2

Title: Security proof using formal method

コンピュータが安全性を保障！ 究極の暗号

～フォーマルメソッドを用いた量子暗号の安全性証明～

どんな研究？

暗号の安全性は、通信における要です。従来、暗号の安全性は手作業により証明されてきましたが、プロトコルの複雑化に伴い、コンピュータを用いた証明が主流になりつつあります。この展示では、私たちが行なった、コンピュータによる量子暗号の安全性証明を紹介します。

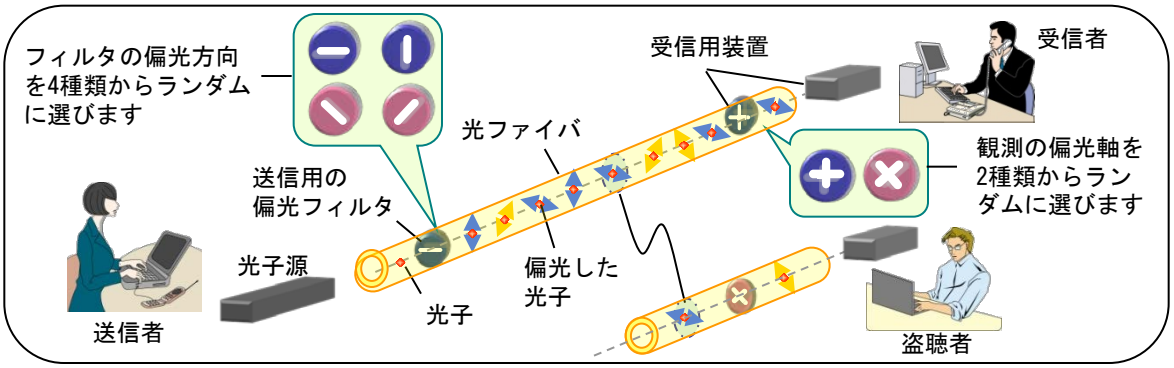
どこが凄い？

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、量子暗号の安全性を、フォーマルメソッドで用いられる項書き換えの理論を応用し、世界で初めてコンピュータで証明する枠組みを提案しました。

どんな風に役立つ？

量子暗号は盗聴者への情報漏洩をゼロにできる画期的な暗号です。本研究で、このことをコンピュータにより厳密に証明したことにより、量子暗号を安全性が極めて高い究極の暗号としてアピールできます。

1. 量子暗号のシステム概念図



送受信者間でランダムに選んだフィルタの向きと受信結果を照合し、一致率が高い場合、安全な秘密鍵が生成できます。情報を盗むために盗聴者が光子を観測すると、光子の状態が壊れ、盗聴が発覚します。

2. 量子暗号をプログラミング言語で表現

コンピュータで扱えるようにするために、量子暗号を量子プログラミング言語で表現します。

```
送信者: Rnd(da[1.. '(4+d)n]|);
送信者: for i := 1 to '(4+d)n do qb[i] := da[i]; end
送信者: Rnd(ba[1.. '(4+d)n]|);
送信者: for i := 1 to '(4+d)n do if ba[i] then qb[i] *= H; end
盗聴者: Eve_Attack(ke[], qe[], qb[]|);
受信者: Rnd(bb[1.. '(4+d)n]|);
...
```

3. 項書き換え規則を用いて量子暗号を単純化／安全性証明

フォーマルメソッドで用いられる項書き換えの理論を用いて、安全性に関する等価性を保ちながら量子暗号を単純化し、得られた暗号の安全性をコンピュータで証明します。例えば「ランダムなキュービットを得るためには、エンタングル状態の片方を観測すればよい」という項書き換え規則は以下のように表現されます。

```
Rnd(da[i]);          書き換え      qbit qa[i];
qb[i]:=da[i];        ------>       EPR(qa[i], qb[i]);
                                   da[i] := measure qa[i];
                                   discard qa[i];
```

関連文献

[1] Takahiro Kubota, Yoshihiko Kakutani, Go Kato and Yasuhito Kawano, “A formal approach to unconditional security proofs for quantum key distribution," The Proceedings of the 10th International Conference on Unconventional Computation, LNCS Volume 6714, pp. 125-137, 2011.

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{at}lab.ntt.co.jp （{at}の部分を@に置き換えてください）