■1 群（信号・システム） - 3 編（暗号理論）

6 章 ディジタル署名

（執筆者：藤崎英一郎）

■概要■

【本章の構成】

■1 群 - 3 編 - 6 章

6-1 ディジタル署名の概要

（執筆者：藤崎英一郎）[2009 年 2 月 受領]

ディジタル署名は，電子文書の正当性を公開の検証手段によって保証する技術である．ディジタル署名では，公開鍵暗号同様，署名者が自分の検証鍵（公開鍵）pk と署名鍵（秘密鍵）sk を作成し，検証鍵を公開し署名鍵は秘密に保持する．署名者は，署名鍵 sk を用いて電子文書 m の署名 σ を生成する．(m, σ) を入手した検証者は，σ が m の正当な署名であるかを署名者の検証鍵 pk を用いて検証できる．

ディジタル署名 σ が電子文書 m の正当な署名であると検証されるならば，電子文書は署名者以外の第三者により改ざんされていないことが保証される．同時に，署名生成者は検証鍵を公開した署名者に限定され，ひとたび署名をした後，署名者はその事実を否認できなくなる．

暗号学的には，ディジタル署名は三つのアルゴリズムの組 $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ として，次のように定義される：

- 鍵生成アルゴリズム Gen: セキュリティパラメータ 1^k ($k \in \mathbb{N}$) を入力としてとり，検証鍵，署名鍵の組 (pk, sk) を出力する（k に関する）確率的多項式時間アルゴリズム．この (pk, sk) を出力する試行を $(pk, sk) \leftarrow \mathsf{Gen}(1^k)$ と書く．

- 署名生成アルゴリズム Sig: 署名鍵 sk と平文 $m \in \{0,1\}^*$ を入力としてとり署名 σ を出力する（入力長に関する）確率的多項式時間アルゴリズム．この署名を生成する試行を $\sigma \leftarrow \mathsf{Sig}_{sk}(m)$ と書く．

- 署名検証アルゴリズム Ver: 検証鍵 pk と平文 m，署名 σ を入力としてとり，ビット $b \in \{0,1\}$ を出力する（入力長に関する）多項式時間アルゴリズム．ここで，ビット b は，平文 m に対する署名 σ の正当性を判断する指標である．例えば，Ver が，σ を m の正しい署名と判断した場合は 1 を，正しくない署名と判断した場合は 0 を出力するように b は定められる．

これらの三つのアルゴリズムは，（十分大きな）すべての k で，$\mathsf{Gen}(1^k)$ の出力する可能性のあるすべての (pk, sk)，すべての $m \in \{0,1\}^*$，$\mathsf{Sig}_{sk}(m)$ の出力する可能性のあるすべての σ に対して，常に $\mathsf{Ver}_{pk}(m, \sigma) = 1$ を満たす．

上記は，あくまでディジタル署名アルゴリズムの機能を定義したものであり，この機能のみでは，我々がディジタル署名に期待する電子文書の正当性や否認防止性などの性質を保持していない．

暗号学では，まずアルゴリズムの機能を定義し，次に安全性の定義で，好ましい満たすべき性質を厳密に定義するのが通例である．次節でディジタル署名の満たすべき安全性の定義を示す．

■1 群 - 3 編 - 6 章

6-2 ディジタル署名の安全性の定義

（執筆者：藤崎英一郎）[2009 年 2 月 受領]

Goldwasser, Micali, Rivest は，ディジタル署名に対する攻撃者の目標と攻撃環境を整理して，ディジタル署名の安全性クラスを定義した [21].

ディジタル署名の安全性は，ディジタル署名への攻撃の種類に応じて定義される．ディジタル署名への攻撃は，攻撃者の「攻撃のシナリオ」と「偽造のレベル」の二つの異なる軸の組合せで定義できる．そのような攻撃に対して安全なディジタル署名の集合は，安全性クラスを定義する．

このようにディジタル署名の安全性クラスは攻撃の種類に応じて複数存在するが，本稿では，（適応的）選択文書攻撃（(adaptive) chosen message attack）（攻撃のシナリオ）での存在的偽造（existential forgeability)）という偽造を考える．（適応的）選択文書攻撃に対して存在的偽造不可な署名方式からなる安全性のクラスは EUF-CMA（existential unforgeability against chosen message attacks）と呼ばれる．通常，ディジタル署名が安全であるというときは，その署名方式が選択文書攻撃に対して存在的偽造不可（EUF-CMA）であるときをいう．より詳細には次のように定義する．

ディジタル署名 $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ を攻撃する次のような攻撃者 A を考える．A は検証鍵 pk をとり，署名アルゴリズム Sig_{sk} に $q(k)$ 回まで質問することができる（A の戦略に沿って適応的につくられた文書に署名アルゴリズム Sig_{sk} が署名をする）．A の Sig_{sk} へ質問した文書の集合を $\mathcal{M}$ とする．A が最終的に $\mathcal{M}$ に含まれない文書とその署名を出力してきた場合，偽造成功とする．A のディジタル署名 Σ に対する偽造成功確率を $\mathsf{Adv}^{\Sigma}_{A}(k) \triangleq$

$$\Pr[(pk, sk) \leftarrow \mathsf{Gen}(1^k); (m, \sigma) \leftarrow A^{\mathsf{Sig}_{sk}}(pk) : \mathsf{Ver}_{pk}(m, \sigma) = 1 \wedge m \notin \mathcal{M}]$$

によって定義する．上記確率は，$\mathsf{Gen}, \mathsf{Sig}, A$（の内部乱数）に依存して決定される．

任意の $t(k)$-時間アルゴリズムの攻撃者 A に対して，十分大きなすべての k で，$\mathsf{Adv}^{\Sigma}_{A}(k) \leq \epsilon(k)$ が成立するとき，ディジタル署名 Σ は，$(t(k), q(k), \epsilon(k))$-EUF-CMA であるという．

$\epsilon(k) : \mathbb{N} \to \mathbb{R}$ がどんな多項式 k^{-c} より早く 0 に収束するとき，$\epsilon(k)$ を無視できる関数という．$t(k), q(k)$ が（k に関して）多項式制限で，$\epsilon(k)$ が（k に関して）無視できる関数であるとき，ディジタル署名 Σ は，「適応的選択文書攻撃に対して存在的偽造不可（EUF-CMA）」であるという．

■1 群 - 3 編 - 6 章

6-3 ディジタル署名の歴史

（執筆者：藤崎英一郎）[2009 年 2 月 受領]

6-3-1 公開鍵暗号，ディジタル署名の発見

1976 年，スタンフォード大学の Diffie と Hellman により，画期的な論文 [11]が発表された．彼等はその論文の中で，現在の公開鍵暗号とディジタル署名の概念，及び公開鍵暗号の構成法として現在の Diffie-Hellman 鍵配送方式を提案した．同時期カリフォルニア大学バークレイ校の Merkle が独立に（公開）鍵配送の問題を考えていたが [29]，彼等は問題の本質が同じであることに気がつき，Merkle と Hellman は独自に新たな鍵配送方式を発表している [30]．

Diffie, Hellman, Merkle は，ディジタル署名の概念は示したが，その具体的な構成法は提案しなかった．最初にその具体的な方式を提案したのは，MIT の Rivest, Shamir, Adleman である [37]．その提案方式は，発明者の頭文字を取って RSA と呼ばれる．RSA は，公開鍵暗号でありかつディジタル署名にも利用できる．やはりほぼ同時期に，Rabin により Rabin 暗号・署名が提案されている [36]．現在では，RSA や Rabin は公開鍵暗号・署名ではなく，素因数分解問題に基づく落し戸つき一方向性関数（置換）の構成例とみなされている．

公開鍵暗号とディジタル署名は，落し戸つき一方向性置換を介すことで，次のような表裏の関係として理解できる．f を落し戸つき一方向性置換とする．すなわち，f と，$x \in \{0,1\}^k$ が与えられたとき，$f(x)$ を計算するのは容易であるが，f と $y \in \{0,1\}^k$ が与えられても，$f^{-1}(y)$ を計算することは困難であるような関数のことである．$pk = \{f\}, sk = \{f^{-1}\}$ とすると，f を暗号化関数，f^{-1} を復号関数とする公開鍵暗号が自然に定義できる．次に $H : \{0,1\}^* \to \{0,1\}^k$ を衝突発見困難なハッシュ関数とする．ハッシュ関数 H が与えられたとき，$H(x) = H(x')$ なる $x \neq x' \in \{0,1\}^*$ を見つけ出すことが困難であるならば，H を衝突発見困難（collision-resilient）と呼ぶ．このとき，署名生成アルゴリズム $\mathrm{Sig}_{sk}(m) \triangleq f^{-1}(H(m))$，署名検証アルゴリズム Ver を $\mathrm{Ver}_{pk}(m,\sigma) = 1 \Leftrightarrow$ "$f(\sigma) = H(m)$" と定義することで，ディジタル署名が定義できる．このように公開鍵暗号とディジタル署名は落し戸つき一方向性置換を介して深く関係している．

6-3-2 もう一つの公開鍵暗号発見の歴史

英国政府通信本部（British Government Communications Headquarters（GCHQ））の（主に Cocks による）いくつかの文書によれば，GCHQ は，Diffie, Hellman や，Rivest, Shamir, Adleman に先駆けて既に公開鍵暗号に関する重要な発見をしていた．

Cocks が，暗号の国際会議 EUROCRYPT 2008 の招待講演で語ったことによれば，1969 年の時点で既に同組織の研究者であった Ellis が，公開鍵暗号と等しい概念を考えていた．また 1973 年に Cocks 自身が，RSA 暗号とほぼ同一の方式を発明しており，1976 年には，同 GCHQ の Williamson が Diffie と Hellman より先に，DH 鍵配送方式を発明していたらしい．ただし，GCHQ がディジタル署名について考えていたかは触れられていない．

■1 群 - 3 編 - 6 章

6-4 様々なディジタル署名方式

（執筆者：藤崎英一郎）[2009 年 2 月 受領]

6-4-1 ディジタル署名の存在可能性

ディジタル署名の発見の生い立ちと上記の構成法からも分かるように，ディジタル署名は公開鍵暗号と強い関連をもっているが，理論的には公開鍵暗号よりはるかに弱い一方向性関数が存在すれば十分であることが知られている．

1978 年に Rabin は，共通鍵暗号を用いることでディジタル署名に似たプロトコルを提案した [35]．この方式は，署名者と検証者の対話が必要であることと，署名検証鍵を使い捨てなければいけない点が，現在のディジタル署名と異なっている．その後，Lamport が一方向性関数を用いることで，Rabin の方式の欠点であった対話をなくすことに成功した．この方式を Lamport の使い捨て署名 [28] という．

一方，Goldwasser, Micali, Rivest は，ディジタル署名の安全性クラスを定義した [21]．その安全クラスの一つが，上記に示した EUF-CMA である．彼等は，「クローフリー置換対」（claw-free permutation pairs）という関数の存在を仮定して，最初の適応的選択文書攻撃（CMA）に対して存在的偽造不可（EUF）である（使い捨てでない）ディジタル署名を提案することに成功した（クローフリー置換対が存在するという仮定は，落し戸つき一方向性置換が存在するという仮定より強い）．

この後，Naor と Yung が，Lamport の使い捨て署名 [28] を改良して，汎用一方向性ハッシュ関数族（universal one-way hash function family）が存在すれば，（使い捨てでない）EUF-CMA 安全なディジタル署名が構成できることを示した [31]．彼等は，汎用一方向性ハッシュ関数族が一方向性置換から構成できることのみを示したが，その後 Rompel が汎用一方向性ハッシュ関数族は，一方向性関数から構成できることを示した [38]．よって，一方向性関数が存在すれば，EUF-CMA なディジタル署名方式が存在することが分かった．

6-4-2 実用的なディジタル署名とランダムオラクルモデル

Naor-Yung [31] や Goldwasser-Micali-Rivest [21] の構成法は，あくまで理論的興味を満たすものであり実用的とはいえない．そこで理論的な構成法とは別に，80 年代から 90 年代初頭にかけて，安全性証明は備えていないが，実用的で安全そうに思えるディジタル署名方式が多数提案された．当時提案されて，現在も残っている方式はほとんど素因数分解問題に関係するかか離散対数問題に関係するものである．

素因数分解問題系の代表的な方式としては，上記の RSA 署名 [37]，Rabin 署名 [36] のほかには，Rabin 署名の変形版である Rabin-Williams 署名 [44]，特殊な合成数の素因数分解問題の求解困難性を利用した ESIGN [32]，更にゼロ知識証明から派生した Fiat-Shamir 署名 [12]，Guillou-Quisquater 署名 [22, 23] などがある．

離散対数問題系の方式としては，El Gamal 署名 [14]，その El Gamal 署名を基に米国連邦標準技術局（NIST）により提案された DSA 署名（現在 FIPS 186-2），更に，Schnorr 署名 [40] などがある．

1993 年，M. Bellare と P. Rogaway は理論的に安全な方式と実用的な方式の「橋渡し」となるような安全性のモデルを提案した．現実の公開鍵暗号やディジタル署名には，ハッシュ

関数が使われているが，彼等はハッシュ関数が理想的なランダム関数であると仮定するモデルを考えた．これをランダムオラクルモデルという．このモデルの導入により，ランダムオラクルで安全性証明可能な暗号プロトコルが数多く提案されるようになる．

1996 年，Bellare と Rogaway は，上記で紹介したような落し戸つき一方向性置換 f とハッシュ関数の組合せで自然にできる署名方式（f-FDH （full-domain hash）署名）が，ランダムオラクルモデルで適応的選択文書攻撃に対して存在的偽造不可（EUF-CMA）であることを証明した [3]．彼等は更に，電子文章を乱数と二種類のハッシュ関数を使って変換した PSS パディング及び PSS-R パディングを提案しており，落し戸つき一方向性置換 f と組み合わせることで f-PSS 署名，f-PSS-R 署名を構成できる．これらの方式は，ランダムオラクルモデルで EUF-CMA であり，かつ FDH 署名より（一方向性置換 f への）安全性の帰着効率が良い．RSA 関数を落し戸つき一方向性置換とみなした RSA-PSS, RSA-PSS-R が方式として有名であるが，PSS, PSS-R は，一方向性置換以外の署名関数と組み合わせることが可能である．Rabin-Williams 署名 [44]，Guillou-Quisquater 署名，ESIGN 署名を PSS と組み合わせた RW-PSS, GQ1-PSS, ESIGN-PSS は，RSA-PSS と共に国際標準化機構 ISO に採用されている [25]．

一方，DSA 署名の変形版や Schnorr 署名が，離散対数問題の求解困難性仮定のもと，ランダムオラクルモデルで EUF-CMA であることが，Pointcheval と Stern によって示されている [34]（オリジナルの DSA 署名に対しては，現在までランダムオラクルモデルでの安全性証明は知られていない）．

有限体の乗法群上で定義される離散対数問題を（通常の）離散対数問題と呼び，有限体上定義された楕円曲線の点からなる有限群の離散対数問題を，楕円曲線離散対数問題と呼ぶ．現在の知られている攻撃法では，素因数分解問題は準指数時間で解くことができるのに対して，楕円曲線離散対数問題を解くには指数時間を必要とする．そのため，楕円曲線離散対数問題ではより短いセキュリティパラメータを選択でき，一般に素因数分解系の署名方式より，署名サイズ，署名生成速度，検証速度で有利になると思われている．ただし，変形 DSA 署名，Schnorr 署名は，ランダムオラクルモデルでの帰着効率が悪いため，「現時点では」一概に楕円曲線離散対数問題に基づく署名が素因数分解問題に基づく署名より効率が良いとはいえない．ただし，（楕円曲線離散対数問題の攻撃法が進展しないならば）コンピュータの計算能力向上に依存して鍵長が伸びるにつれ，近い将来明らかに離散対数問題に基づく署名が，素因数分解問題に基づく署名より効率が良くなる．

離散対数問題系のより帰着効率の良い署名は，文献 8, 18, 19, 27) で研究されている．

（通常の）離散対数問題のもと定義されている FIPS 186-2 の DSA 署名と，楕円曲線離散対数問題版 DSA 署名を区別して，後者を ECDSA と呼ぶ．ECDSA は，DSA と共に国際標準化機構 ISO に採用されている [26]．

6-4-3 最近の署名方式

ランダムオラクルモデルに対して，ランダムオラクルを仮定しないモデルを標準モデルと呼ぶ．ランダムオラクルは，現実世界では実装不可能である．更に，ランダムオラクルモデルでの安全性は，標準モデルの安全性を常に保証するものではないという結果が知られている [7]．よって，標準モデルで効率の良いディジタル署名を構成することは，長いこと未解決

問題であった．

標準モデルで安全性証明を備えた効率の良いディジタル署名は，90 年代の最後になって Gennaro, Halevi, Rabin [15] と Cramer と Shoup [9] によって独立に提案された．どちらの方式も強 RSA 仮定 [2, 13] という素因数分解問題に関係する仮定に基づいている．

その後，標準モデルで安全性証明を備えた効率の良いディジタル署名は，境，大岸，笠原 [39]，及び Boneh，Franklin [5] に端を発する効率の良い ID 型暗号の研究からもたらされることになる．これらの ID 型暗号は，Weil ペアリング や Tate ペアリングと呼ばれる楕円曲線（または超楕円曲線）上の二点を有限体に埋め込む双線型写像を利用する．ID 型暗号は，ディジタル署名に効率よく変換できる [5]（文献 5) によると，これを発見したのは Naor である）．EUF-CMA ディジタル署名に変換できる ID 型暗号の安全性クラスについては，文献 10) に詳しく書かれている．

Boneh などは，文献 5) の方式を基にした効率の良いディジタル署名方式を提案した [6]．この方式は，（文献 5) がランダムオラクルを必要とする ID 型暗号だったため）ランダムオラクルモデルで安全な署名であったが，その後，文献 4, 16, 43) のような，双線型写像を利用した標準モデルで安全な署名方式が提案された．これらの署名方式は，いずれも双線型写像をもつ（楕円曲線）離散対数系問題の求解困難性仮定に安全性の根拠を置いている．

素因数分解問題や離散対数問題は，量子計算機が実現した場合，Shor のアルゴリズム [41, 42] により容易に解けることが知られている．また，素因数分解問題や離散対数問題に依存する方式は，べき乗剰余演算を必要とするため，低計算能力のデバイスでも実現できる方式として，多変数多項式問題や格子問題を利用したディジタル署名方式の研究も近年再び盛んになってきている（多変数多項式問題に基づく署名の代表例として，文献 1, 33, 45)，格子問題に基づく署名の代表例として，文献 20, 24) がある）．しかし，これらの方式は安全性証明が付いていないか，付いていたとしても帰着する数学的問題の難しさが不明であり多くの方式はその後破られてしまっている．

2008 年，Gentry, Peikert, Vaikuntanathan が格子問題に基づくランダムオラクルモデルで安全なディジタル署名を提案した [17]．彼等が帰着した格子問題は Hard-on-average 問題と呼ばれるものであり，その格子問題集合の平均的な問題を解く難しさが，ある別の格子問題の中で最も難しい問題を解くに等しいという特徴がある．

素因数分解問題または離散対数問題に依存しない安全でかつ効率の良い（ディジタル署名も含む）暗号プロトコルの構成は，重要な研究テーマであり，今後ますます研究されていくと予想できる．

■参考文献

1) L. Goubin, A. Kipnis, and J. Patarin, “Unbalanced oil and vinegar signature schemes,” In Jacques Stern, editor, Advances in Cryptology–EUROCRYPT‘ 99, Springer-Verlag, vol.1592 of Lecture Notes in Computer Science, pp.206-222,1999.

2) N. Baric and B. Pfitzmann, “Collision-free accumulators and fail-stop signature schemes without trees,” In W. Fumy, editor, Advances in Cryptology–EUROCRYPT ‘ 97, Springer-Verlag, vol.1233 of Lecture Notes in Computer Science, pp.480-494, 1997.

3) M. Bellare and P. Rogaway, “The exact security of digital signatures – how to sign with rsa and rabin,” In Uei Maurer, editor, Advances in Cryptology–EUROCRYPT ‘ 96, Springer-Verlag, vol.1070 of Lecture Notes in Computer Science, pp.399-416, 1996.
4) D. Boneh and X. Boyen, “Short signatures without random oracles,” In C. Cachin and J. Camenisch, editors, Advances in Cryptology–EUROCRYPT ‘ 04, Springer-Verlag, vol.3027 of Lecture Notes in Computer Science, pp.56-73, 2004.
5) D. Boneh and M. Franklin, “Identity-based encryption from Weil paring,” In J. Kilian, editor, Advances in Cryptology–CRYPTO‘ 01, Springer-Verlag, vol.2139 of Lecture Notes in Computer Science, pp.213-229, 2001.
6) Dan Boneh, Ben Lynn, and Hovav Shacham, “Short signatures from the weil pairing,” In C. Boyd, editor, Advances in Cryptology–Asiacrypt‘ 01, Springer-Verlag, vol.2248 of Lecture Notes in Computer Science, pp.514-532, 2001.
7) R. Canetti, O. Goldreich, and S. Halevi, “The random oracle methodology, revisited,” In Proceedings of the 30th annual ACM Symposium on Theory of Computing (STOC ‘ 98), pp.209-218, New York City, 1998.
8) B. Chevallier-Mames, “An efficient cdh-based signature scheme with a tight security reduction,” In CRYPTO ‘ 05, Springer-Verlag, vol.3621 of Lecture Notes in Computer Science, pp.511-526, 2005.
9) Ronald Cramer and Victor Shoup, “Signature schemes based on the strong rsa assumption, ACM Trans. Inf. Syst. Secur., vol.3, no.3, pp.161-185, 2000.
10) Y. Cui, E. Fujisaki, G. Hanaoka, H. Imai, and R. Zhang, “Formal security treatments for IBE-to-signature transformation: Relations among security notions, IEICE Transaction of Fundamentals of electronic Communications and Computer Science, vol.E92-A, no.1, Jan. 2009.（An earlier version appeared in ProvSec 2007 (LNCS 4784)）.
11) W. Diffie and M.E. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, vol.IT-22, no.6, pp.644-654, 1976.
12) A. Fiat and A. Shamir, “How to prove yourself: Practical solutions to identification and signature problems,” In A. M. Odlyzko, editor, Advances in Cryptology–CRYPTO ‘ 86,,Springer-Verlag, vol.263 of Lecture Notes in Computer Science, pp.186-199, 1986.
13) E. Fujisaki and T. Okamoto, “Statistical zero knowledge protocols to prove modular polynomial relations,” In B. S. Kaliski Jr., editor, Advances in Cryptology–CRYPTO ‘ 97, Springer-Verlag, vol.1294 of Lecture Notes in Computer Science, pp.16-30, 1997.
14) T. El Gamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” In IEEE Transactions on Information Theory, vol.IT-31, pp.469-472, 1985.
15) R. Gennaro, S. Halevi, and T. Rabin, “Secure hash-and-sign signatures without the random oracle, In Jacques Stern, editor, Advances in Cryptology–EUROCRYPT‘ 99, Springer-Verlag, vol.1592 of Lecture Notes in Computer Science, pp.123-139, 1999.
16) C. Gentry, “Practical identity-based encryption without random oracles,” In S. Vaudenay, editor, Advances in Cryptology–EUROCRYPT ‘ 06, Springer-Verlag, vol.4004 of Lecture Notes in Computer Science, 2006.
17) C. Gentry, C. Peikert, and V. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” In Proceedings of the 40th annual ACM Symposium on Theory of Computing (STOC ‘ 08), ACM, 2008.
18) E. Goh and S. Jarecki, “A signature scheme as secure as the diffie-hellman problem,” In E. Biham, editor, Advances in Cryptology–EUROCRYPT ‘ 03, Springer-Verlag, vol.2656 of Lecture Notes in Computer Science, pp.401-415, 2003.
19) E. Goh, J. Katz, S. Jarecki, and N. Wang, “Efficient signature schemes with tight security reductions to

the diffie-hellman problems," Journal of Cryptology, vol.20, no.4, pp.29-66, 2007.
20) O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," In B. S. Kaliski Jr., editor, Advances in Cryptology–CRYPTO ' 97, Springer-Verlag, vol.1294 of Lecture Notes in Computer Science, pp.112-131, 1997.
21) S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosenmessage attacks," SIAM Journal of Computing, vol.17, no.2, pp.281-308, Apr. 1988.
22) L.C. Guillou and J.-J. Quisquater, "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory," In C.G. Günther, editor, Advances in Cryptology–EUROCRYPT ' 88, Springer-Verlag, vol.330 of Lecture Notes in Computer Science, pp.123-128, 1988.
23) L.C. Guillou and J.-J. Quisquater, "A paradoxical identity-based signature scheme resulting from zero-knowledge," In S. Goldwasser, editor, Advances in Cryptology–CRYPTO ' 88, Springer-Verlag, vol.403 of Lecture Notes in Computer Science, pp.216-231, 1990.
24) J. Hoffstein, N. Howgrave-Graham, J. Pipher, J.H. Silverman, and W. Whyte, "NTRUSIGN: Digital signatures using the NTRU lattice," In Marc Joye, editor, Topics in Cryptology–CT-RSA ' 03, SV, vol. 2612 of LNCS, pp.122-140, 2003.
25) ISO/IEC 14888-2: Information technology–Security techniques–Digital Signatures with appendix– Part 2: Integer factorization based mechanisms, 2008.
26) ISO/IEC 14888-3: Information technology–Security techniques–Digital Signatures with appendix– Part 3: Discrete logarithm based mechanisms, 2006.
27) J. Katz and N. Wang, "Efficiency improvements for signature schemes with tight security reductions," In S. Jajodia, V. Atluri, and T. Jaeger, editors, Proceedings of the 10th ACM Conference on Computer and Communications Security, ACM, CCS 2003, pp.155-164, 2003. ISBN 1-58113-738-9.
28) Leslie Lamport, "Constructing digital signatures from one-way functions," Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, Oct. 1979.
29) R. Merkle, "Secrecy communication over an insecure channel," submitted to Communications of the ACM.
30) R.C. Merkle and M.E. Hellman, "Hiding information and signatures in trapdoor knapsacks," IEEE-IT, vol.IT-24, pp.525-530, 1978.
31) M. Naor and M. Yung, "Universal one-way hash functions and their cryptographic applications," In Proceedings of the 21st annual ACM Symposium on Theory of Computing（STOC ' 89）, pp.33-43, 1989.
32) T. Okamoto and A. Shiraishi, "A fast signature scheme based on quadratic inequalities," In Proceedings of the 1985 Symposium on Security and privacy（SSP ' 85）, pp.123-133, 1990.
33) J. Patarin, N. Courtois, and L. Goubin, "FLASH: A fast multivariate signature algorithm," In Topics in Cryptography–CT-RSA 2001, Springer-Verlag, vol.2020 of Lecture Notes in Computer Science, pp.297-307, 2001.
34) D. Pointcheval and J. Stern, "Security proofs for signature schemes," In U. Maurer, editor, Advances in Cryptology–EUROCRYPT ' 96, Springer-Verlag, vol.1070 of Lecture Notes in Computer Science, pp.387-398, 1996.
35) M.O. Rabin, "Digitalized signatures," In R.A. DeMillo, D.P. Dobkin, A.K. Jones, and R.J. Lipton, editors, Foundations of Secure Computation, Academic Press, pp.155-168, 1978.
36) M.O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Technical report, MIT, 1979. Technical Report, MIT/LCS/TR-212.
37) R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, vol.21, no.2, pp.120-126, 1978.
38) J. Rompel, "One-way functions are necessary and sufficient for secure signature," In Proceedings of the

21st annual ACM Symposium on Theory of Computing (STOC ‘ 90), pp.387-394, 1990.

39) R. Sakai, K. Ohgishi, and K. Kasahara, “Cryptosystems on pairing,” Technical Report C20, 2000. Symposium on Cryptography and Information Security (SCIS 2000), Jan. 2000. (submitted to ASIACRYPT 2000).

40) C.P. Schnorr, “Efficient signature generation for smart cards,” Journal of Cryptology, vol.4, no.3, pp.239-252, 1991.

41) P. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” In Proceedings of the 35th IEEE Annual Symposium on Foundations of Computer Science (FOCS‘ 94), pp.124-134, 1994.

42) P. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM. J. Computing, vol.26, no.5, pp.1484-1509, Oct. 1997.

43) B. Waters, “Efficient identity-based encryption without random oracles,” In R. Cramer, editor, Advances in Cryptology–EUROCRYPT ‘ 05, Springer-Verlag, vol.3494 of Lecture Notes in Computer Science, pp.114-127, 2005.

44) H.C. Williams, “Some public-key crypto-functions as intractable as factorization,” In G. R. Blakley and D. Chaum, editors, Advances in Cryptology–CRYPTO ‘ 84, Springer-Verlag, vol.196 of Lecture Notes in Computer Science, pp.66-70, 1985.

45) C. Wolf1, A. Braeken, and B. Preneel, “Efficient cryptanalysis of rse(2)pkc and rsse(2)pkc,” In SCN ‘ 04, Springer-Verlag, vol.3352 of Lecture Notes in Computer Science, pp.294-309, 2004.