (Optimal Asymmertric Encryption Padding) が標準的な電子決済プロトコル SET でも用いられている。

2.2 ディジタル署名

2.2.1 安全性の定義

ディジタル署名に関する安全性は、2つの観点から考えることができる。1つは、どのような偽造ができるかという観点であり、もう1つが攻撃者にどのような攻撃法を許すかという観点である。

まず最初の観点では、偽造できるレベルで次のような安全性（偽造困難性）が存在する。

1. **一般的偽造不可 (universally unforgeable)** 署名の偽造ができない文書が存在する。

2. **偽造不可 (selectively unforgeable)** ある決められた文書以外に対しては署名の偽造ができない。

3. **存在的偽造不可 (existentially unforgeable)** どのような文書に対しても署名の偽造ができない。

2つ目の観点では、次のような攻撃法が存在する。

1. **受動攻撃 (passive attack; key-only-attack** 公開鍵だけを使って偽造を行なう。

2. **一般選択文書攻撃 (generic chosen-message attack)：** 署名偽造者が前もって選んだ文書に対して真の署名者に署名させた後に、そこで得た情報を用いて第三の文書の署名を偽造する攻撃である．

3. **適応的選択文書攻撃 (adaptively chosen-message attack)：** この攻撃法は，署名偽造者が任意に選んだ文書に対して真の署名者に署名させた後に，そこで得た情報を用いて第三の文書の署名を偽造する攻撃である．

従って、最も安全なディジタル署名法は、適応的選択文書攻撃に対して存在的偽造不可な署名法である [7]。以下では、このようなディジタル署名法を単に「安全な」ディジタル署名法とよぶ。

2.2.2 「安全な」ディジタル署名方式

素因数分解問題が困難である（より一般的には、クローフリー（claw-free）関数対が存在する）という仮定のもとで、「安全な」署名法の構成法が示されている [7]。その後，仮定を一般化する試みがなされ，Bellare と Micali が一方向性落とし戸置換の存在を仮定した「安全な」署名方式を，Naor と Yung，さらに Rompel が一方向性関数の存在のみを仮定した方式を提案した [1, 8, 11].

しかし実用的な観点では、上記の方式は効率が悪く、実用的とは言えない。実用的で上記の意味での安全性の証明の付いた「安全な」方式としては、以下のような方式がある。

まず、仮想的なランダム関数を前提にすれば、RSA 関数や ESIGN 関数の解読が困難であると仮定して、RSA 署名法や ESIGN 署名法が「安全」であることが証明できる [3]。

さらに、仮想的なランダム関数を前提にすれば、素因数分解や離散対数問題が困難であると仮定して拡張 Fiat-Shamir 署名や Schnorr 署名（さらに改良 ElGamal 署名）が「安全」であることが証明できる [10]。

一方、仮想的なランダム関数よりも弱い仮定である無相関一方向性関数（correlation-free one-way hash function）を仮定すれば素因数分解や離散対数問題が困難であると仮定して Fiat-Shamir 署名や PSSS 署名方式が「安全」であることが証明できる [9]。

3 今後の課題

上で示したように、仮想的なランダム関数を前提とすれば、安全性の証明の付いた暗号・署名方式を実現することは比較的容易であることが分かってきた。実際には、そのようなランダム関数は実現不可能であり、実用的ハッシュ関数で代用して構成する。このとき、実用的な構成に対する安全性は未知となる。

従って、これからの大きな研究課題としては、仮想的なランダム関数といった非現実的な仮定ではなく、実用的にフィーシブルな仮定に基づき、「安全な」実用的公開鍵暗号方式・ディジタル署名方式を実現することであろう。

References

[1] Bellare, M. and Micali, S.: How to Sign Given Any Trapdoor Function, Proceedings of 21st Annual ACM Symposium on Theory of Computing, pp.32–42 (1989).

[2] Bellare, M. and Rogaway, P. : Optimal Asymmetric Encryption, Proc. of Eurocrypt' 94, LNCS 950, Springer–Verlag (1994).

[3] Bellare, M. and Rogaway, P. : The Exact Security of Digital Signatures – How to Sign with RSA and Rabin, Proc. of Eurocrypt'96, LNCS 1070, Springer–Verlag, pp.399–416 (1996)

[4] De Santis, A. and Persiano, G.: Communication Efficient Zero-Knowledge Proofs of Knowledge (with Applications to Electronic Cash) Proceedings of STACS 92, pp. 449-460 (1992).

[5] Dolev, D., Dwork, C. and Naor, M.: Non-Malleable Cryptography, Proc. of STOC, pp.542–552 (1991).

[6] Goldwasser, S. and Micali, S.: Probabilistic Encryption, JCSS, Vol.28, No.2, 1984, pp.270-299.

[7] Goldwasser, S., Micali, S. and Rivest, R.: A Digital Signature Scheme against Adaptive Chosen Message Attack, *SIAM Journal on Computing*, Vol.17, No.2, pp.281–308 (Apr., 1988).

[8] Naor, M. and Yung, M.: Universal One-Way Hash Functions and Their Cryptographic Applications, Proc. of STOC, pp.33–43 (1989).

[9] Okamoto, T.: Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes, Proceedings of Crypto 92, pp. 31-53 (1993).

[10] Pointcheval, D. and Stern, J.: Security Proofs for Signature Schemes, Proc. of Eurocrypt'96, LNCS 1070, Springer–Verlag, pp.387–398 (1996)

[11] Rompel J. : One-Way Functions are Sufficient for Secure Signatures, Proceedings of 22nd Annual ACM Symposium on Theory of Computing, pp.387–394 (1990).