■1 群（信号・システム）- 3 編（暗号理論）

12 章 量子暗号

（執筆者：西野哲朗・大久保誠也）［2009 年 4 月 受領］

■概要■

現在，量子情報処理の研究が盛んに進められている．量子情報処理とは，従来の情報処理方式に量子力学の原理を導入したものであり，従来手法では不可能であった様々な技術が実現できると考えられている．この量子情報処理の考え方に基づいて構築された暗号が，量子暗号である．実際，多くの量子暗号は，その安全性の根拠を量子力学の原理に置いている．そのため，将来，どのように技術が進歩したとしても，量子暗号の安全性は物理的に保証される．

量子暗号技術のなかで，最もよく知られているのは量子鍵配送方式である．この技術を用いると，盗聴されることなく，秘密鍵暗号で使用する鍵を二者間で安全に共有することができる．その物理的実装に関する研究も着実に進んでおり，実現可能性は極めて高いと考えられている．

一方，量子情報処理技術を用いた情報共有の研究も行われている．この技術を用いると，物理的な通信路なしに情報のやり取りを行うことや，共有している情報を後から変更することも可能となる．ゲーム理論の量子版である量子ゲームも，ある種のプロトコルと解釈することができるが，量子ゲーム理論においては，従来のゲーム理論では解決できない，「囚人のジレンマ」などを解決することが可能となる．このほかにも，量子コイン投げや量子ゼロ知識証明など，様々な量子暗号技術の研究が行われている．本章では，以上のような内容について，その概要を紹介していく．

【本章の構成】

最初に，本章の内容を理解するために必要な，量子情報処理の基礎知識について述べる．次に，量子鍵配送方式の原理と，その基本的なアイディアを解説する．更に，量子情報処理を用いた情報共有や量子ゲーム，種々の量子暗号への取り組みについても紹介する．

■1 群 - 3 編 - 12 章

12-1 量子情報処理の基礎

（執筆者：西野哲朗・大久保誠也）[2009 年 4 月 受領]

本節では，量子暗号を理解する際に必要となる，量子情報処理の基礎知識を概観する．量子情報処理は，量子力学の原理を導入した新たな情報処理方式である[5, 6, 15, 21]．量子暗号を理解するうえで，特に重要な物理原理は，量子重ね合せの原理と量子もつれ合いの原理である．量子暗号が絶対に安全な暗号であるとされる根拠は，この二つの原理にある[20]．

従来の 1 ビットに対応する情報の基本単位として，量子情報処理では 1 量子ビットという単位を使用する．通常の 0 に表現する状態ベクトルを $|0\rangle$ と，1 を表現する状態ベクトルを $|1\rangle$ と，それぞれ表記する．通常の 1 ビットの情報量には，0 または 1 のどちらかの値を保存することができる．一方，量子情報処理においては，1 量子ビットに 0 と 1 の任意の重ね合せ状態を保持することが可能である．これが量子重ね合せの原理である．量子重ね合せ状態は，一般に，$\alpha|0\rangle+\beta|1\rangle$ と記述される．ここで，α と β は $\|\alpha\|^2+\|\beta\|^2=1$ を満たす複素数であり，確率振幅と呼ばれる．$\alpha|0\rangle+\beta|1\rangle$ は，$|0\rangle$ と $|1\rangle$ が基底ベクトルであるような，あるヒルベルト空間内のベクトルである．2 量子ビットの場合には，基底ベクトル $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ の線形和によって量子重ね合せ状態を表現する．ここで，$|01\rangle$ は $|0\rangle$ と $|1\rangle$ のテンソル積を表している．量子状態の時間発展は，量子重ね合せ状態に対応する状態ベクトルに対する，ユニタリ行列 U の適用として表現される．

量子情報処理装置から値を読み出すためには，観測と呼ばれる処理を行う必要がある．観測を行うと，量子重ね合せ状態の中から，確率振幅の絶対値の 2 乗の確率値にしたがって，ある一つの基底状態を読み出すことができる．例えば，$\alpha|0\rangle+\beta|1\rangle$ を観測すると，$|0\rangle$ が確率 $\|\alpha\|^2$ で，$|1\rangle$ が確率 $\|\beta\|^2$ で，それぞれ読み出される．このとき，異なる基底で観測を行うことも可能である．例えば，

$$
\begin{aligned}
|+\rangle &= 1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle \text{ と} \\
|-\rangle &= 1/\sqrt{2}\,|0\rangle - 1/\sqrt{2}\,|1\rangle
\end{aligned}
$$

の二つの基底で観測を行った場合には，$|+\rangle$ もしくは $|-\rangle$ のどちらかを観測することができる．このような観測を行うと，重ね合せ状態は破壊され，それ以後，観測された値しか読めなくなる．この現象を，波束の収縮という．

次に，量子状態 $\alpha|01\rangle+\beta|10\rangle$ を考えよう．この 2 量子ビットのうちの，左側の量子ビットのみの観測した結果，$|0\rangle$ を観測したとすると，状態は $|01\rangle$ に収縮する．このようにして，左側の量子ビットと右側の量子ビットは無関係ではなく，ある種の関係性を保っている．この現象を量子もつれ合いという．量子情報処理を実現する物理系によっては，量子ビットが離れた場所に存在していても，このような量子もつれ合い状態を保つことができる．そして，片方の量子ビットを観測し波束の収縮が起きた場合には，ほかの量子ビットにも，その結果が直ちに反映される．

量子情報処理を用いると，従来よりも格段に高速に計算が行えることが知られている．例えば，小さな誤り確率で因数分解を高速に実行するショア（Shor）のアルゴリズム[16]を用いると，RSA 公開鍵暗号を高速に解読することができる．また，グローバー（Grover）の解探

索アルゴリズム[9]を用いると，秘密鍵に対する総当たり攻撃を従来よりも高速に実行できる．量子情報処理の物理的実現方法については，現在，様々な研究が行われている．具体的には，光を用いる方式やイオントラップを用いる方式などが検討されている．IBM は核磁気共鳴機を用いて 7 量子ビットの量子計算を行い，15 の因数分解に成功している[17]．また，光を用いた方式は，量子鍵配送の物理的実現において，非常に大きな成果を上げている．

■1 群 - 3 編 - 12 章

12-2 量子鍵配送

（執筆者：西野哲朗・大久保誠也）[2009 年 4 月 受領]

大量の情報を暗号化して送受信する際には，高速に処理可能な秘密鍵暗号が用いられることが多い．しかし，秘密鍵暗号を使用するためには，送信者と受信者が，事前に鍵を秘密裏に共有する必要がある．この鍵共有をどのようにして行うかという問題が，鍵配送問題である[1)]．この問題の解決のために，現在は，RSA 暗号や楕円曲線暗号などの公開鍵暗号方式が用いられることが多い．つまり，秘密鍵暗号で用いる秘密鍵を，公開鍵暗号を用いて暗号化することにより，安全に受け渡そうとするのだ．しかし，この方法は，計算量的な安全性に基づいているため，将来，技術が進歩すれば，解読されてしまう危険性がある．

一方，量子情報処理に基づく量子鍵配送ならば，数学的に安全性が保証されたかたちで，秘密鍵を共有化することが可能である．量子鍵配送方式としては，ベネット（Bennett）とブラッサール（Brassard）により 1984 年に提案された BB84 がよく知られている[1)]．

以下では，BB84 における量子鍵配送の基本的な考え方を説明する．そこでの基本的なアイディアは，1 量子ビットずつ，2 種類の基底の組を用いて，受信者に送ることである．例えば，Alice から Bob に秘密鍵を送る場合を考える．使用する 2 種類の基底は，前節で示した $|0\rangle$ と $|1\rangle$ に加えて，$|+\rangle$ と $|-\rangle$ でであるとしよう．その場合，以下のような手順によって，Alice と Bob は，安全に秘密鍵を共有することができる．

1. Alice は 2 種類の基底の組 $|0\rangle$ と $|1\rangle$ または $|+\rangle$ と $|-\rangle$ のどちらか一方を選択する．そして，選択した基底の組のうち，どちらか一方の基底状態をランダムに一つ選択して，Bob に送る．
2. Bob は Alice から送られてきた状態を受け取る（まだ，観測は行わない）．
3. 1〜2 を十分な回数繰り返す．
4. Bob は，基底の組をランダムに選択し，最初の数個の状態の観測を行う．
5. Bob は通常の通信路を用いて，どのビットをどの基底で観測したかを Alice に伝える．また，Alice は，自分の選択と Bob の選択で，一致した部分を Bob に伝える．そして，選択が一致した部分における，Alice と Bob の観測値が一致しているか否かを検証する．
6. 一致しなかった場合には，それまでの通信をすべて破棄し，1 からやり直す．
7. 一致した場合には，Alice と Bob は残りの各ビットをどの基底で観測したかを照合する．基底が一致した部分の Alice と Bob の観測値は一致するので，秘密鍵として使用できる．

記のステップ 5 で，盗聴が行われたか否かの検証がなされている．もし，攻撃者による観測（盗聴）が行われていなければ，Alice と Bob の観測値は一致する（表 12･1 参照）．一方，通信路に攻撃者が潜んでいて，攻撃者が選択した基底による観測を行った場合，Alice と異な

る基底を選択したならば，Alice と Bob の観測値は 1/2 の確率で異なる（表 12･2 参照）．この性質を用いて，攻撃者による盗聴が行われているか否かを判定することができる．

表 12･1　BB84 の通信例

ステップ 1 で Alice が選択した基底の集合					…				…
ステップ 2 で Alice が送信した基底	$\|1\rangle$	$\|\alpha\rangle$	$\|\beta\rangle$	$\|1\rangle$	…	$\|\beta\rangle$	$\|0\rangle$	$\|1\rangle$	…
ステップ 4 で Bob が選択した基底の集合					…				…
ステップ 4 で Bob が観測した基底	$\|1\rangle$	$\|1\rangle$	$\|\beta\rangle$	$\|\alpha\rangle$	…	$\|\beta\rangle$	$\|0\rangle$	$\|\beta\rangle$	…
ステップ 5 で一致した基底の集合					…				…
ステップ 5 で一致した基底	$\|1\rangle$		$\|\beta\rangle$		…				
ステップ 7 で確定した秘密鍵					…	$\|\beta\rangle$	$\|0\rangle$		…

表 12･2　BB84 の通信例（盗聴が行われた場合）

ステップ 1 で Alice が選択した基底の集合					…				…
ステップ 2 で Alice が送信した基底	$\|1\rangle$	$\|\alpha\rangle$	$\|\beta\rangle$	$\|1\rangle$	…	$\|\beta\rangle$	$\|0\rangle$	$\|1\rangle$	…
盗聴者が選択した基底の集合					…				…
盗聴者が観測した基底	$\|\alpha\rangle$	$\|1\rangle$	$\|\beta\rangle$	$\|0\rangle$	…	$\|1\rangle$	$\|0\rangle$	$\|\beta\rangle$	…
ステップ 4 で Bob が選択した基底の集合					…				…
ステップ 4 で Bob が観測した基底	$\|0\rangle$	$\|1\rangle$	$\|\beta\rangle$	$\|\alpha\rangle$	…	$\|\beta\rangle$	$\|0\rangle$	$\|\beta\rangle$	…
ステップ 5 で一致した基底の集合					…				…
ステップ 5 で一致した基底	**一致せず**		$\|\beta\rangle$		…				

量子鍵配送方式は，数学的に安全であることが証明されているが，完全な安全性を達成するためには完全なシステムの実現が要求されるため，理想的な鍵配送を行うことは，現実的には不可能である．そこで，様々な安全性の評価に関する研究が行われている．また，BB84 以外の鍵配送手法として B92 や E91 などが提案されている[2, 8]．

量子鍵配送は，数ある量子暗号技術の中でも，最も実現性が高いと考えられており，物理的な実証実験も数多く行われている．特に活発に研究されているのは，光子を用いた通信を利用する方式である．1980 年代には数十センチの距離でしか通信できなかったが，21 世紀に入ってから著しく通信可能な距離が伸びた．三菱電機により，2002 年には 87km，2004 年には 96km 離れた地点間での通信が行われた[19]．そして，2007 年にはロス・アラモス研究所により 107km，2006 年にはウィーン大学などにより 144km，2007 年には NTT により 200km 離れた地点間での通信が行われている．

■1 群 - 3 編 - 12 章

12-3 そのほかの量子暗号

（執筆者：西野哲朗・大久保誠也）[2009 年 4 月 受領]

量子秘密鍵配送は，1 量子ビットを送ることが可能であれば物理的に実現できるため，量子もつれ合いを考慮に入れる必要はなかった．その一方で，量子もつれ合いを用いることにより，従来の暗号方式とは本質的に異なるプロトコルが提案されている．

例えば，量子もつれ合いを用いた，秘密分散プロトコルが提案されている[13, 14]．密分散とは，ある情報が複数の集団に分散したかたちで保持されており，すべての集団が保持している情報を集めると，元の情報を入手することができるプロトコルである．通常の秘密分散プロトコルにおいては，実際に情報の分散を行った集団は，どの集団にどのような情報が渡ったかを知りえるし，また，情報を集める際にはどの集団がどのような情報をもっていたかが明らかとなってしまう．しかしながら，量子もつれ合いを用いた量子プロトコルでは，どの集団がどのような情報をもっているかを，一切明らかにすることなく，情報を分散することが可能である．

そのほかにも，量子もつれ合いを用いた認証方式や証明書なども提案されている．また，量子もつれ合いを用いた量子情報処理と関連して，量子ゲーム理論が研究されている[4, 7, 12]．ゲーム理論は，ゲームを行う複数のプレイヤが存在するときに，各プレイヤの意思決定方法を研究する学問であり，生物学や経済学などに幅広く応用されている．量子ゲーム理論では，以下のようにして意思決定が行われる．

1. 各プレイヤは，1 量子ビットずつ保持している．すべてのプレイヤのもっている量子ビットは量子もつれ合い状態にある．
2. 各プレイヤは，自分の量子ビットに，自分の行動に対応するユニタリ変換を適用する．
3. 量子ビット全体に，あるユニタリ変換が適用される．
4. 各プレイヤは自分のもっている量子ビットを観測し，観測値にしたがって行動を行う．

ステップ 3 により，各プレイヤの行動方針がほかのプレイヤに間接的に伝送される．つまり，量子ゲーム理論では，量子もつれ合いを利用することで，各プレイヤの選択がほかのプレイヤに影響を与えることを可能にしている．この一連の処理は，ある種の情報のやり取りを行うプロトコルと解釈することもできる．その結果として，量子ゲーム理論では，囚人のジレンマなど，従来のゲーム理論では解決することができなかった問題が解決可能になることが知られている．

自分が保持しているビット値を秘密にしたまま，そのビット値を所持していることを，検証者に対して確約するためのプロトコルをビットコミットメントというが，その量子版である量子ビットコミットメントは，1997 年に無条件に安全に行うことは不可能であることが証明された[3]．そこで，現在では何らかの条件を付けた量子ビットコミットメントが研究されている．量子コイン投げも，同様に不可能であることが示されているため，条件を緩めた弱量子コイン投げが研究されている[10]．対話型証明や，ゼロ知識証明の量子版である量子対話型証明や，量子ゼロ知識証明などの研究も盛んに行われている[11, 18]．

■参考文献

1) Bennett, C.H., “Quantum cryptography : Public key distribution and coin tossing,” Proc. IEEE Int. Conf., On Computers, Systems, and Signal Processing, Bangalore, India, 1984, pp.175-179, 1984.
2) Bennett, C.H., “Quantum cryptography using any two non-orthogonal states,” Phys. Rev. Lett., vol.68, pp.3121-3124, 1992.
3) Brassard, G., Cŕepeau, C., Mayers, D. and Salvail, L., “A brief review on the impossibility of quantum bit commitment,” ArXiv Quantum Physics e-prints, 1997.
4) Cheon, T. and Tsutsui, I., “Classical and quantum contents of solvable game theory on Hilbert space,” Physics Letters A, vol.348, no.3-6, pp.147-152, 2006.
5) Deutsch, D., “Quantum Computational Networks,” Proc. R. Soc. Lond., vol.A400, pp.97-117, 1985.
6) Dutsch, D., “Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer,” Proc. R. Soc. Lond., vol.A400, pp.97-117, 1985.
7) Eisert, J., Wilkens, M. and Lewenstein, M., “Quantum Games and Quantum Strategies,” Physical Review Letters, vol.83, p.3077, 1999.
8) Ekert, A.K., “Quantum Cryptography Based on Bell ’ s Theorem,” Physical Review Letters, vol.67, pp.661-663, 1991.
9) Grover, L., “Quantum Mechanics Helps in Searching for a Needle in a Haystack,” Physical Review Letters, vol.79, no.2, pp.325-328, 1997.
10) Kerenidis, I. and Nayak, A., “Weak coin flipping with small bias,” Information Processing Letters, vol.89, 2004.
11) Kobayashi, H., “Non-interactive Quantum Perfect and Statistical Zero-Knowledge,” ISAAC, pp.178-188, 2003.
12) Meyer, D.A., “Quantum Strategies,” Physical Review Letters, vol.82, pp.1052-1055, 1999.
13) Mihara, T., “Splitting information securely with entanglement,” Inf. Comput., vol.187, no.1, pp.110-122, 2003.
14) Mihara, T., “BASIC OPERATIONS AMONG ENTANGLED STATES AND THEIR APPLICATIONS TO QUANTUM PROTOCOLS,” nternational Journal of Quantum Information, vol.4, no.2, pp.307-323, 2006.
15) Nielsen, M. and Chuang, I., “Quantum Computation and Quantum Information,” Cambridge university press, 2000.［邦訳：木村達也訳, “量子コンピュータと量子通信, ” オーム社, 2004.］
16) Shor, P., “Algorithms for Quantum Computation : Discrete Log and Factoring,” in Proceedings of the 35th Anniual IEEE Symposium on Foundations of Computer Science, 1994.
17) Vandersypen, L.M.K., Steffen, M., Breyta, G., Yannoni, C.S., Sherwood, M.H. and Chuang, I.L., “Experimental realization of Shor ’ s quantum factoring algorithm using nuclear magnetic resonance,” Nature, vol.414, p.883, 2001.
18) Watrous, J., “Limits on the Power of Quantum Statistical Zero-Knowledge,” In Proceedings of the 43rd Annual Symposium on Foundations of Computer Science, IEEE Computer Society, pp.459-468, 2002.
19) 安部淳一, 長谷川俊夫, 西岡毅, 石塚裕一, 清水克宏, 松井充, “96km 既設光ファイバを用いた量子暗号通信システム実験（インターネット・フォトニックネットワークアプリケーション, 一般）, 電子情報通信学会技術研究報告. PN, フォトニックネットワーク, vol.105, no.8, pp.19-24, 2005.
20) 西野哲朗, “量子コンピュータと量子暗号,” 物理の世界 59, 岩波書店, 2002.
21) 西野哲朗, 渡辺昇, 荒井隆訳, “量子コンピューティング,” シュプリンガー・フェアラーク東京, 1998.［原著：C.P.Williams, and S.H. Clearwater, “Exploration in Quantum Computing,” Springer-Verlag, 1998.］