共有情報からの秘密鍵生成

上野　成道†　　水木　敬明††　　曽根　秀昭††

† 東北大学大学院情報科学研究科
†† 東北大学サイバーサイエンスセンター

あらまし　情報を盗聴者に知られずに安全にやり取りするために暗号技術が用いられる．暗号の中には共通の秘密鍵を用い暗号化，復号化を行う共通鍵暗号があるが，その秘密鍵自体をどうやって受け渡すかが大きな問題である．本研究では，無限の計算能力を有していても解読不能な情報理論的安全性を持つような秘密鍵共有を実現する方法として，身近に利用可能なものである棒状の剛体を用いた通信を提案し，理論化して他の暗号への応用を検討する．

共有情報からの秘密鍵生成

上野成道†, 水木敬明‡, 曽根秀昭‡
†東北大学大学院情報科学研究科
‡東北大学サイバーサイエンスセンター

1.1 背景

安全な通信のため暗号を用いる

盗聴者
Eve

暗号文

Alice → Bob

鍵　鍵

本研究の目的

- 将来的にも解読不能な情報理論的安全性を持つ新たな秘密鍵共有法の提案

何の仮定もなしに盗聴者Eveに知られずに鍵を共有することはできない

秘密鍵の事前共有が問題

暗号化には秘密鍵の事前共有が必要
どうやって鍵を共有するか

1.2 既存の関連研究

- 情報理論的安全性を持つ暗号
  - 量子暗号
  - 無線を使った暗号[1]
  - 電気を使った暗号[2]
  - Keyless暗号[3]

各々の仮定から
秘密鍵共有法を提案している

新たに棒状の剛体を使った秘密鍵共有法を提案
理論化して他の暗号への応用を検討

[1] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, H. Sasaoka,"Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," IEEE Trans. on Antennas Propag., vol. 53(11), pp.3776-3784, 2005.
[2] L. B. Kish, "Totally secure classical communication utilizing Johnson (-like) noise and Kirchoff's law," Physics Letters A, vol.352, no.3, pp.178-182, Mar, 2006.
[3] B. Alpern, and F. Schneider, "Key exchange using keyless cryptography," Information processing, letters 16, 2,pp.79-82, Feb, 1983.

2. 剛体による秘密鍵共有

盗聴者Eve

Alice　$X_A=\pm1$　$X_B=\mp1$　Bob

表1　入力と生成される鍵の関係

Alice	Bob	合力	動き	鍵
押す $X_A=1$	押す $X_B=-1$	0	停止	0
押す $X_A=1$	引く $X_B=1$	2	→	廃棄
引く $X_A=-1$	押す $X_B=-1$	−2	←	廃棄
引く $X_A=-1$	引く $X_B=1$	0	停止	1

- 変形しない棒状の剛体を用いる
- Alice,Bobは表1のように一定クロックで同時にランダムに棒に力を入力
- 盗聴者は合力による棒の動きからしかAlice,Bobの入力の内訳は判別できない
- 盗聴者の判別できない情報を鍵にする
- 必要鍵長が得られるまで繰り返す
- 一度に平均0.5ビットを共有

→一度により多くの情報を共有できないか？

3. 共有情報からの多値秘密鍵生成
3.1 提案手法の説明

- 強弱の違いによる多値通信
  - 加える力の強弱のバリエーションを増やす

盗聴者
Eve

Alice　$X_A=1$ $X_A=2$　$X_B=-1$ $X_B=-2$　Bob

弱く押す　1[N]
強く押す　2[N]
弱く引く　-1[N]
強く引く　-2[N]

弱く押す　-1[N]
強く押す　-2[N]
弱く引く　1[N]
強く引く　2[N]

3. 共有情報からの多値秘密鍵生成
3.1 提案手法の説明

表2　入力と生成される鍵の関係(多値)

Alice	Bob	合力	秘密鍵
−2	−2	−4	廃棄
−2	−1	−3	0
−2	1	−1	0
−2	2	0	00
−1	−2	−3	1
−1	−1	−2	廃棄
−1	1	0	01
−1	2	1	0
1	−2	−1	1
1	−1	0	10
1	1	2	廃棄
1	2	3	0
2	−2	0	11
2	−1	1	1
2	1	3	1
2	2	4	廃棄

(鍵の長さ)
$=\log_2$(等しい合力を持つ組み合わせの個数)

$$\frac{1}{4^2}(\log_2 1+\log_2 2+\log_2 2+\log_2 4+\log_2 2+\log_2 1+\log_2 4+\log_2 2+\log_2 2+\log_2 4+\log_2 1+\log_2 2+\log_2 4+\log_2 2+\log_2 2+\log_2 1)=1$$

一度に平均1ビット(2倍)の情報が共有できる

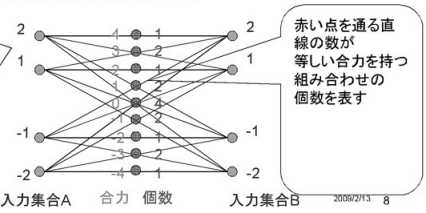
3. 共有情報からの多値秘密鍵生成
3.1 提案手法の説明

- 強弱の違いによる多値通信を用いれば一度に多くの情報を共有できる
- 一度に共有できる情報量の平均値 $L_n(A,B)$
  - 加える力の強弱のバリエーションnの値を大きくしていくと $L_n(A,B)$は大きくなる
    - n=2, 入力集合A=B={-1,1}では $L_n(A,B)$ =0.5
    - n=4,入力集合A=B={-2,-1,1,2}では $L_n(A,B)$=1

3. 共有情報からの多値秘密鍵生成
3.1 提案手法の説明

- 一度に共有できる情報量の平均値 $L_n(A,B)$
  - nの値が等しい場合でも入力集合A,Bの組み合わせを変えると $L_n(A,B)$ は変わる
    - n=4, A=B={-2,-1,1,2}では $L_n(A,B)$=1

表2の n=4 入力集合A=B ={-2,-1,1,2} の場合の 入力集合A,Bと 等しい合力を持つ 組み合わせの 個数を表した グラフ

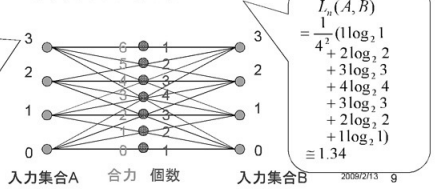


赤い点を通る直線の数が 等しい合力を持つ 組み合わせの 個数を表す

3. 共有情報からの多値秘密鍵生成
3.1 提案手法の説明

- 一度に共有できる情報量の平均値 $L_n(A,B)$
  - nの値が等しい場合でも入力集合A,Bの組み合わせを変えると $L_n(A,B)$ は変わる
    - n=4, A=B={-2,-1,1,2}では $L_n(A,B)$=1
    - n=4, A=B={0,1,2,3}では $L_n(A,B)$≒1.34

n=4 入力集合A=B ={0,1,2,3} の場合の 入力集合A,Bと 等しい合力を持つ 組み合わせの 個数を表した グラフ



$$L_n(A,B) = \frac{1}{4^2}(1\log_2 1 + 2\log_2 2 + 3\log_2 3 + 4\log_2 4 + 3\log_2 3 + 2\log_2 2 + 1\log_2 1) \fallingdotseq 1.34$$

3. 共有情報からの多値秘密鍵生成
3.1 提案手法の説明

- 一度に共有できる情報量の平均値 $L_n(A,B)$
  - nの値が等しい場合でも入力集合A,Bの組み合わせを変えると $L_n(A,B)$ は変わる
    - n=4, A=B={-2,-1,1,2}では $L_n(A,B)$=1
    - n=4, A=B={0,1,2,3}では $L_n(A,B)$≒1.34

入力集合A,Bが“等間隔”に並んでいるとき最大？

- どのような入力集合A,Bの組み合わせの場合 $L_n(A,B)$ が最大になるか証明し、そのときの $L_n(A,B)$ の値をnを用いた式で表す

3. 共有情報からの多値秘密鍵生成
3.2 問題の定式化

- 問題の定式化
  - 入力集合A,B

$$A=\{a_0,a_1,a_2,\cdots,a_i,\cdots,a_{n-1}\}$$
$$B=\{b_0,b_1,b_2,\cdots,b_j,\cdots,b_{n-1}\} \qquad |A|=|B|=n$$

  - 等しい合力を持つ a,bの組み合わせ：同値関係

$$R=\{((a,b),(a',b'))\mid a+b=a'+b'\}$$

  - 等しい合力を持つ a,bの組み合わせの集合：商集合

$$(A\times B)/R=\{\{(a,b),(a',b')\},\cdots\} \qquad ex:\{\{(0,0)\},\{(0,1),(1,0)\},\cdots\}$$

  - ある a_i,b_j と等しい合力を持つ組み合わせの数：(a_i,b_j) が含まれる商集合の要素の大きさ

$$\nu_{(A,B)}(a_i,b_j)=|C((a_i,b_j))| \quad C:\text{同値類}$$

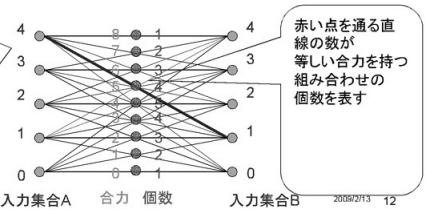
3. 共有情報からの多値秘密鍵生成
3.2 問題の定式化

グラフを利用して $\nu_{(A,B)}(a_i,b_j)$ を調べる

例 $\nu_{(A,B)}(a_i,b_j)$ は(4,1)の場合

$$\nu_{(A,B)}(4,1)=4$$

n=5の場合の 入力集合A,Bと 等しい合力を持つ 組み合わせの 個数を表した グラフ

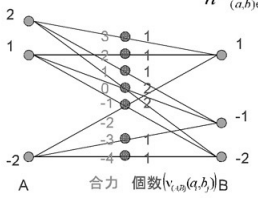


赤い点を通る直線の数が 等しい合力を持つ 組み合わせの 個数を表す

3. 共有情報からの多値秘密鍵生成
3.2 問題の定式化

- 問題の定式化
  - $L_n(A,B)$(一度に共有できる情報量の平均値)

$$L_n(A,B)=\frac{1}{n^2}\sum_{(a,b)\in A\times B}\log_2 \nu_{(A,B)}(a_i,b_j)$$



(各鍵の長さ)= $\log_2 \nu_{(A,B)}(a_i,b_j)$

を全ての組み合わせ(線)について
足し合わせ平均

3. 共有情報からの多値秘密鍵生成
3.3 提案手法

定義

(A,B) は等間隔であるとは，ある定数 m,α,βが存在して，

$A=\{\alpha, m+\alpha, 2m+\alpha, 3m+\alpha, 4m+\alpha, \cdots, (n-1)m+\alpha\}$
$B=\{\beta, m+\beta, 2m+\beta, 3m+\beta, 4m+\beta, \cdots, (n-1)m+\beta\}$

であるということ(公差mが等しい等差数列)

例
A={0,1,2,3,4}, B={0,1,2,3,4}
A={-4,-2,0,2,4}, B={10,12,14,16,18}
など

3. 共有情報からの多値秘密鍵生成
3.3 提案手法

補題

(A^*,B^*)が等間隔ならば

$$L_n(A^*,B^*)=\frac{1}{n^2}\left(2\sum_{k=1}^{n-1}k\log_2 k+n\log_2 n\right)$$

3. 共有情報からの多値秘密鍵生成
3.4 提案手法の最適性の証明

定理

(A^*,B^*) を等間隔とする.
任意の (A,B) に対して

$$L_n(A,B)\le L_n(A^*,B^*)$$

4. 本提案手法の他の暗号への応用

本研究の提案手法の理論

Alice,Bobが入力した合計(和)を盗聴者も知ることはできるが
その入力内訳を知ることはできないとき
Alice,Bobは秘密の情報を共有できる
多値通信でより多くの情報量 $L_n(A,B)$ が得られる

提案手法では棒状の剛体を用いたが
この理論は他の暗号にも応用が期待できる

5. まとめ

- 剛体による秘密鍵共有法の提案した
  - 棒状の剛体を使った秘密鍵共有法を提案
  - より多くの情報を一度に共有できる強弱の違いによる多値通信を提案した
  - 入力集合A,Bが等間隔のとき一度に共有できる情報量の平均値$L_n(A,B)$が最大になることを証明し、そのときの$L_n(A,B)$の値をnを用いた式で表した
- 提案手法を理論化して他の暗号への応用を検討した