49

コンピュータを用いた量子暗号の安全性証明
～形式手法の量子情報処理への応用～

SCIENCE PLAZA 2012

Motivation　どんな問題に取り組むのか？

暗号の安全性は通信における要です。従来、暗号の安全性は高度な数学を用いて手作業により証明されてきましたが、近年、暗号プロトコルの複雑化に伴い、コンピュータを用いた安全性証明手法が盛んに研究されています。一方、究極の暗号と呼ばれる量子暗号は、理論的な枠組みが複雑なため、これまでコンピュータを用いた安全性証明がありませんでした。

Originality　得られた結果はどう新しいのか？

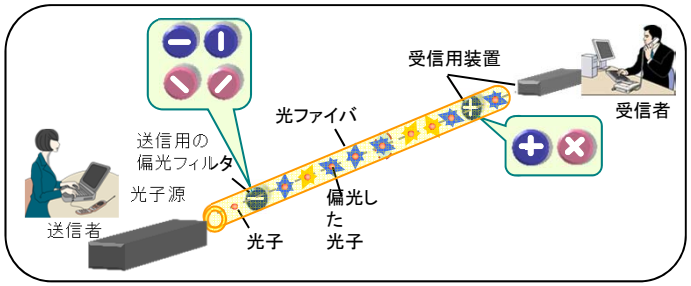
量子暗号は、光子（光の粒子）の一つ一つに情報を載せて通信するプロトコルで、量子力学を使って記述されています。私たちは、量子力学により記述される安全性証明を、コンピュータを用いた形式手法の体系にのせることにより、世界で初めてコンピュータによる量子暗号の安全性証明の枠組みを作りました。

Impact　この研究が成功した場合のインパクトは？

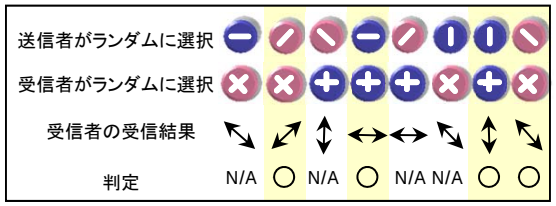
本研究では、最も標準的な量子暗号BB84において、盗聴者への情報漏洩をゼロにできることを、コンピュータを用いて厳密に証明しました。現在、この証明手法の一般化にも取り組んでいます。こうした研究の成果により、通信の安全性がより確かなものになります。

量子暗号が盗聴を検出するしくみ

■BB84は1984年にBennett-Brassardによって提案された最初の量子暗号です
■秘密鍵を共有するために偏光した光子と古典データを送受信します
■盗聴者に漏れる鍵の情報量をゼロにできます。これは無条件安全性と呼ばれています

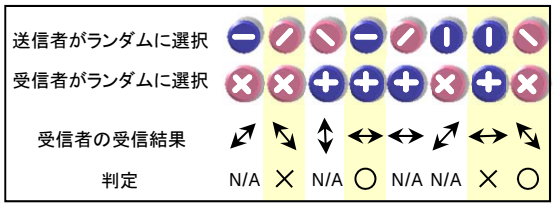


盗聴されていない場合



同じ色の偏光フィルタを選んだ場合を比較すると、送信した光子の偏光面と受信した光子の偏光面が一致します

盗聴されている場合



同じ色の偏光フィルタを選んでも、送信した光子の偏光面と受信した光子の偏光面は必ずしも一致しません

形式手法（フォーマルメソッド）による証明方法

第1ステップ：BB84を量子プログラミング言語で表現します
第2ステップ：項書き換え規則を用いて、盗聴者から見て見分けのつかない別のプロトコルに変形します
第3ステップ：第2ステップで得られたプロトコルの無条件安全性を、量子ホーア論理で証明します

BB84

```
          : bit ka[1..40]; bit kb[1..40];
          : qbit qb[1..600]; bit ba[1..600];
          : bit bb[1..600]; bit c[1..200];
          : bit da[1..600]; bit db[1..600];
          : bit e[1..7]; bit ua[1..100];
          : bit ub[1..100]; bit x[1..100];
          : bit sx[1..100]; bit ke[1..65536];
          : qbit qe[1..65536];
送信者 : Rnd(da[1..600]|);
送信者 : for i := 1 to 600 do
送信者 : qb[i] := da[i]; end
送信者 : Rnd(ba[1..600]|);
送信者 : for i := 1 to 600 do
送信者 : if ba[i] then qb[i] *= H;
送信者 : end
盗聴者 : Eve_Attack(ke[],qe[],qb[]|);
受信者 : Rnd(bb[1..600]|);
受信者 : for i := 1 to 600 do
受信者 : if bb[i] then qb[i] *= H;
受信者 : db[i] := measure qb[i];
受信者 : end
...
```

BB84と見分けのつかない別のプロトコル

```
          : bit ka[1..40]; bit kb[1..40];
          : qbit qa[1..200]; qbit qb[1..200];
          : bit b[1..200]; bit c[1..200];
          : bit da[101..200]; bit db[1..200];
          : bit e[1..7]; bit ke[1..65536];
          : qbit qe[1..65536];
送信者 : for i := 1 to 200 do
送信者 : EPR(qa[i], qb[i]|);
送信者 : end
送信者 : Rnd(b[1..200]|);
送信者 : for i := 1 to 200 do
送信者 : if b[i] then qb[i] *= H;
送信者 : end
盗聴者 : Eve_Attack(ke[],qe[],qb[]|);
盗聴者 : for i := 1 to 200 do
盗聴者 : if b[i] then qb[i] *= H;
盗聴者 : end
...
```

無条件安全

この証明のキーポイントは第2ステップの項書き換え規則を新たに導入し、合流性と停止性を証明した点です
このことから、上記の証明が、コンピュータにより自動化可能なことが保証されます

注：本研究は、東京大学萩谷研究室との共同研究成果です

NTT

NTTコミュニケーション科学基礎研究所
NTT Communication Science Laboratories

連絡先
河野泰人 (Yasuhito Kawano)
協創情報研究部 情報基礎理論研究グループ
E-mail： kawano.yasuhito@lab.ntt.co.jp