ノイズを秘密鍵生成源としたセキュア通信

Secure Communications Using Secret Keys Generated from Noise

日立 研開　○戸丸 辰也

Hitachi, Research & Development Group,　○Tatsuya Tomaru

E-mail: tatsuya.tomaru.yq@hitachi.com

はじめに：ビット誤りがあり且つ Bob-Eve 間に差異を形成できれば秘匿通信が可能である。図１にその原理を示す。想定する通信手順は量子暗号と同様で、乱数の送受信、その乱数からの秘密鍵生成（秘匿性の増強）、メッセージの暗号通信からなる。秘密鍵生成量はビット誤りのエントロピ分に限る。通信の安全性はビット誤りが予測できないことから保証される。但し、Bob が Eve よりも有利な条件が形成されなければこの原理は利用できない。

Bob-Eve 間の差異形成：Alice-Bob 間で事前に共通鍵を共有し Eve よりも Bob を有利にする。一般に情報は重要性が高い程限られた人だけで共有されるためにこの前提は可能であろう。共通鍵の利用法を図２に示す[1]。送信する乱数 $\boldsymbol{x}$ を共通鍵 $\boldsymbol{k}$ を利用して $\boldsymbol{x}_1 \times \boldsymbol{x}_2$ に符号化する。$\boldsymbol{x}_1$ が情報記号で $\boldsymbol{x}_2$ が冗長情報である。Bob は共通鍵を持っているので $\boldsymbol{y}$ から $\boldsymbol{y}_1 \times \boldsymbol{y}_2$ に復号できて誤り訂正を経て $\boldsymbol{x}_1$ を得る。Eve は共通鍵を持たないために $\boldsymbol{z}_1 \times \boldsymbol{z}_2$ に復号できず $\boldsymbol{x}_1$ が得られない。メッセージ伝送で利用する秘密鍵はノイズから秘匿性の増強を経て生成されており Eve が共通鍵に関係した情報を得る機会はない。よって解読には共通鍵の有効鍵長分の全数探索が必要になり、安全性はこれにより定まる。

ノイズ源：以上の方法はノイズ源が送信機内にあっても成立する。そのため伝送路は任意になる。

試作機：試作機は LAN ケーブルを接続するだけの構成である（図３）。ノイズ源として LD の位相ノイズを利用した。LD の位相ノイズは自然放出光を起源とするために乱雑度が高い[2,3]。伝送速度は 500 kbps 程度である。

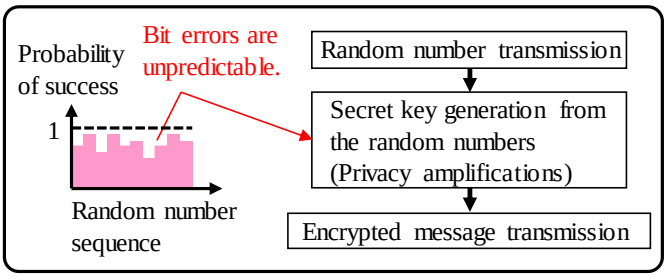

Fig. 1. Secure communication protocol.

フィールド試験：埼玉県鳩山・国分寺間及び鳩山・駒場間で実施した。

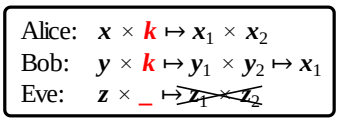

Fig. 2. How to use a common key.

[1] 戸丸辰也、2015 年暗号と情報セキュリティシンポジウム 3F3-3.
[2] 戸丸辰也、第 74 回応用物理学会秋季学術講演会(2013 秋) 16p-A14-8.
[3] 戸丸辰也、第 61 回応用物理学会春季学術講演会(2014 春) 17a-D10-10.

Fig. 3. Secure communication unit. Left: Noise generation part. Right: Main body.