暗号技術の最先端

Leading Edge of Cryptography

● 下山武司　● 竹本一矢　● Arnab Roy　● Avradip Mandal

あらまし

暗号技術は，デジタルTV放送や電子マネー，携帯端末など，日常生活のあらゆるところで使われている情報セキュリティの基盤技術である。暗号の歴史は解読の歴史と言っても過言ではない。絶対に安全と言われた暗号も，時代とともに新しい解読法の発見や，計算機・ネットワークの急速な進歩によって危険にさらされ(暗号の危殆化)，やがて新しい暗号技術の開発へと進んできた。

本稿では，これらを踏まえた富士通研究所の取組みを中心に最新の暗号技術を解説し，暗号解読技術の進歩を考慮することで暗号の寿命を正しく把握する技術や，従来の暗号にない優れた機能を持った新しい暗号技術を紹介する。更に，解読が不可能な究極の暗号と言われる量子暗号を解説する。

Abstract

Cryptography is a fundamental technology for information security used in all scenes of daily life including digital TV broadcasting, e-money and mobile devices. It is not too much to say that the history of cryptography is the history of cryptanalysis. Cryptograms said to be absolutely safe have been exposed to threats (compromise of cryptograms) as new decryption methods have been discovered and computers and networks have made rapid progress along with the times and eventually led to development of new encryption technologies. This paper presents the latest encryption technology mainly including Fujitsu Laboratories' activities with this situation taken into account. It describes a technology for correctly grasping the life of a cryptogram in view of the development of decryption technology, new encryption technology provided with excellent features that conventional cryptograms do not have and quantum cryptography, which is said to be the ultimate cryptogram impossible to decrypt.

ま え が き

今日，様々な機器がネットワークにつながり，情報がインターネットを通じてやり取りされ，多くのデータが日々生成され続けている。こうした情報には，生成されてすぐにその価値を失ってしまうものから，半永久的に個人や社会に影響を及ぼし続けるものまで，実に様々である。その中でも機密性・機微性の高い情報については，情報を確実に守るための手段が強く求められている。これまでこうしたデータを守る技術的な手段の一つとして，暗号技術が使われてきた。

暗号技術の歴史は，古代ローマ時代の極めて古典的なものから始まったとされている。その後，中世ヨーロッパでは複数の換字表の利用により強度が向上した多表式暗号が開発され，第二次世界大戦中に使われた機械式暗号，更に現代に入りコンピュータプログラムによる複雑な暗号アルゴリズムへと進化を続けてきた。これらのうち，古代から近代にかけて利用された暗号技術は，科学技術が進歩した現在では通用するものではない。一方で，当時の最先端技術が駆使されていることから，時代を映す鏡であるとも言える。

そして，現在の暗号技術を見てみると，例えば公開鍵暗号の主流であるRSA暗号は，1977年に開発されたものである。当時最先端の数論技術により暗号鍵を公開するという画期的な概念を実現することで，それまで実現できなかった秘密鍵配送の問題を解決するに至り，現在の情報社会の基盤技術となっている。このように，数十年前に開発された暗号が現在普及していることを考えると，今まさに最先端で研究されている暗号技術は，未来の社会を予測することにもつながるのかも知れない。このような中，富士通研究所でも最新の暗号技術の研究開発に取り組んでいる。

本稿では，まず現代暗号の解読技術とそこから導かれる暗号の寿命，およびライフサイクルについて述べる。次に，暗号技術の機能面にフォーカスし，これまでの暗号では実現が難しかった新しい機能を持つ暗号技術の一つとして，暗号の宿命である鍵管理の手間を大幅に削減可能なRelational Hashについて述べる。更に，あらゆる暗号が解読されるようになる（危殆化）問題を根本から解決可能な究極の暗号と言われている量子暗号について述べる。

解読技術～暗号寿命とライフサイクル

● 暗号の種類と暗号強度のバランス

インターネット，携帯電話，デジタル放送，電子マネーなど，現代の情報化社会を構築する重要な基盤技術の一つとして，暗号技術が重要な役割を果たしている。これらの情報システムのほとんどは，多種類の暗号要素技術，すなわち共通鍵暗号・公開鍵暗号・ハッシュ関数などの組合せで実現されている。このような暗号の組合せを考えるに当たり，安全性と処理性能をうまくバランスさせることは，安全かつ実用的な情報システムを構築する上での重要な課題である。例えば，情報システムのセキュリティにおいて，最も脆弱な部分がシステム全体の強度を決定している。このことから，各種情報セキュリティのアプリケーションで選択された暗号には一つたりとも脆弱性があってはならない。更に，暗号の安全性は永久不変ではなく，解読技術の進歩や計算機の処理性能の向上により，いずれは危殆化する運命にある。その一方で，必要以上に強度の高い暗号がシステムの一部に用いられた場合，システム全体のセキュリティにはあまり寄与しないにも関わらず，無駄に計算機資源や電力を消費するため不適切である。よって暗号を利用する場合，それがどのぐらいの強度でいつまで利用できるのかを適切に見極めることが重要である。

次節では，標準暗号として使われているRSA暗号について，計算機による世界記録レベルの暗号解読実験に基づいた解読計算量を基に精密に暗号の強度を評価した結果と，世界最高性能のスーパーコンピュータに今後予想される性能の伸び率をも考慮に入れた，暗号強度評価法について述べる。

● 暗号解読計算量と安全性評価

RSA暗号は，公開鍵暗号の標準技術としてあらゆるシステムで使われてきた。これまで様々な攻撃に対する安全性を再評価することで，その都度パラメーターが見直され，安全な暗号として現在でも使われ続けている。

暗号が使われ続けるためには，最先端の技術と最高性能の計算機能力をもってしても，事実上解

読が不可能であるという保証が必要なことから，暗号技術と解読技術は表裏一体の関係にある。つまり最先端暗号解読技術をベースとした，安全なパラメーターの設定が暗号強度を保証する理論的根拠となるわけである。このように，暗号解読は単に暗号の穴を見つけるためだけではなく，実際の攻撃に先んじて穴をふさぎ，適切な暗号利用法や脆弱性回避手段を提示する。そして，暗号の危殆化が進むことが予想される場合には，その代替となる新技術を前もって開発し，あらゆる強度評価・性能評価を事前に実施する。これによって，スムーズな暗号の移行を促し，安定した暗号ライフサイクルの実現により，安全な情報社会を継続させることにつながるのである。

RSA暗号に対する強度を評価する場合，その安全性の根拠となっている素因数分解に着目するのが妥当である。素因数分解アルゴリズムとして，現時点で最も効率的な解法として知られている手法は，一般数体ふるい法（GNFS：General Number Field Sieve）である。[1] 一般数体ふるい法は，1990年にLenstraによって提案されたもので，近年の一般的な合成数に対する素因数分解の大きさに関する世界記録は，全てこの方法によるものである。そのアルゴリズムは，以下の4種類のステップをそれぞれ実施することで結果が得られる。

（1）多項式選択部
（2）ふるい処理部
（3）線形代数部
（4）平方根計算部

これらのうち，（2）のふるい処理が，理論的にも実際においても本質的に最も困難な部分を占めることが知られている。実際に素因数分解の計算量を詳細に求めるためには，実際に素因数分解する必要がある。しかし，RSA暗号において，標準で使われている2048ビットの素因数分解は現実的な時間ではとても実施できない（現在の素因数分解の世界記録は768ビット）。そこで，世界記録レベルのアルゴリズムや実験装置を用いて，その一部を実施することにより，全体の計算量を算出する方法が採られている。

日本では，安全な電子政府を構築する政府推奨暗号技術を定めているCRYPTREC（Cryptography Research and Evaluation Committees）の毎年の報告書で，RSA暗号において標準で使われている1024ビット，1536ビット，2048ビットの各パラメーターの解読に必要な計算量と，安全に利用可能な期間について記載している。[2] その根拠となっているのは，先に述べた統一的な環境で計測されたふるい処理の計算量である。これらの値には，解読アルゴリズムの進歩も加味し，数種類の評価値が記載されている。またこれらを基にした評価値に加え，更に一般数体ふるい法の理論的計算量評価式

$$L_N(s, c) = \exp(c(\log(N)^s \log(\log(N))^{1-s})$$

を用いることで，実験で用いられたビット数以外のパラメーターについても，その解読計算量を評価できる。[3]

暗号の安全性を検討する上で，更に重要なポイントとして計算機能力の向上が挙げられる。計算機の能力は常に進歩を続けているため，現時点の計算機能力を基にした評価ではなく，今後登場すると予想される計算機の能力を基に算出しなければならない。この評価指標として，世界最高性能のスーパーコンピュータにおける性能ランキングTOP500のデータが利用できる。[4] この性能を基に未来のスーパーコンピュータ性能を予測し，暗号を1年間で解読可能な世界最高性能のスーパーコンピュータが登場する時期の推測が可能となる（**図-1**）。

表-1は，RSA暗号の鍵長と計算機能力の向上を考慮に入れたその危殆化時期，および共通鍵暗号の強度について示している。

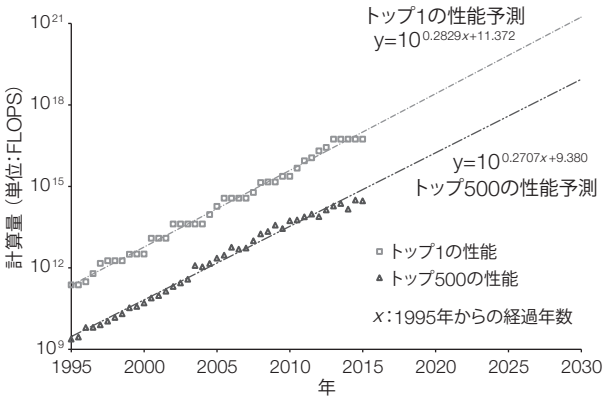


図-1　TOP500のデータを用いたスーパーコンピュータの予測性能

表-1　暗号強度評価と危殆化時期

暗号強度（ビット）	共通鍵暗号方式	公開鍵暗号（RSA）鍵長	危殆化時期
52以下	DES	512	
56		696	1995年
60		768	2000年
64	2TDES	850	2004年
72		1024	2013年
80		1219	2021年
92		1536	2035年
108		2048	2052年
112	3TDES	2206	2056年
128	AES-128	2832	2074年
192	AES-192	6281	2143年
256	AES-256	11393	2213年

Relational Hash ～暗号機能の更なる進化

近年，暗号技術はこれまで主な用途であったデータの秘匿機能を超え，様々な機能を持つ暗号へと進化している。本章では，これまでの暗号技術では実現できなかった用途に向けた機能の拡大について解説する。

●　秘密鍵管理の問題

例えば，過去の犯罪者の指紋データベースがあったと仮定する。このデータベースは，たとえ組織内部の者でも安易にアクセスさせるべきものではないことから，暗号化などで保護しておく必要がある。一方で，捜査の際には容疑者の指紋照合に利用する必要があるため，従来は一時的に暗号を解き，照合することになる。しかし，昨今のデータベースのプライバシー性を重視する場合，指紋照合の際にもデータ自身を秘匿しておく必要がある。このようなことが果たして可能だろうか。

本特集号に掲載されている論文「パーソナルデータのプライバシー保護を実現する匿名化・暗号化技術」で述べられている準同型暗号を用いることがその一つの解決法ではあるが，この技術も完全ではない。準同型暗号では照合結果は暗号化されているため，その結果を得るためには秘密鍵を用いて復号する必要がある。しかし，この秘密鍵を使うとデータベース自身も復号できてしまうため，秘密鍵を持つ検証者にとってはデータが秘匿化されていないのと同じ状況となる。

このような問題を根本から解決する最新の暗号技術が「Relational Hash」である。[5] この技術を用いると，二つの異なるハッシュ関数の値から，値を秘匿したままその二つの入力値の関係を知ることができる。また，検証者が持つ秘密鍵を用いてもデータを復号できないという特長を持つ。もちろん，暗号として要求される一方向性，双一方向性，偽造不可能性といった様々な安全性の要求を満たしている。更に，生体情報のように，採取されるたびにデータに揺らぎがあるような入力に対しても，適切な検索結果が得られるという特長を持っている。

●　関連する既存技術

従来から知られているMD5やSHA-3といった確定的なハッシュ関数の場合，データの一方向性，すなわち，計算は容易だが，逆算は非常に困難である性質を持っているものの，同じ平文に対しては同じハッシュ値となってしまう。このことから，ハッシュ値のみからその関係が類推されてしまい，このような用途に対し十分な安全性があるとは言えない。また，確率的ハッシュ関数と呼ばれる従来技術[6), (7)] を使った場合，ハッシュ値が一意になる問題は解決されるものの，利用可能な平文に強い制約があり，使い勝手が悪い。更に，上記いずれの場合も揺らぎを持つ生体情報のようなデータでは，そのハッシュ値が全く関連のないランダムな値に変換されるため役に立たない。

そのほかの関連技術として，Fuzzy Extractorと呼ばれる種類の技術，例えばFuzzy valut,[8] Fuzzy commitment,[9] Secure sketch[10), (11)] などが知られている。これらは生体情報を用いた認証技術であり，生体情報テンプレートの保護を目的とした技術でもあり，いずれも登録情報のみ保護される。これらは，認証時にはデータが保護されないため，安全性の面で課題があった。Boyen[12] は，「Zero Strage」と名付けられたリモート生体認証によってこの課題の解決を試みた。しかし，データのやり取りが非常に複雑で，実用的な技術とは言いがたかった。

また，関連のある技術として，多重入力関数型暗号（MIFE：Multi-Input Functional Encryption）がある。[13] これは，複数の暗号文から平文の演算で得られる値を算出できる技術である。しかし，本技術で演算可能な値には制約があり，特に近傍の

計算（二つの値の近さ）などは処理が難しかった。

● Relational Hashの仕組み

本節では，Relational Hashの仕組みについて説明する。Relational Hashは，入力された平文について関係式（Relation）を満たすかどうかをハッシュ関数（Hash）を用いてデータを秘匿したまま判定できる。ここでは，例えば0,1から成る三つ組の値x,y,zについて，関係式$x+y=z$の成立を判定する構成を例に説明する。

鍵生成：

与えられたセキュリティパラメーターに対し，素数qの位数を持つ群$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T$上のペアリング演算子$e$を考える。$\mathbb{G}_1$の要素$\mathbf{g}_0$,$\mathbb{G}_2$の要素$\mathbf{h}_0$を抽出し，$\mathbb{Z}_q^*$から，ランダムな要素$\langle a_i\rangle_{i=1}^{n+1}$,$\langle b_i\rangle_{i=1}^{n+1}$を抽出する。また，$\mathbf{g}_i=\mathbf{g}_0^{a_i}$, $\mathbf{h}_i=\mathbf{h}_0^{b_i}$とし，Hashを計算する際に用いる公開鍵を以下のように定める。

$pk_1:=\langle\mathbf{g}_i\rangle_{i=0}^{n+1}$, $pk_2:=\langle\mathbf{h}_i\rangle_{i=0}^{n+1}$, $pk_R:=\sum_{i=1}^{n+1}a_i b_i$

ハッシュ関数1：

与えられた0,1からなる平文$x=\langle x_i\rangle_{i=1}^{n}$と公開鍵$pk_1:=\langle\mathbf{g}_i\rangle_{i=0}^{n+1}$に対し，ハッシュ値を次のように定める。なお$r\in\mathbb{Z}_q^*$は，ランダムサンプリングされた値とする。

$hx:=(\mathbf{g}_0^r,\langle\mathbf{g}_i^{(-1)^{x_i}r}\rangle_{i=1}^{n},\mathbf{g}_{n+1}^r)$

ハッシュ関数2：

同様に，与えられた0,1からなる平文$y=\langle y_i\rangle_{i=1}^{n}$と公開鍵$pk_2:=\langle\mathbf{h}_i\rangle_{i=0}^{n+1}$に対し，ハッシュ値を次のように定める。なお$s\in\mathbb{Z}_q^*$は，ランダムサンプリングされた値とする。

$hy:=(\mathbf{h}_0^s,\langle\mathbf{h}_i^{(-1)^{y_i}s}\rangle_{i=1}^{n},\mathbf{h}_{n+1}^s)$

検証：

二つのハッシュ値$hx=\langle hx_i\rangle_{i=0}^{n+1}$, $hy=\langle hy_i\rangle_{i=0}^{n+1}$と，$z=\langle z_i\rangle_{i=1}^{n}$に対し，以下の式の成立を検証する。

$$e(hx_0,hy_0)^{pk_R}=e(hx_{n+1},hy_{n+1})\prod_{i=1}^{n}e(hx_i,hy_i)^{(-1)^{z_i}}$$

（アルゴリズム終了）

● Relational Hashの応用

本節では，Relational Hashの更に便利な機能として，二つのデータの近さを検証する方法について述べる。具体的には，値の組x,yが，次の関係式$\mathrm{dist}(x,y)<\delta$を満たすかどうかをハッシュ値の値から判定する。なお，$\mathrm{dist}(x,y)$はハミング距離を意味し，δはn未満の整数である。この処理は，生体認証スキームをサーバで行う際に，より安全に行うための応用として期待されている（**図-2**）。

Relational Hashの構成には，$(n,k,2\delta+1)$線形誤り訂正符号を準備し，線形符号の符号化をEncode，復号Decodeとする。またweight(x)をxのハミング重みとする。このとき，誤差ベクトルeがweight$(e)<\delta$を満たせば，次式が成立する。

$\mathrm{Decode}(\mathrm{Encode}(m)+e)=m$

またweight$(e)>\delta$のときは，Decodeは記号$\perp$を出力することとする。本応用の手続きは以下のとおりである。

鍵生成：

上記線形符号に対して，線形性に関するRelational Hashを構成し，それぞれ鍵生成KeyGenLinear，ハッシュ $\mathrm{HashLinear}_1$, $\mathrm{HashLinear}_2$，検証VerifyLinearを構成しておく。また，KeyGenLinearの出力をpk_{lin}とするとき，公開鍵を以下のように決める。

$pk:=(\mathrm{Encode},\mathrm{Decode},pk_{lin})$

ハッシュ関数1：

平文xと乱数rに対し$hx:=(hx_1,hx_2)$とする。

$hx_1:=x+\mathrm{Encode}(r)$

$hx_2:=\mathrm{HashLinear}_1(pk_{lin},r)$

ハッシュ関数2も同様である。

検証：

二つのハッシュ値$hx:=(hx_1,hx_2)$, $hy:=(hy_1,hy_2)$に対し，以下を実施する。

$z:=\mathrm{Decode}(hx_1+hy_1)$を求め，記号$\perp$が出力された場合は否，すなわち$\mathrm{dist}(\mathrm{Encode}(z),hx_1+hy_1)>\delta$であることを出力して処理を終了し，そうでない場合は，以下を出力する。

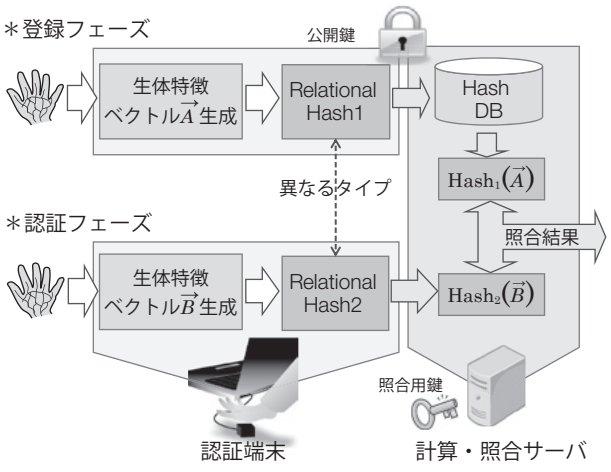


図-2　Relational Hashの生体認証への応用

VerifyLinear (pk_{lin},hx_2,hy_2,z)

（アルゴリズム終了）

本アルゴリズムはパラメーターを適切に設定することで，実用的な処理性能かつセキュリティプリミティブとして，安全な強度とされている80ビットセキュリティを満たすことが数学的に証明できることも大きな特長の一つである。

量子暗号～未来の安全な暗号通信

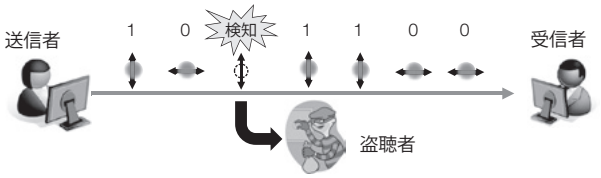
● 現代暗号に潜むリスク

本稿の「解読技術～暗号寿命とライフサイクル」の章で述べたように，現代暗号においては解読技術の進歩を予測した上で暗号強度を適切に設定することにより，情報の秘匿性を担保している。一方で，暗号寿命を越えた解読不可能性は必ずしも保証されない。このため，遺伝子情報など数十年以上の長期にわたって守る必要のある情報の伝達には，より高度な暗号技術が必要とされる。更に，超並列計算可能な量子ゲート型の量子コンピュータが実現すれば，素因数分解に基づくRSA暗号はShorのアルゴリズム[14]により多項式時間で解読できることが知られている。こうした潜在リスクに対応するため，将来的には計算機能力に依存せず絶対解読不可能な暗号技術が求められる。

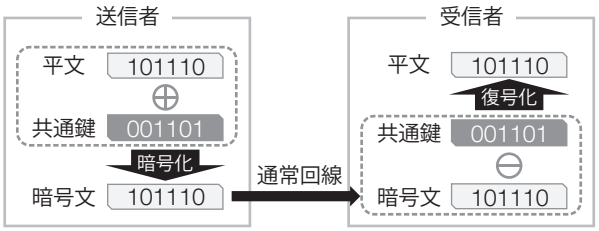
● 量子暗号の概要

量子暗号は，単一光子の量子性を利用した盗聴検知可能な暗号鍵送信と，情報理論的に安全性が証明された使い捨て鍵暗号（ワンタイムパッド）を組み合わせることにより，無条件安全性を保証する暗号通信技術である（**図-3**）。特に前者は量子鍵配付（QKD：Quantum Key Distribution）と呼ばれ，現在世界中の機関で実用化に向けた研究が活発に進められている。QKDのうち最もスタンダードなBB84プロトコル[15]では，光子一つひとつの偏光や位相に暗号鍵の基となる乱数列を載せて送る。単一光子は，それ以上分割できないため部分的に盗み取ることができない。更に，盗聴者が鍵情報のコピーを試みれば，量子力学の不確定性原理により光子の状態に変化が生じる。正規ユーザーはこれを検知して排除することで，残された乱数を秘密鍵として安全に共有できる。

BB84プロトコルに基づくQKDでは，光子を任意のタイミングで一つずつ発生させる単一光子源



(a) 量子鍵配付（暗号鍵となる乱数列を光子一つひとつに載せて伝送・共有）



(b) ワンタイムパッドによる暗号化（共有した乱数列を共通鍵として暗号化通信）

図-3　量子暗号の仕組み

（SPS：Single-Photon Source）が必要となる。しかし，SPSの開発が容易でないことから，ほとんどの実証実験ではレーザー光を著しく弱めた微弱レーザー光（WCP：Weak Coherent Pulses）が用いられてきた。WCPを用いる場合，盗聴の原因となる複数光子が高い割合で同時発生してしまう問題がある。この場合，盗聴者は複数光子のうち1個だけを盗み，残りを受信者に送ることで盗聴検知を回避できてしまう。そのため，送信者は伝送距離が長くなるほど（すなわち，光ファイバーの伝送損失が大きくなるほど）レーザーの出力光を弱めて複数光子発生確率を下げねばならず，早い段階で検出器ノイズの割合が信号光レベルを上回り，暗号鍵が生成できなくなる（**図-4**点線）。こうした問題に対抗する手段として，WCPに強度の異なる数種の微弱光（おとり光）を人為的に混ぜて盗聴検知に用いる修正型のBB84プロトコル（デコイ方式）が提案され，[16]現在広く用いられている。デコイ方式を用いれば，単純なWCPに比べ鍵生成率の低下を抑え，伝送距離を大幅に伸ばせる（図-4一点鎖線）。一方で，装置構成や鍵抽出処理が複雑化し，セキュリティを維持するためには装置の管理・運用に細心の注意が必要となるといった問題も生じる。これに対し，理想的なSPSを用いれば，理論上最も高い伝送性能を実現できるだけでなく（図-4実線），1パルスあたり1個の光子しか発生しないため，

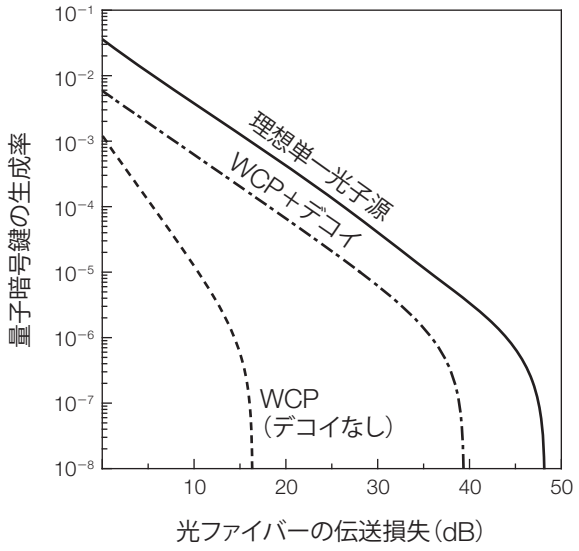


図-4　量子暗号鍵生成率と伝送損失の関係

鍵処理や装置構成の大幅な単純化も可能となり，量子力学によって証明可能な高い安全性が得られる。

●　1.5 μm帯単一光子源とQKDシステム

富士通研究所では，こうした単一光子QKDの実現に向けて，文部科学省イノベーションシステム整備事業「先端融合領域イノベーション創出拠点形成プログラム」において，東京大学の荒川泰彦教授，NECとの3者共同による，波長1.5 μm帯での高性能単一光子源の開発，およびこれを組み込んだ長距離単一光子QKDシステムの開発に取り組んできた。

1.5 μm帯量子ドット単一光子源の構成を**図-5**に示す。単一光子を発生させるには，量子ドットと呼ばれるナノメートルサイズの半導体微結晶を利用する方法が一般的である。量子ドットへ光照射を行うと電子－正孔対が内部に生成され，これらが再結合するタイミングで光子が放出される。筆者らは更に，光学的ホーン構造と呼ばれる微細なパラボラ型形状を量子ドットの周囲に形成し，外部への光子取り出し効率を高める工夫を行っている。[17]

SPSの重要な性能指数の一つが，複数光子の発生がどれだけ抑制されているかを示す$g^{(2)}(0)$という指標である。$g^{(2)}(0)$は単一光子の純度を示し，WCPでは$g^{(2)}(0)=1$，理想的なSPSでは$g^{(2)}(0)=0$となる。この値が低いほど複数光子の発生が少なく，より長距離のQKDが実現できることを意味する。従来，1.5 μm帯SPSを用いてQKDの実証実験を行った際は伝送距離が50 kmにとどまっていたが，[18] これは$g^{(2)}(0)$値が0.055と比較的高めであったことが理由の一つである。これに対し筆者らは最近，量子ドットに照射する励起パルスを圧縮することで複数光子発生を抑制することに成功し，従来比25分の1以下となる$g^{(2)}(0)=0.002$を達成した。これは，複数光子の同時発生率に換算するとパルスあたり100万分の1であり，単一光子純度としては世界最高水準となる。更に，この高純度SPSを超低ノイズの超伝導単一光子検出器をベースとするQKDシステムに組み込んで伝送実験を行った結果，単一光子方式で世界最長となる120 kmでの安全鍵伝送が実証された。[18] これは，首都圏の主要都市をカバーできる距離であり，盗聴不可能な都市圏セキュアネットワーク実現に向けた大きなマイルストーンと位置づけられる。

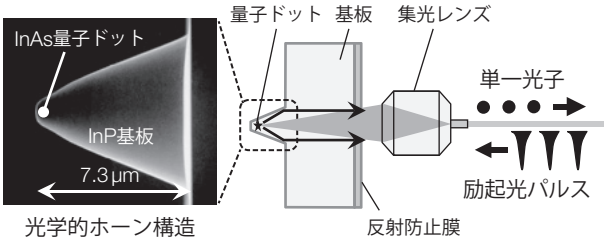


図-5　1.5 μm帯量子ドット単一光子源

む　す　び

本稿では，暗号解読技術の進歩を考慮して暗号の寿命を正しく把握する技術や，従来の暗号にない優れた機能を持った新しい暗号技術，更に解読が不可能な究極の暗号と言われる量子暗号など，最先端の暗号技術を紹介した。

冒頭でも述べたように，現在広く普及している暗号技術が数十年前に開発されたものであることを考えると，本稿で紹介した最先端技術が実用化されるのは，同じく数十年先のことになるかも知れない。しかし，富士通研究所が開発しているこれら最先端の暗号技術は，長年の研究実績を積み重ねて得られたものである。これらの取組みによって，現在はもとより将来にわたって，富士通が担うべき安全な情報化社会のインフラ構築の実現が

可能になる。本稿で記載した技術が，将来の安全なシステムの基盤技術として役立てられれば幸いである。

なお，本稿の「量子暗号～未来の安全な暗号通信」の章に記載された研究は，文部科学省イノベーションシステム整備事業の支援により遂行されたものである。

参考文献

(1) A. Lenstra et al.：The Number Field Sieve, STOC 1990，p.564-572，ACM，1990.
(2) CRYPTREC：CRYPTREC Report 2014. 情報処理推進機構・情報通信研究機構，2014.3.
(3) M. Yasuda et al.：On the Strength Comparison of the ECDLP and the IFP. SCN2012，p.302-325，2012.
(4) TOP500 Supercomputer Sites. http://top500.org
(5) Avradip Mandal and Arnab Roy：Relational Hash：Probabilistic Hash for Verifying Relations, Secure against Forgery and More. CRYPTO 2015, volume 9215 of LNCS，p.518-537. Springer，August 2015.
(6) R. Canetti：Towards realizing random oracles：Hash functionsthat hide all partial information. CRYPTO'97，volume 1294 of LNCS，p.455-469. Springer，August 1997.
(7) R. Canetti et al.：Perfectly one-way probabilistic hash functions（preliminary version）. In30th ACM STOC，p.131-140. ACM Press，May 1998.
(8) A. Juels et al.：A fuzzy vault scheme. Cryptology ePrint Archive，Report 2002/093，2002.
(9) A. Juels et al.：A fuzzy commitment scheme. In ACM CCS 99，p.28-36. ACM Press，November 1999.
(10) Y. Dodis et al.：Fuzzy extractors：How to generate strong keys from biometrics and other noisy data. EUROCRYPT 2004, volume 3027 of LNCS, p.523-540. Springer，May 2004.
(11) Y. Dodis et al.：Correcting errors without leaking partial information. 37th ACM STOC，p.654-663. ACM Press，May 2005.
(12) X. Boyen：Reusable cryptographic fuzzy extractors. ACM CCS 04，p.82-91. ACM Press，October 2004.
(13) S. Goldwasser et al.：Multi-input functional encryption. EUROCRYPT 2014，volume 8441 of LNCS，p.578-602. Springer，May 2014.
(14) P. W. Shor：Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 26，p.1484-1509（1997）.
(15) C. H. Bennett et al.：Quantum Cryptography：Public Key Distribution and Coin Tossing. IEEE Int. Conf. on Computers, Systems & Signal Processing，p.175-179（1984）.
(16) H.-K. Lo et al.：Decoy State Quantum Key Distribution. Phys. Rev. Lett., 94，230504（2005）.
(17) K. Takemoto et al.：An optical horn structure for single-photon source using quantum dots at telecommunication wavelength. J. Appl. Phys., 101，081720（2007）.
(18) K. Takemoto et al.：Transmission Experiment of Quantum Keys over 50 km Using High-Performance Quantum-Dot Single-Photon Source at 1.5 μm Wavelength. Appl. Phys. Exp., 3，092802（2010）.

著者紹介

下山武司（しもやま　たけし）
知識情報処理研究所
データ・プライバシー保護プロジェクト 所属
現在，暗号技術の研究に従事。

Arnab Roy
米国富士通研究所
ソフトウェアシステムイノベーショングループ 所属
現在，暗号技術の研究に従事。

竹本一矢（たけもと　かずや）
デバイス＆マテリアル研究所
次世代実装プロジェクト 所属
現在，量子情報処理技術の研究に従事。

Avradip Mandal
米国富士通研究所
ソフトウェアシステムイノベーショングループ 所属
現在，暗号技術の研究に従事。