Tamagawa
K-12 & University

情報理論的安全な鍵共有の安全性評価の不完全性について（解説）

玉川大学量子情報科学研究所

ISEC研究会@機械振興会館
H24年5月18日

■情報理論的安全性の定義

◆**Shannonの定義：** 暗号システム $\left\{\begin{array}{l} x \in X : \text{平文} \\ k \in K : \text{鍵} \\ c \in C : \text{暗号文} \end{array}\right\}$ **が完全秘匿とは**

(1) 全ての $\left\{\begin{array}{l} x \in X \\ c \in C \end{array}\right\}$ に対して $p(x \mid c) = p(x)$

(2) $p(K \mid C) = p(K) = 2^{-|K|}$ $\quad |K| = |X|$: 鍵の長さ＝データ長

鍵系列の推定確率が一様分布

■暗号システムの理論解析の概念的比較

◆共通鍵暗号システムの安全性解析

- 盗聴者は暗号文から平文あるいは秘密鍵を解読することが目的。
  （暗号文単独、既知平文、など）

暗号文からどれだけ“情報”が漏れるかを評価する

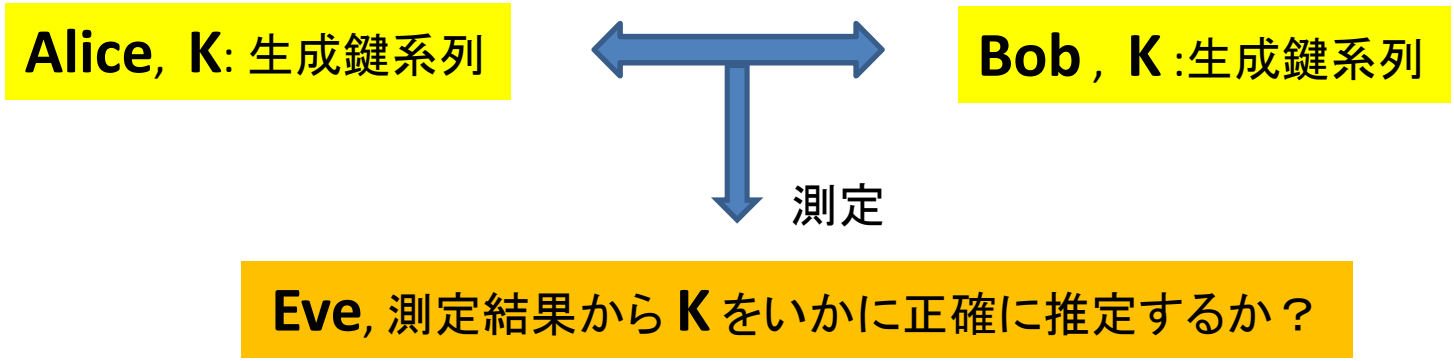
◆鍵配送システムの安全性解析

- 盗聴者は伝送される“裸”の鍵系列を正確に測定することが目的。

測定値からどれだけ鍵系列が推定できるかを評価する

■鍵配送のモデルに必要な機能

- 暗号解析は通信路から盗聴者が得たデータを基に実施される。
  （量子鍵配送の場合には、量子測定と古典測定を経由する）
- 配送された鍵系列は共通鍵暗号の秘密鍵として利用される。
  （秘密鍵は真正乱数でなければならない）
- 鍵配送の安全性は、配送され共有された鍵系列が盗聴者にとって
  一様分布となることを保証する必要がある（Shannonの定義の２）



■鍵配送問題の定量的評価へ

鍵系列推定：

$K_G \in \mathrm{K}_{AB}$: 生成鍵系列

$K_E \in \mathrm{K}_E$: 盗聴者受信系列

◆システムの情報理論的安全性は鍵推定成功確率で評価される

$$p_{suc}(K_G) = \max\ p(K_G \mid K_E)$$

◆生成鍵：K_G が完全秘匿One time padに利用されるためには

$$p_{suc}(K_G) = 2^{-|K_G|} \quad |K_G| : \text{生成鍵系列の長さ}$$

上記がShannonの完全秘匿の概念の鍵配送問題における対応
（無条件安全鍵配送）

■鍵配送研究グループの誤解の原点

暗号システムの理論体系 ⇨ 鍵配送システムへ転用

- 情報理論的安全性評価
  相互情報量評価 → D.Mayers, 1996
  H.K.Lo and H.F. Chau, 1999
  P.Shor and J.Preskill, 2000

- 計算量的安全性評価
  識別不可能性評価
  ⇩
  情報理論的安全性への拡張 → R.Renner 2005

スライド２，３，４、５のような鍵配送独自の評価理論が必要であった

■共通鍵暗号システムの計算量的安全性と情報理論的安全性

[A] 計算量的安全性: 攻撃者は多項式時間の計算資産を利用可能.

多項式時間の計算資産のもとで真正乱数あるいは保証された乱数と設計された乱数の識別問題を考察する。

[B] 情報理論的安全性: 攻撃者は無限の計算資産を利用可能.

無限の計算資産のもとで真正乱数と設計された乱数の識別問題を考察する。

◆識別不可能性の評価法 ⇨ **変動距離：d** $d_{\text{古}} \leq \varepsilon$

課題： ε がゼロでないとき、その操作的意味を明確にする必要がある

一般に [A]に対する意味 $\neq$ [B]に対する意味

■評価関数の操作的意味の課題

[A] 計算量的安全性: 計算量の観点で色々な確率的解釈が可能
（各種のゲームによる定式化の上で攻撃者のアドバンテージ、プロセス計算の観測等価性など）

[B] 情報理論的安全性:

情報理論的識別不可能性 ⇒ **定量的な評価理論は十分に議論されていない**

計算量的安全性からの単純なアナロジーは危険

■量子鍵配送の理論モデルへの識別不可能性評価の導入(R.Renner)

◆送受信者が共有する鍵系列Kに対する識別不可能性評価

量子的変動距離（トレース距離）の採用

$$d \equiv \frac{1}{2} \| \rho_{KE} - \rho_U \otimes \rho_E \|_1$$

$$\rho_E = \sum_k p(k) \rho_E^k$$

$$\rho_{KE} = \sum_k p(k) | k >< k | \otimes \rho_E^k$$

$$\rho_U = \sum_k U(k) | k >< k |$$

$p(k)$: 先験確率

定義： εが無視できるほど小さいとき、システムは無条件安全である

$$d \leq \varepsilon$$

■ εに対する意味ずけの試み

QKDコミュニテイが採用した識別不可能性の解釈

1. システムの理想状態と実際のシステムが等しい確率は

$$P = 1 - \varepsilon$$

R.Renner, et al, *TCC, Springer*, 2005.
R.Konig, et al, *Physical Review Letters*, 2007.

2. εは実際のプロトコルが失敗する最大の確率である

V.Scarani, et al, *Review of Modern Physics*, 2009.
J.Mullae-Quade, et al, *New J. Physics*, 2009.

3. εは生成鍵が一様になる確率である　　珍説　？

So what ?

■鍵系列の無条件安全を保証するには？

Shannonの定義２より　鍵系列の推定確率が一様分布

$$p_{suc}(K_G) = 2^{-|K_G|} \qquad |K_G| = \text{鍵長}$$

$|K_G| = 10^4$のとき

無条件安全を保証するには

$$p_{suc}(K_G) = 2^{-|K_G|} = 2^{-10000} \approx 10^{-(3000)}$$

でなければならない

相互情報量評価	$\leq \varepsilon$
トレース距離評価	$\leq \varepsilon$

で実装可能な物理的システムモデルに対して上式の性能は保証できない

■従来の理論による数値例

$$\text{鍵長} = 10^{4} \qquad d \leq \varepsilon = 10^{-6}$$

もし、上記εが現実の誤り訂正符号、秘密増幅によって
実現されることが保証されたとしても、鍵推定成功確率は
最悪の場合として 10^{-2} を否定することができない。

すなわち識別不可能性の評価が100万分の1を保証しても
鍵系列の推定成功確率が1%になる可能性を否定できない。

■まとめ

Shannonの鍵系列の無条件安全の条件

鍵長 $=10^4$

$$p_{suc}(K_G) = 2^{-|K_G|}$$

$$= 2^{-10000} \approx 10^{-(3000)}$$

識別不可能性評価

鍵長 $=10^4$

$$p_{suc}(K_G) \approx \varepsilon^{1/3}$$

$$= 10^{-2} = 0.01$$

上記を否定できない

意味： 1. OTPに使う前に１％の確率で全鍵系列が推定可能の危険性
2. AESの256bitの秘密鍵を選定するとき、その鍵が暗号に使われる前にほぼ確実に推定可能の危険性を排除できない

■むすび

Tamagawa
K-12 & University

- BB-84型の量子鍵配送は原理的に無条件安全性を実現することができない

- 今後の情報理論的安全な暗号の研究は鍵系列の推定成功確率を評価基準として実行されるべきである。これはShannonの概念の自然な一般化である。

量子鍵配送の場合、個別量子測定、一括量子測定を含む
多元量子信号検出理論が基盤となって公式化される。