新技術説明会
New Technology Presentation Meetings!

無条件安全性を確保する線形ランダム符号の実装・安全性評価方法

電気通信大学 大学院情報理工学研究科
准教授　小川 朋宏

2022年5月10日

従来技術とその問題点

暗号の安全性

- 現在の公開鍵暗号系（RSA暗号，楕円曲線暗号など）
  - 現行計算機の計算量理論が安全性の根拠（計算量的安全性）
  - 量子アルゴリズムにより理論的に解読可能である (Shor, 1994)
  - 計算原理の更新（量子コンピュータの実現）や新しいアルゴリズムの発見によって安全性が崩れる可能性がある
- 情報理論的暗号（ワンタイムパッド，量子暗号など）
  - 計算原理によらない理論的安全性を与える（情報理論的安全性）
  - データの安全性を未来まで理論保証
  - 公開鍵暗号系と比べ，鍵共有のコスト等により，近年あまり使われなかった

⇓

（本発表）情報理論的暗号の実用化を目指す新技術

情報理論的安全性（例１）：ワンタイムパッド

送信者アリス

受信者ボブ

送信メッセージ “HELLO”	受信メッセージ “HELLO”
$a = 11010000\cdots$	$a = 11010000\cdots$

共有鍵	(1) ランダムなビット列を事前に共有	共有鍵
$b = 01101010\cdots$		$b = 01101010\cdots$

$\Downarrow \oplus$ (2) 共有鍵に基づき反転　　復号 $\oplus \Uparrow$

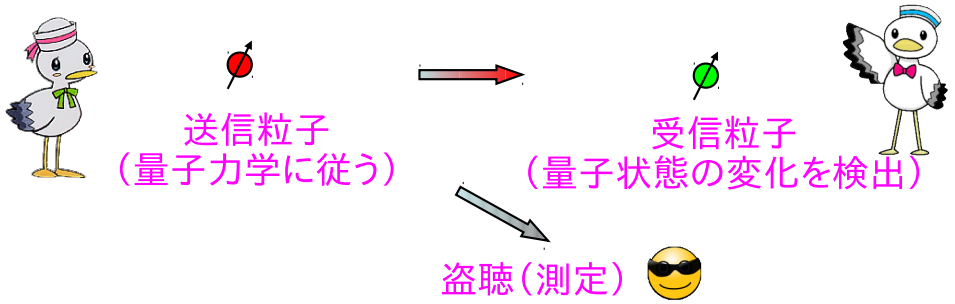
暗号文	公開通信路	暗号文
$c = 10111010\cdots$	$\longrightarrow$	$c = 10111010\cdots$

(3) 盗聴者にとっては ↘ 

暗号文とメッセージが統計的に独立（ランダムに反転しているため）

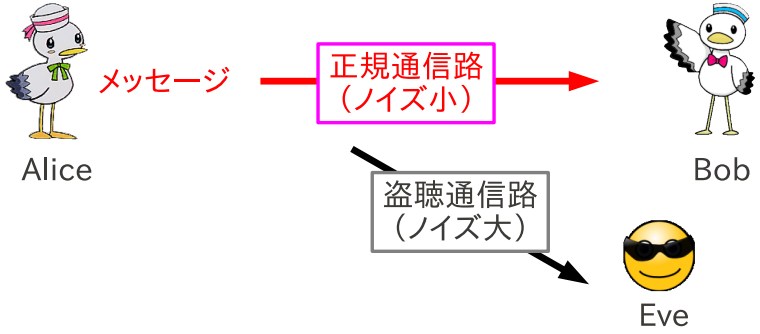
問題点：遠隔で離れているため，鍵共有の問題が生じる
鍵の更新・管理にコストがかかる

情報理論的安全性（例２）：量子鍵共有



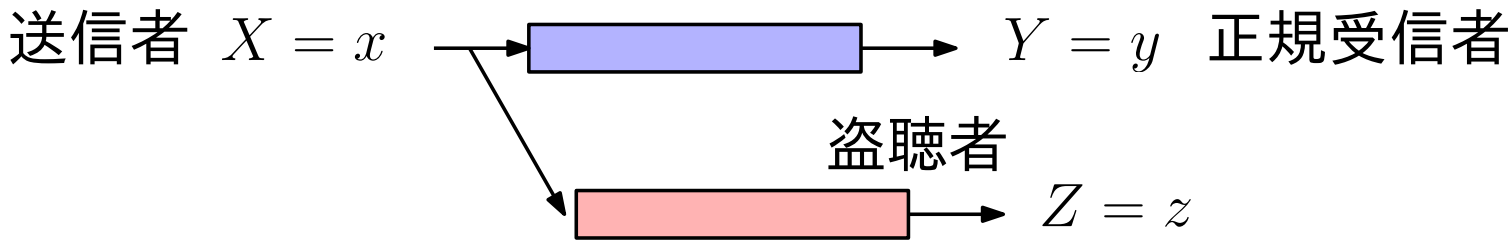
- ワンタイムパッドの鍵共有方法を与える
- 物理法則が安全性を確保（量子状態はコピー不可），現状の導入コスト大

情報理論的安全性（例３）：盗聴通信路符号化



- ノイズ差の条件のもと，情報理論的な符号化により安全性を確保

盗聴通信路モデル

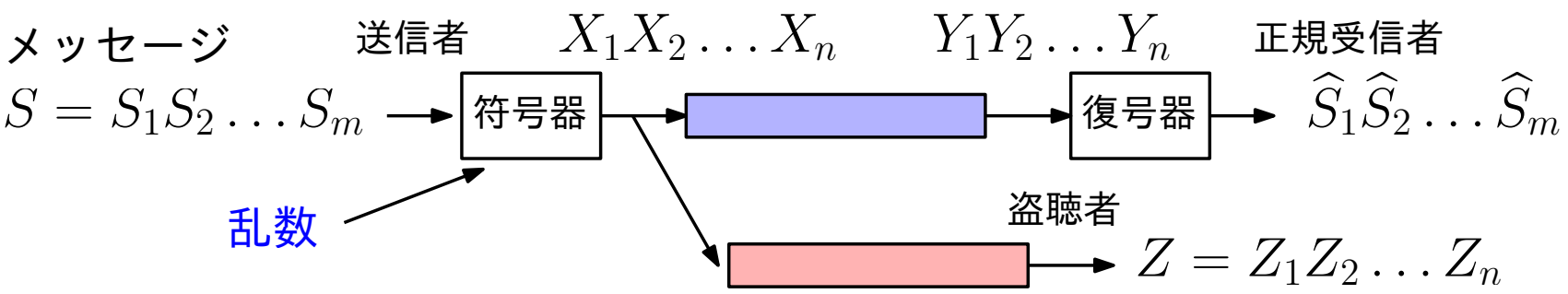


- 部屋の中と外など，盗聴者のノイズが多い状況を想定している
- 条件付き確率で通信路ノイズをモデル化

正規受信者 $P(y|x)$, 盗聴者 $P(z|x)$



盗聴通信路符号化モデル (Wyner, 1975)



- 通信路を繰り返し使用（符号化）：$(m < n)$
  メッセージ（メッセージ長 m）$\Rightarrow$ 通信路への入力（符号長 n）
- 乱数を付加して盗聴者を撹乱する

盗聴通信路符号化の目的

- 送信者 Alice は正規受信者 Bob に対して誤りなくメッセージを伝送
- 盗聴者 Eve にはメッセージに関する情報が一切伝わらない
  （メッセージ $S = (S_1, \ldots, S_m)$ と盗聴データ $Z = (Z_1, \ldots Z_n)$ が独立）

盗聴通信路符号化定理 (Wyner 1975†, Csiszár-Körner 1978‡)

上記要請を満たす通信レート $\frac{m}{n}$ の最適値 $= \max_{X \text{ の確率分布}} \{I(X;Y) - I(X;Z)\}$

ここで，$I(X;Y) = \sum_x \sum_y P(x,y) \log \frac{P(x,y)}{P(x)P(y)}$ および $I(X;Z)$ は相互情報量

$\Downarrow$

通信路の品質差 $I(X;Y) - I(X;Z) > 0$ ならば暗号通信が可能

† A. D. Wyner, The wire-tap channel, Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, 1975.

‡ I. Csiszár, J. Körner, Broadcast channels with confidential messages, IEEE Trans. Inform. Theory, vo. 24, no. 3, pp. 339-348, 1978.

理論による符号構成方法

符号長 n が十分に長い符号をランダムに作成すると，
高い確率で，安全な符号を作成可能

⇓ しかし

実用的に安全性を確認する手段はなかった

- 実際に作成した符号が安全か？
- 符号長 n はどれぐらいにすれば良いか？

これまでは，符号の安全性確認において，計算量的な困難があった

新技術の特徴・従来技術との比較

従来の問題

盗聴通信路符号化における符号器の安全性評価について，頻度テーブルを作成して，メッセージ，盗聴データとの相関を調べる手段しかなかった（符号長 n の指数オーダ計算量）

新技術の特徴

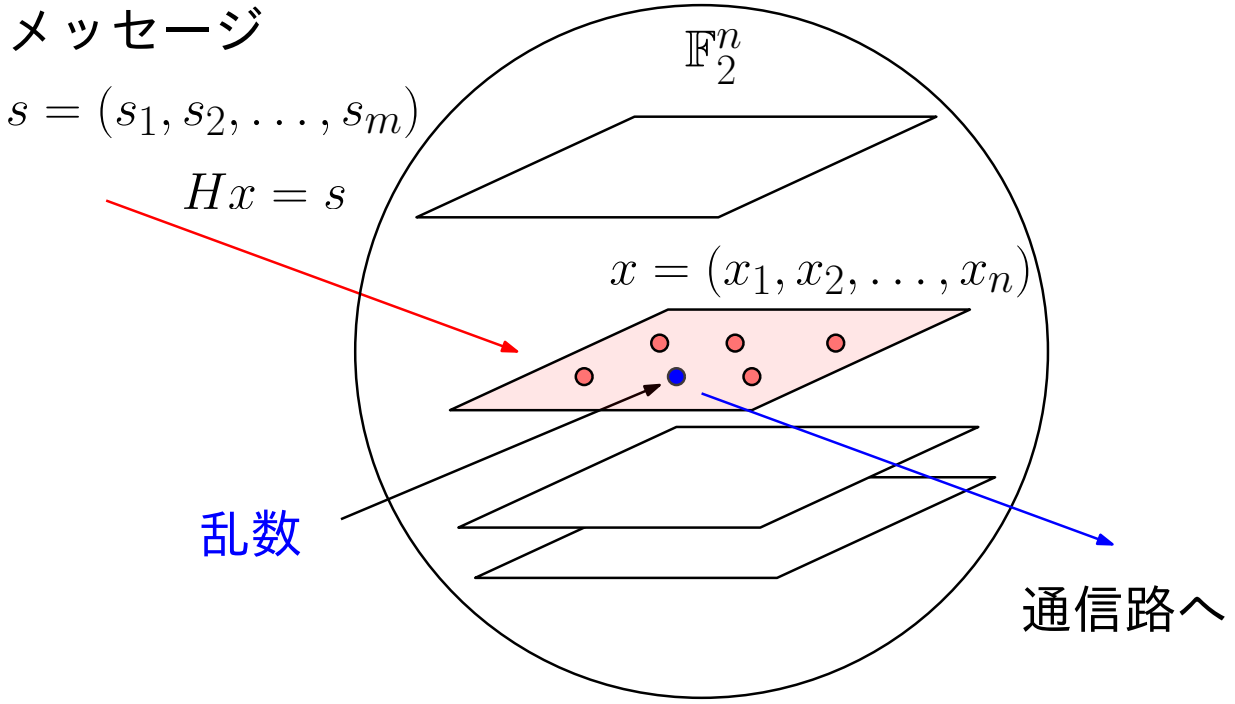
メッセージ長 m，符号長 n の線形符号について

符号長 $n = 400$，メッセージ長 $m = 32$ まで安全性指標の計算が可能

- 符号長 n：計算量 $O(n)$ で，いくらでも大きくすることが可能
- メッセージ長 m：CPU レジスタに格納出来る範囲で高速化可能
- $n = 256$，$m = 32$ 程度なら，ノート PC で数分で安全性確認が可能

技術構成(1)：線形符号によるコセット符号化†

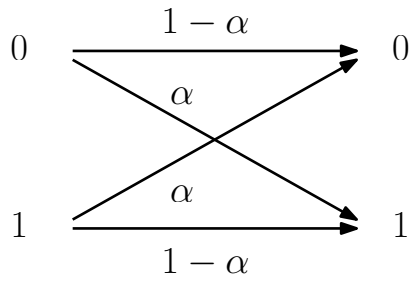
- 符号器として$m \times n$ 行列 H （線形ハッシュ）を用いる
- （コセット符号化）メッセージ $s = (s_1, s_2, \ldots, s_m)$ に乱数を付加して，$Hx = s$を満たすように符号語 $x = (x_1, x_2, \ldots, x_n)$ $(m < n)$ を作成



† K. Zhang *et al.* , IET Commun., Best binary equivocation code construction for syndrome coding, vol. 8, pp. 1696-1704, 2014. 等

技術構成(2)：安全性に関する理論保証

- 二元対称通信路 (BSC) は確率 α $(0 < \alpha < 1)$ でビット反転を起こす通信路



- 入力 $x = (x_1, \ldots, x_n)$ とEveの出力 $z = (z_1, \ldots, z_n)$ の関係は，

$$z = x + e \pmod 2$$

$e = (e_1, \ldots, e_n)$ はエラーベクトル

各成分独立に確率 α で1，
確率 $1-\alpha$ で0の値をとる

- 盗聴推定エラー[†] $s_e := He$ とおく

$$Hz = Hx + He = s + s_e$$

確率変数として扱うときは
大文字 S_e で表す．

定理[‡]

盗聴者の通信路がBSCであるとき，盗聴推定エラー S_e が一様分布に従えば，メッセージ S と盗聴データ Z は独立になる

† K. Zhang *et al.* , IET Commun., vol. 8, pp. 1696-1704, 2014.
‡ 高崎幸太郎, 小川朋宏, 信学技報, IT2020-62, 2020.

技術構成(3)：安全性指標と特性関数

- 複素関数 $f : x \in \mathcal{X} = \mathbb{F}_2^m \to f(x) \in \mathbb{C}$ のノルム：

$$\text{（1-ノルム）} \quad \|f\|_1 = \sum_{x \in \mathcal{X}} |f(x)|, \quad \text{（2-ノルム）} \quad \|f\|_2 = \left(\sum_{x \in \mathcal{X}} |f(x)|^2 \right)^{\frac{1}{2}}$$

- 確率分布 $P(x)$, $Q(x)$ 間の距離

（変動距離，1-距離）$\|P - Q\|_1$, （ユークリッド距離，2-距離）$\|P - Q\|_2$

一様乱数 U と推定エラー S_e の分布間の変動距離 $\|P_U - P_{S_e}\|_1$ が十分ゼロに近ければ安全な符号化である．ノルムの関係式より

$$\|P - Q\|_1 \leq \sqrt{|\mathcal{X}|} \cdot \|P - Q\|_2$$

ユークリッド距離を高速計算することで変動距離を見積もる

多変数の特性関数を，$t = (t_1, \ldots, t_m) \in \mathbb{F}_2^m$

$$\phi_P(t) = \sum_{x=(x_1,\ldots,x_m)\in\mathbb{F}_2^m} P(x) \exp\left\{\pi\sqrt{-1}\,\langle t, x\rangle\right\} \quad \left(\langle t, x\rangle = \sum_{i=1}^{m} t_i x_i\right)$$

とすると（離散フーリエ変換の一般論により），

$$\|P - Q\|_2 = \frac{1}{\sqrt{2^m}} \|\phi_P - \phi_Q\|_2$$

符号器 H の安全性指標（特性関数に基づく）

一様分布 U と盗聴推定エラー S_e のユークリッド距離を安全性指標として計算

$$F(H) = \|P_U - P_{S_e}\|_2 = \frac{1}{\sqrt{2^m}} \|\phi_U - \phi_{S_e}\|_2 \quad (S_e = He)$$

技術構成(4)：特性関数の高速計算方法

- 符号器 H（$m \times n$行列）をm次元縦ベクトルの列とし，ランダムに生成

$$H = [h_0, h_1, \ldots, h_{n-1}]$$

  各ベクトルを計算機内でmビット表現する（整数表現）

- 独立な確率変数和 $S_e = He = \sum_{l=0}^{n-1} e_l h_l$ として特性関数を分解

$$\phi_{S_e}(t) = \prod_{l=0}^{n-1} \phi_{e_l h_l}(t) = \prod_{l=0}^{n-1} \left\{(1-\alpha) + \alpha(-1)^{\langle t, h_l \rangle}\right\} = (-2\alpha+1)^{N(t)}$$

  ここで，$N(t)$は$\langle t, h_l \rangle = 1$となる縦ベクトル$h_l$の数．最後の等式は以下による

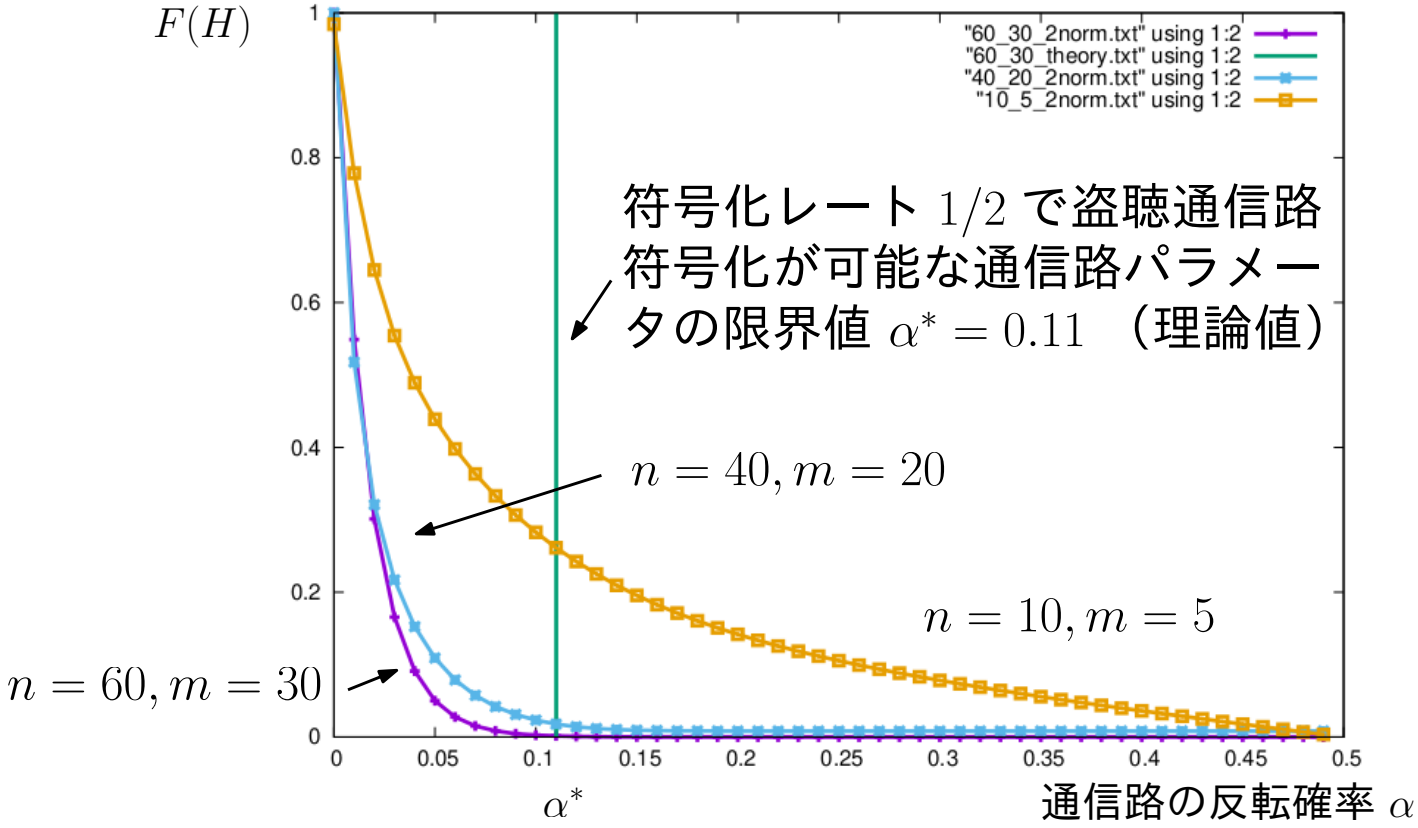
$$(1-\alpha) + \alpha(-1)^{\langle t, h_l \rangle} = \begin{cases} 1 & \langle t, h_l \rangle = 0 \\ -2\alpha + 1 & \langle t, h_l \rangle = 1 \end{cases}$$

- $N(t)$の計算をCPU内部命令 (popcnt) で高速化する
- $N(t)$は通信路パラメータαを変えても使い回せる

実行例

安全性指標（ユークリッド距離，2-ノルム）の計算例†

- 符号 H をランダムに作成して盗聴者への影響に注目（正規通信路はノイズレス）
- 安全性指標 $F(H)$ は $n = 60,\ m = 30$ 程度で十分小さくなる



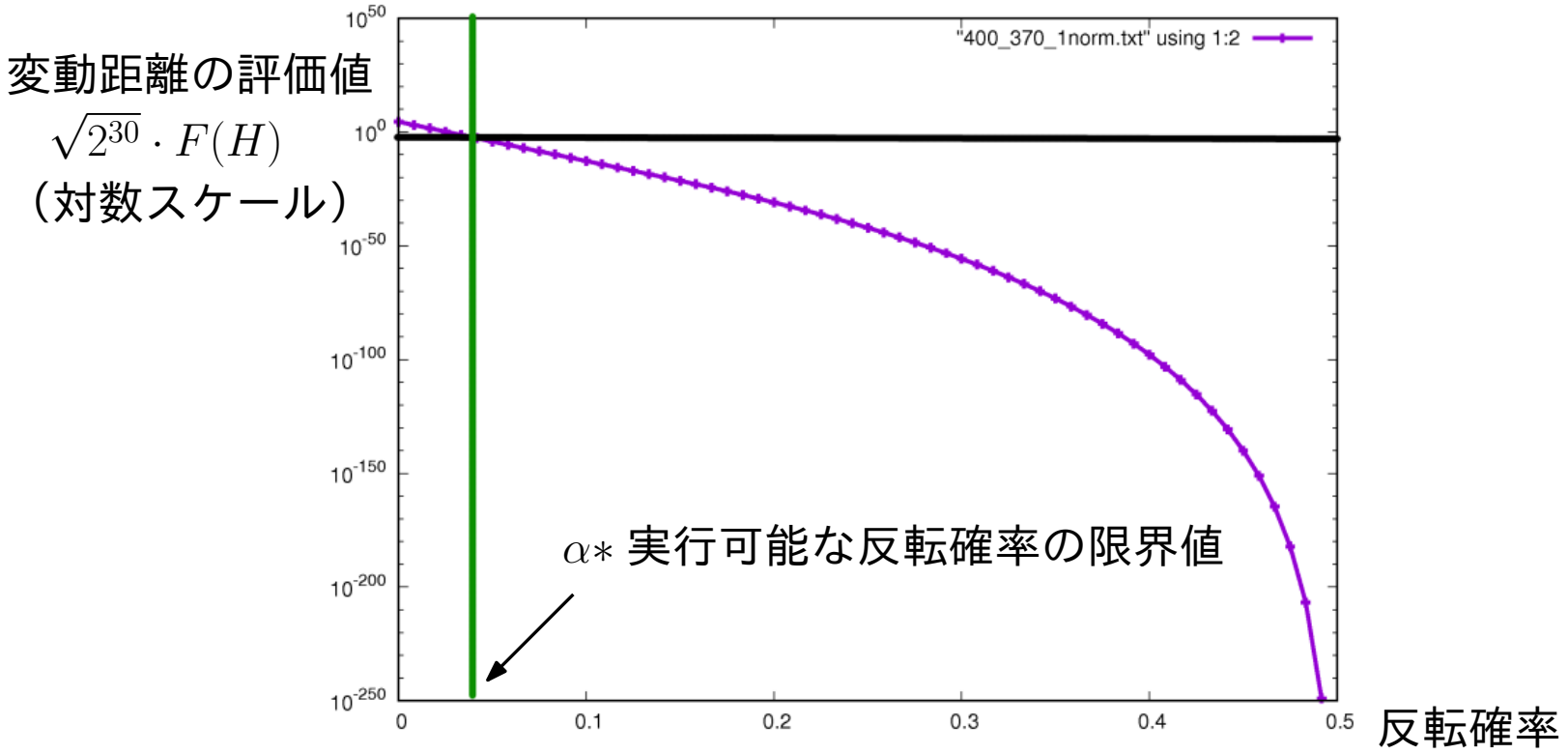
† 森雄喜，小川朋宏，盗聴通信路符号化におけるコセット符号化の安全性評価方法について，信学技報，ISEC2017-131，2017.

新技術説明会
New Technology Presentation Meetings!

変動距離（1-ノルム）の評価例†

- 符号長 $n = 400$, メッセージ長 $m = 30$ の符号 H をランダムに作成
- 符号化レート $30/400$ における実行可能な通信パラメータ限界 α^* で評価
- 厳しい安全性基準（変動距離，1-ノルム）のもとで良い性能を発揮した

$$\|P_U - P_{S_e}\|_1 \leq \sqrt{2^{30}}\|P_U - P_{S_e}\|_2 \simeq 0.054$$



† 森雄喜, 盗聴通信路符号化における特性関数を用いた安全性評価について, 電気通信大学大学院情報理工学研究科, 修士論文, 2018.

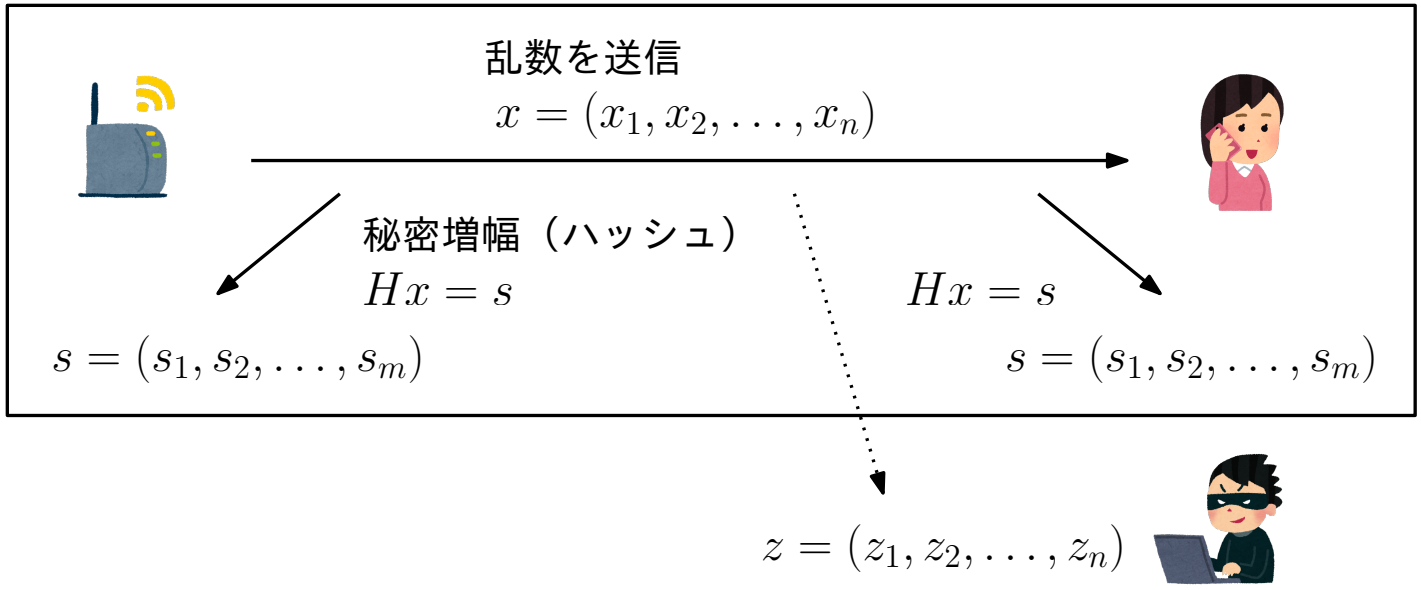
新技術説明会
New Technology Presentation Meetings!

想定される用途

- 無線通信や衛星通信において，物理的状況から盗聴者の通信品質劣化が保証できる場合に本技術が適用可能

鍵生成レート $\frac{m}{n}$ と安全性指標（2-ノルム，1-ノルム）について
トレードオフを考慮した符号設計・運用が可能

- 乱数鍵共有，量子鍵配送における秘密増幅プロセス（ハッシュ関数） †



† R. Ahlswede, I. Csiszár, IEEE Trans. Inform. Theory, vol. 39, pp. 1121-1132, 1993.

† C. H. Bennett, G. Brassard, C. Crépeau, U. M. Maurer, IEEE Trans. Infrm. Theory, vol. 41, no. 6, pp. 1915-1923, 1995.

- ビットコミットメントなどの暗号応用（立会人なしで「将棋の封じ手」をする方法）：盗聴通信路符号化を応用することで，情報理論的にビットコミットメントを実現できることが知られている[†]

公開鍵暗号によるビットコミットメント[‡]

 アリス　　ボブ 

(1) 委託：アリスは“$a=0$”または“$a=1$”を箱に入れ錠前を閉める

 a ↷  a　箱をボブへ送信 ⟶

(2) ボブは鍵がないので箱の中身が分からない

 a

 a

(3) 開示・検証： アリスは鍵とaを送る．ボブは鍵を開けて検証．

aと鍵をボブへ送信 ⟶　　$a \overset{\text{検証}}{=} a$ ↶ 

[†] A. Winter, A. Nascimento, H. Imai, IMA Conf. Coding and Cryptography, LNCS 2898, Springer-Verlag, 2003.

[‡] M. Blum, Coin fipping by telephone: a protocol for solving impossible, Proc. IEEE Computer Conference, pp. 133-137, 1982.

実用化に向けた課題

- 誤り訂正符号とのハイブリッド符号化
  - これまでリードソロモン符号とのハイブリッド実験を行った†
  - LDPC符号など様々な符号化技術との組み合わせが望まれる
- メッセージ長mの大規模化：本技術では$O(2^m)$オーダの計算（$N(t)$ の計算）を1回だけ必要とする．GPUの利用や並列化より，どこまでメッセージ長mを伸ばせるか実証が望まれる
- 既存技術，特に無線LAN規格 (IEEE 802.11) との整合性
- 理論の一般化（一般の通信路の安全性を BSC の安全性に帰着させることは可能だが効率が悪い）

† 高崎幸太郎, ノイズを含む盗聴通信路符号化の実装と安全性評価, 電気通信大学大学院情報理工学研究科, 修士論文, 2021.

企業への期待

- 実用に向けた課題：
  - GPUの利用や並列化
  - 無線LAN規格など，既存技術との整合性
  - 誤り訂正符号との組み合せ

  などで，企業の皆様との共同研究・開発を通して，本技術がお役に立てれば嬉しく思います.
- また，私自身は量子情報理論に関する理論研究者であるため，量子技術の共同研究・開発，将来を担う研究者・技術者の育成について，産学連携の機会となれば望外の喜びです.

文部科学省「光・量子飛躍フラッグシッププログラム (Q-LEAP) 」
多様な専門分野で活躍する「量子ベース思考型」人材育成のための体験型プログラムの開発,（代表者）電気通信大学 岸本哲夫 准教授

https://www.uec.ac.jp/news/announcement/2021/20210623_3479.html

電通大には量子情報（実験・理論）の研究者が数多く在籍 ⇒ 卒業生も輩出中！

本技術に関する知的財産権

- 発明の名称　評価装置
- 発明者　小川 朋宏、森 雄喜
- 出願人　国立大学法人電気通信大学
- 出願番号　特願2018-035547
- 公開番号　特開2019-153837
- 登録番号　特許7040761

産学連携の経歴

- 2005年～2008年　JSTさきがけ「量子と情報」領域に採択

お問い合わせ先

国立大学法人電気通信大学
産学官連携センター
産学官連携ワンストップサービス

TEL　042-443-5871
FAX　042-443-5725
E-mail　onestop@sangaku.uec.ac.jp