特集

電子社会を推進する暗号技術

0. 編集にあたって

現代暗号の構図

辻井 重男
情報セキュリティ大学院大学
tsujii@iisec.ac.jp

住民基本台帳カード発行風景

ある夏の日，筆者は，公的個人認証付き住民基本台帳カード申請[1]のため，区役所へ足を運び，申請用紙に住所，氏名等を記入して，窓口へ提出した．本人確認せずに受け付けてくれたので，不審に思ったが，「電子署名および認証業務に関する法律」や「公的個人認証」制定等に関係してきた筆者としては，自治体の電子化への取り組みをチェックしてやろうという魂胆から，黙ってロビーで待っていたところ，しばらくして，係の人が，本人確認を忘れましたと言う．忘れられては困るのだが，運転免許証を見せて本人確認を済まし，いったん帰宅した．3日ほどして，「住民基本台帳カード交付通知書兼照会書」なる書類が郵便で届き，回答書に記入して，区役所に持参した．公的個人認証申請のための公開鍵暗号ペアは，パスワードを入れて生成した．RSAであれば物理乱数から素数を生成するのだろう．以前，総務省，経済産業省，法務省からなる電子署名法に関する委員会で，ある裁判所の長官に「素人がどうやって，良い素数など発行できるのですか」と叱られ，「それはソフトで自動的にできます」と座長として答えたことを思い出した．

区役所から都庁の認証局へネットワークで飛ばし，都庁の電子証明書を付したカードが交付されるまで，15分位であった．

写真付きの住基カードは物理的な身分証明にも使えるが，主目的は，もちろん，サイバーパスポートとして国，自治体，民間の多様な用途である（**図-1**）．しかし，神奈川県に住む私の知人が，電子申請をトライしてみたところ，かなりインターネットに精通してないと，使いこなせないようで，普及するまでには，自治体やベンダはもちろん，本会員を始めとする関係者の協力を待たねばならない．

暗号技術の構図

暗号技術は，今や現代社会に深く根を下ろし，電子社会化[2]を推進する基盤技術として認知されている[3)〜8)]．本特集では，暗号技術と社会的利用に関する全貌を素描することを狙いとして，第一線で活躍されている方々に目次のような執筆をお願いした．

筆者なりに，暗号技術とその利用を構造化したのが**図-2**である．そのすべてにわたって，解説するだけの誌面のゆとりはなかったが，各著者の論説がどのような位置づけになるかも付記しておいたので，参考にしていただきたい．

暗号に対する人々の認識には次の4段階があると思われる．

第1段階：暗号は古来，軍事・外交に用いられ，世界と日本の歴史を舞台裏で動かしたことを知っている．
第2段階：暗号はIT社会を支えていることを知っている．
第3段階：現代暗号の分野では，安全性について，きわめて厳密な理論的考察を進めており，暗号設計者が新方式を学会や標準化機関に提案する場合，原則として，少なくとも既知の攻撃法に対して，1ビットの情報も解読されないこと等を数学的に証明を付すことを習慣としているが，そのことを知っている．
第4段階：第3段階の手法を理解している．

本会員であれば，第2段階までは楽にクリアしておられるだろうし，第4段階を暗号研究者以外の会員に求めるのは厳しすぎるので，問題は第3段階である．そのあたりの状況を少し説明しておきたい．

というのは，著名な評論家をはじめ一般の方々はともかく，情報工学・コンピュータの専門家たちでさえ，「暗号は必ず破られると思え」と軽々に口走るのをよく耳に

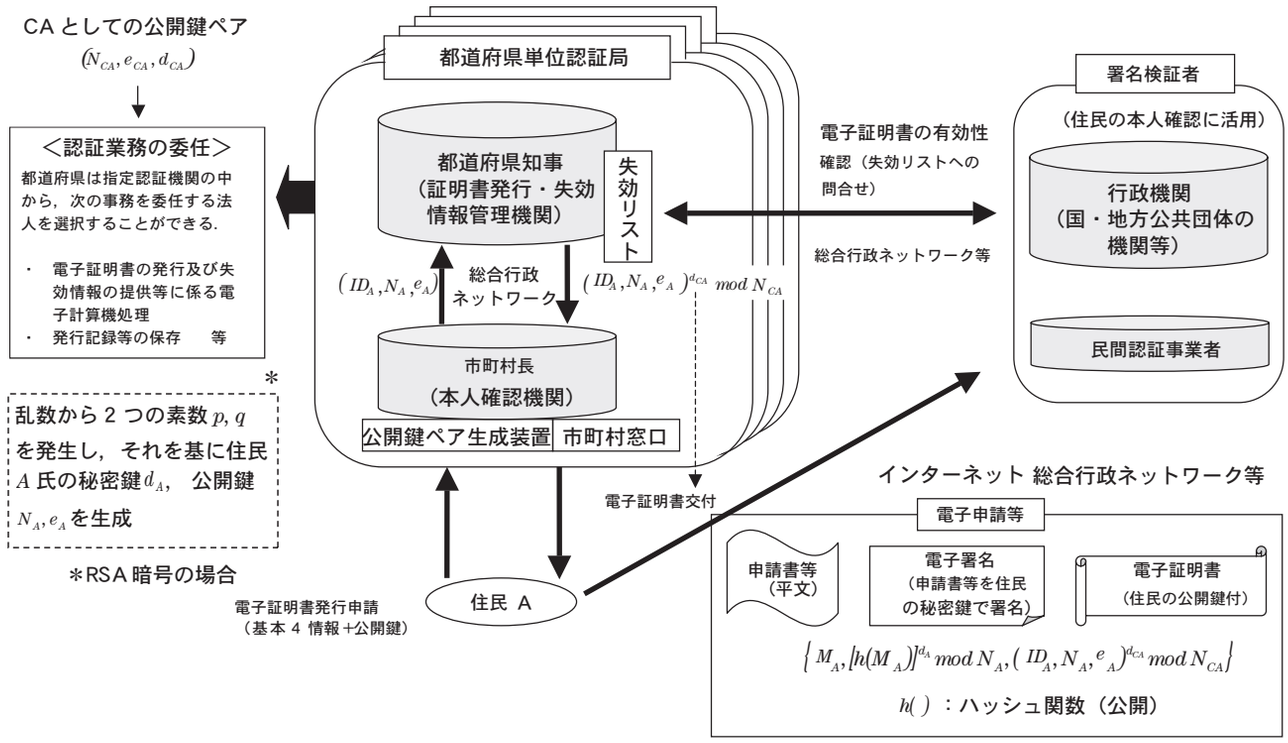

図 -1　地方公共団体による公的個人認証サービス（総務省広報誌 2003 年 6 月号の図に数式説明等を付加）

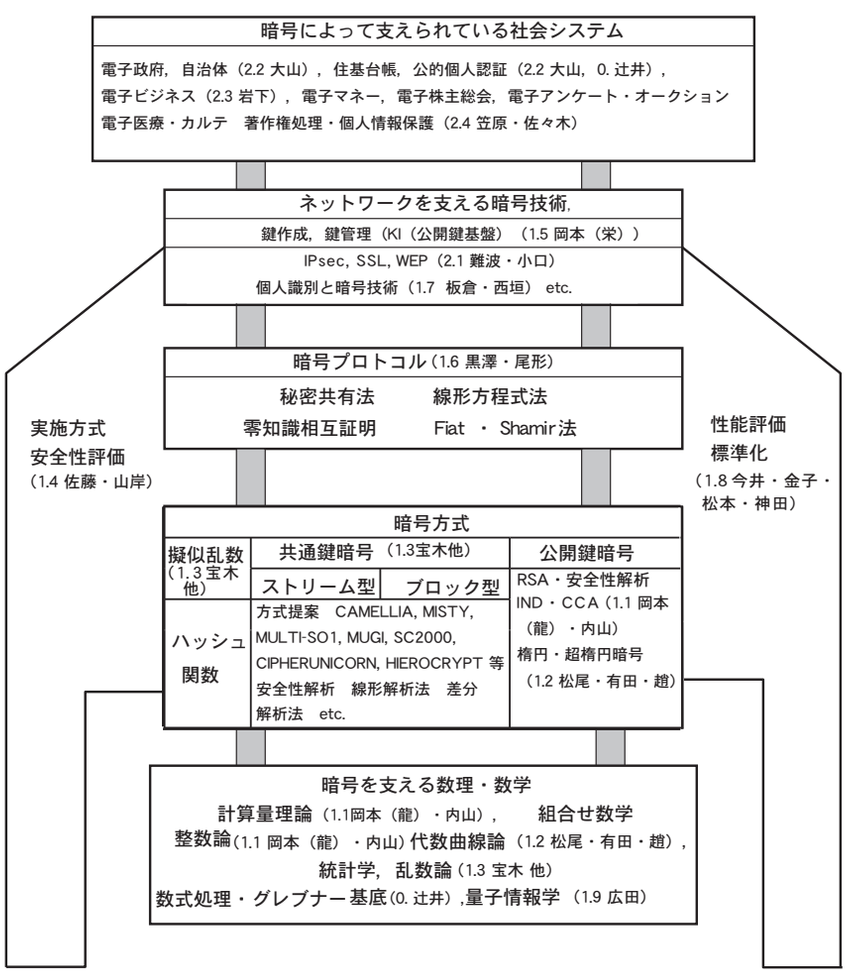

図 -2　暗号技術の構図

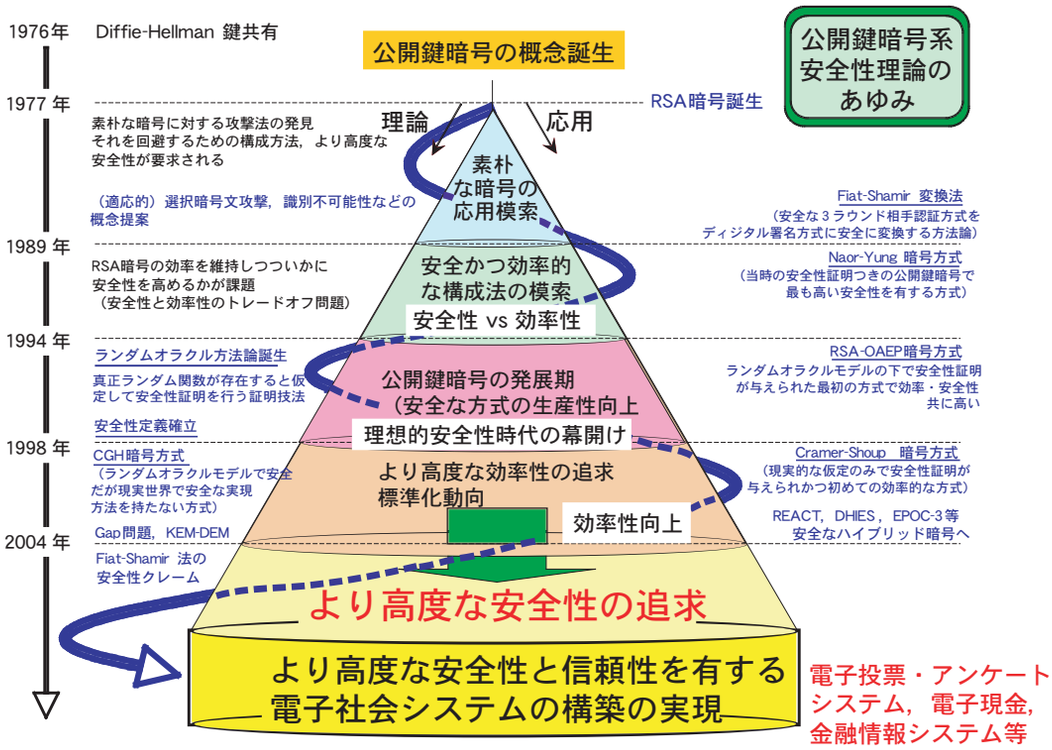

図 -3　公開鍵暗号の安全性理論の歩み（中央大学大学院学生　小林良成　作成）

するからである．そして，我々暗号の専門家としても，絶対に破られませんとも言えないから，困るのである．しかし，そう簡単に破られてしまっては，電子社会は成立しない．問題は，どのような状況で破られたとき，暗号が解読されたと言うのかである．

どのような暗号でも破ってみせると豪語している（悪い意味の）ハッカーがいるそうである．それは「ネットワークに侵入して，鍵を盗んでみせる」ということで，アルゴリズミックに解読してみせるという意味ではないだろう．

暗号が解読される状況を場合分けすれば，

I.　アルゴリズムが破られる．
II.　コンピュータの進歩によって鍵の長さが不足したことによって破られる．
III.　カード等の実装上の弱点を突かれて破られる．
IV.　鍵の管理に不備があって破られる．

が考えられる．一般のユーザからみれば，そのようなことはどうでもよく，要するに破られないようにしてくれということになろう．しかし，情報システムの設計者や管理者は上に述べた状況を理解しておくことが必要である．

I, II は 1.1（数論アルゴリズムと公開鍵暗号の安全性），1.2（代数曲線上の公開鍵暗号），1.3（共通鍵暗号の発展）で，III は 1.4（暗号ハードウェア実装性能と安全性評価）で解説している．IV は技術，管理・運営，法制度，企業・個人倫理からなる情報セキュリティ全般[2]の問題であるが，本特集でも重要な問題として，1.5（鍵生成と鍵管理）で扱っている．

I の中で，特に公開鍵暗号理論において，暗号が破られるということをどう定義するか，どのような攻撃を想定するかについては，1980 年代から厳密な理論が構築され，実用化されている．その歴史を**図-3**に示しておく．詳しくは，1.1 をお読みいただきたい．

以下，本稿では，他の執筆者によって取り上げられていない課題などについて述べておくこととする．

二, 三の話題から

●グレブナー基底アルゴリズムの進歩 ── 非線形連立方程式の強力な解法

暗号方式は，共通鍵暗号と公開鍵暗号に大別される．共通鍵暗号は，内外から多くの方式が提案され，商用化

されていることは，1.3に見られるとおりであるが，いずれにしても，巨大な非線形システムであり，原理的には非線形連立方程式で書き下せるはずである．また，公開鍵暗号についても，素因数分解の困難性に基づくRSA等の方式（1.1参照），離散対数問題の困難性に基づく楕円エルガマル方式（1.2参照）のほかに，多次多変数連立方程式型の方式の研究も盛んである．

ここで取り上げる，グレブナー基底（Gröbner basis）は，20世紀後半，可換代数と組合せ理論の境界領域に生まれた魅惑的で，実用性にも優れた理論である．元々はイデアル剰余類環の計算のために考案されたのだが，その応用範囲は，イデアル所属判定問題，整数計画問題，三角形分割問題など多岐にわたり，特に，多次多変数連立方程式の解法に威力を発揮しつつある．したがって，暗号の安全性をグレブナー基底の観点から解析することは重要な課題である．

1965年，ブーフバーガー（Buchberger）は，学位論文において，多次多変数連立方程式の解法等に有効なブーフバーガーアルゴリズムを提案するとともに，課題を与えてくれた師のグレブナーに敬意を表し，多項式環のある優れた生成系をグレブナー基底と命名した．そのアルゴリズムは，線型方程式に対するガウス消去法（掃きだし法）を非線形系に飛躍的に拡張したものであり，多項式を単項式で操る魔術である[9)〜12)]．

その後，ブーフバーガーアルゴリズムに対し，悲観的な見方もなされたが，2000年前後から，J.C.Faugèreが，F4，F5と名付けるアルゴリズムを精力的に開発し，暗号解析などに適用して注目を集めている[13), 14), 23)]．

多次多変数方程式型公開鍵暗号の動向

筆者の苦い体験談を交えてご参考に供したい．1985年，筆者は，回路解析における順序解析にヒントを得て，多次多変数方程式を3角行列系で表現し，その前後に線形行列を乗じて，それらの構造を秘密鍵とし，それらの積の結果のみを公開鍵とする方式を考案した[15), 16)]．それに対し，長谷川・金子が，1段型の場合に対して解読に成功した[17)]．そこで筆者らは，新たに核変換というアイディアを考案して，1989年に発表した[18)]．これは現在まで攻撃されてない．その後もこのテーマを追求すべきであったが，諸般の事情から最近まで遠ざかっていた．

その当時，筆者はグレブナー基底について勉強不足であったし，ブーフバーガーアルゴリズムもそれほど強力ではなかった．しかし，コンピュータとF4，F5などのアルゴリズムが進歩した今となっては，1989年型[18)]は（核変換と名付けた双有理変換を利用しているから）別として，1986年型[16)]で，かつ非線形行列が1段の場合は，グレブナー基底攻撃の格好の餌食になるかもしれないとも思われる．なぜなら，3角形行列は正にグレブナー基底の望ましい姿であり，線形変換はグレブナー基底が依拠するイデアルという概念から見れば本質的ではないからである．そこで，昨年，持ち駒行列（Piece in Hand Matrix）という概念装置を考案し，最近，藤田，只木の協力を得て，グレブナー基底の観点も含めて具体的検討を進めている[19), 20)]．

また，松本・今井は1988年，隠れ単項式暗号系と名付ける方式をEUROCRYPTで提案した[21)]．これは，拡大体のベクトル表現と多項式表現の関係を巧妙に使い分けた2次多項式系の興味深い方式であったが，1995年，Patarinによって，これまた巧妙なアイディアで解読された．これを契機に2次多項式系の公開鍵暗号の研究が活発に進展している[22)]．その1つの成果が，NESSIE（本特集　1.8参照）でリストアップされたSFLASHである．これはディジタル署名であり，方程式の個数を変数より少なくして安全性を確保しているが，この手法は秘匿用暗号には使えない．

他方，笠原・境は多次多変数連立方程式を導く際に，連立方程式の係数をランダムに与えるという手法を提案している[24), 25)]．この手法においては，線形変換された入力メッセージを小ブロックに分割した上でランダム変換を施しており，代数的構造を与えていない．このため，組織的な復号を適用することが困難となるが，これをテーブル参照復号法を採用することによって解決している．さらに線形変換されたメッセージが小分割されていることを利用して，ランダムな多次多変数多項式を逐次的に加算することによって公開鍵としての連立方程式を導いており，これにより高いレベルのランダム性を実現している．

多次多変数型公開鍵暗号は，鍵長，暗・復号速度などの点で，RSA暗号や楕円暗号に勝る特性が期待されることに加えて，多次多変数方程式の解法はNP完全であるから，量子コンピュータ時代を遙かに望む今日，それに立脚する方式は検討に値するという意識もあって，現在活発な研究が進められているのである．

情報量的安全性を目指す暗号方式

現代暗号は，その安全性を素因数分解や離散対数問題の計算量が準指数時間以上と信じられていることに依存している．これは現実的に優れた戦略ではあるが，次のような課題を抱いている．

(1) 量子コンピュータのような，現在の性能を遙かに上回るコンピュータが出現したことへの対応．量子コン

ピュータはできるとしても30年以上先と言われている．ジャーナリスティックに騒ぐのは早いのだが，しかし，60年前，イギリスで開発された，世界初のコンピュータ，コロッサスの前に，エニグマ暗号が解読されナチスドイツが敗退して，世界地図を塗り替えた歴史を想えば，暗号研究者としては，今から覚悟して危機管理をしておくことは必要であろう．

(2) 新コンピュータが出現しなくても，素因数分解問題や離散対数問題が多項式時間に落ちないということが，証明されているわけでないから，その意味での危機管理も必要であろう．

(3) (1)，(2) の問題がなくても，多項式時間以上とも言うべきコンピュータの進歩に合わせて，鍵長を伸ばすというような対抗策をとらねばならないのは，システム管理上，好ましくない．

そこで，安全性を情報量に依拠する方式も期待されている．その実現には，速度，メモリ量などの現実的条件を考慮に入れた方式を考案せねばならない．これについては，花岡，今井らの提案も含めて，文献26) を参照されたい．

量子暗号

量子暗号の動向については，1.9 (量子暗号の最新動向) に解説されているが，筆者の私見を述べておきたい．BB-84の開発はすでに20年に及んで進められてきたが，それと合わせて，Y-00についても，研究を前向きに進めるべきであろう．BB-84も1984年の提案以来，性能は向上しているものの，平文情報そのものの暗号化は原理的に不可能であり，鍵の配送のみにしか使えないという致命的限界がある上，暗号化・復号装置の冷却の必要性などを考えると特殊用途に限られるのではないかと筆者は見ている．

これに対し，Y-00方式は，平文情報そのものを光通信の速度で高速に暗号化でき，暗号文を盗聴することの不可能性が量子検出理論により証明されている方式で，今後のブロードバンド通信や長距離通信に適した方式である．

米国では，すでに数百メガビット／秒，数百kmの実証実験も推進されている．Yuen・広田らの実績を踏まえ，実証実験を国家的レベルで計画すべき時である．

参考文献

1)「電子政府・自治体」の運営のキーワード：情報セキュリティの確立に向けて，総務省広報誌，2003年6月号．
2) 辻井重男：電子社会を推進する情報セキュリティ総合科学のパラダイム，電子情報通信学会論文誌，Vol.J87-A, No.6, pp.710-720 (June 2004)．
3) 辻井重男：暗号－ポストモダンの情報セキュリティ，講談社メチエ，(Apr. 1996)．
4) 辻井重男：暗号と情報社会，文春新書 (Dec. 1999)．
5) 岡本龍明：現代暗号，産業図書 (June 1997)．
6) 岡本栄司：暗号理論入門，共立出版 (Apr. 2002) (2版)．
7) 笠原正雄，境　隆一：暗号－ネットワーク社会の安全を守る鍵－，共立出版 (Sep. 2002)．
8) 辻井重男，笠原正雄編：情報セキュリティ－暗号・認証・倫理まで，昭晃堂 (2003)．
9) 日比孝之：グレブナー基底，朝倉書店 (June 2003)．
10) N. コブリッツ著，林　　彬 訳：暗号の代数理論，シュプリンガー・フェアラーク東京 (Oct. 1999)．
11) 野呂正行・横山和弘：グレブナー基底の計算　基礎編，東京大学出版会 (June 2003)．
12) 斉藤友克，竹島　卓，平野照比古：グレブナー基底の計算 実践編，東京大学出版会 (June 2003)．
13) Faugère, J. C.: A New Efficient Algorithm for Computing Gröbner Bases(F4), Journal of Pure and Applied Algebra, 139, pp.61-68 (1999)．
14) Faugère, J. C.: A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5), Proceedings of ISSAC, ACM Press, pp.75-83 (2002)．
15) 辻井重男：非線形連立方程式の順序解法を利用する公開鍵暗号方式，情報理論とその応用研究会，第8回シンポジウム資料，pp.156-157 (Dec. 1985)．
16) 辻井重男，黒澤　馨，伊東利哉，藤岡　淳，松本　勉：非線形連立方程式の順序解法による公開鍵暗号方式，電子情報通信学会論文誌D, Vol.J69-D, No.12, pp.1963-1970 (Dec. 1986)．
17) 長谷川栄，金子敏信：非線形連立方程式の順序解法による公開鍵暗号方式の攻撃法，第10回情報理論とその応用シンポジウム資料，江ノ島，(JA5-3 1987)．
18) 辻井重男，藤岡　淳，平山裕介：順序解法の一般化による公開鍵暗号系，電子情報通信学会論文誌A, Vol.J72-A, No. 2, pp.390-397 (Feb. 1989)．
19) Tsujii, S. : A New Structure of Primitive Public Key Cryptosystem Based on Soldiers in Hand Matrix, Technical Report TRISE 02-03, Chuo University (July 2003)．
20) Tsujii, S., Fujita, R. and Tadaki, K. : Proposal of MOCHIGOMA (Piece in Hand) Concept for Multivariate Type Public Key Cryptosystem, to appear in Technical Report of IEICE, ISEC 2004 (Sep. 2004)．
21) Matsumoto, T. and Imai, H. : Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption, Proc. EUROCRYPT'88, Lecture Notes in Computer Science, Vol.330, pp.419-453, Springer (1988)．
22) Patarin, J. : Hidden Fields Equations (HFE) and Isomorphisms of Polynomals (IP) : Two New Families of Asymmetric Algorithms, Proc. EUROCRYPT'96, Lecture Notes in Computer Science, Vol.1070, pp.33-48, Springer (1996)．
23) Faugère, J. C. and Joux, A.: Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner Bases, Proc. CRYPTO 2003, Lecture Notes in Computer Science, Vol.2729, pp.44-60, Springer (2003)．
24) Kasahara, M. and Sakai, R. : A Construction of 100 Bit Public-key Cryptosystem and Digital Signature Scheme, Proc. SCIS2003, 8C-2, pp.599-604 (2003)．
25) Kasahara, M. and Sakai, R. : A Construction of Public-key Cryptosystem Based on Singular Simultaneous Equations, Proc. SCIS2004, 1B5-1, pp.155-160 (2004)．
26) 今井秀樹，花岡悟一郎：情報量的安全性に基づく暗号技術，電子情報通信学会論文誌，Vol.J87-A, No.6, pp.721-733 (June 2004)．

(平成16年9月30日)