暗号技術と鍵回復システム
Development of Cryptography and Key Recovery System

新保　淳 SHIMBO Atsushi
佐野 文彦 SANO Fumihiko
丹羽 朗人 NIWA Akito

暗号技術は共通鍵（かぎ）暗号と公開鍵暗号に大別されるが，その両分野で，より強度の高い方式を巡る開発が盛んになっている。すなわち，共通鍵暗号では128ビット以上の鍵長をもつ新アルゴリズム，公開鍵暗号ではビット当りの安全性の高い楕（だ）円曲線暗号の開発が注目を集めている。こうした動向の下で，当社ではDESやTriple-DES以上の強度をもつ独自の共通鍵ブロック暗号や楕円曲線暗号の効率的演算方式を開発している。開発した暗号技術の応用として，復号鍵の紛失時でも承認者の合意の下で暗号データからメッセージを復号できる鍵回復システムを試作した。

Safer encryption algorithms and signature schemes have been actively researched in recent years. Candidates for the advanced encryption standard (AES), which use a key length exceeding 128 bits, and the elliptic curve cryptosystem are prominent in the fields of symmetric-key cryptography and public-key cryptography, respectively.

Toshiba has developed original symmetric-key block ciphers that are safer than Data Encryption Standard (DES) or triple-DES, as well as a fast algorithm for computing in the elliptic curve cryptosystem, and has applied these results to the development of a key recovery system. In this system, an encrypted message is decryptable under agreement by approvers, even if the decryption key is lost at lawful nodes.

1 まえがき

暗号は情報セキュリティ技術を支える基盤技術である。周知のように暗号方式は，一つの鍵を暗号化・復号の両方に利用する共通鍵方式と，暗号化（または署名処理）と復号（または検証処理）のそれぞれに異なる鍵を利用し，片方の鍵を公開できる公開鍵方式の二つに分類される。70年代後半にDES（Data Encryption Standard）の制定，RSA（Rivest-Shamir-Adleman）暗号とDH（Diffie-Hellman）鍵共有方式の発明がなされた。それ以降，DESとRSA（およびDH）が共通鍵暗号と公開鍵暗号それぞれのデファクト標準としての地位を固め，特に90年代に入ってインターネット技術の進展によりそれらの実用化が進んだ。

ところが，計算機性能の急激な発展はこれら標準方式自体の寿命を縮めることにもつながり，特に鍵長が固定のDESはそれに代わるアルゴリズムの選定作業が開始されている。鍵長可変の公開鍵暗号でも鍵長を増加させる必要が生ずる一方で，楕円曲線暗号に代表される，よりビット当りの強度の高い方式が注目を集めている。このように現在は，実用的な面で暗号アルゴリズムが世代交代にさしかかった時期ととらえることができる。

ここでは，こうした暗号技術の動向を解説し，当社の新規技術に対する取組みとして，独自共通鍵暗号の設計と楕円曲線暗号の高効率実装を中心に述べる。さらに，暗号技術の応用として一分野を形成しつつある“鍵回復システム”の開発動向についても述べる。

2 共通鍵暗号と安全性評価技術

77年にFIPS（Federal Information Processing Standard）に制定された米国の商用標準暗号DESは，鍵が56ビットと短いため，現在では，専用のハードウェアを使えば鍵をしらみつぶしに調べて1～2日で解読することが可能となっている。そのため，DESをベースとして鍵を長くし処理を三重に行うTriple-DESが代替として用いられる一方で，2000年頃をめどに米国の次期標準暗号としてAES（Advanced Encryption Standard）の策定が進められている。策定の基本要件はTriple-DES以上の性能と安全性である。このような背景により，従来のDES方式よりも安全性の高い暗号方式の開発が求められている。

共通鍵ブロック暗号では強度の一つの基準として，鍵長が指標に使われる。鍵長は鍵の組合せをしらみつぶしに調べるのに必要なデータ量や計算量の目安となるためである。安全な暗号では，その暗号アルゴリズムで作られた暗号文や入出力データから暗号化に使った鍵を推定するのに，鍵をしらみつぶしに調べるよりも効率的な方法がないことを示す必要がある。

当社では，従来方式をベースに，より安全性を高めたアルゴリズム公開型と，要求仕様に基づいて新たに設計する特定顧客向けのアルゴリズム非公開型の二つの方針に添っ

てそれぞれ開発している。

暗号アルゴリズムを秘密にすることにより，鍵の推定はより困難になる。しかし，装置に組み込まれている暗号アルゴリズムの解析によってアルゴリズムの再構築が不可能ではないことに注意が必要である。このため，アルゴリズム非公開の場合であっても，既存の攻撃法による十分な評価を行う必要があると考えている。

すなわち，設計の流れは次のとおりである。専門の知識に基づいて，まず，部品となる非線形変換テーブルや，ビット攪拌（かくはん）テーブルなどを設計し，その部品を組み立てて共通鍵ブロック暗号アルゴリズムを設計する。次に，暗号安全性評価技術により，暗号アルゴリズムの解読に対する耐性（安全性）を複数の観点から評価する。例えば，差分攻撃や線形攻撃に対する特性を探索し，これらの攻撃法を使っても鍵のしらみつぶしよりも効率よく解読できないことを確認する。

非線形変換テーブルを設計する際には，差分攻撃や線形攻撃に対する耐性だけでなく，代数次数，入出力の統計的相関などの他の既存の攻撃法や可能性のある攻撃法に対する特性も考慮しなければならない。図1はテーブルへの入力のあるビットを反転させたときに出力のあるビットが反転する頻度を調べた結果である。悪い例のような特性に偏りのあるテーブルは弱点となる可能性があるので候補から外す。部品の評価以外に，これらを組み合せた結果である暗号アルゴリズム全体も十分に安全性の性能を発揮しているか確認する必要がある。

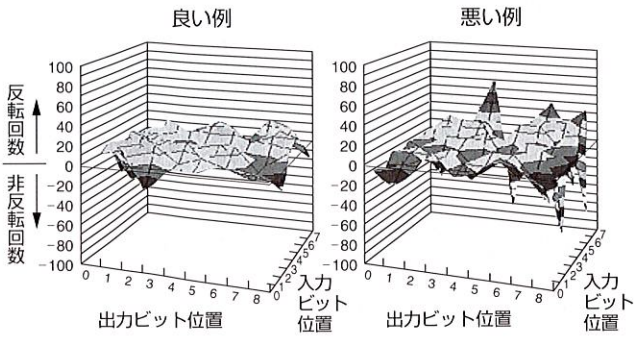

図1．非線形変換テーブル入出力の相関特性の評価例　変換テーブルにおいてある入力ビットを反転した場合の出力ビットの反転回数をカウント。良い例では，ビット反転率がすべての位置において1/2に近い。

Evaluated sample of input and output correlation in substitution table

図2は，特定顧客向けに独自設計した暗号の差分攻撃および線形攻撃に対する安全性を評価したグラフである。この独自方式では大域構造はDESと同じであるが，内部に含まれる非線形変換テーブルやビット攪拌テーブルを再設計し，より安全性の高いもので置き換えている。グラフの横軸は暗号の使用段数，縦軸はその攻撃法で解読を行うのに必要な入力ブロック数を表す。図2では，比較の対象としてDESを取り上げた。DESの鍵は56ビットなので，2^{56}よりも少ないデータで解読可能ならば，鍵のしらみつぶしよりも効率よく解読できる有効な攻撃法になる。また，64ビット入力のブロック暗号なので，必要なデータ量が2^{64}よりも多いならば，入力のあらゆる組合せを上回っているので，その攻撃に必要なデータ量を確保することは原理的に不可能であり，攻撃法が有効でないことを意味する。図2の例では，差分攻撃に対しては12段以上，線形攻撃に対しては5段以上でこれらの攻撃法に対して安全であることを示している。

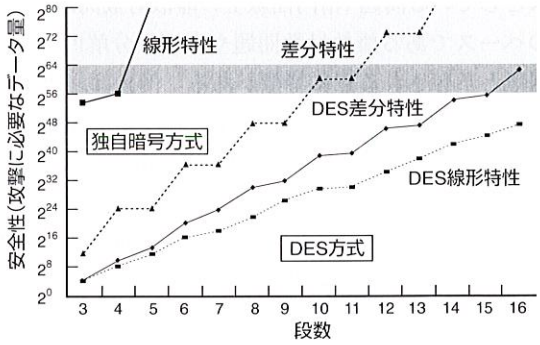

図2．差分攻撃・線形攻撃耐性の評価例　差分攻撃と線形攻撃に対する安全性の評価結果の一例。独自方式ではDESよりも高い安全性をもっている。

Evaluated sample of security against differential/linear cryptanalysis

当社ではDESの置換えに適したアルゴリズム公開型の暗号も開発している。既存の暗号アルゴリズムの多くはブロックサイズが64ビットであるのに対して，AESでは128ビットに拡大されている。既存の64ビット単位での暗号化処理を前提として設計されたシステムでは，ブロックサイズの異なる方式での置換えは困難である。例えば，DESを将来選定されるAESで置き換えることは困難な場合があり，ニーズとしてDESよりも安全な64ビット入力のブロック暗号が考えられる。

こうしたニーズに対して，Triple-DESよりもより強力な暗号としてTRIPLOを開発した。TRIPLOは鍵のビットパターンにより，DES, DES-SS[1]，Triple-DESといった既存の3種類の64ビット入力ブロック暗号を切り替えて実現できる独自機構を備えている。TRIPLOはTriple-DESよりも長い256ビットの鍵をサポートするとともに，独自に設計した非線形変換テーブルを組み込むことにより，安全性を向上させた。また，Triple-DESと比較して，回路規模および速度はほとんど変らない特長がある。

3 公開鍵暗号技術

3.1 動向と当社の取組み

公開鍵暗号でも近年の計算機性能の飛躍的な向上に伴い，セキュリティ強度を向上させる動きが生じている。例えばRSA方式では，その強度を決定するパラメータである公開モジュラスの標準サイズが512ビットから1,024ビットに倍増した。DH鍵共有方式やDSA（Digital Signature Algorithm）などの離散対数ベースの方式も同様である。モジュラスサイズの増加により，処理速度の低下や暗号・署名データのサイズ増加などの性能劣化が生ずる。無線通信環境やICカードなどの計算能力の乏しい環境でこの影響は特に大きい。

こうした状況で，楕円曲線暗号が注目を集めている。楕円曲線暗号は従来の離散対数系暗号の変形方式であるが，ベースとしている問題（楕円曲線上の離散対数問題）が従来方式のベースである離散対数問題や素因数分解問題よりも解読困難と予想される点に特徴がある。例えば，RSA方式での1,024ビットおよび2,048ビットと同等の安全性が，楕円曲線暗号では160ビットおよび234ビットでそれぞれ実現可能と予想されている。したがって，鍵や署名データなどが現在小さいだけでなく，将来にわたって鍵サイズの増加量がはるかに小さく抑えられるものと期待される。鍵サイズの縮小は処理性能の向上ももたらし，楕円曲線での代表的な署名法であるECDSA－160ビットによる署名時間はRSA－1,024ビットの1/5から1/10程度である。

楕円離散対数問題の安全性は重要なテーマであり，ここ数年活発に研究され，解読できることが判明した曲線もある。今後，安全性の検証が進展するにつれ徐々に楕円曲線暗号の利用分野の拡大が予想される。

当社では，RSA，DH，DSAなどの現在の標準方式から次世代の有力方式である楕円曲線暗号に対し，パソコンからICカードまでさまざまな環境において高性能な処理を可能とする実装技術を一つの課題ととらえて開発を行なっている。また，独自の公開鍵方式ではElGamal署名をベースにその効率の良い多重署名を可能とする変形署名アルゴリズム[(2)]（変形ElGamal署名方式）を開発している。

3.2 モンゴメリ演算を利用した素体型楕円曲線暗号

汎（はん）用CPUやDSP（Digital Signal Processor）などでの楕円曲線暗号のソフトウェア実装法としてモンゴメリ演算を応用した演算手法を提案している[(3)]。

楕円曲線暗号は有限体上で定義された三次曲線上の点の間で定義される群演算（点の加算）を利用して構成される。点の加算には有限体での四則演算を組み合わせた公式が利用される。よく利用される有限体の一つに，多倍長の素数をモジュラスとした整数の剰余値で構成される“素体”があり，この手法は素体上の楕円曲線暗号に利用できる。

モンゴメリ乗算は，多倍長整数での四則演算のうちもっとも処理時間がかかる除算処理を用いずに，剰余付き乗算を効率よく計算する手法である。ただし，モンゴメリ乗算は通常の素体の元を定数倍した領域で乗算結果を求める手法であるため，演算の前処理として乗算対象パラメータの変換を行い，後処理として演算結果の逆変換を行う必要がある。モンゴメリ乗算のたびにこれらの変換処理を行うのでは全体としてオーバヘッドが大きくなる可能性がある。

そこでモンゴメリ乗算を中心にモンゴメリ系での四則演算を定義し，さらにこの演算系を利用して定義される楕円曲線上で点の演算処理を実行することにより，パラメータ変換処理の削減と剰余算処理の効率化を達成する方法を開発した。

図3にモンゴメリ演算系を利用した楕円曲線暗号の演算手順を示す。暗号処理に必要なパラメータのうち，固定的なものは事前にモンゴメリ系に変換しておく。相手の公開鍵など可変なものだけを必要なたびにモンゴメリ系に変換する。点の加算回数を制御するスカラ値はそのまま利用できる。以上のパラメータを用いてモンゴメリ系での四則演算を利用して楕円曲線上の基本演算処理を実行する。結果として得られる点のデータを通常の素体での値に逆変換し，さらに通常の素体で若干の処理を行なって所望の結果を得る。モンゴメリ系での演算が素体での演算に比べて高速であるため，全体として高速処理ができる。

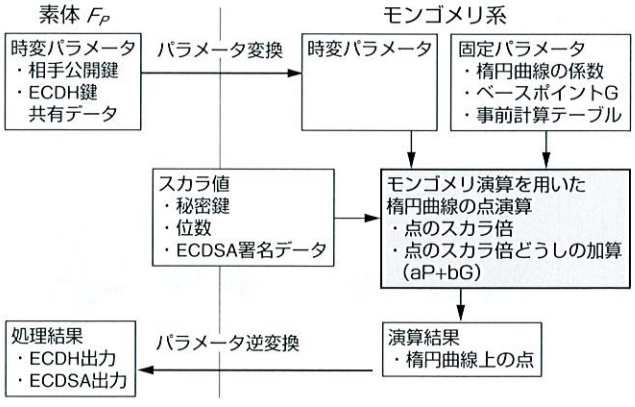

図3．モンゴメリ演算を利用した楕円曲線暗号処理　楕円曲線暗号の基本的な演算要素である点演算処理部をモンゴメリ系での演算を用いて実行し，補足処理だけを通常の剰余演算で実施した。
Elliptic curve cryptography implementation applying Montgomery arithmetic

4 鍵回復システム

重要な情報の盗聴／改ざん防止には電文の暗号化が有効であるが，一方で復号鍵の紛失などによって正当な利用者がその情報を利用できなくなる可能性も生ずる。こうした

場合の対策となるものが鍵供託／鍵回復システムと呼ばれるシステムである。ここでは，この鍵回復システムの動向および当社が開発した鍵回復システムについて述べる。

4.1 動向

鍵回復システムはもともと米国政府が，93年頃から国際的規模で暗号製品の利用や輸出の条件としたもので，ここ数年，TIS, Cylink, IBMなどの米国企業を中心に積極的に技術開発が行われ，導入が議論されてきた。ところが，最近の輸出規制の大幅な緩和により，この推進が停滞している。

しかし，Key Recovery Alliance（米国IBM中心の鍵回復技術の研究会。日本からは当社のほか5企業が参加）などではいまだ活発に議論が行われており，ビジネスユースとしての必要性は大きいと考えられる。事実，日本電子工業振興協会が98年12月に実施したアンケートによれば，回答（559社）の38％に上る企業が鍵回復システムをシステム基本機構として導入すべきとしている。

4.2 鍵回復システムの開発

当社では，98年に企業内ユーザー間での暗号メールの利用や保管を対象にした鍵回復システムを試作した[(1)]。

鍵回復技術の基本的な枠組みは，暗号通信する当事者以外に鍵回復エージェント（KRA：Key Recovery Agent）と呼ばれるシステム構成要素を用意し，その公開鍵で暗号通信に用いるセッション鍵を暗号化した情報を暗号電文に付加するものである。さらに，各ユーザーの公開鍵に証明書を作成／管理する認証局が存在する。このシステムの特長として鍵回復申請の承認を行う承認者（複数）を構成要素に加えた。また，鍵回復エージェントも複数用意し，セッション鍵をピースに分解，それぞれ別の鍵回復エージェントの公開鍵で暗号化したもの（KRF：Key Recovery Field）を暗号電文に付加する。鍵回復は次の手順で行われる。

(1) ユーザーは承認者に鍵回復承認願を提出し，承認者より多重署名を付加した鍵回復承認書を受け取る。
(2) ユーザーは各KRAにKRFと鍵回復承認書を添付した鍵回復要求を送付し，各KRAはKRFより自分の秘密鍵を用いて鍵ピースを取り出し，ユーザーに返す。
(3) ユーザーは返却された各鍵ピースよりセッション鍵を回復する。

(1)ではユーザーは承認者全員の署名を必要とするが，(3)では鍵ピースをすべて集める必要はなく，ある一定数以上で鍵を回復可能にした。このシステムの概念を図4に示す。

また，このシステムでは次の技術を採用した。これら暗号機能をパソコン上の既存のメールシステムに簡易的に付加して暗号通信環境を実現している。

(1) 共通鍵暗号　　Triple-DES, DES-SS[(1)]
(2) 公開鍵暗号　　楕円曲線暗号
(3) 承認者署名　　楕円変形ElGamal方式による多重署名[(2)]

今後の課題としてはこうした鍵管理インフラの簡便化，

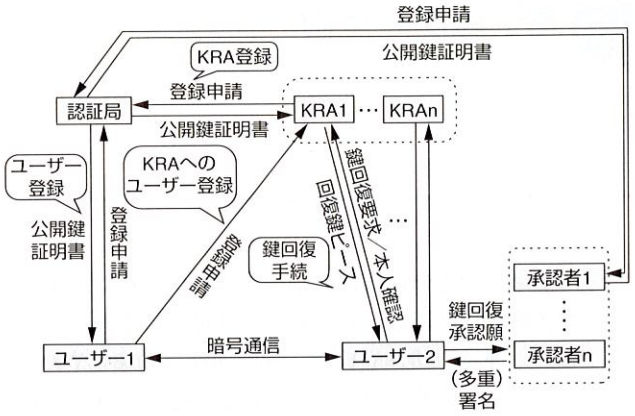

図4．鍵回復システムの構成　　鍵回復システムの構成および鍵回復手続きなどに伴う各構成要素間でやり取りされるデータを示す。
System function model of key recovery system

第三者が暗号電文を復号せずに鍵回復可能であることを検証する技術の開発などが挙げられる。

5 あとがき

最近の暗号技術の動向を受けた当社の技術開発の取組みについて述べた。暗号技術は今後も，より安全でより高性能な手法を目ざした技術開発が続けられる一方で，電子商取引などの応用技術が進展していくものと予想される。

当社では，今後も基盤である暗号技術の動向を注視しながら，セキュリティ製品・システムの開発を行なっていく。

文　献

(1) 佐野文彦, 他. DES-SS：DES互換な128ビット鍵長ブロック暗号. 情報理論とその応用シンポジウム SITA96，1996.
(2) 新保　淳. 変形ElGamal署名の設計.「暗号アルゴリズムの設計と評価」ワークショップ，1996，p.37-44
(3) 新保　淳. 楕円曲線暗号へのモンゴメリ演算の適用. 暗号と情報セキュリティシンポジウム，SCIS97-14D，1997.
(4) 佐野文彦, 他. イントラネットにおける暗号データ回復システムの試作. 暗号と情報セキュリティシンポジウム SCIS99，1999，p.123-128

新保　淳　SHIMBO Atsushi
研究開発センター コンピュータ・ネットワークラボラトリー研究主務。暗号技術・応用システムの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Computer & Network Systems Lab.

佐野　文彦　SANO Fumihiko
情報・社会システム社 SI技術開発センター SI技術担当。暗号技術・応用システムの研究・開発に従事。電子情報通信学会，情報処理学会会員。
System Integration Technology Center

丹羽　朗人　NIWA Akito
情報・社会システム社 SI技術開発センター SI技術担当主務。暗号技術・応用システムの研究・開発に従事。情報処理学会会員。
System Integration Technology Center