線形符号の相対パラメータによって表される秘密分散法の安全性

栗原 淳

IT/WBS/ISEC研究会
2015年3月3日

今日の発表の目的

秘密分散法の安全性に対する，符号理論的な言葉を用いたアプローチを詳細に解説すること.

- 既存の代表的な秘密分散法とその安全性を例示
  - Shamirの(k, n)しきい値法
  - 山本・Blakley-Meadowsの(k, l, n)ランプ型しきい値法
- 同じ例を用いて，秘密分散法の線形符号を用いた表現方法を紹介
- 秘密分散法の安全性が，線形符号の符号パラメータで記述できることを紹介

今日の発表内容

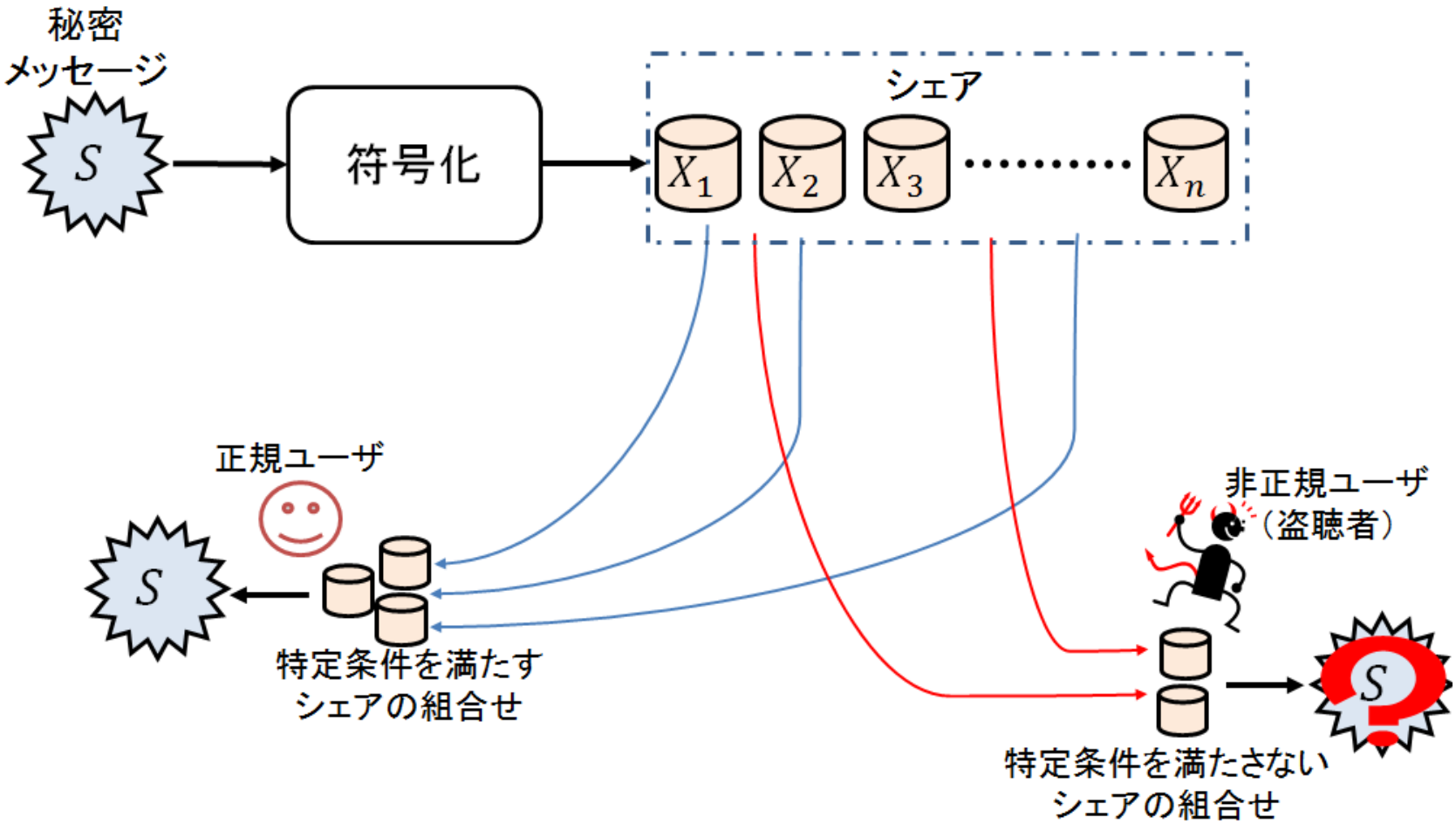
1. 秘密分散法とは
2. 線形符号による線形秘密分散法の表現
3. 相対符号パラメータによる線形秘密分散法の安全性の表現

1. 秘密分散法とは
   - しきい値法とその安全性
   - ランプ型しきい値法とその安全性
2. 線形符号による線形秘密分散法の表現法
3. 相対符号パラメータによる線形秘密分散法の安全性の表現

秘密分散法とは

秘密メッセージ S を符号化，n 個の情報片(シェア) $X_1, \ldots, X_n$ を生成する手法.

$X_1, \ldots, X_n$ の特定の組合せからのみ S を復号可能とし，それ以外からは S の情報が得られないようにすることが目的.



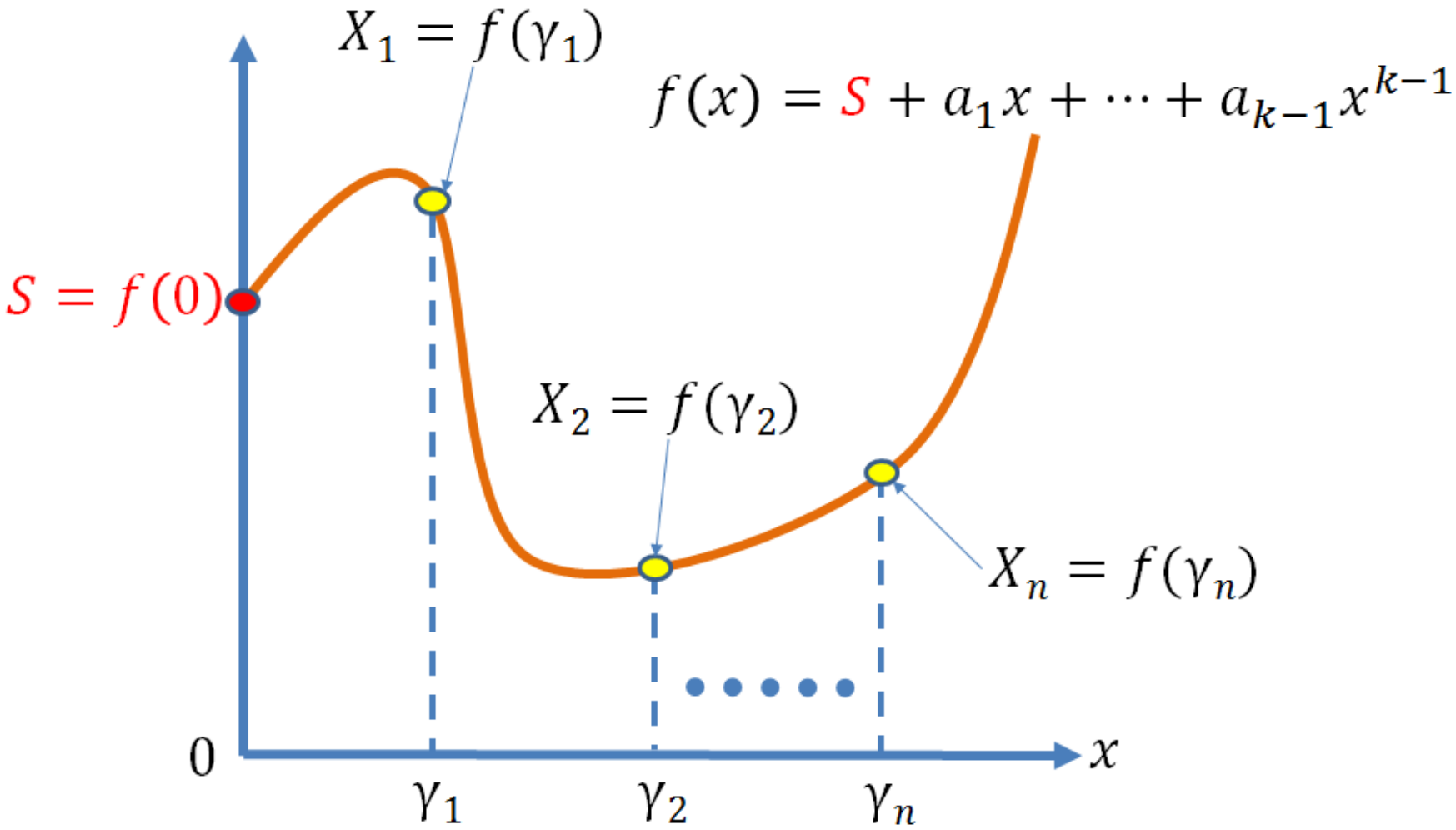
(k, n)しきい値法

- 任意のk個以上のシェアから秘密メッセージ S を常に復号できる.
- 任意の$k-1$個以下のシェアからは秘密メッセージ S の情報を一切得られない.

Shamirの(k, n)しきい値法 [Sha79]

$\gamma_1, \ldots, \gamma_n \in \mathbb{F} \setminus \{0\}$：相異なる$\mathbb{F}$の非ゼロの元

$S \in \mathbb{F}$：秘密メッセージ，　$a_1, \ldots, a_{k-1} \in \mathbb{F}$：乱数



シェアX_i $(1 \leq i \leq n)$は，　上記$f(x)$上の点$f(\gamma_i)$として定義される.

秘密メッセージ S の復号：

- k個以上の点から，Lagrange の多項式補間により$f(x)$が一意に定まり，Sが得られる.
- $k-1$個以下の点からは，$f(x)$が一意に定まらないためSの情報を得られない.

(k,n)しきい値法の漏洩情報量

logの底は$|\mathbb{F}|$.
Sは$\mathbb{F}$上の一様分布と仮定.
部分集合 $\mathcal{I} \subseteq \{1,\ldots,n\}$ について, シェアのタプル $X_{\mathcal{I}} \triangleq (X_i : i \in \mathcal{I})$.

(k,n)しきい値法の特徴は, 相互情報量 $I(S;X_{\mathcal{I}})$ を用いて

$$I(S;X_{\mathcal{I}}) = \begin{cases} 1, & \forall \mathcal{I} \subseteq \{1,\ldots,n\}, |\mathcal{I}| \geq k \\ & \quad \cdots \text{ 一意に復号できる} \\ 0, & \forall \mathcal{I} \subseteq \{1,\ldots,n\}, |\mathcal{I}| < k \\ & \quad \cdots S \text{の情報は一切得られない} \end{cases}$$

によって表される.

(k, l, n)ランプ型しきい値法

(k, n)しきい値法を構成するには，個々のシェアサイズが最低でも秘密メッセージと同じサイズになる.
⇒ シェアの保管や伝送の点で効率が悪い.

そこで，(k, l, n)ランプ型しきい値法が提案された.

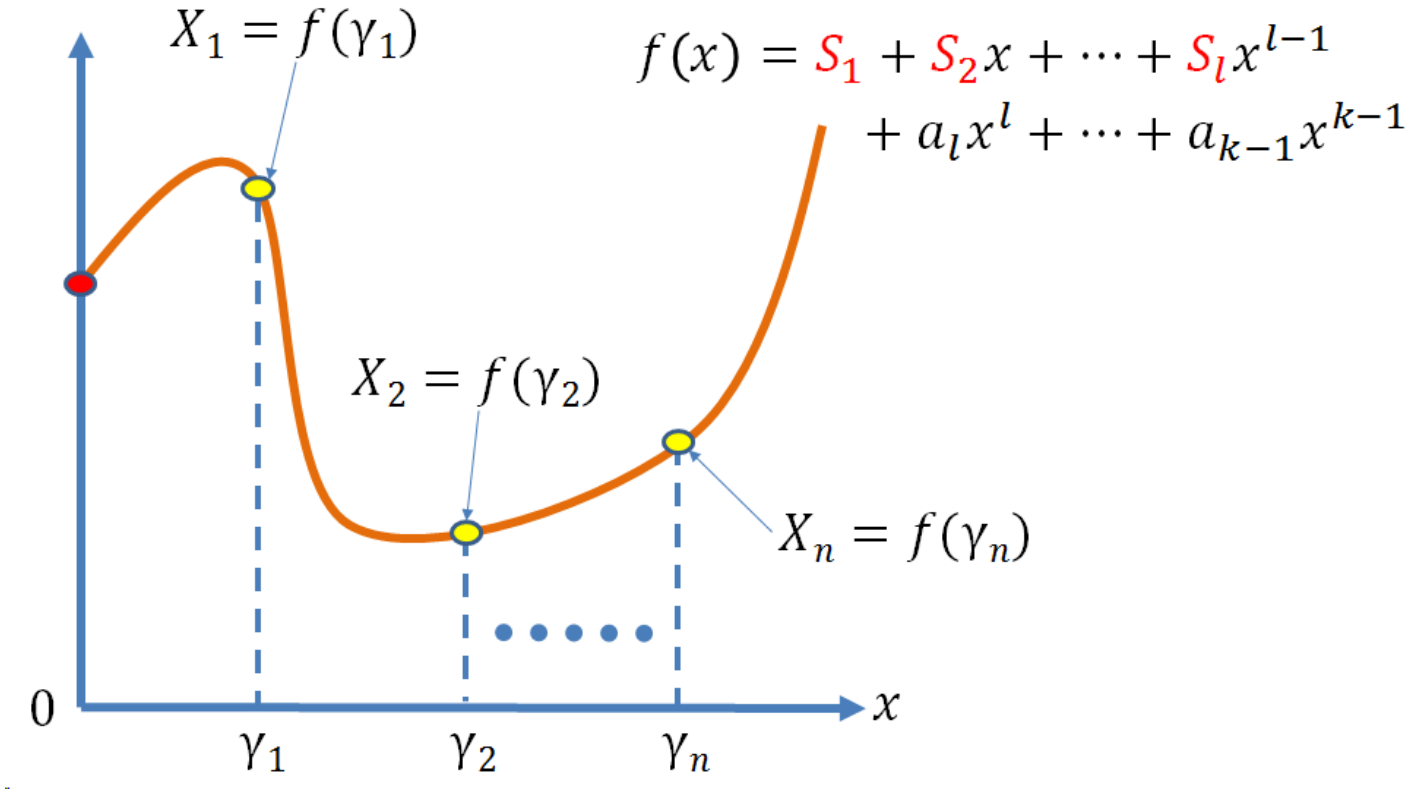
- (k, n)しきい値法のシェアサイズを維持したまま，秘密メッセージサイズをl倍に大きくすることが出来る．$(1 \leq l \leq k)$
- 任意のk個のシェアからSを一意に復号できる.
- 任意の$k-1$個のシェアから，Sを一意には復号できない(※).

※ただし，Sに関する一部の情報が漏れ出す場合が存在する.

山本 [山85]，Blakley-Meadows [BM85] の(k, l, n)ランプ型しきい値法

$\gamma_1, \ldots, \gamma_n \in \mathbb{F} \setminus \{0\}$：相異なる$\mathbb{F}$の非ゼロの元

$S = (S_1, \ldots, S_l) \in \mathbb{F}^l$：秘密メッセージ，　$a_l, \ldots, a_{k-1} \in \mathbb{F}$：乱数



Shamir のしきい値法の多項式のランダム係数の一部を秘密メッセージの要素で置き換えている．　$l = 1$のときShamirの(k, n)しきい値法に一致．　復号はLagrangeの多項式補間．

(k,l,n)ランプ型しきい値法の漏洩情報量

Sは$\mathbb{F}^l$上を一様分布と仮定
部分集合 $\mathcal{I} \subseteq \{1,\ldots,n\}$ について, $X_{\mathcal{I}} \triangleq (X_i : i \in \mathcal{I})$.

(k,l,n)ランプ型しきい値法の特徴は,

$$I(S;X_{\mathcal{I}}) = \begin{cases} l, & |\mathcal{I}| \geq k \\ & \cdots S\text{を一意に復号できる} \\ |\mathcal{I}| - k + l, & k - l < |\mathcal{I}| < k \\ & \cdots S\text{についての一部の情報が漏れ出す} \\ 0, & |\mathcal{I}| \leq k - l \\ & \cdots S\text{の情報は一切得られない} \end{cases}$$

によって表される.

1. 秘密分散法とは
2. 線形符号による線形秘密分散法の表現法
   - 線形秘密分散法とNested coset coding
   - 線形符号によるしきい値法・ランプ型しきい値法の表現
3. 相対符号パラメータによる線形秘密分散法の安全性の表現

線形秘密分散法 [CCG+07]

ある秘密分散法について,

- $S = s$に対するシェア $(X_1 = x_1, \ldots, X_n = x_n)$
- $S = s'$に対するシェア $(X_1 = x'_1, \ldots, X_n = x'_n)$

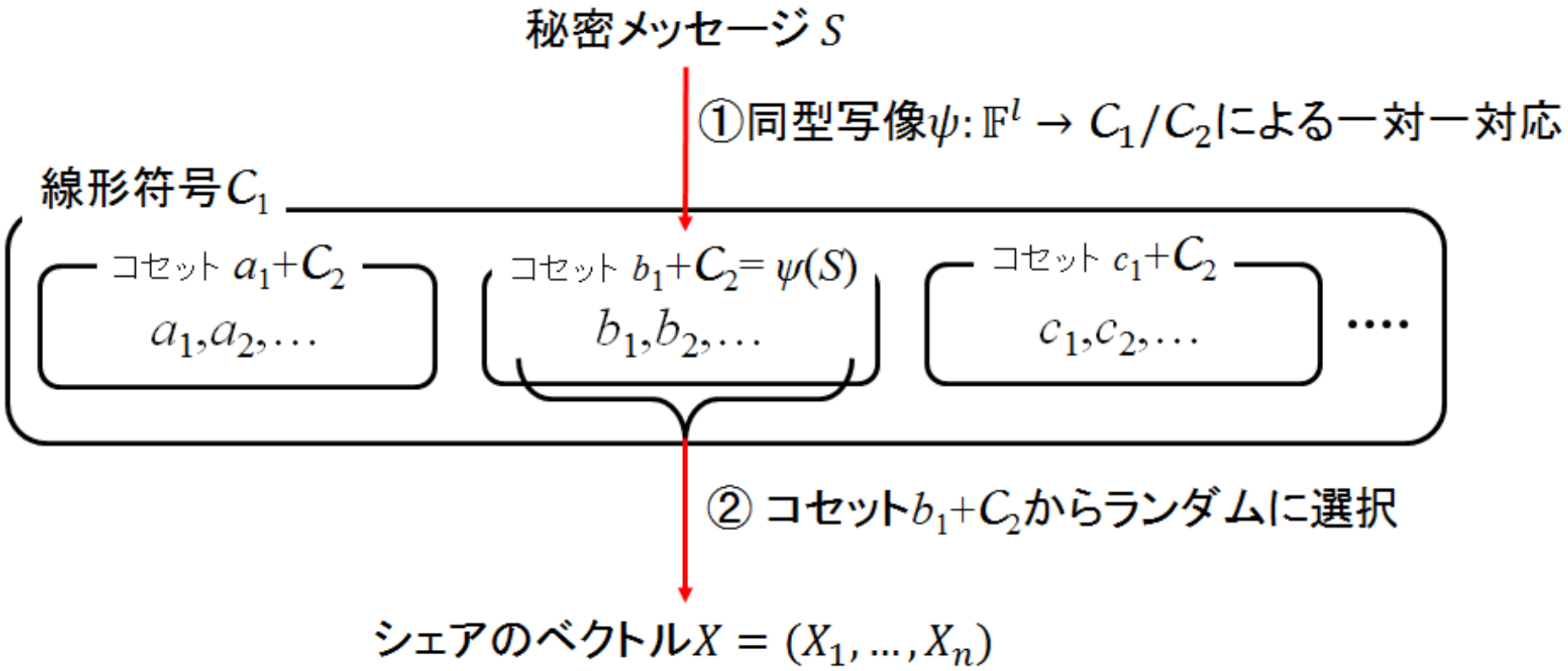
このとき，任意のスカラa, bについて，$(ax_1 + bx'_1, \ldots, ax_n + bx'_n)$ が $as + bs'$ のシェアを成すとき，その秘密分散法を「線形秘密分散法」という.

Shamirのしきい値法，山本・Blakley-Meadowsのランプ型しきい値法 のいずれも線形秘密分散法.

現在研究されているほとんどの秘密分散法は線形秘密分散法.

Nested coset coding [ZSE02]

秘密メッセージ $S = (S_1, \ldots, S_l) \in \mathbb{F}^l$
線形符号 (線型部分空間) $C_1 \subseteq \mathbb{F}^n$
その部分符号 (線型部分空間) $C_2 \subsetneq C_1$, $\dim C_1 - \dim C_2 = l$
$\mathbb{F}^l$から商空間C_1/C_2への任意の同型写像 $\psi : \mathbb{F}^l \to C_1/C_2$



C_1はC_2によって類別（隙間なく分割）されている.

[CCG+07]

任意の線形秘密分散法は，C_1, C_2, ψを適切に定めることで，Nested coset coding で表現できる.

※本発表では，シェアが $\mathbb{F}$ の1要素で表される線形秘密分散法のみを取り扱う.

山本・Blakley-Meadowsのランプ型しきい値法の線形符号による表現

$\gamma_1, \ldots, \gamma_n \in \mathbb{F} \setminus \{0\}$：相異なる$\mathbb{F}$の非ゼロの元

元の定義

$a_l, \ldots, a_{k-1}$：乱数

$f(x) = S_1 + S_2 x + \cdots + S_l x^{l-1} + a_l x^l + \cdots + a_{k-1} x^{k-1} \in \mathbb{F}[x]$

シェア：$X_1 = f(\gamma_1), \ldots, X_n = f(\gamma_n)$.

$$\Updownarrow$$

Nested coset coding による表現

$$h_S(x) = S_1 + S_2 x + \cdots + S_l x^{l-1}$$

$$C_1 = \{(f(\gamma_1), \ldots, f(\gamma_n)) : f(x) \in \mathbb{F}[x], \deg(f) < k\}$$

$$C_2 = \left\{(f(\gamma_1), \ldots, f(\gamma_n)) : f(x) = x^l p(x), p(x) \in \mathbb{F}[x], \deg(p) < k - l\right\}$$

$$\psi(S) = (h_S(\gamma_1), \ldots, h_S(\gamma_n)) + C_2$$

$$= \left\{(f(\gamma_1), \ldots, f(\gamma_n)) : f(x) = h_S(x) + x^l p(x), p(x) \in \mathbb{F}[x], \deg(p) < k - l\right\}$$

線形符号による表現を考える理由

任意の線形秘密分散法は Nested coset coding で書くことができる

$$\Downarrow$$

線形秘密分散法を表現するC_1, C_2のパラメータを用いて，　線形秘密分散法を解析できる.

次のスライドから

しきい値法やランプ型しきい値法に限定せず，C_1とC_2で表現された一般の線形秘密分散法の安全性を，C_1とC_2の符号パラメータで表現していく.

1. 秘密分散法とは
2. 線形符号による線形秘密分散法の表現法
3. 相対符号パラメータによる線形秘密分散法の安全性の表現
   - ランプ型しきい値法の漏洩情報量
   - 最大漏洩情報量と相対一般化Hamming重み

線形秘密分散法の漏洩情報量

インデックス集合 $\mathcal{I} \subseteq \{1, \ldots, n\}$.

線形符号$C \subseteq \mathbb{F}^n$について，$\mathcal{I}$**への短縮符号**：

$$C_{\mathcal{I}} \triangleq \{x = [x_1, \ldots, x_n] \in C : x_i = 0 \text{ if } i \notin \mathcal{I}\}$$

$C_1^{\perp}, C_2^{\perp}$：それぞれC_1, C_2の**双対符号**.

盗聴されたシェアのタプル $X_{\mathcal{I}} = (X_i : i \in \mathcal{I})$から得られる$S$に関する相互情報量 $I(S; X_{\mathcal{I}})$ (**漏洩情報量**)を，符号理論的な量へ翻訳する.

Lemma ([KMU13, Lemma 26])

$$I(S; X_{\mathcal{I}}) = \dim (C_2^{\perp})_{\mathcal{I}} - \dim (C_1^{\perp})_{\mathcal{I}}$$

$I(S; X_{\mathcal{I}})$ は，双対符号の$\mathcal{I}$への短縮符号の次元の差に等しい.

山本・Blakley-Meadowsのランプ型しきい値法の漏洩情報量

ランプ型しきい値法の既知の安全性が符号理論的な量から求まるということを確認する.

復習：山本・Blakley-Meadowsのランプ型しきい値法を表す符号C_1, C_2は,

$$C_1 = \{(f(\gamma_1), \ldots, f(\gamma_n)) : f(x) \in \mathbb{F}[x], \deg(f) < k\}$$
$$C_2 = \left\{(f(\gamma_1), \ldots, f(\gamma_n)) : f(x) = x^l p(x), p(x) \in \mathbb{F}[x], \deg(p) < k - l\right\}.$$

によって定めることができる.
C_1, C_2はともに Reed-Solomon 符号.

Reed-Solomon 符号の双対符号はやはり Reed-Solomon 符号.

$\Rightarrow C_1^\perp, C_2^\perp$ともに Reed-Solomon 符号

$\mathcal{I} \subseteq \{1, \ldots, n\}$.
線形符号 $C \subseteq \mathbb{F}^n$について，$C_{\mathcal{I}}$は$\mathcal{I}$への短縮符号.
$C_{\mathcal{I}} = \{x = [x_1, \ldots, x_n] \in C : x_i = 0 \text{ if } i \notin \mathcal{I}\}$

$\overline{\mathcal{I}} \triangleq \{1, \ldots, n\} \setminus \mathcal{I}$：$C_{\mathcal{I}} \subseteq C$の符号語の【常にゼロとなる要素】のインデックス集合

線形符号 $C \subseteq \mathbb{F}^n$ が Reed-Solomon 符号.

$\Rightarrow$ Cの生成行列の任意の$\dim C$列が線形独立.

Cの生成行列を$G \in \mathbb{F}^{\dim C \times n}$と表すと，$C$は$G$の行空間：$C = \left\{uG : u \in \mathbb{F}^k\right\}$

$\Rightarrow$ Cを$\mathcal{I}$について短縮して$C_{\mathcal{I}} \subseteq C$を得るとき，その次元は単純に$\dim C$から $\min\{\dim C, |\overline{\mathcal{I}}|\}$ だけ減少する.

$$\dim C_{\mathcal{I}} = \max\left\{0, \dim C - |\overline{\mathcal{I}}|\right\}$$

$C_1^\perp, C_2^\perp$ともにReed-Solomon 符号.
$|\overline{\mathcal{I}}| = n - |\mathcal{I}|$
$\dim C_1 = k, \quad \dim C_2 = k - l \Leftrightarrow \dim C_1^\perp = n - k, \quad \dim C_2^\perp = n - k + l$
から

$$
\begin{aligned}
I(S\,;X_{\mathcal{I}}) &= \dim\,(C_2^\perp)_{\mathcal{I}} - \dim\,(C_1^\perp)_{\mathcal{I}} \\
&= \max\{0, \underbrace{\dim C_2^\perp}_{=n-k+l} - \underbrace{|\overline{\mathcal{I}}|}_{=n-|\mathcal{I}|}\} - \max\{0, \underbrace{\dim C_1^\perp}_{=n-k} - \underbrace{|\overline{\mathcal{I}}|}_{=n-|\mathcal{I}|}\} \\
&= \max\{0, |\mathcal{I}| - k + l\} - \max\{0, |\mathcal{I}| - k\} \\
&= \begin{cases} 0, & |\mathcal{I}| \le k - l \\ |\mathcal{I}| - k + l, & k - l < |\mathcal{I}| \le k \\ l, & |\mathcal{I}| > k \end{cases}
\end{aligned}
$$

が得られる.

最大漏洩情報量

一般的な秘密分散法の安全性の尺度として，盗聴シェア数 μ についての任意の$\mathcal{I}, |\mathcal{I}| = \mu$に関する 漏洩情報量の最大値 (**最大漏洩情報量**) を導入する.

Definition (最大漏洩情報量)

秘密分散法において，$\mu(\leq n)$個のシェアとSの間の相互情報量の最大値

$$\Delta_\mu \triangleq \max_{\mathcal{I}\subseteq\{1,\ldots,n\},|\mathcal{I}|=\mu} I(S;X_{\mathcal{I}})$$

を最大漏洩情報量Δ_μと呼ぶ.

Δ_μをC_1, C_2の「相対符号パラメータ」によって表現する.

相対一般化Hamming重みによる最大漏洩情報量の表現

Definition ([LMHC05, 相対一般化 Hamming 重み])

線形符号$C \subseteq \mathbb{F}^n$とその部分符号$C' \subsetneq C$の**i-次相対一般化Hamming重み**は，　$1 \leq i \leq \dim(C/C')$について，

$$M_i(C, C') \triangleq \min_{\mathcal{I} \subseteq \{1,\ldots,n\}} \left\{ |\mathcal{I}| : \dim C_{\mathcal{I}} - \dim C'_{\mathcal{I}} \geq i \right\}$$
$$= \min_{\mathcal{I} \subseteq \{1,\ldots,n\}} \left\{ |\mathcal{I}| : \dim C_{\mathcal{I}} - \dim C'_{\mathcal{I}} = i \right\}$$

によって定義される.

相対一般化Hamming重みと最大漏洩情報量の定義から,

$$\begin{aligned}
&\min\{\mu : \Delta_\mu \geq j\} \\
&= \min\left\{\mu : \exists \mathcal{I}, |\mathcal{I}| = \mu, \text{ such that } \dim (C_2^\perp)_{\mathcal{I}} - \dim (C_1^\perp)_{\mathcal{I}} \geq j\right\} \\
&= \min_{\mathcal{I} \subseteq \{1,\ldots,n\}} \left\{|\mathcal{I}| : \dim (C_2^\perp)_{\mathcal{I}} - \dim (C_1^\perp)_{\mathcal{I}} \geq j\right\} \\
&= M_j(C_2^\perp, C_1^\perp)
\end{aligned}$$

が成り立ち，次の定理が得られる.

Theorem ([Kur12, Theorem 5.2])

$1 \leq j \leq l$について，盗聴者がSの情報をj単位 ($j \log_2 |\mathbb{F}|$ ビット) 得ようとすると，必ず$M_j(C_2^\perp, C_1^\perp)$個以上のシェアの盗聴が必要.
より詳細には，次の3つの性質が成り立つ.

1. $\mu < M_j(C_2^\perp, C_1^\perp)$個のシェアについては，最大漏洩情報量$\Delta_\mu < j$.
2. $\mu \geq M_j(C_2^\perp, C_1^\perp)$個のシェアについては，最大漏洩情報量$\Delta_\mu \geq j$.
3. $I(S; X_{\mathcal{I}}) = j$を満たす要素数$|\mathcal{I}| = M_j(C_2^\perp, C_1^\perp)$のシェアの組み合わせが存在.

安全性と同じく，シェアの個数に対する復号条件も相対一般化 Hamming 重みで記述できる.

Theorem ([KUM12, Theorem 9])

- 任意の$\mu > n - M_1(C_1, C_2)$個のシェアからSを一意に復号できる.
- $\mu = n - M_1(C_1, C_2)$の場合，Sを一意に復号できない組み合わせが存在する.

線形秘密分散法の安全性と復号条件を，符号パラメータの世界に持ち込んで解析できることが明らかになった

まとめ

まとめとこの研究の発展について

本発表では，線形秘密分散法の安全性を表現するための，符号理論的な枠組みについて解説した.

- 最大漏洩情報量が，符号パラメータ「相対一般化 Hamming 重み」によって記述できることを示した.
- 上記の事柄について，既存のしきい値法・ランプ型しきい値法の例を与えた.

この研究の発展として，次のようなものが挙げられる.

- セキュアネットワーク符号化への拡張・一般化
- $M_i(C_1, C_2)$と$M_j(C_2^\perp, C_1^\perp)$の値が固定された時の，線形符号$C_1$とその部分符号$C_2$の存在条件など

参考文献

[BM85] G. R. Blakley, Jr. and C. Meadows, “Security of ramp schemes,” in Proc. CRYPTO 1984, ser. Lecture Notes in Computer Science, G. R. Blakley, Jr. and D. Chaum, Eds., vol. 196. Springer-Verlag, 1985, pp. 242–268.

[CCG+07] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, “Secure computation from random error correcting codes,” in Proc. EUROCRYPT 2007, ser. Lecture Notes in Computer Science, vol. 4515. Springer-Verlag, 2007, pp. 291–310.

[KMU13] J. Kurihara, R. Matsumoto, and T. Uyematsu, “Relative generalized rank weight of linear codes and its applications to network coding,” Jan. 2013. [Online]. Available: http://arxiv.org/abs/1301.5482

[KUM12] J. Kurihara, T. Uyematsu, and R. Matsumoto, “Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight,” IEICE Trans. Fundamentals, vol. E95-A, no. 11, pp. 2067–2075, Nov. 2012.

[Kur12] J. Kurihara, “A study on design and security analysis of secret sharing schemes,” Ph.D. Thesis, Tokyo Institute of Technology, Sep. 2012.

[LMHC05] Y. Luo, C. Mitrpant, A. J. Han Vinck, and K. Chen, “Some new characters on the wire-tap channel of type II,” IEEE Trans. Inf. Theory, vol. 51, no. 3, pp. 1222–1229, Mar. 2005.

[Sha79] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[ZSE02] R. Zamir, S. Shamai, and U. Erez, “Nested linear/lattice codes for structured multiterminal binning,” IEEE Trans. Inf. Theory, vol. 48, no. 6, pp. 1250–1276, Jun. 2002.

[山85] 山本博資, “(k, L, n)しきい値秘密分散システム,” 電子通信学会論文誌, vol. J68-A, no. 9, pp. 945–952, Sep. 1985.

以降，予備資料

山本・Blakley-Meadowsのランプ型しきい値法の最大漏洩情報量と復号条件が相対一般化 Hamming 重みで求まることを確認

Reed-Solomon符号$C \subseteq \mathbb{F}^n$と任意の部分符号$C' \subsetneq C$に対し次が成立 [LMHC05].

$$M_i(C, C') = n - \dim C + i \text{ for } 1 \leq i \leq \dim C/C'$$

山本・Blakley-Meadowsの手法で，C_1, C_2は Reed-Solomon 符号.

Reed-Solomon 符号の双対符号はやはり Reed-Solomon 符号なため，以下が成立する.

$$M_j(C_2^\perp, C_1^\perp) = \dim C_2 + j \text{ and } M_1(C_1, C_2) = n - \dim C_1 + 1$$

$\dim C_1 = k$, $\dim C_2 = k - l$と表す.

$$\Downarrow$$

- S についてj単位 ($j \log_2 |\mathbb{F}|$ ビット) の情報を得るためには，必ず $\mu = \dim C_2 + j = k - l + j$ 以上のシェアの盗聴が必要.
- $\mu = \dim C_1 = k$ 個以上のシェアから必ず S を一意に復号できる.