INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

量子暗号通信システムに関する世界的な動向調査報告書
三菱電機株式会社

はじめに

近年になり，相次ぐフィールド試験の報告，試作機の販売等，量子暗号通信システムの実用化がすぐそこまで来ている．量子暗号は物理学の基礎法則に基づき安全性が保証されるため無条件安全性を提供できるはずなのだが，具体的な通信システムにおいては，装置の不完全さにより安全性が低下する可能性が指摘されている．また，従来の量子暗号プロトコルにおける性能限界を凌駕するために提案された新プロトコルの中には，当初の理論解析で期待されたほどの安全性を実現しない，と指摘されているものもある．このため理論的解析のみにとどまらず，実験結果や実装例に着目して安全性を調査・分析することが，今後の量子暗号の普及推進のためにも重要となる．

本調査では，量子暗号通信システムの安全性を，理論および実装の両面から調査する．また 2006 年になって米国や英国で量子暗号システムの標準化の動きが出始めたが，これについても概要を調査する．そしてそれらの結果を反映して，安全な量子暗号システムを選定する際に役立つ明確な判断基準を示す．

量子暗号通信システムに関する文献を入手し，その内容を精査し整理する．また，当社所有の量子暗号実験設備を用いて測定を行える部分に関しては，その測定結果も加えて内容を補足する．そしてそれらを体系化し，調査結果としてまとめる．

１．量子暗号の概要

量子暗号システムの最終的な目標は，従来型の暗号方式(公開鍵暗号など)と同様で，秘密通信(secret communication)を安全に行うことである．一方で従来型の暗号との最大の違いは，「無条件安全性」(unconditional security)が実現できることである．既存の暗号であれば，PC とインターネットがあればほぼ何でも出来るのに対して，量子暗号においては，レーザや光ファイバなど大掛かりな装置が必要となる理由はここにある．そこでこの節ではまず，量子暗号と従来型暗号の機能上の差異は何か，無条件安全性とは何か，また量子暗号ではそれをいかにして実現しているかについて，概要を説明する．

なお一般に暗号というと，広義では秘密通信以外にもデジタル署名(digital signature)や認証(authentication)も含む．しかし現状の量子暗号研究において，実現可能性が見えている暗号機能は量子鍵配送(quantum key distribution, QKD)のみであり，署名や認証用の量子暗号プロトコルの研究は発展途上である．そこで本報告書では専ら，量子鍵配送についてのみ記述する．

１.１ 量子暗号の機能および無条件安全性

量子鍵配送の目的は，送信者 Alice と受信者 Bob の間で，秘密のビット列 $k=(k_1,\mathrm{K},k_n)$，

$k_i \in \{0,1\}$を共有することである．なおかつこのkが，いかなる盗聴者 Eve にも盗み見られていないことを，証明つきで保証できる．ただし“盗み見られない”の意味が通常の暗号とはやや異なる．

- まず，秘密のビット列$k = (k_1, \mathrm{K}, k_n)$を送信者または受信者が自由に選ぶことはできない．もしkを自由に選べるとすれば，初めからメッセージmをkとして選べば，直接に暗号通信ができる．しかし実際のところkの具体的な値は，このプロトコルが終わるまで判明しない（これはプロトコルの構造に起因する）．
- 次に，送ったビット列を途中で誰かに盗み見られた場合，事後の検証でそのことをほぼ 1 の確率で検出できるが，kが盗み見られた事実は覆すことができない．従ってこの場合は，その乱数列kは捨て去って，このプロトコルを再び実行する．そして，乱数列kが盗聴されていないことが検証できるまで繰り返す（この場合もちろん，kの値は毎回異なる）．ここでもし攻撃者 Eve がいつまでも盗聴を続けるとした場合には，Alice と Bob は永遠に秘密通信ができないことになる．
- ただし古典暗号通信の場合でも，攻撃者が通信線を遮断すると同じ状況になるので，このことは決して量子暗号の方が弱いことを意味するものではない．なおここでいう「古典暗号」(classical cryptography)とは，量子力学的性質を利用せずとも実装できる従来型の暗号，たとえば AES や RSA 暗号方式をさす．物理の分野において，量子力学を用いなくても記述できる系や現象を「古典的」(classical) と呼ぶのが慣例となっているため，一般にこのような用語が用いられる．

まとめると量子暗号の機能は，Alice－Bob 間で(毎回異なる)ビット列kを共有することであり，事後の検証に成功した場合には，それが途中で盗聴されていないことを確信できる，というものである．特定のメッセージmを秘密に送るには，まず乱数列kをmと同じ長さだけ共有し，それを秘密鍵として，ワンタイムパッド（one-time pad）で通信する．つまり$C = m \oplus k$を暗号文として送ればいい．

１.２ 無条件安全性

冒頭で触れたとおり，量子暗号の最大の売りは無条件安全性(unconditional security)である。

従来型の暗号はほぼすべて，何らかの計算量的仮定(computational assumption)をおいた上で始めて安全性が保証される．たとえば現在広く用いられている RSA 暗号方式は，素因数分解問題を解く効率的アルゴリズムが現状では知られていない，ということを安全性の根拠としている．しかし一方で，素因数分解問題が困難であるという数学的な証明が得られているわけでもなく，将来そのようなアルゴリズムが見つかって RSA 暗号が破られる，という可能性が残っている．別の言い方をすれば，RSA 暗号の安全性は数学的に無条件に保証されたものではなく，つきつめると，ある経験則に基づいて保証されているにすぎないといえる．

一方で量子暗号においては安全性の根拠として，量子力学のみを仮定して数学的に厳密に安全性証明を行う．したがって量子暗号を破る方法を見つけた場合には，量子力学に反する現象を見つけたことを意味する．しかし量子力学はいわば物理学における大原則であり，実際にその成立以降 80 年近くにわたって矛盾する現象は一切見つかっていない．この意味で，量子暗号は無条件安全性を達成しているといえる．

１.３ 量子暗号の実現方法の概要　―BB84 方式を例として―

このように無条件安全性は重要な概念であるが，その数学的な詳細に立ち入ると内容が専門的になりすぎる上に，紙数も膨大になる．そこで本報告書においては，本節で安全性に関して直感的な説明を行うにとどめる．そして第２節以降で，無条件安全性の証明の進展状況について，結果を中心に述べることにする．

以下本節では「どのような原理によって量子鍵配送の安全性が保たれているのか」という疑問に対する直感的な説明をするために，代表的な量子暗号方式である BB84 方式[BB84]を例に挙げて概略を説明する．量子鍵配送方式としては BB84 方式以外にも，B92 方式，DPSQKD 方式ほか数多くの方式が提案されているが，これらの方式もすべて，多かれ少なかれ BB84 方式の改良版であるので, BB84 方式に集中して説明することによって一般性は失われない．

２．量子暗号の理論的安全性

第 1 節で述べたとおり，量子暗号の最大の目的は無条件安全性を達成することであり，そのためには，理論的な安全性証明が与えられていることが必須である．

２.１ 理想的な装置における量子暗号の安全性証明

送信者・受信者ともに理想的な性能を持つ装置を持っている場合については，BB84 方式の安全性は比較的容易に示せる．安全性証明の理解を助けるために，本節ではまずこの場合に関しての説明を行う．

２.２ 現実的な装置を用いた場合の安全性

現実の装置には必ず不完全性があり，盗聴者がいない場合でも，装置の不完全性によって誤りが発生する．

特に量子暗号においては，通常の光通信に比べて光信号の強度が 7 桁程度小さいため，装置としては雑音の巣窟となる．これまで多くの研究機関によって 100km 前後の長距離実装の報告がなされてきたが，そこでの典型的なビット誤り率は 10%弱である．また Alice が信号を送り出す際に用いる光源も，理想的には厳密な単一光子源を用いることが望ましいのだが，実装しようとすると技術的制約があって困難である．

本節では，このような現実的な装置における量子暗号の安全性解析に関する研究の進展

状況について詳細に報告する．

３．構成要素に求められる要件

前節までの結果を踏まえ，量子暗号にもちいる構成要素の性能に関して，調査結果を報告する．とりわけここでは，安全性および装置の速度性能に影響の大きい二大構成要素として，光子生成器および光子検出器に注目する．そしてそれらに求められる性能要件，および現状の研究開発の状況について報告する．

３．１ 光子生成器

安全性の観点からすると，光子生成器においては光子数分布が重要である．光子数分布が単一光子のそれに近ければ近いほど，量子暗号がより安全となる．すなわち，単一光子(single-photon)の生成率(p(1))が大きく，かつ複数光子(multi-photon)の生成率(p(n) for n>1)が小さい状況である．実験装置を工夫することによって複数光子の確率を下げる方式が複数提案されている．本節では特に以下の３種類の方式に着目して報告する．

- 伝令つき単一光子源(Heralded Single Photon Source, HSPS)
- ターンスタイル素子
- 量子ドット

３．２ 光子検出器

量子暗号の安全性解析を行う場合，光子検出器で重要となるパラメタは検出効率および暗計数である．検出器が敏感であればあるほど，盗聴者の存在によってもたらされた雑音に対しても敏感になり，量子暗号として安全になる．また，検出効率が高ければ高いほど，光ファイバによる損失分を補填できる．具体的には検出効率が高く，暗計数が少ないことが理想である．特に以下の３種類の方式に着目して報告する．本節では特に以下の３種類の方式に着目して報告する．

- APD(avalanche photo-diode)素子
- パラメトリック上方変換
- 量子ドット

４．既存の実装報告および既存製品

本節では量子暗号の実装報告および既存製品についての調査結果を報告する．

量子暗号ではすでに，通信距離 100km 超での実装報告が多くの研究機関によってなされている．また複数のベンチャー企業から量子装置が発売されている．本節では以下の評価基準に従って，これらの製品を評価する．

① 価格
② 装置の大きさ

③ 基本性能

④ 量子暗号としての安全性

⑤ 使いやすさ

安全性に関しては，第２節で最近の理論研究の進展状況を報告した．しかし現状の量子暗号実装において，理論的な要請に従って，安全性要件を厳密に適用して無条件安全性を達成した例は皆無といってよい．これは，実際的な実験環境下において量子暗号の無条件安全性が証明されたのが 2001 年以降であることが大きな要因である．

安全性証明の得られていない時代にも実装は着実に進み，そこでは安全性に関していくつかの楽観的な仮定をおいたまま実装報告がなされてきている．安全性証明が得られた現在においても，そのような仮定をおいたまま量子暗号の通信距離や鍵共有速度を評価することが慣例となっている．主な仮定としては以下のものがある．

- コヒーレント光を単一光子源とみなす
- 個別攻撃のみを想定する
- プラグアンドプレイ方式を安全とみなす

そこで本節では，各製品または実装において無条件安全性を議論するかわりに，これらのうちのどの仮定が用いられているかに着目し，無条件安全性の達成於ける課題を指し示すことにする．

具体的には以下の製品および実装について報告を行う．

- MagiQ Technologies 社製品，MAGIQ QPN SECURITY GATEWAY 7505
- id Quantique 社製品，Vectis および Clavis
- SmartQuantum 社製品, SQBox
- 東芝欧州研による実装報告

５．量子暗号の安全性評価動向

量子暗号の長距離実装の進展および製品化を受けて，量子暗号の標準化を目的とした以下の会議が 2006 年に開催された．同会議に国内から唯一参加された NEC の富田章久氏のご好意により，同氏の報告をベースに会議の内容について紹介する．

- 会議名：Toward Quantum Standards：A Workshop on Quantum Information Technology
- 期間：2006 年 5 月 25-26 日
- 場所：Royal Society, London
- 主催：Quantum Technology Group, Cambridge-MIT Institute & NIST
- 参加者：名簿上 36 名(NIST2, NSA2, NPL3, GCHQ, DTI など米英の政府関係者，
  MagiQ 2, ARC 2, id quantique 1, NEC1, Toshiba 1 等のベンダー，
  Telecordia, AboveNet, Quantum Information Partners, HP2, その他大学)

尚，この会議の運営委員は以下の通りである．

- 組織委員会：Clarles Clark, Chair (NIST)；Mattthias Christandl (Cambridge), Artur Ekert (Cambridge/QTG) and Sonia Schirmer (Cambridge/QTG)
- プログラム委員：Nicolas Gisin (Geneva), Andy Hammond (MagiQ), Richard Hughes (Los Alamos)；Sir Peter Knight (Imperial/NPL)；Mark Heiligman (NSA), Peter Landshoff (CMI)；Seth Lloyd (MIT), Peter Smith (GCHQ), Larry Parker (TBC), Nabil Amer (TBC)

また，同会議について，インターネット上で紹介されている HP は次のものである．
http://www.cambridge-mit.org/events/article/default.aspx?objid=1345

会議の要点をまとめると次の通りである．

- 今回はワークショップを持つことに意義があるという様子で，具体的に決定されたことがあるわけではない．
- 今後継続していくということで，日本でも対応できる体制を作っていくことが必要（日本の政府関係機関の参加が期待されている）．
- 技術的な標準化だけでなく，アプリケーションやビジネスモデルも視野に入っている．
- 量子鍵配送システムの標準化が主目的で開かれたが，物理量の量子標準なども議論された．
- 安全性基準，相互接続性などのワーキンググループと，既存ネットワーク・現代暗号システムとの統合からビジネスモデルまで商業的な検討をするワーキンググループの設置が議論された．
- 各国の標準化機関，関連分野の専門家に参加を呼びかけるべき，等の意見があった．
- 今後も NIST の Charles Clark 氏を中心にこうした議論が展開していくものと思われる．

６．まとめ

本報告書では，量子暗号通信システムの安全性を，理論および実装の両面から調査した．量子暗号の研究が盛んになった 1990 年代後半は，この分野の主眼は安全性の理論的研究，および実験室レベルでの実証実験にあったが，やはて量子暗号装置は徐々に安定性を増し，フィールド実験の報告が複数なされるようになった．そして 2006 年になって，第５節で述べたような量子暗号システムの標準化の動きが出始めるにいたった．

これらの活動は，実態としては標準化活動というよりも量子暗号製品実現に向けたワークショップという色彩が強い．第４節で述べたとおり，現在でもすでに，MagiQ Technologies 社， id Quantique 社，SmartQuantum 社から量子暗号製品が発売されているが，広く利用されているという状況とは言いがたい．このため上記の標準化活動も，すでにある程度の需要が存在している製品に対して標準化を行うものではない．むしろ未だ基礎研究の段階にある製品の需要を，いかにして掘り起こすかという点に主眼がおかれている．

一方で第１節でも述べたとおり，量子暗号と従来型暗号との最大の違いは，「無条件安全

性」の達成である．２.２.２節や４.１節でも述べたとおり，現在では実際にこれが実験室レベルで可能となっている．実装例としては伝令つき単一光子源を用いたもの(２.３.２節)や，デコイ方式によるもの(２.５.２節)がある．しかしこれは主に 2006 年以降の流れであり，それ以前の実装報告では，以下の２種類の仮定を置き，安全性の要件を緩めたうえで安全性評価を行っていた：

- 平均光子数 $\mu = 0.1$ のコヒーレント光を単一光子とみなす．
- 個別攻撃を仮定する．

上記 3 社の製品に関しては，安全性のよりどころとなるパラメタ(ビット誤り率 ε や複数光子生成率 P_{multi})が非公開であるため断言は難しいが，実際に無条件安全性が達成されているとは考えがたい状況証拠がある(４節参照)．

これらの例に見られるように，現在は量子暗号実装における評価基準の端境期であり，これまでの仮定つきの安全性から，仮定なしの厳密な無条件安全性へ移行がなされている．今後の量子暗号研究においては無条件安全性が最低条件となることは必至であり，その流れは当然市販製品にも及ぶと予測される．そして標準化活動（もし今後も持続するなら）においてもこの流れの影響を強く受けると考えられる．

ただし無条件安全性への移行はまだ始まったばかりであり，どこまで安価に効率的に実現できるかが今後の重要な研究課題となる．この方向性の一つとして２.５節で紹介した新プロトコルがあり，例えばデコイ方式は実際に，従来型の BB84 よりも安価に無条件安全性を実現することに成功している．現在これ以外にも DPSQKD 方式などの多くの有望な方式が提案されており，最適方式の決定には少なく見積もっても数年を要すると思われる．つまり従来型の暗号研究の歴史と同様に，方式提案と改良の繰り返しの時代が続くと予測される．

このように現在は，標準化を行って方式を固定するにはあまり時期尚早である．むしろ重要なことは，これまでなされてきたように理論と実験のバランスを保ちつつ方式改良を進めていくことである．そしてそのような量子暗号装置の経済性向上へのたゆまぬ努力が，結果として顧客開拓へと結びついていくと考えられる．