情報理論的セキュリティと秘密増幅定理

松本　隆太郎 [1]

[1] 東京工業大学

IBIS 2010

情報理論的セキュリティとは？

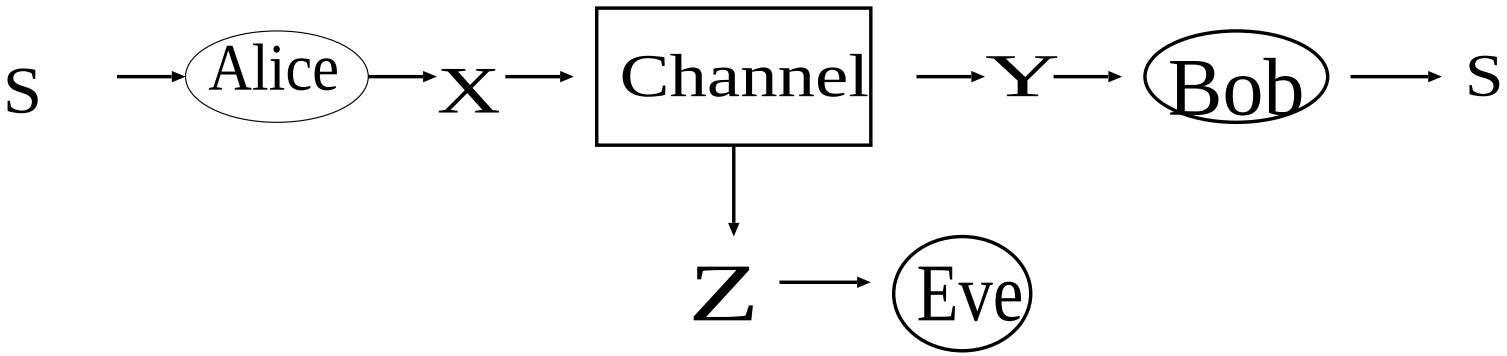
- 従来のセキュリティは、素因数分解の困難さなど特定の問題の計算困難さによって安全性を保証している
- 優れたアルゴリズムの発見などで安全性の根拠が崩れる恐れがある

情報理論的セキュリティの長所

計算困難さなどに依存せずに、秘密情報と敵の所持する情報の統計的独立性を保証

情報理論的セキュリティの代表的問題を紹介する

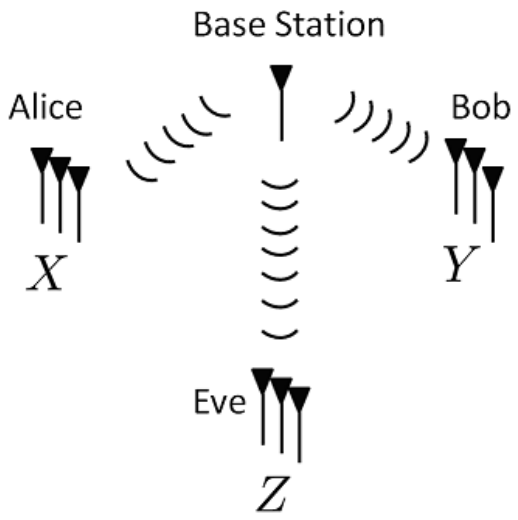
盗聴通信路



- 秘密メッセージ S を正規受信者 Bob に送りたい
- 盗聴者 Eve には S の内容を知られたくない

Wyner (1975), Csiszár-Körner (1978) により考察された。

情報理論的に安全な鍵共有



上記図は渡辺-大濱 (2010) より借用

- X, Y, Z は相関を持つ確率変数
- Alice と Bob の間には盗聴されるが内容は変更されない公開通信路がある
- Alice と Bob は Eve に知られていない乱数列 S を共有したい

共有した乱数列を用いて、情報理論的に安全なメッセージの送信を、すべての情報が盗聴される公開通信路を用いて行える。

Bennett-Brassard (1984) の量子鍵共有に基づいて、Maurer (1993) および Ahlswede-Csiszár(1993) が考察した。量子鍵配送の場合 Z が確率変数ではなくて Eve の量子メモリーを表現する量子状態になる。

安全性の基準

S: 秘密にしたい情報（確率変数）
Z: 盗聴者 Eve の所有する情報（確率変数）

S と Z がほぼ統計的に独立ならば、Z の実現値を知っていても S の実現値を推測するために役に立たない

S と Z の相互情報量 $I(S;Z) = 0 \Longleftrightarrow S$ と Z が統計的に独立

$I(S;Z)$ が十分に小さければよい

計算量的安全性と何が違うのか？

現在広く使われている秘密通信や鍵共有の方式は計算量的安全性に基づいている

計算量的安全性

特定の計算問題（例えば大きな合成数の素因数分解）に必要な計算時間が長いことから、秘密情報を知るために必要な計算時間が長いことを保証する安全性

- 量子計算機の実現
- 未知の高速なアルゴリズムの発見

によって素因数分解は高速に解けるようになってしまい安全性の根拠は崩れるが、情報理論的安全性にはそういう問題点は無い。

統計的独立性を実現する基本的な道具

情報理論的な安全性は確率変数の統計的な独立の実現である

- two-universal ハッシュ関数族
- 秘密増幅定理
  - Bennett ら (1995)-林 (2009) の秘密増幅定理（これを紹介）
  - Csiszár(1996), Csiszár-Narayan(2004) の秘密増幅定理
  - Renner(2005) の秘密増幅定理

Family of two-universal hash functions

定義

$\mathcal{F}$: 有限集合 $\mathcal{S}_1$ から有限集合 $\mathcal{S}_2$ への写像の集合
F: $\mathcal{F}$ 上の（一様）確率変数
もしすべての $x_1 \neq x_2 \in \mathcal{S}_1$ について

$$\Pr[F(x_1) = F(x_2)] \leq \frac{1}{|\mathcal{S}_2|}$$

が成り立つなら、$\mathcal{F}$ を two-universal ハッシュ関数族と呼ぶ.

例: $\mathcal{S}_1$ から $\mathcal{S}_2$ への線形写像の集合

秘密増幅定理

(X, Z): 有限確率変数の組（Z は離散ではなく実は何でもよい。確率密度が無くても可）
$\mathcal{F}$: $\mathcal{X}$ から $\mathcal{S}$ への two-universal ハッシュ関数族
F: (X, Z) とは統計的に独立な $\mathcal{F}$ 上の確率変数（関数）

$$I(F(X); Z|F) \leq \frac{|\mathcal{S}|^\rho \mathbf{E}[P_{X|Z}(X|Z)^\rho]}{\rho}$$

for all $0 < \rho \leq 1$.

H と I の中に暗に現れる対数も含めてすべての対数は自然対数

$\rho = 1$: Bennett et al. (1995).
$0 < \rho \leq 1$: Hayashi (2009).

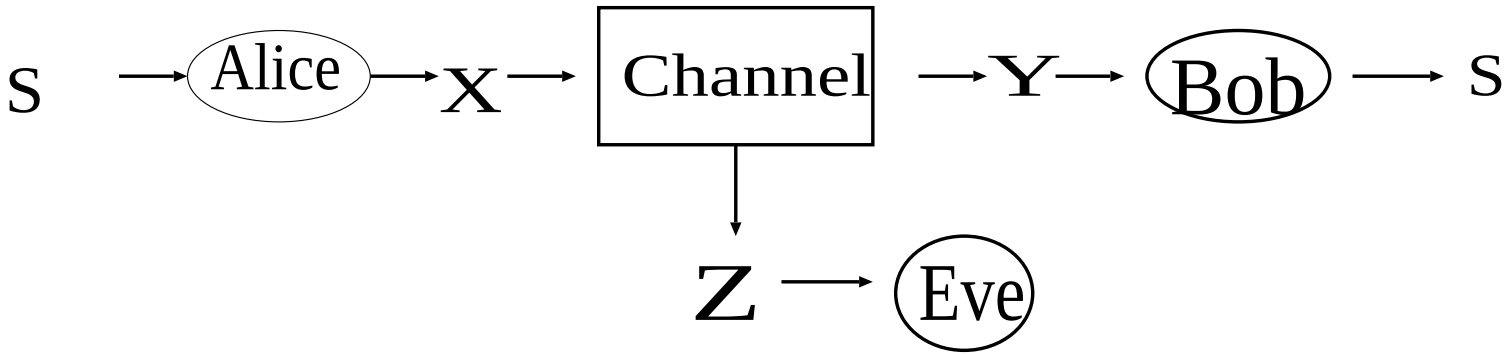
秘密増幅定理の数式の意味

$$I(F(X); Z|F) \leq \frac{|\mathcal{S}|^{\rho}\mathbf{E}[P_{X|Z}(X|Z)^{\rho}]}{\rho}$$

for all $0 < \rho \leq 1$.

- ハッシュ関数の値域 $\mathcal{S}$ を小さくするほど相互情報量が小さくなるので $F(X)$ と Z はより独立になる
- より多くの秘密情報が得られることが望ましいから $\mathcal{S}$ は大きいほうがよい
- (X, Z) の実現値が i.i.d. で多数得られる場合、一つの X あたり条件付きエントロピー $H(X|Z)$ の秘密情報 $F(X)$ を生成できる
- $H(X|Z)$ は Z を所有する Eve から見た X の曖昧さと解釈できるから、Eve から見て秘密に見える情報 $F(X)$ は X 一つあたり Eve から見た X の曖昧さの分だけ生成できると解釈できる
- $F(X)$ の実現値を制御できないから秘密情報の伝達にそのままでは使えない。では盗聴通信路でどうするか？

Csiszár (1996) の逆ハッシュ構成法



S: 秘密情報, $\mathcal{S}$ 上の一様確率変数
F: $\mathcal{F}$ 上の一様確率変数, S とは独立.
$F^{-1}(S)$: $\{x \in \mathcal{X} \mid F(x) = S\}$ 上で条件付き一様な確率変数（集合ではない）

秘密情報 S を送りたいときは、$F^{-1}(S)$ を誤り訂正符号で符号化して X を作って通信路を介して送る

送る秘密情報の量があまり大きくなければ、Eve の受信信号 Z と送信情報 $F^{-1}(S)$ に秘密増幅定理を適用して、

$$I(S; Z, F) = I(S; Z|F)$$

が小さくなることを保証できる

どの程度の情報を秘密に送ることができるのか

通信路は i.i.d. と仮定
X: 送信信号を表わす確率変数
Y: 正規受信者 Bob の受信信号
Z: 盗聴者 Eve の受信信号

通信路の使用 1 回あたり

$$I(X;Y) - I(X;Z) (= H(X|Z) - H(X|Y))$$

の情報を秘密に送ることができる。これは Bob への通信路容量から Eve への通信路容量を引いた分の情報を秘密に送ることができることを意味する。

しかし、もっと多くの情報を秘密に送ることができる

通信路を劣化させると送ることができる秘密情報が増える

送ることができる通信路の使用 1 回あたりの最大の秘密情報は

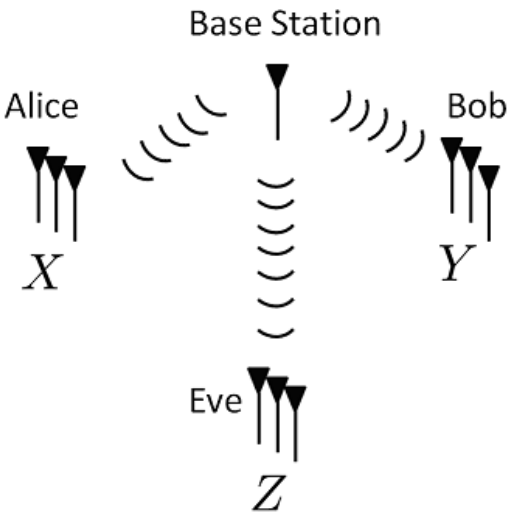
$$\max_{U \leftrightarrow X \leftrightarrow YZ} I(U;Y) - I(U;Z)$$

で与えられる。

- $P_{YZ|X}$ は通信路の統計的性質で決まる
- $P_{X|U}$ は Alice が雑音を付加して本来の通信路を劣化させていると考えられる

Alice が通信路を劣化させることによって、 Bob への通信路容量の減少よりも Eve への通信路容量の減少が大きくなることがあるから、 結果として秘密裏に送ることができる情報量が増える

秘密裏の共有できる鍵の量（鍵共有の復習）

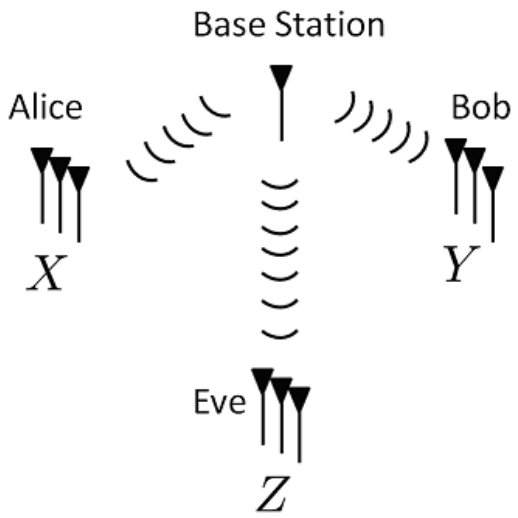


上記図は渡辺-大濱 (2010) より借用

- X, Y, Z は相関を持つ確率変数
- Alice と Bob の間には盗聴されるが内容は変更されない公開通信路がある
- Alice と Bob は Eve に知られていない乱数列 S を共有したい

(X, Y, Z) が i.i.d. と仮定

秘密裏の共有できる鍵の量



上記図は渡辺-大濱 (2010) より借用

(X, Y, Z) が i.i.d. と仮定

- Alice が Bob に X 一つあたり $H(X|Y)$ の情報を Bob に送ると、Bob は自分の Y と合わせて X を推測できる (Slepian-Wolf 符号化)
- Alice が送った情報は Eve も見ているから、Eve から見た X の曖昧さは $H(X|Y)$ 減少する
- 元々Eve から見た X の曖昧さは $H(X|Z)$

Alice と Bob は (X, Y) 一つあたり

$$H(X|Z) - H(X|Y)$$

の乱数列を秘密裏に共有できる。しかしよりうまくやる方法がある。

自分で雑音をのせると秘密裏に共有できる乱数列が増える

(X, Y, Z) が i.i.d. のときに、秘密裏に共有できる最長の乱数列の量は (X, Y) 一つあたり

$$\max_{V \leftrightarrow U \leftrightarrow X \leftrightarrow YZ} H(U|VY) - H(U|VZ)$$

である。これは

- Alice に X から確率的に U を作り
- Alice が U から確率的に V を作り Bob に公開通信路を介して送り、
- Alice が Bob に $H(U|VY)$ の情報を送って Bob に U を推測させ
- Alice と Bob は U に秘密増幅して $H(U|VY) - H(U|VZ)$ の乱数列を秘密裏に共有する

ということを意味する

まとめ

- 秘密増幅定理を用いて盗聴通信路と鍵共有問題に対する最適な効率を持つ手法を構成できる
- 他の情報理論的安全性の問題にも秘密増幅定理は有効である