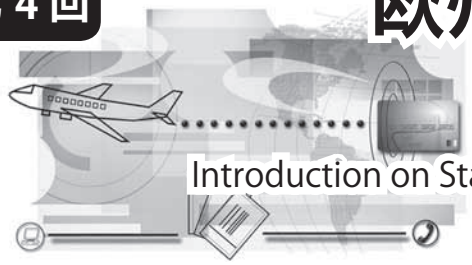
第4回

欧州における量子暗号通信標準化活動の紹介



Introduction on Standardization of Quantum Key Distribution in Europe

内古閑修一　東芝欧州研究所ケンブリッジ研究所
Shuichi Uchikoga　Toshiba Research Europe Limited Cambridge Research Labs.

量子暗号通信は，観測によって量子の状態が変化してしまうという量子論が成り立つ限り，無条件に安全であり，個人情報や金融情報など，高い機密性が必要とされる場面で使用されることが期待されている情報手段です．本稿では東芝欧州研究所ケンブリッジ研究所で行われている研究内容とともに，欧州電気通信標準化機構 ETSI（European Telecommunications Standards Institute）内に設置されている量子暗号鍵配信標準化の活動内容について紹介します．

東芝欧州研究所ケンブリッジ研究所の紹介

東芝欧州研究所ケンブリッジ研究所の紹介とともに量子暗号通信の研究背景についてご紹介したいと思います．正式名は Toshiba Research Europe Limited Cambridge Research Laboratory であり，1991 年に英国ケンブリッジのサイエンスパーク内に設立されました．ケンブリッジ大学との連携を主軸に最先端研究に取り組むことを目標としています．現在は本稿に関係する量子デバイス以外に，画像処理，音声合成・認識について研究を進めています．

量子デバイス研究はケンブリッジ大学 Cavendish 研究所との共同研究のもと，設備の共同使用，学生支援などを通して，大学と一体となって研究を進めています．その結果として Nature，Physical Review など世界が注目する学会誌に数多くの論文が採択されています．

このような背景の中，量子暗号技術の発展に寄与すべく，さまざまな欧州プロジェクトに参加しています．その 1 つとして，後述する 2008 年 10 月に行われた世界初の量子暗号通信の実地試験を行った学会 SECOQC（Secure Communication based on Quantum Cryptography）に参加しました．SECOQC は同時に量子暗号通信標準化グループをスタートする契機を作りました．

量子暗号通信技術について

量子暗号通信技術は送信する情報に量子状態の重ね合わせを利用した秘密鍵配信技術です．**図 -1** は量子暗号技術を模式的に表現したものです．送信者（習慣的に Alice と称します）は送信したいテキストを暗号化し Cipher text とします．これを既存の通信網にのせて受信者（習慣的に Bob と称します）に送ります．Alice は同時に，暗号解読に必要な鍵を他人に読み取られることなく，量子論によって保証されたチャネルを通して Bob へ送信します．

現状では量子暗号通信は**図 -2** に示す Bennett と Brassard によって提案された BB84 というプロトコルが基本として使われています．ここでは，正確性が欠けますが，定性的な表現で通信方法を簡単に説明したいと思います．

Alice からの送信信号に対して，Bob は 2 つの測定法（図 -2 内の ″x″analyser と ″+″analyser 参照）を用いて受信します．どの方式の組合せで測定すべきかを送信側と受信側で共有することで意味のある情報の通信が成立します．途中で盗聴者（習慣的に Eve と称します）が通信情報を観測すると観測者効果による波束の収縮が起こり不確定性原理により量子情報が変化してしまいます．その結果，第 1 に Alice と Bob は受信した情報が意味を持たなくなることで盗聴が行われたことが分かります．第 2 に，仮に測定法の組合せが漏洩していたとしても，送信情報に対して変化した量子情報では意味不明になるということになります．このように，盗聴された情報に意味がないこと，盗聴が行われたことが分かることによって情報の盗聴防止を可能にしています．

Alice の送信する情報は量子もつれ光子対発生に基づいた原理によって，Bob へ伝わります．上述したプロトコルに従うことを前提に，量子もつれ光子対発生の

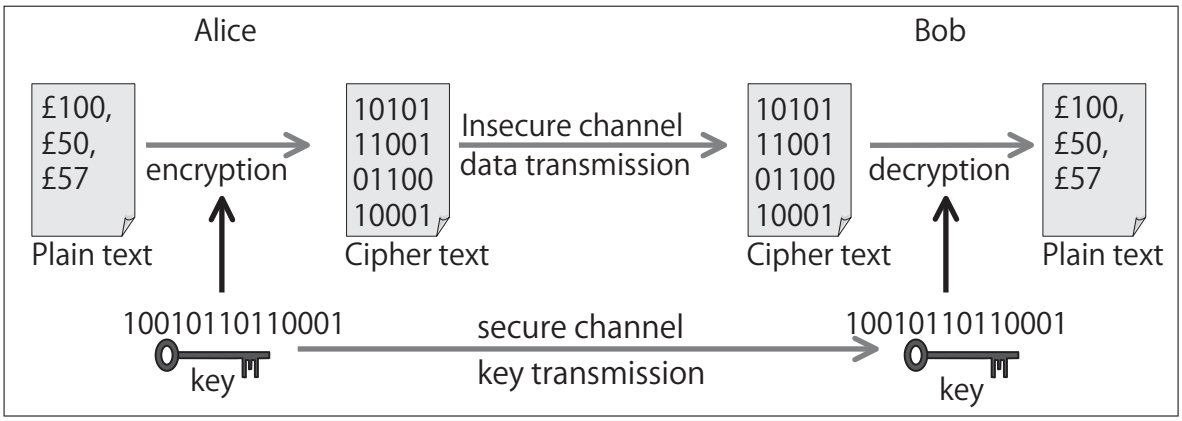


図 -1　量子暗号通信の概略

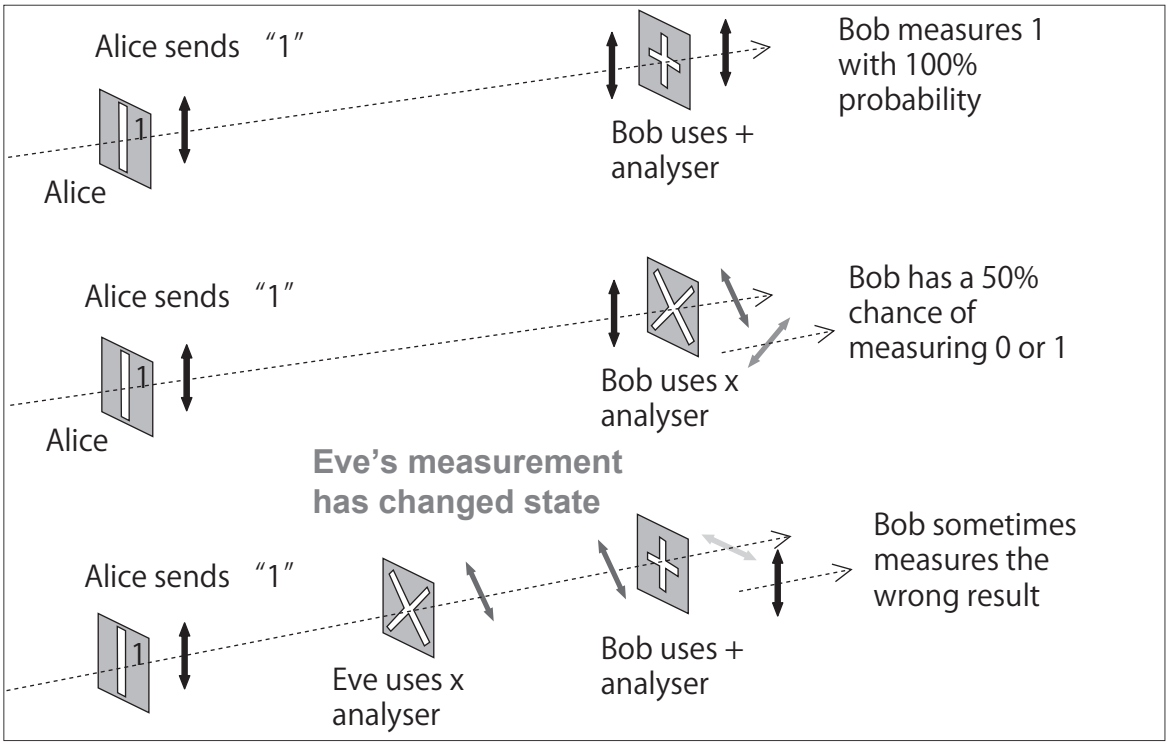


図 -2　BB84 プロトコルの説明図

さまざまな方法が検討されています．各国の大学研究機関をはじめとして，スイスの id Quantique，フランスの SmartQuantum，米国の MagiQ Technologies などのベンチャー企業に加え HP，IBM，日本では三菱，NEC，NTT などがさまざまな工夫を施し高速，長距離の暗号鍵配信技術にしのぎを削っている状況です．現状は限定的な用途とはいえ，ベンチャー企業の出現は実用化が現実のものとなっていることを示しています．さまざまな方法によって発生した量子もつれ光子対がプロトコルに沿って通信が可能になる必要があります．そのための標準化プロジェクトの一環として SECOQC による実地試験が行われました．

ETSI-ISG-QKD の構成と活動内容

SECOQC は学会に合わせ，世界初の量子暗号鍵配信の実地試験が 2008 年 10 月，ウィーンにて行われました．ことなる方式を持った各研究グループが 1 つのプロトコル（BB84）のもと通信を行う試みです．さらに，実用化を意識して実験室で検討してきた成果をラックに収められる程度のシステム（**図 -3**）で実現することも必要条件として実地試験が行われました．

この実地試験の実現を可能にするために標準化に重点が置かれてきました．そのため，SECOQC は実地試験を目指し，同年 6 月より準備を進めてきた ETSI ISG-QKD（ETSI Industry Specification Group on Quantum Cryptography and Quantum Technologies）のキックオフ

図 -3　量子暗号システムの概観

応用	
1	User requirements
2	Application interface
QKD ネットワーク	
3	Components and internal interfaces
4	QKD devices integratikon within standard optical networks
5	QKD security specification
6	Security assurance requirements
7	Security proofs
8	Ontology, vocabulary and terms of reference
QKD 実用化	
9	Promoters and inhabitators for QKD
10	Prospects of QKD in Europe

表 -1　ISG-QKD の検討項目一覧

としての役割も有していました．SECOQC の概要については http://www.secoqc.net/ を参照してください．

ISG-QKD は Austrian Research Centers，HP，id Quantique，University of Madrid，Telefonica および TREL/CRL が Founder メンバとしてスタートしました．現在は 16 の企業や研究機関が ISG-QKD を構成しています．ISO/EN 15408 Common Criteria のような 26 カ国で認知されている基準に準拠できるよう量子暗号技術を高めることを目標として掲げています．その目標達成のための検討項目を**表 -1** に示しました．

量子暗号システムの構成に関する案件（2, 3），量子暗号通信システムが現存する情報通信技術との適合性に関する案件（4），暗号の保証，評価方法確立に関する案件（5 〜 8），また，市場導入に関する案件（9, 10）という構成になっています．ここで挙げられた各項目のビジョンについては参考文献を参照ください．

6 つの研究機関・企業を Founder としてスタートした組織も現在では 41 の研究機関・企業が参加するに至っています．ISG-QKD メンバは提案事項に対して 1 票を投じ案件を決定していくという仕組みで運営がされています．これらの項目について 2010 年 12 月までに ETSI に第 1 回目の提案をする計画となっています．

むすび

量子暗号通信は単一光子源や繊細な光子検出器が必要となるなど，既存の通信手段に比較して費用がかさむことが課題であります．量子暗号通信は既存技術を一気に代替するのではなく適切な市場を求めて発展するものと考えられます．今後，標準化が進む中，量子暗号技術がより広く使われるためには情報通信の安全性の確保と同時に，コストのバランスが必要になると思われます．本稿で紹介した ETSI-ISG-QKD の紹介が何かしらのご参考になれば幸いです．

参考文献

1）東芝レビュー，Vol.61, No.2 (2006).
2）Langer, T. and Lenhart, G.: New Journal of Physics11 055051 (2009).
3）Shields, A. and Yuan, Z.: Physics World (Mar. 24. 2007).

（平成 22 年 2 月 3 日受付）

内古閑修一

shuichi.uchikoga@crl.toshiba.co.uk

1987 年東芝入社．液晶ディスプレイ用の薄膜半導体素子研究に従事．2009 年より東芝欧州研ケンブリッジ研究所副所長．工学博士．IEEE，MRS，SID および応用物理学会各会員．