1. 21世紀初頭の暗号技術

9. 量子暗号の最新動向

広田　修
玉川大学学術研究所
hirota@lab.tamagawa.ac.jp

量子暗号が発明されて以来，多くの研究成果が発表されている．しかし，通信速度等の改良技術の困難さから，実用化が見えてこない．本稿は，従来の鍵配送量子暗号と最近提案された実用的な直接暗号通信実現の可能性を持つ新量子暗号の両方についてそれらの基本的考え方と将来展望を解説する．

まえがき

現代の主要暗号は安全性の根拠を複雑性理論あるいは計算量に置き，数理科学とともに著しい発展を見せている[1]．他方，通信過程において，その信号系の物理現象に関する物理学の原理を安全性の保証に使う形式がある．これは物理暗号と呼ばれ，近年，開発が進んでいる量子暗号はこれに属している．具体的技術としての最初の量子暗号は1984年のC. H. BennettとG. Brassardによる秘密鍵の配送プロトコル（BB-84）である[2]．しかし，量子暗号の開発においては，BB-84のような鍵配送のみではなく，従来の暗号のように直接暗号化する共通鍵暗号も考察の対象となり得る．最近，現状の光ネットワーク上で実用化が期待できる共通鍵量子暗号が開発された[3)〜5)]．本稿では両者の原理とその将来展望を解説する．

Bennett-Brassard量子鍵配送

暗号学において完全安全性を実現するには平文より多い鍵数を用いるone time pad法で実行せねばならない．もし大量の鍵を通信によって安全に配送可能であればone time pad法は現実的な暗号になり得る．BB-84は，そのような鍵の配送を量子通信を応用して実現しようとするものである．鍵となる乱数を単一光子などの量子信号で伝送するとしよう．このとき，盗聴者は通信回線に対して測定という行為を実施しなければならない．そこで，「盗聴者は正規通信者に気づかれないように量子信号によって運ばれている情報を測定可能か？」という問題が設定される．量子力学には非直交する量子状態は正確にコピーできないという定理がある．また，量子信号は一度測定すれば測定行為による変化が発生して元に戻せない．BB-84プロトコルはこのような原理を組み合わせて，盗聴者が量子通信回線で正規通信者の通信を傍受しているか否かを検知することによって，安全性を確保する方法である．したがって，情報を送信するための量子信号は単一光子のような量子性の強いものでなければならない．現実の光ファイバー通信回線で単一光子による通信の実施は難しく，実用性は期待できない．では，なぜ欧米で盛んに研究されているのか．それは実用性ではなく，暗号学における原理的な興味による．すなわち，現代暗号では安全性の保証を厳格に証明できないのに対し，この量子暗号系では原則的に安全であることを証明できるのである．すべての通信装置が理想的であればその証明は簡単であるが，非理想系ではかなり難しい．そのため学問的にきわめて魅力的である．現在，無条件安全な機構の存在は証明されているが，有限なパラメータを持つ実験系に対する証明はない．現在報告されている量子暗号の諸実験は無条件安全という保証はなく，それを証明・実装することがホットな話題となっている．現実にBB-84プロトコルを実行するためには，前述のように信号光源として単一光子が必要であり，発明者らによって，そのシステムは現実的な環境では通信速度（鍵伝送速度：100 bps程度）や通信距離（100km程度）に制限があるため，原理実験の域を出ないことが示唆された．これらの欠点を改善するため，量子中継，単一光子生成技術，等々多くのアイディアが提案されているが，いずれも巨視的環境で動作する通信システムとしての実現は期待できそうにない．特に量子中継は量子暗号に何も貢

献しないことは確実である．なぜなら，巨視的環境での量子相関現象（エンタングルメント）の破壊，さらに中継距離の増加に比例して鍵配送速度が指数的に遅くなる深刻な特徴があることによる．このように，BB-84 プロトコルは暗号学における原理の探求の一里塚としてきわめて重要な役割を果たすが，実用化を目指すものではない．

新量子暗号

情報理論的安全性が保証された高速直接暗号通信が通常の光通信によって実現可能な新量子暗号の原理をここに紹介する．

●情報理論的暗号の基礎

情報理論的暗号とは盗聴者が無限の計算能力を有していたとしても，一意に平文を決定できない暗号系である．もちろん，理想的な暗号は one time pad であり，Shannon によりその完全安全性を達成する必要条件は $H(X) \leq H(K)$ であることが示されている．これは Shannon 限界と呼ばれ，盗聴者が正規受信者とまったく同じ暗号文に関する情報を得ることができる場合の条件である．もし，物理的に盗聴者の得る情報に制限があれば，上記のような大量の鍵は必要ないことが知られている．このような観点に立つ研究は情報理論の分野では古くから行われていた．特に，Wyner, Csiszár-Körner は盗聴者の SN 比が正規通信者のそれより悪い通信路では共通鍵なしで完全秘匿通信が可能であることを示している．しかし，一般に盗聴者の SN 比が正規通信者のそれより悪いのは非現実的である．先出の BB-84 は，盗聴者が優位であっても量子通信と公衆回線における通信の組合せによる完全安全な鍵配送の実施法の先駆的成果でもある．U. Maurer は一般的なモデルで，盗聴者の SN 比が正規通信者のそれより良い状況での安全な鍵配送の情報理論的解析を展開した．彼の理論は次の観点から情報理論的暗号理論に重要な概念を提供した．すなわち「環境が盗聴者にとって優位であっても，何らかの手段で正規通信者が優位になり得るなら，安全な暗号通信が成立する」．これは優位さの確立（advantage distillation）と呼ばれる．しかし，BB-84 を含む情報理論的暗号理論は漸近的であり，それから所望の安全性を持つ具体的な暗号通信を設計することは困難である．すなわち，実用化の際にはすべて有限系で設計されねばならない．ゆえに，実際には共通鍵暗号である AES やストリーム暗号を使用せざる得ない．しかし，このような共通鍵暗号では鍵が有限で，かつ再使用されるため原理的に完全安全な暗号にはならない．理論的には計算量的な保証しかできず，真の“provable”な暗号は不可能である．以上が現代暗号学のジレンマである．ここで，次のような問題設定が可能である．「有限の共通鍵による完全安全な暗号は可能か？」．一見，不可能なように思えるが，それへの挑戦が新量子暗号である．

●量子暗号の安全性の保証原理

一般に共通鍵暗号通信では盗聴者は正規受信者と同じ精度で通信回線の信号を入手可能とされる．その設定下では原理的に安全な共通鍵暗号は Shannon 限界によって不可能であることは明白である．しかし，もし，盗聴者の得ることができる信号の精度に原理的な制限を科すことができれば完全安全な暗号を構成できる可能性はある．ここで原理的な制限とは自然界のすべての物理的，数理的な理論を採用しても絶対に超えることができない制限を意味する．量子情報理論によれば情報を伝送する信号の処理に量子力学の原理による種々の制限がある．量子暗号はその制限を利用して情報の秘匿性を保証する技術である．以下に量子暗号に必要不可欠な定理を示す．まず，量子通信のモデルが次のように定義される．情報は量子状態に写像され，それが伝送された後，その量子状態を識別する測定過程を伴う通信路モデルを量子通信と言う．量子状態の識別には不可避な誤りが発生し，量子測定過程の最適問題が公式化される．これまで Bayes 規範が Helstrom－Holevo－Yuen によって，ミニマックス規範が広田–池原によって確立されている．それらの帰結として，量子情報原理の 1 つである定理が成立する．

定理 1：非直交な量子状態は誤りなく識別することはできず，誤り確率の下限が存在する．

一方，量子状態のコピーに関する問題が W. Wootters－W. Zurek, Yuen によって考察され，以下のような結果が得られた．

定理 2：既知の 2 つ以上の量子状態が互いに非直交であれば，それらを正確にクローンする変換処理は存在しない．

これは量子非複製定理と呼ばれる．上記 2 つの定理が量子暗号の原理を支える．BB-84 などは定理 2 が基盤となる．しかし，Yuen は定理 1 に基づき，以下のような新量子暗号の原理に到達した[3), 5)]．

原理（優位性の確立原理）：鍵を知る者と知らない者の量子最適測定の性能差によって優位性の確立が設定されれば，その優位性を破ることは量子力学の法則を破

ることに等しい.

新量子暗号の実装法

● Yuenプロトコルの基本型

送信者と受信者は短いシード鍵Kを共有する．このシード鍵を物理暗号として構築される新型のストリーム暗号のシード鍵として用い，その鍵の知識で盗聴者が優位である通信路に正規通信者の優位性を確立する．このような方式はYuen-2000（Y-00）プロトコルと呼ばれており，その基本型は以下である[4]．

(a) 光送信器において，$2M$値PSKに対応する準巨視的コヒーレント状態が用意され，それぞれ2つを組として情報1と0を送る基底状態とする.
(b) 送信者はシード鍵Kを擬似乱数生成器で長い擬似乱数K^*に伸長し，その列の$\log M$ビットのブロックの十進数に対応する基底をM個の基底集合から選ぶ．ビット信号は選ばれた基底で送信される.
(c) 受信者は送信者と同じ擬似乱数を持つので，どの基底が用いられているか既知のため，信号間距離の長い状況で受信が可能である．ただし，その受信時の誤りは十分小さい条件で使用する.
(d) 盗聴者はシード鍵（さらに擬似乱数列）を知らないので，送信直後の光信号をモニタする際，盗聴者に対して信号は$2M$個のコヒーレント状態の一様な混合状態となり，光波の量子揺らぎに関するSN比は受信者のそれよりきわめて悪い状況となる.

以上より，優位性の確立が達成されており，その優位性の度合いは量子信号検出理論におけるHelstrom公式によって求められる．もし，その誤り率が$P_e(E)\to 1/2$であれば量子力学的原理として盗聴者は情報を得ることができない．Mを十分大きくすれば常に$P_e(E)\to 1/2$となる．このように，盗聴者が最適量子測定を用いてもデータの情報はまったく得られないことが保証される．また，鍵への直接攻撃では，どの量子状態が送信されたかを判定せねばならないが，その際の盗聴者の誤りは量子ミニマックス規範によって評価され，Mを大きくすれば$P^*_e\cong 1$となり，盗聴者の情報はゼロとなる．本方式では，盗聴者の測定に量子力学的に超えることのできない限界があり，その限界はシステムのパラメータを設定すれば厳密に計算可能であるため安全性の保証が理論的に明記できる．さらに，正規受信者と盗聴者のビット誤り特性において，正規受信者のそれがほんの僅かでも優位性があれば，適切なrandamizationによって正規受信者の優位性を増強できるため長距離通信にも適用可能である.

●安全性の証明

ストリーム系の暗号が情報理論的安全であるとは，すべての攻撃に対して以下の条件が成立することである[3]．(a) データに対する暗号文単独攻撃に対し$H(X|Y_E)>H(K)$.(b)既知平文／選択平文攻撃（擬似乱数生成器の構造推定を含む）に対し$H(K|Y_E, X)>0$．ここでXは平文，Y_Eは盗聴者の測定値である．これらは従来の理論や方式では実現不可能である．Y-00は量子個別攻撃に関して上記の特性を有することが証明されているが[5]，量子一括攻撃に関してはまだ証明されていない．しかし，近日中に論文が公開される予定である．最後に，最近いくつかのY-00に対する攻撃の試みがあるがすべて量子力学の原理を破っており，正当な議論ではないことを附記する[5), 6]．

参考文献
1) 辻井重男：暗号と情報社会，文春新書，078(1999).
2) Bennett, C.H. and Brassard, G. : Quantum Cryptography, in Proc. IEEE, Int. Conf. on Computers and et al, p.175 (1984).
3) Yuen, H.P.: A New Approach to Quantum Cryptography, Los Alamos arXiv: quantuph/0311061 v5(2003).
4) Barbosa, G. A., Corndorf, E., Kumar, P. and Yuen, H.P. : Secure Communication Using Mesoscopic Coherent State, Phys. Rev. Lett., Vol.90, 227901(2003).
5) Hirota, O., Kato, K., Sohma, M. and Usuda, T. : Quantum Stream Cipher based on Optical Communication, SPIE Proc. Vol.5551(2004).
6) Yuen, H.P. : Security of Y-00 and Similar Quantum Cryptographic Protocols, to be appeared in Phys. Lett. A(2004).

(平成16年9月30日受付)