作成者：吾妻広夫

古典暗号：従来の古典論に基づく暗号
数学的に解くのが難しい問題の性質を使って盗聴を防ぐ
(例)RSA(Rivest–Shamir–Adleman)暗号
→巨大な整数を素因数分解するのが難しい事実を利用

量子暗号：量子論に基づく暗号
盗聴の危険性を量子力学の法則で排除する
→物理法則で盗聴を防ぐ点が特徴的

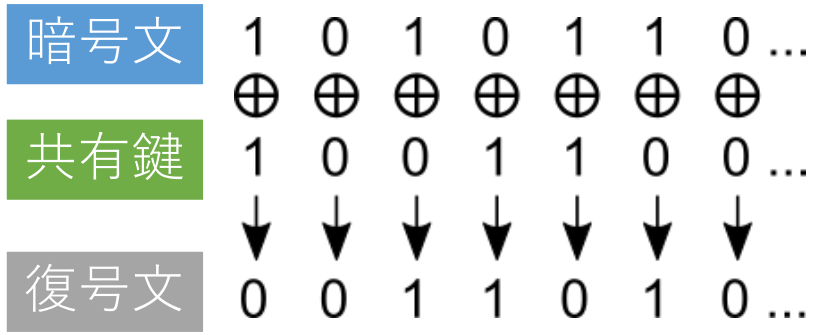
現在主流の量子暗号は、量子鍵配布と呼ばれるタイプのものである。これは、理想的な古典暗号の一種である、one-time padを念頭に置いている。

One-time padプロトコル

[Step 1]
AliceとBobは、あらかじめ、二人だけで秘密裡に'0'と'1'の乱数列を共有する(共有鍵と呼ぶ)

[Step 2]
AliceがBobに、'0', '1'のビット列から成るメッセージを送りたいとする。Aliceは、メッセージと共有鍵の間で、各ビットをXORし、暗号文を作成する。この暗号文を、例えば無線でBobに送る。

[Step 3]
Bobは、暗号文と共有鍵の各ビットをXORして、メッセージを復号化する



[one-time padの利点]
盗聴者Eveが無線を傍受して暗号文を入手しても、共有鍵を持っていないなら、復号化は不可能である。
なぜなら、n文字のメッセージの場合、共有鍵は2^n個の乱数列から無作為に選んだもののため、暗号文は完全にランダム化されているから。

[one-time padの欠点]

1. AliceとBobの間で、あらかじめ秘密裡に乱数列を共有しなくてはならない。
2. 共有鍵は、一度使ったら、必ず捨てなくてはならない。(one-time padという名前は、このことに由来する。)共有鍵を何度も使い回すと、盗聴者Eveによって、統計的な手法で共有鍵が推測されてしまう。
3. 共有鍵は、厳重に保管しなくてはならない。(保管コストが無視できない。)

One-time padは、AliceとBobの間で秘密鍵を共有するプロセスが難しい。
→この問題を解決する方法として、量子鍵配布プロトコルが考案された。

鍵配布とは、AliceとBobが、秘密裡に乱数列を共有する操作のことである。
量子鍵配布の代表的なプロトコル→BB84, E91