産業界の技術動向

身近になった暗号技術

三菱電機株式会社　情報技術総合研究所
情報セキュリティ技術部長
松　井　　充

1. はじめに

暗号技術は、かつては軍事・外交のための道具でしたが、今ではプライバシーを保護する技術としてきわめて身近なところで利用されています。今や携帯電話、IC カード、車の電子キーなど私たちのかばんの中に暗号が２つや３つ入っているのはあたりまえ、逆に暗号を一度も使わずに一日を過ごすことの方が少ないという時代になりました。

三菱電機は 1980 年代前半に暗号技術の研究開発を開始しましたが、当時の PC は 16 ビット DOS の時代、もちろん個人用携帯電話はまだ影も形もなく、暗号技術の応用製品といってもごく限られたものでした。しかし 1990 年代のインターネットの広がりとプライバシー保護意識の高まり、そして情報通信機器の小型軽量化により、暗号技術が爆発的にさまざまな製品に適用されるようになりました。最近ではクラウド時代の情報セキュリティのキーテクノロジーとして暗号技術が注目されています。

本稿では、三菱電機における暗号技術の研究開発の例をいくつかご紹介しながら、暗号技術の広がりと可能性について述べてみたいと思います。

2. 現代暗号と暗号解読

現代暗号と呼ばれる、オープンな暗号研究が本格的にはじまったのは 1970 年代のことです。1976 年には米国で連邦政府標準暗号 DES（Data Encryption Standard）が制定されるとともに、その仕様が完全に公開されました。また、インターネットにおけるプライバシー保護に欠かせない公開鍵暗号や、その応用である電子署名の技術が発明されたのも 1970 年代です。ここから現代暗号が情報科学の一分野としてスタートしたと言えます。

現代暗号では、暗号の設計技術と暗号の解読技術が等しく重要視されます。学会などで仕様が公開された暗号アルゴリズムは、世界中の研究者が（学術的な）解読を試み、その結果は論文として公開されます。そして何年にもわたる解読研究に耐えて生き残ったアルゴリズムこそが世界からの信頼を獲得できるのです。この意味で、世界標準を目指すレベルの暗号は、その設計指針を含め仕様を公開することは必須であるとのコンセンサスが研究者の間であります。

三菱電機は現代暗号の研究を解読技術からスタートしました。その結果生まれたのが「線形解読法(linear cryptanalysis)」と名付けた新しい暗号解読手法です [1]。この原理は、与えられた暗号アルゴリズムを線形近似し、もとのアルゴリズムを解読するかわりにこの近似された、より簡単なアルゴリズムを解読するという考え方です。もちろんもととは違うものを解読している以上、この解読が常に成功するとは限りませんが、解読に利用できるデータ量が多ければ、それによってアルゴリズムの差を補うことができ、成功確率が高まっていきます。

筆者は 1993 年に線形解読法をもちいて世界ではじめて DES の解読実験に成功しました [2]。第１図はその時にもちいた 12 台の計算機のうちの１台です。これは、当時最新鋭のワークステーションコン

ピュータでしたが、現在の PC は価格性能比（例えば 10 万円あたりの性能）でみると、これより 1000 倍以上高速です。当時 12 台で 50 日かかった計算も、今では 1 台の PC で 1 日か 2 日あれば同じ実験が再現できるでしょう。暗号解読技術における計算機の役割はきわめて大きいものがあります。

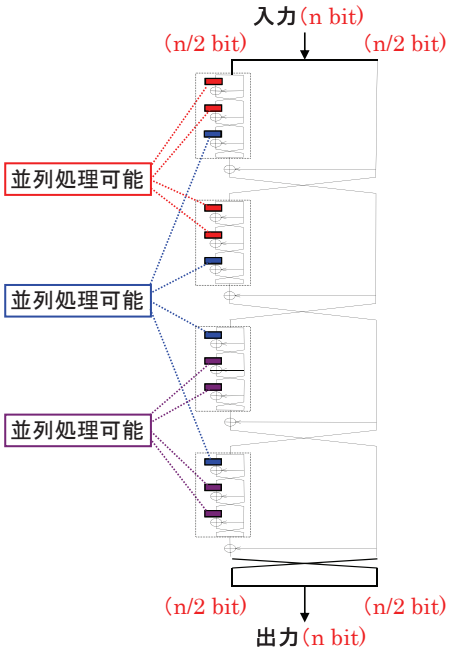
第 1 図　DES 解読にもちいた計算機

3. MISTY の開発と標準化

次にわれわれが取り組んだのは、新しい暗号アルゴリズムの開発でした。線形解読法でも解読できない暗号、しかもソフトウエアでもハードウエアでも小型かつ高速に実装できる暗号を目標にしました。この結果生まれたのが MISTY です [3]。MISTY は線形解読法で解読することが困難であることが数学的に証明されていることが大きな特徴のひとつです。

ところでこの当時 1990 年代半ばは、PC の急速な高性能化と低価格化にともない、PC 上のソフトウエアで高速な暗号化が求められていた時代でした。しかしながら MISTY は高速化もさることながら、小型化にも力点をおいて設計されました。これは半導体部門からの要請があったことによるのですが、当時の暗号の設計指針としてハードウエアを考慮したのは珍しい部類にはいると思います。小型というキーワードはのちに携帯電話の暗号標準化において、消費電力の低減の観点から重要な役割を果たすことになります。

第 2 図は MISTY の基本構造をあらわしています。MISTY の特徴は入れ子構造（Recursive Structure）にあります。小さな関数を何回も繰り返して全体の暗号アルゴリズムを構成しているため、小型化したい場合には、この最小のコンポーネントを 1 つだけ持たせてそれを繰り返し用いることで暗号化することができますし、またこのコンポーネントを複数持ってそれらを並列処理させることにより高速化することも可能です。



第 2 図　MISTY の再帰構造

MISTY の解読困難性の数学的証明や、ハードウエアでの小型・低消費電力が評価され、2000 年には MISTY を携帯電話用にカスタマイズした KASUMI 暗号が第三世代携帯電話（W-CDMA）の世界標準暗号に採用されました [4]。この規格は標準化団体 3GPP により制定されたもので、日本では NTT ドコモ , SoftBank の携帯電話に採用されています。さらに 2002 年には欧州現世代（第二世代）の携帯電話通信規格 GSM の標準暗号のひとつにも KASUMI が採用されました。現在 KASUMI 搭載の携帯電話の総加入数は世界中で数十億に達すると報告されています [5][6]。このほか、MISTY は日本の電子政府推奨暗号（CRYPTREC）や ISO 標準暗号（ISO/IEC 18033-3）にも採用されています。

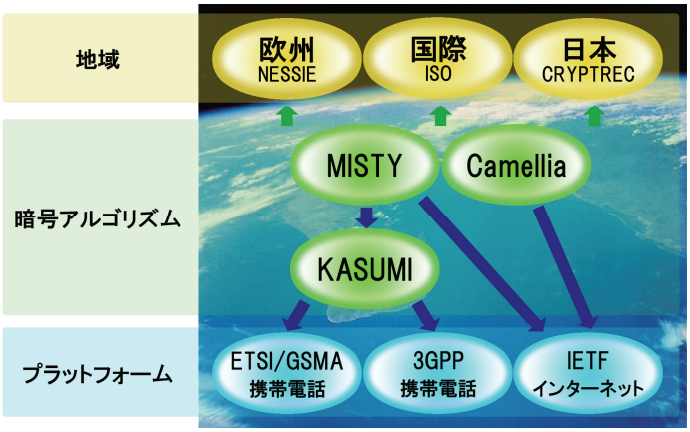
情報通信機器の小型化にともなって、そこで使われる暗号には、高速化よりも小型・低消費電力が強く求められる時代になったことが、小型を設計指針のひとつとしていた MISTY の世界標準採用につながったと言えると思います。

4. Camellia 暗号の開発

MISTY が世に出たのち、米国では DES にかわる新しい連邦政府標準暗号の制定プロジェクトが開始され、2000 年には Rijndael と呼ばれる暗号が米国政府新暗号 AES（Advanced Encryption Standard）に選定されます。MISTY はデータの暗号化が 8 バイト単位であるなど、DES と同じくいわば旧世代に属するインターフェースをもっているのに対し、AES は 16 バイト単位の暗号化や 256 バイトなど長い鍵のサポートなど新しいインターフェースをもつものです。

NTT と三菱電機は 2000 年に、共同で AES と同じインターフェースをもつ次世代暗号 Camellia を開発し、その仕様を公開しました [7]。Camellia はインターネットでの標準暗号化を目指しており、現在まで ITU-T, ISO/IEC, IETF など数多くの標準化団体で認定されています [8]。また商用製品とともに、さまざまなオープンソースプロジェクトでも採用されています。これには世界中で用いられているブラウザである FireFox が含まれます。

なお、MISTY, Camellia ともその基本特許は無償化されています。これは DES や AES など米国政府標準暗号の多くが無償で利用できることにならったもので、実際、暗号の標準化においては無償化が要求されることも少なくありません。暗号開発にコストをかけた企業にとっては、特許の無償化は勇気のいることですが、一方で、無償化することによりユーザが増え、第 3 図に示すような標準採用で知名度が高まったことは、結果的にビジネスの機会が増えることに結びついたため、無償化の意味は十分あったと考えています。



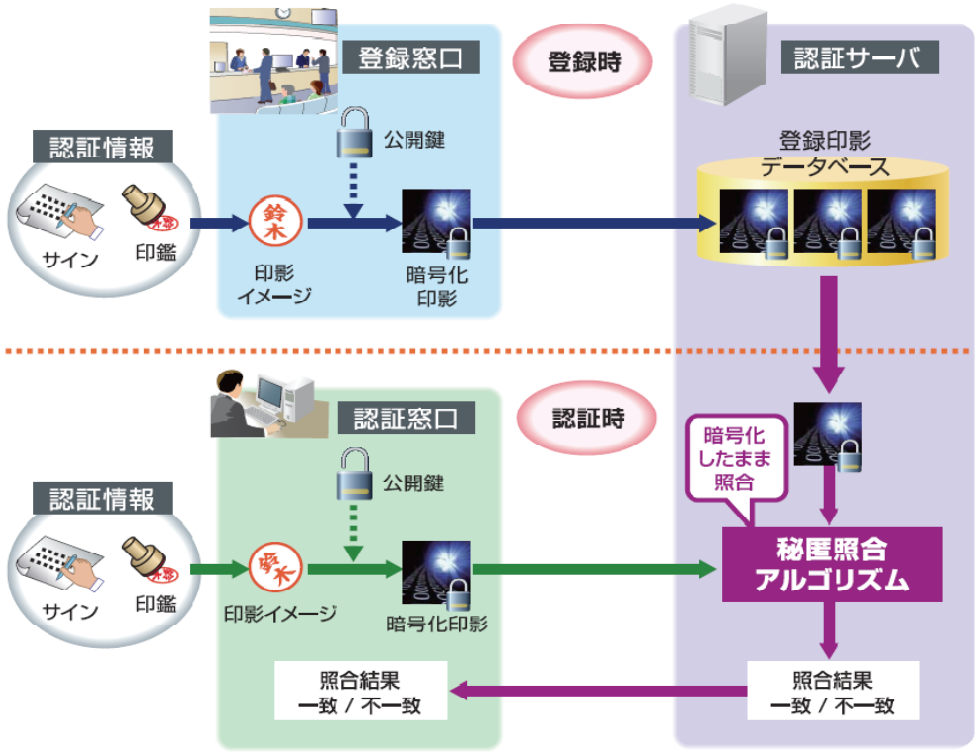
第 3 図　MISTY, Camellia の標準化

5. クラウド時代の暗号技術

昨今のクラウドコンピューティングの普及にともない、情報資産やその利用環境を自前で維持管理するのではなく、アウトソースすることにより、運用コストを削減する動きが盛んになっています。一方でこれにともない、データセンターなどサービス提供者側のセキュリティリスクの増大に対する対策がこれまで以上に重要となっています。このリスクには、設定のミスや機器の障害によるものだけでなく、データセンターの管理者による意図的な情報操作も含まれています。

三菱電機では、クラウド時代の暗号技術として、暗号化したまま情報処理を行うことにより、プライバシー保護とクラウド環境での情報サービスの利便性の両立をはかる技術開発にとりくんでいます。このモデルでは、プライバシー情報は常に暗号化してからデータセンターに登録され、データセンター側は、ユーザからのリクエストに応じてこの暗号化された情報を復号することなく、所定のサービスを行います。この技術が実現すると、データセンターは情報流出のリスクを最小限に抑えたサービスの提供が可能になります。

第 4 図は、2009 年に三菱電機が開発した「秘匿照合」技術の概要を示したものです [9]。これは個人を特定するための情報（認証情報）を暗号化したまま個人認証を行う技術で、図では印影の例で示していますが、指紋などの生体認証にも応用することができます。まずユーザは登録窓口で認証情報を暗号化してからデータセンターの認証サーバーに登録します。そして本人認証が必要になったら認証窓口でふたたび認証情報を暗号化して認証サーバーに送信します。認証サーバーは、登録時と認証時の（暗号



第 4 図　秘匿照合の例

化される前の）認証情報が類似していたかどうかを、暗号化された 2 つのデータだけから、秘匿照合アルゴリズムを使って判定します。

登録時の認証情報と認証時の認証情報（図では印影イメージ）はディジタル情報として完全には一致しませんので、類似しているかどうかを暗号化したまま判定しなければならいことに注意してください。ここでは 2 つのベクトルの内積を暗号化したまま計算できるという、新しいタイプの暗号技術が利用されています [10]。このような技術の必要性は、今後のクラウド環境の広がりとともにますます高まってくるものと考えられます。

6. 耐タンパー技術

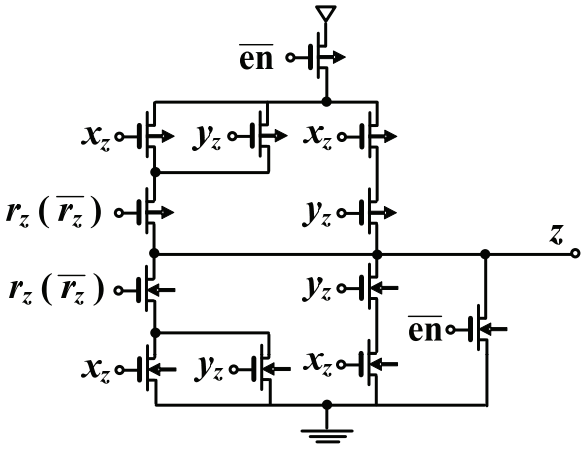
暗号技術の応用範囲が広がり、個人がもつ情報通信機器に暗号が搭載されることが普通になるにつれ、暗号を搭載した半導体に対する不正アクセス対策も重要になってきています。特にサイドチャネル攻撃と呼ばれる、暗号システムの外側から観測可能な物理現象をもとに非破壊で秘密情報を暴く手法が、IC カードなどの実システムで有効であることが示されて以来、暗号ハードウエアを物理的に守る耐タンパー技術が現代暗号において重要な研究分野として確立されるようになりました。

サイドチャネル攻撃として有効な物理現象にはさまざまなものがありますが、例えば秘密情報の値によって暗号化時間が変化するような実装を行っていると、逆に暗号化時間から秘密情報が推定できることになります。このような手法はタイミング攻撃と呼ばれ、これを防ぐためには、どのような入力に対しても同じ時間で暗号化が終了するようなプログラムあるいは回路を設計する必要があります。

さらに高度で有効なサイドチャネル情報として、半導体の電流消費量があります。電流消費量を何度も観測して得られた情報を統計処理すると秘密情報が得られるという電力攻撃は、強力なサイドチャネル攻撃手法として知られています。この解読を防止するためには電流消費量が一定になる、あるいはランダム化されるになる必要がありますが、三菱電機では RSL（Random Switching Logic）と名付けた

ハードウエア回路とそのシミュレーション技術を用いることにより、電力攻撃を有効に阻止することに成功しています [11]。第 5 図は RSL による NAND/NOR 回路の一例です。乱数入力による電力情報のランダム化と、信号の伝達速度を一定するメカニズムから構成されています。

また最近では PUF（Physical Unclonable Function）と呼ばれる、半導体素子の物理的なばらつきを利用してチップ個々に異なる情報をとりだし、それを暗号化に有効に利用する回路設計技術が注目を集めています。これは半導体のいわば指紋認識技術ともいえますが、このような高度な暗号ハードウエアの技術は今後ますますに重要になると思います。



第 5 図　RSL を用いた NAND/NOR 回路

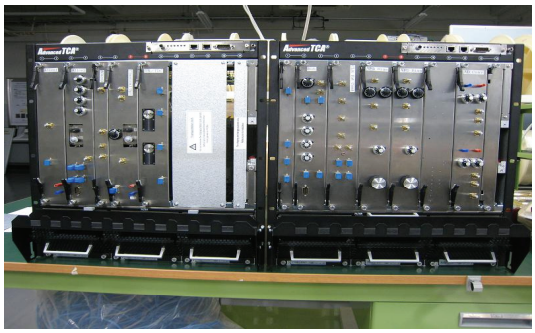
7. 究極の暗号：量子暗号

量子暗号は、現在我々が利用している暗号技術とは全くその原理が異なった、量子物理の法則を解読困難性の根拠とする暗号です。量子暗号は基本的には光通信なのですが、光の粒 1 つ 1 つに情報をのせて伝送するという点で従来の光通信とは根本的に異なっています。光の粒、すなわち光子は観測をうけると物理状態が必ず変化するという量子力学的特性をもっています。このことは、単一光子レベルで情報のやりとりをした場合、第三者による盗聴がおきると通信路のノイズが必ず増えるので、盗聴行為そのものがほぼ即座に検知できることを意味しています。このことから量子暗号は解読が不可能な究極の暗号と呼ばれているのです。

現代暗号のほとんどは、その解読困難性の根拠を計算量においています。たとえば解読するにはスーパーコンピュータで 1 億年かかるから実際には解読はできませんというわけです。しかし、将来量子コンピュータのような、超並列計算を瞬時に行ってしまう計算機が実現したら（いつ量子コンピュータが実現するかには楽観的な意見から悲観的なものまでさまざまあるようですが）、現代暗号は簡単に解読されてしまうかもしれません。特に現在インターネットで広く用いられている公開鍵暗号は、量子コンピュータができると多項式時間でその解読ができてしまうことが理論的に知られています。

このような背景のもと現在量子暗号の研究開発が世界的に行われており、当社も 2000 年ごろから量子暗号の研究開発にたずさわっています。第 6 図はわれわれが現在開発している量子暗号装置であり、今のところ現代暗号のように安価なものとはいえないものの、量子暗号はもはや未来の暗号ではなく、その技術はすでに実用レベルに到達したということができます。

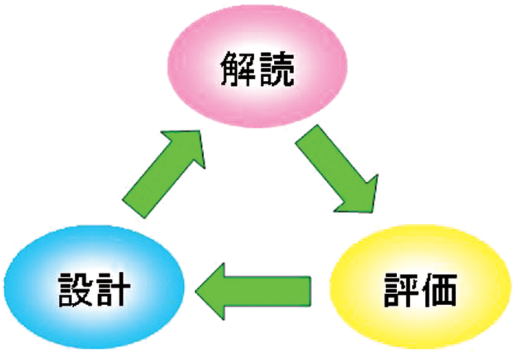
一方で量子暗号は単一光子によって情報を伝送するため、通信距離が増えると損失も増加し、伝送速度が低下するという特性をもっています。たとえば 50km で 1Mbps 程度が現在の世界記録です。また量子暗号でできることは、正確には 2 点間の乱数の共有であり（ただし乱数が共有できればそれを鍵として暗号通信ができる）、速度や距離を向上させるとともに、量子暗号の応用プロトコルを増やしていくことも今後の研究課題となっています。



第 6 図　現在開発中の量子暗号装置

8. まとめ

本稿では三菱電機における暗号技術の研究開発の実例を紹介しながら、現代暗号におけるいくつかのトピックを取り上げました。われわれが暗号の解読技術からスタートしたというのは今考えると重要であったと思います。暗号を解読するということは、別の見方をすると暗号の安全性を評価しているとも言えるわけで、この点では新しい暗号解読法を考案することは、新しい暗号評価指標を考案することと同じといえます。そして新しい暗号評価指標が打ち立てられれば、その評価指標でよいスコアが出るような新しい暗号方式を設計するまでの道のりは遠くありません。第７図のように解読、評価、設計のサイクルをまわしていくことは、暗号技術だけではなく、実はあらゆる新技術開発で有効なのではないかと考えています。



第７図　暗号技術研究開発のサイクル

参考文献

[1] M. Matsui: “Linear Cryptanalysis Method for DES Cipher”, Proceedings of Eurocrypt’93, Lecture Notes in Computer Science 765, Springer Verlag (1993)

[2] M. Matsui: “The First Experimental Cryptanalysis of the Data Encryption Standard”, Proceedings of Crypto’94, Lecture Notes in Computer Science 839, Springer Verlag (1994)

[3] M. Matsui: “New Block Encryption Algorithm MISTY”, Proceedings of FSE’97, Lecture Notes in Computer Science 1297, Springer Verlag (1997)

[4] “KASUMI (block cipher)”, http://en.wikipedia.org/wiki/KASUMI_(block_cipher)

[5] UMTS Forum, http://www.umts-forum.org/

[6] GSM World, http://www.gsmworld.com/

[7] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, “Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis”, Proceedings of SAC 2000, Lecture Notes in Computer Science 1297, Springer Verlag (2000)

[8] Camellia Homepage, http://info.isl.ntt.co.jp/crypt/camellia/index.html

[9] 服部充洋，柴田陽一，伊藤隆，松田規，高島克幸，米田健：“2-DNF 準同型暗号を用いた秘匿生体認証”，信学技報，vol.109, no.271, ISEC2009-68 (2009)

[10] T. Okamoto, K. Takashima: “Homomorphic Encryption and Signatures from Vector Decomposition”, Proceedings of Pairing 2008, Lecture Notes in Computer Science 5209, Springer Verlag (2008)

[11] D. Suzuki, M. Saeki, T. Ichikawa: “Random Switching Logic: A New Countermeasure against DPA and Second-Order DPA at the Logic Level”, IEICE Transactions 90-A (1): 160-168 (2007)