暗号アルゴリズム設計技術の動向

— 暗号技術研究タスクフォースの紹介 —

岡本 栄司
北陸先端科学技術大学院大学 情報科学研究科
okamoto@jaist.ac.jp

あらまし: 暗号技術研究タスクフォースは、情報処理振興事業協会の創造的ソフトウェア育成事業の助成を受けて、認証実用化実験協議会における認証技術に必要な暗号アルゴリズムの研究開発を行っている。2 年の予定で 1995 年 4 月に大学・企業の研究者を中心に発足した。主たる目的は、日本で自由に使える暗号アルゴリズムの開発である。本報告では、それらの活動を踏まえ、暗号アルゴリズム開発の設計指針とその動向について概説する。

キーワード: 暗号アルゴリズム、公開鍵暗号、ディジタル署名、共通鍵暗号、ハッシュ関数、暗号鍵管理

Design Technology of Encryption Algorithms

Eiji Okamoto
School of Information Science
Japan Advanced Institute of Scinence and Technology(JAIST)
okamoto@jaist.ac.jp

Abstract: Tha task force of Cryptography Research was established in April last year as 2 year project and is funded by IPA(Information-technology Promotion Agency) as one of the creative software research projects. Its purpose is to develop encryption algorithms for free use in ICAT(Initiatives for Computer Authentication Technology).

This paper introduce the activity of the task force, and shows the design criteria of encryption algorithms.

Keyword: Encryprion Algorithm, Public Key Cryptosystem, Digital Signature, Common Key Cryptosystem, Hash Function, Encryption Key Management

1　まえがき

コンピュータネットワークの広範な利用に際して必要となる利用者認証およびデータの保全技術の開発と、それらシステムの相互運用性を確保することを目的に、認証実用化実験協議会 (ICAT) が設立された。

暗号技術研究タスクフォース (暗号 TF) は、情報処理振興事業協会 (IPA) の「創造的ソフトウェア育成事業」の助成を受けて、 ICAT における認証技術に必要な暗号アルゴリズムの研究開発を行っている。この結果は、 ICAT における広域認証技術研究タスクフォースの証明書発行局実験等に活用され、評価されることになっている。

暗号 TF は 2 年間の研究期間の予定で、 1995 年 4 月に大学・企業の研究者を中心に発足した。主たる目的は、日本で自由に使える暗号アルゴリズムの開発である。具体的な中間結果は、それぞれの報告を参照して戴くとして、ここでは暗号 TF の活動とそれに関連した設計基準の動向について概説する。

設計に決定的な影響を与えるのは、解読技術の進歩である。差分解読の発表以来、多くの解読手法が提案され、その有効性も実証されている。そこで、解読手法にも必要な範囲で触れる。

2　暗号技術研究タスクフォースとは

認証実用化実験協議会は、理事会と実験諮問委員会および事務局からなり、実験諮問委員会のもとに広域認証技術研究タスクフォース、暗号技術研究タスクフォースがある。

理事会は関連企業等により構成され、運用実験に関する技術情報の交換等連絡調整および定例研究会の開催等事業計画を策定する。

実験諮問委員会は、相互運用性を確保するための調査・研究・実験等を推進するために設置された全体調整機関で、各タスクフォースにおける研究課題を調整する。

広域認証技術研究タスクフォースは、実用的な広域認証基盤技術を確立し、それに基づく認証システムの開発および各種アプリケーションへの適用をおこなう。また、認証システムの運用を通じて証明書発行の運用方針を検討・実証する。

暗号技術研究タスクフォースは、認証技術に必要な暗号アルゴリズムの研究開発を行っている。この結果は、認証実用化実験協議会における広域認証技術研究タスクフォースの証明書発行局実験に活用され、評価されることになっている。なお、情報処理振興事業協会の創造的ソフトウェア育成の助成を受けて、統合暗号化システムにおける基盤技術の研究開発も行っており、その成果の一部が広域認証技術研究タスクフォースに利用される。

暗号技術研究タスクフォースは 2 年間の研究期間の予定で、 1995 年 4 月に大学・企業の研究者を中心に発足した。主たる目的は、日本で自由に使える暗号アルゴリズムの開発である。公開鍵暗号グループ、共通鍵暗号グループ、暗号鍵管理グループおよびインテグレーショングループに別れて活動し、月 1 回程度の全体調整会議を持ちながら進めてきた。公開鍵暗号グループ、共通鍵暗号グループの開発は、既にかなり進んでおり、広域認証技術研究タスクフォースには、 11 月 15 日に公開鍵暗号と共通鍵暗号案をプログラムの形で引き渡した。今後、他のグループは、公開鍵暗号グループと共通鍵暗号グループの研究結果を利用して、今年度終了までに統合暗号化システムにおける基盤技術の研究開発を行う予定である。さらに本タスクフォースは新しい暗号アルゴリズムの提案をも目指す予定である。

3　暗号技術研究タスクフォースがなぜ必要か ── 暗号技術の普及を妨げる諸問題 ──

暗号技術研究タスクフォースが作られた主たる理由は、日本で自由に使える暗号アルゴリズムが欲しかったからである。現在よく用いられている暗号アルゴリズムにはいろいろ規制がある。特に、問題になるのがアメリカの輸出規制、特許それに鍵寄託方式の動きである。

鍵寄託方式については、 OECD で議論が進められており、間もなくガイドラインが発表になる予定である。これについては、本予稿集の「暗号をめぐる最近の話題」を参考にされたい。

3.1　輸出規制

アメリカは暗号製品の輸出を規制している。これは、武器輸出規制の Title 22, Code of Federal Regulations, Parts 120 – 131 (International Traffic of Arms Regulations – ITAR) によっている。暗号のベンダを始め、暗号に携わる人々には極めて評判の悪い規則である。みすみす商売のチャンスを逃しているからであり、このため、開発にも熱が入らないということである。そこで、アメリカ政府は Escrowed Encryption Standard の改訂発表において、武器輸出規制の緩和策を提案した。それは、

- 輸出できる暗号製品の鍵長を今までの 40 ビットから 64 ビットに拡大
- 鍵の供託

である。供託先は、政府とは限らず民間もあり得る。しかし、この緩和策では上記の不満の解消にはならないものと思われる。例えば、 Clipper Chip の鍵は 80 ビット長なので、まだ輸出できない。

日本では、ココム輸出規制に替わるワッセナー協定以外の規制はない。ワッセナー協定は特に暗号装置だけの規制ではなく、一般の機器に関する規制である。

3.2 暗号の基本特許

特許の有効期限は、米国では出願から 17 年、日本では出願から 20 年である。 1995 年までは、日本では出願から 20 年または公告から 15 年の短い方であったが、1996 年から公告制度がなくなった。

付録に DES、 一般的公開鍵暗号系、 RSA 暗号、Diffie-Hellman 鍵配送の特許出願状況を示しておく。

DES の特許はもう切れているので問題は少ないが、非対称暗号については問題が多い。

まず、 一般的な公開鍵暗号系の特許はアメリカで 1997 年 8 月 18 日まで有効である。日本にも特許登録されているが、暗号のみで、ディジタル署名は含まれていない。なお、この日本における特許も有効性について議論が多い。日本は先出願主義であるため、最初この発明は発明者の論文に引っかかって拒絶された。その後、ディジタル署名部分を外し、構成を 2 つの部分に分けて申請したところ、通った。従って、裁判をすれば無効となる可能性が無いとは言えない。

RSA 暗号のアメリカ特許は 2000 年 9 月 19 日まで有効であるが、日本には出願していない。

公開鍵暗号系の特許はアメリカの Public Key Partners 社が持っていたが、この会社が最近解散した。その結果、一般的な公開鍵暗号の権利は Cylink 社に、 RSA 暗号の権利が RSA Data Security 社に所属し、他は元の権利者に戻ったようである。

以上の特許は基本的であるが、権利関係が複雑な上に曖昧な点も多く、実際には裁判を起こしてみないとわからないようなこともある。従って、わが国でこれらを使う時は注意が必要である。

暗号技術研究タスクフォースでは、出来るだけ複雑な特許には触れないように心がけているが、上位概念を抑えられている場合のように、限界がある。それにひきかえ、協力が得られるような国内特許については、排除するというような配慮は特に払っていない。

4 暗号技術の設計について

暗号の歴史については、 David Kahn による The Codebreakers[Ka] が詳しいが、 [Ok1] にも簡単な要約が載っている。

これらによると、設計の発展は解読技法の発展と軌を一にしていることがよくわかる。すなわち、まずある暗号が提案されるとそれに対する解読法が示され、次にそれを防ぐ改良が暗号に施され、また暫くして破られるということが続いてゆく。

第 2 次世界大戦以前の暗号は [Ka] などを参考にしていただくとして、戦後の商用・民間用の暗号技術の発展は、大きく次のように分けられるであろう。

1. DES や公開鍵暗号の発表
2. 計算論的複雑度に基づく暗号や署名の提案
3. 差分解読、線形解読とそれらを防ぐ暗号の発表
4. 暗号実装に対する攻撃法の提案

4.1 DES の設計基準

DES の設計にあたっては、 D. Coppersmith による回想が出ている [Co]。それによると、差分解読 [BS] は 'T-attack' と称して、既にわかっていてその対策も盛り込んであったと述べている。しかし、線形解読 [Ma] については新しい解読法として、若干触れられているが、DES 設計時にわかっていたとは述べられていない。論文 [Co] 発表時点で線形解読が単なる鍵全数アタックより大変だと述べて過小評価している所から判断すると、知らなかったと思われる。

S ボックスについての設計基準については、次のような点を考慮したとのことである。ただし、それ以外考慮していないとは言ってない。むしろ、 DES がまだ使われている現状からは、発表されていない基準があると考えるのが自然である。

1. DES を 1 チップ化できるような、最大の S ボックス入出力ビット数とする。具体的には 6 入力 4 出力である。
2. 非線形で、しかも線形に近くないようにする。
3. 入力の最上位と最下位ビットを固定した時、 4 ビット入出力関数が 1 対 1 関数である。
4. ハミング距離が 1 である 2 入力に対する、 2 出力のハミング距離は 2 以上である。
5. $I_1 \oplus I_2 = 001100$ となる 2 入力 I_1, I_2 に対する 2 出力のハミング距離は 2 以上である。

6. $I_1 \oplus I_2 = 11\cdots00$ となる 2 入力 I_1, I_2 に対する 2 出力は異なる。
7. ある一つの入力差分を与える 2 入力の組みは 32 組存在するが、そのうちの 9 組以上が同一の出力差分を与えない。
8. ある段でアクティブで、その上下段で非アクティブな連続した 3 つの S ボックスが存在しないようにすること。アクティブな S ボックスとは、その入力差分が 0 ではないといことである。これがあると、 1 段おきに入力差分が 0 となるパターンが繰り返されることになり、極めて有力な手がかりを差分解読者に与える。

P 置換についての設計基準は次の通りである。

1. i 段の S ボックスの出力 4 ビットのうち、 2 ビットは i+1 段の各 S ボックスの入力 6 ビットの真中 2 ビットに影響を与え、残りの 2 ビットは i+1 段の各 S ボックスの入力 6 ビットの最上位 2 ビットか最下位 2 ビットに影響を与える。
2. i 段の S ボックスの出力 4 ビットは i+1 段の 6 つの S ボックスに影響を与える。ただし、 4 ビット中 2 ビットが次段の同一 S ボックスに影響を与えない。
3. 二つの S ボックス S_j, S_k に対して、ある段における S_j が次段の S_k の入力の真中 2 ビットに影響を与えるならば、逆にある段の S_k が次段の S_j の入力の真中 2 ビットに影響を与えない。$j = k$ の時を考えると、ある S ボックス S_j の出力は次段の S_j の入力の真中 2 ビットに影響を与えないことになる。

馴染みのない基準も見受けられるが、これらは要するに、 12 段ないし 16 段では全てがアクティブ S ボックスになるようにするためである。

DES はその後、線形解読でともかくも解かれたので、線形解読や差分解読に強い暗号が提案されている [Ma2]。そこでの設計評価基準は最大平均差分確率と最大線形特性確率である。差分解読や線形解読に強くするためには、例えば線形解読がどのように行われたかを思い起こせば明らかなように、入出力変数間に線形近似が成立しないようにすれば良い。線形近似は確率的に定義されるので、入出力変数間の線形近似確率が 1/2 にどれだけ近いかが評価尺度となる。差分解読でも入出力差分確率により、同様に評価尺度を作ることができる。これらをもとに、具体的な評価指数として最大平均差分確率と最大線形特性確率が定義され、この値が小さいほど差分解読手法や線形解読手法に強いことが保証される。

また、似た手法によるハッシュ関数が暗号技術研究タスクフォースで提案されつつある。

それらについての詳細は、本予稿集のブロック暗号とハッシュ関数に関する報告を参照されたい。

DES は使えなくなったわけではなく、 triple DES とする他に、 M. Bellare and P. Rogaway が示したように

$$DESX_{k,k1,k2}(x) = k2 \oplus DEC_k(k1 \oplus x)$$

とすると強くなる [BR2]。彼らの設計基準は、まず暗号の安全性とは何かを厳密に定義し、その意味で安全な暗号を構成するというものである。定義自体に 1 年以上かけているとのことである。実際のインプリメントでは、既存の暗号を利用することが多い。

4.2 公開鍵暗号の設計基準

公開鍵暗号については、次の「公開鍵暗号研究の動向」に詳しく述べられる。公開鍵暗号の設計基準は、通常、数学の難問と計算量的に等価となるように作ることである。よく用いられる数学的難問には次のようなものがある。

1. 因数分解問題
2. 離散対数問題
3. ナップサック問題

因数分解問題に基づくものとしては、 RSA 暗号、 Rabin 暗号などがあり、離散対数問題に基づくものとしては、 Diffie-Hellman 鍵配送方式、 ElGamal 暗号がある。ナップサック問題に基づくものには、ナップサック暗号がある。

RSA 暗号などは因数分解問題に基づいてはいるが、等価という証明があるわけではない。厳密な意味での等価性は、例えば離散対数問題については [Sh] に詳しい。

なお、コンピュータによる因数分解の記録は上がっており、 Rivest が懸賞に出した RSA130 は web を使って 1996 年 4 月に因数分解されており [CD]、単一マシンでも 110 桁の因数分解が JAIST の Pasytec を用いて成功している [PO]。従って、 512 ビット (=167 桁) 整数を使うのはもはや危ないかも知れない [Od1]。

また、 RSA 暗号では、小さな冪指数を用いると、線形関係にある未知 2 入力に対する 2 出力がわかれば、入力がわかるというような欠陥がわかった [Pa]。従って、

冪指数は 100 ビット以上に取る必要があり、これも一つの設計指針を与えることになる。

注意すべきは、たとえ、暗号文アタックが NP 完全問題に等価に作っても、既知平文アタックには多項式時間で解けることがあることである [Ok2]。そこで、やはり M. Bellare and P. Rogaway は、安全性を設計向きに厳密に定義し、それに基づいて安全な暗号 OAEP (Optimal Asymmetric Encryption Padding) を提案した。これは、SET でも採用されている [BR1]。これは、次のように与えられる。

$$f(x0^{k_1} \oplus G(r) \parallel r \oplus H(x0^{k_1} \oplus G(r)))$$

ここで、f は RSA 暗号や ElGamal 暗号などの変換であり、G は疑似乱数生成器、H はハッシュ関数、r は乱数である。

4.3 計算論的複雑度に基づく設計基準

ゼロ知識証明方式は、計算論的複雑度に基づく設計基準を用いて構築されているといえよう。また、ユーザ認証方式では、あるユーザになり済ますこととそのユーザの秘密情報を多項式時間で計算できるのが等価となるように作るのが、最近の設計基準である。

これについては幾つかの方式が提案されている。日本からでは、岡本龍明によるユーザ認証方式が有名である [St]。

いずれも、対話証明であるのが特徴である。

4.4 暗号実装に対する攻撃法の提案

今年になって、暗号実装に対する攻撃法が幾つか提案されている。タイミングアタックや IC カード等への外部刺激による攻撃法である。設計に大きな影響を与えるので、少し言及しておく。

タイミングアタックは、暗号系において暗号 / 復号処理時間がわかれば鍵がわかるというものである。これは、鍵が変われば暗号 / 復号処理時間が微妙に異なってくることを利用した攻撃法であり、従来の思考の盲点をついているかも知れない。もともと離散対数を求めるのに考案されたため、公開鍵暗号系に有効な手法であるが、共通鍵暗号にも適用できる可能性もある。ただ、まだアイディアが出された段階なので、今後つめる必要があろう。ただし、このタイミングアタックの威力は暗号・復号処理をどのようにインプリメントするかによって効果が異なる。通常のインプリメントでは、完全に逃れることは困難である。しかし、指数演算に基づいている暗号においては、ブラインド処理を導入することにより、多少の負荷がかかるが、タイミングアタックをかわすことが可能となる [KO]。

さらに、IC カードなどに実装された暗号実行中に、外部刺激で 1 ビットエラーが生じると解読できることが Biham and Shamir や Ross Anderson らによって示されている [AK]。

また、Zheng and Matsumoto がわかりやすい別な方法を提案している [ZM]。これは、IC カードに実装した ElGamal 署名で乱数 k を既知なものに置き換えられれば、通信文から得られる情報 ms, r から、秘密情報 x が

$$x = \frac{m - sk}{r} \bmod p - 1$$

により得られるというものである。但し、これに対しては、IC カード作成側も何とか対処法を考えるかも知れない。

4.5 暗号鍵管理方式の設計基準

暗号鍵管理方式は、公開鍵暗号を用いる方式、共通鍵暗号を用いる方式、情報理論的基準に基づく方式があり、それぞれもとの暗号の安全性の他に、プロトコルとしての安全性が問題になる。これらについては、本予稿集の暗号鍵管理方式の設計を参考にされたい

参考文献

[AK] R. J. Anderson and M. G. Kuhn; Improved Differential Fault Analysis, preprint, 1996

[BR1] M. Bellare and P. Rogaway; Optimal asymmetric encryption, Advances in Cryptology — EUROCRYPT'94, LNCS, pp.92–111, 1994

[BR2] M. Bellare and P. Rogaway; How to protect DEA against exhaustive key search, Advances in Cryptology — CRYPTO'96, LNCS, pp.252–267, 1996

[BS] E. Biham and A. Shamir; Differential cryptanalysis of the full 16-round DES, Advances in Cryptology — CRYPTO'92, LNCS, pp.494–502, 1993

[Co] D. Coppersmith; The Data Encryption Standard(DES) and its strength against attacks, IBM J. RES. DEVELOP., vol.38, no.3, pp.243–250, 1994

[CD] J. Cowie, B. Dodson, R. M. Elkenbracht-Huizing, A. K. Lenstra, P. L. Montgomery and J. Zayer; A world wide number field sieve factoring record: on to 512 bits, Advances in Cryptology — ASIACRYPT'95, LNCS, pp.382–394, 1996

[Do] H. Dobbertin; MD4 is not collisionfree, Conf. of Cryptography at Luminy, France, 1995

[FIPS] National Institute of Standards and Technology; Escrowed encryption standard, U.S. Dept. of Commerce, 1994

[ICOT] 認証実用化実験協議会; 認証実用化実験協議会への参加募集について, 1995

[Ka] D. Kahn; The Codebreakers, Macmillan, 1972

[KO] Paul C. Kocher; Timing attack on implememtations of Diffie-Hellman, RSA, DSS, and other systems, Advances in Cryptology — CRYPTO'96, LNCS, pp.104–113, 1996.

[Ma] 松井 充; DES 暗号の線形解読 (III), 1994 年暗号と情報セキュリティシンポジウム, 1994

[Ma2] M. Matsui; New structure of block ciphers with provable security against differential and linear cryptanalysis, Fast Software Encryption, pp.205–218, 1996

[Od1] Andrew M. Odlyzko; The future of integer factorization, Proc. of JAIST International Forum on Multimedia and Information Security, pp.139–151, 1995

[Ok1] 岡本栄司; 明るい情報化社会の実現を目指す暗号技術, bit, Vol.23, No.8–13, 1991

[Ok2] 岡本栄司; 暗号理論入門, 1993

[OM] 岡本、満保; 暗号最新情報, bit, Vol.28, No.1–12, 1996

[Pa] J. Patarin; Some serious protocol failure for RSA with exponent e of less than ≈ 32 bits, Conf. of Cryptography at Luminy, France, 1995

[PO] ペラルタ、岡本、満保; 並列計算機を用いた素因数分解, 電子情報通信学会 信学技法, ISEC96-33, vol.96, no.295, pp.1–8, 1996

[Sh] H. Shizuya; Relationship among the computational powers of breaking discrete log cryptosystems, Advances in Cryptology — EUROCRYPT'95, LNCS, pp.341–355, 1995

[St] D. Stinson; Cryptography, CRC Press, 1996

[ZM] Y. Zheng and T. Matsumoto; Breaking smart card based Elgamal signature and its variants, ASIACRYPT'96 RUMP SESSION, 1996

付録 基本的特許について

1. DES

   (a) 米国
   発明の名称 Block Cipher System for Data Security
   出願人 International Business Machines Corporation
   登録番号 3,962,539
   登録日 1976 年 6 月 8 日
   有効期限 1983 年 6 月 7 日

   (b) 日本
   発明の名称 暗号装置
   出願人 インターナショナル ビジネス マシーンズ コーポレーション
   登録番号 昭 59-45269
   登録日 1984 年 11 月 5 日
   有効期限 1996 年 2 月 17 日

2. 一般的公開鍵暗号系とナップサック暗号

   (a) 米国
   発明の名称 Public Key Cryptographic Apparatus and Method
   出願人 The Board of Trustees of the Leland Stanford Junior University
   登録番号 4,218,582
   登録日 1980 年 8 月 19 日
   有効期限 1997 年 8 月 18 日

   (b) 日本
   発明の名称 公開キー式の暗号装置
   出願人 ザ ボード オブ トラステイーズ オブ リーランド スタンフオード ジユニア ユニバーシテイ
   登録番号 昭 59-50068
   登録日 1984 年 12 月 6 日
   有効期限 1998 年 10 月 5 日

3. RSA 暗号

   (a) 米国
   発明の名称 Cryptographic Communications System and Method
   出願人 Massachusetts Institute of Technology
   登録番号 4,405,829
   登録日 1983 年 9 月 20 日
   有効期限 2000 年 9 月 19 日

   (b) 日本
   米国以外への出願無し

4. DH 公開鍵配送方式

   (a) 米国
   発明の名称 Cryptographic Apparatus and Method
   出願人 Stanford University
   登録番号 4,200,770
   登録日 1980 年 4 月 29 日
   有効期限 1997 年 4 月 18 日

   (b) 日本
   米国以外への出願はカナダのみ