[I486S]
暗号プロトコル理論

藤崎 英一郎

北陸先端科学技術大学院大学

2020 年 7 月 21 日

本日の講義の内容

1. Generalized Linear Secret-Sharing

General Adversary Structures

- Adversary Structure $\mathcal{A}$: A family of subsets of the set of all players $P = \{P_1, \ldots, P_n\}$ that is anti-monotone, i.e., if $A \in \mathcal{A}$, then $B \in \mathcal{A}$ for any subset B of A, i.e., $B \subseteq A$.
  - An adversary structure is said to be Q_2 if for all $A_1, A_2 \in Q_2$, it holds that $A_1 \cup A_2 \subsetneq P$.
  - An adversary structure is said to be Q_3 if for all $A_1, A_2, A_3 \in Q_3$, it holds that $A_1 \cup A_2 \cup A_3 \subsetneq P$.
- Access structure Γ: A family of subsets of the set of all players P that is monotone, i.e., if $A \in \Gamma$, then $B \in \Gamma$ for any superset B of A, i.e., $A \subseteq B$.

Q_2 and Q_3 are natural generalizations of the threshold model for $t < n/2$ and $t < n/3$.

Linear Secret Sharing

Linear Secret Sharing (LSS) のより一般的構成法 [CDN15].

- 行列 $M \in K^{m \times (t+1)}$. M の i 番目の行ベクトルを $\boldsymbol{m_i}$ と書く。
- ラベル関数 $\phi : \{1, \ldots, m\} \to \{1, \ldots, n\}$.
- 列ベクトル $\boldsymbol{r_s} := (s, r_1, \ldots, r_t)^T$.
- 有資格集合 (qualified set) $Q \subseteq P$, i.e., s を復元できる集合。

Dealer は、秘密 $s \in K$ を秘密分散するために、乱数 $r_1, \ldots, r_t \leftarrow K$ を選び、$(s_1, \ldots, s_m)^T := M\boldsymbol{r_s}$ を計算。$s_i (= \boldsymbol{m_i r_s})$ を $P_{\phi(i)}$ に配る。

Reconstruction ができるために、次の条件がいる。

- M_Q で、$\phi(i) \in Q$ となる行ベクトル $\boldsymbol{m_i}$ から構成された行列を表す。
- 全ての有資格集合 $Q \in \Gamma$ に対して、$\boldsymbol{u_Q}^T M_Q = \sum_{\phi(i) \in Q} u_i m_i = (1, 0, \ldots, 0)$ となる reconstruction vector $\boldsymbol{u_Q}$ が存在する。
- $\boldsymbol{u_Q}^T M_Q \boldsymbol{r_s} = s$ より、$M_Q \boldsymbol{r_s}$ と reconstruction vector $\boldsymbol{u_Q}$ から秘密が復元できる。

有資格集合と無資格集合

P の部分集合 A に対して、$M_A \boldsymbol{r_s}$ の分布が、s の分布と独立 (i.e., $H(s) = H(s|M_A \boldsymbol{r_s})$) の場合、$A$ を無資格集合 (unqualified set) という。次の定理から、P の部分集合は、有資格か、無資格のどちらかに別れる。

Theorem

$\boldsymbol{e_Q} := (1, 0, \ldots, 0)$, $\mathrm{Im}(M_Q) := \{\boldsymbol{x}^T M_Q \mid \boldsymbol{x} \in K^{t+1}\}$ とする。

- Q *is qualified* $\Longleftrightarrow \boldsymbol{e_Q} \in \mathrm{Im}(M_Q)$.
- Q *is unqualified* $\Longleftrightarrow \boldsymbol{e_Q} \notin \mathrm{Im}(M_Q)$.

- Q が有資格なら、$\hat{Q}$ $(Q \subset \hat{Q})$ も有資格であり、A が無資格なら、$\hat{A}$ $(\hat{A} \subset A)$ も無資格である。
- 全集合 P が有資格集合であれば、無資格集合の集合を adversary structure $\mathcal{A}$, それ以外の集合の集合を access structure Γ （有資格集合の集合）と分けることができる
- 一般の SS では、有資格でも無資格でもない集合が存在する。そのような SS を Ramp 型 SS という。

定理 1 の証明の肝

$\mathrm{Ker}_r(M_Q) := \{\boldsymbol{w} \mid M_Q\boldsymbol{w} = 0\}$ と M_Q の right-kernel を定義すると、
$\mathrm{Im}(M_Q)(= \{\boldsymbol{x}^T M_Q \mid \boldsymbol{x} \in K^{t+1}\}) = \mathrm{Ker}_r(M_Q)^{\perp}$ が成り立つ.

$$\boldsymbol{e} \in \mathrm{Im}(M_Q) \Longleftrightarrow \forall \boldsymbol{w} \in \mathrm{Ker}_r(M_Q),\ \boldsymbol{e}\boldsymbol{w} = 0.$$

が成り立つ。よって、

$$\boldsymbol{e} \notin \mathrm{Im}(M_Q) \Longleftrightarrow \exists \boldsymbol{w} \in \mathrm{Ker}_r(M_Q),\ \boldsymbol{e}\boldsymbol{w} \neq 0$$

$\boldsymbol{e} \in \mathrm{Im}(M_Q)$ であれば、ある $\boldsymbol{u}^T M_Q = \boldsymbol{e}$ なる $\boldsymbol{u}$ が存在して、
$\boldsymbol{u}^T(M_Q\boldsymbol{r_s}) = \boldsymbol{u}^T M_Q\boldsymbol{r_s} = \boldsymbol{e}\boldsymbol{r_s} = s$. よって、$Q$ は有資格。

$\boldsymbol{e} \notin \mathrm{Im}(M_A)$ であれば、ある $\boldsymbol{w} \in Ker_r(M_A)$ が存在して、$\boldsymbol{e}\boldsymbol{w} \neq 0$ なので、
任意の s' に対して、$\boldsymbol{r_{s'}} := \boldsymbol{r_s} + \frac{(s'-s)}{(\boldsymbol{e}\cdot\boldsymbol{w})}\boldsymbol{w}$ とおくと、

$$M_A\boldsymbol{r_s} = M_A\boldsymbol{r_{s'}}$$

よって、A のシェア $M_A\boldsymbol{r_s}$ と秘密 s は独立。よって、A は無資格。

線型性

$[a; \boldsymbol{r_a}] = M\boldsymbol{r_a}$, $[b; \boldsymbol{r_b}] = M\boldsymbol{r_b}$ から、$\lambda, \eta \in K$ に対して、

$$\lambda[a; \boldsymbol{r_a}] + \eta[b; \boldsymbol{r_b}] = M(\lambda \boldsymbol{r_a} + \eta \boldsymbol{r_b}) = [\lambda a + \eta b; \boldsymbol{r_{\lambda a + \eta b}}]$$

掛け算へ（1）

次のように演算を定義する。

$$[a; \boldsymbol{r_a}] \odot [b; \boldsymbol{r_b}] := (([a; \boldsymbol{r_a}])_{P_1} \otimes ([b; \boldsymbol{r_b}])_{P_1}, \ldots, ([a; \boldsymbol{r_a}])_{P_n} \otimes ([b; \boldsymbol{r_b}])_{P_n})$$

ここで、$([a; \boldsymbol{r_a}])_{P_i} = M_{P_i} \boldsymbol{r_a}$, M_{P_i} をそれぞれ、P_i に配られるシェア（列ベクトル）と、それに対応する行列とする。

$\otimes$ は、テンソル積で、列ベクトル $\alpha \in K^{\ell}$, $\beta \in K^{m}$ に対して、
$\alpha = (\alpha_1, \ldots, \alpha_{\ell})^T$, $\beta = (\beta_1, \ldots, \beta_m)^T$, とすると、

$$\alpha \otimes \beta = (\alpha_1\beta_1, \ldots, \alpha_1\beta_m, \ldots\ldots, \alpha_{\ell}\beta_1, \ldots, \alpha_{\ell}\beta_m)^T \in K^{\ell \cdot m}$$

テンソル積

一般には、行列 $A \in K^{m\times n}$, $B \in K^{\hat{m}\times\hat{n}}$ に対して、次のように定義。

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{pmatrix} \in K^{m\hat{m}\times n\hat{n}}.$$

行列 $M_a \in K^{m\times n}$, $M_b \in K^{\hat{m}\times\hat{n}}$, (列ベクトル) $\boldsymbol{r_a} \in K^n$, $\boldsymbol{r_b} \in K^{\hat{n}}$ とする。
また u, v を M_a, M_b のそれぞれ行ベクトルとすると、

1. $M_a\boldsymbol{r_a} \otimes M_b\boldsymbol{r_b} = (M_a \otimes M_b)(\boldsymbol{r_a} \otimes \boldsymbol{r_b})$.
2. $(u\boldsymbol{r_a}) \otimes (v\boldsymbol{r_b}) = (u \otimes v)(\boldsymbol{r_a} \otimes \boldsymbol{r_b})$.

が成り立つ。(2) から、(1) は導ける。

掛け算へ（2）

$$M_{P_i}\boldsymbol{r_a} \otimes M_{P_i}\boldsymbol{r_b} = (M_{P_i} \otimes M_{P_i})(\boldsymbol{r_a} \otimes \boldsymbol{r_b}) = (M_{P_i} \otimes M_{P_i})(\boldsymbol{r_{ab}})$$

ここで、$\boldsymbol{r_{ab}} = (ab, r'_1, \dots) \in K^{(t+1)^2}$. これより、

$$[a; \boldsymbol{r_a}]_S \odot [b; \boldsymbol{r_b}]_S = [ab; \boldsymbol{r_a} \otimes \boldsymbol{r_b}]_{\hat{S}}$$

ここで、S はもとの秘密分散で、$\hat{S}$ は、$\hat{M} = M \otimes M$ によって新たに定義された秘密分散（ただし、reconstruction できるかは保証されていない）。

もし、秘密分散 $\hat{S}$ に有資格集合 Q が存在するなら、reconstruction vector $\boldsymbol{u}$ が存在して、

$$\boldsymbol{u}^T([a; \boldsymbol{r_a}]_S \odot [b; \boldsymbol{r_b}]_S) = \boldsymbol{u}^T[ab; \boldsymbol{r_a} \otimes \boldsymbol{r_b}]_{\hat{S}} = ab.$$

乗算可能性

Definition

全集合 P が、掛け算によってできた秘密分散 $\hat{S}$ の有資格集合であるならば、元の秘密分散 S を乗算可 (multiplicative) という。もし、adversary structure $\mathcal{A}$ に属さない任意の集合 $Q \notin \mathcal{A}$ ($\leftrightarrow Q \in \Gamma$) が有資格集合であるならば、$S$ を強乗算可 (strongly multiplicative) という。

定理

Theorem

- P を含まない任意の *adversary structure* $\mathcal{A}$ に対して、線型秘密分散 S が存在する。
- 任意の Q_2-*adversary structure* $\mathcal{A}$ に対して、乗算可な線型秘密分散 S が存在する。
- 任意の Q_3-*adversary structure* $\mathcal{A}$ に対して、強乗算可な線型秘密分散 S が存在する。

複製秘密分散 (replicated secret sharing) は上記を満たす。

掛け算（まとめ）

秘密分散 S が乗算可 (multiplicative) とする。S が乗算可であるから、$u^T(M \otimes M)(\boldsymbol{r_a} \otimes \boldsymbol{r_b}) = ab$ となる全集合 P に対する reconstruction vector $u \in K^{m^2}$ が存在する。c_i を、列ベクトル $\boldsymbol{c} = (M \otimes M)(\boldsymbol{r_a} \otimes \boldsymbol{r_b})$ の i 番目の要素とする。

Input: $[a; \boldsymbol{r_a}]_S$, $[b; \boldsymbol{r_b}]_S$.
Output: $[ab; \boldsymbol{r_a} \otimes \boldsymbol{r_b}]_S$.

- 各 P_i が $(M_{P_i}\boldsymbol{r_a}) \otimes (M_{P_i}\boldsymbol{r_b})$ をローカルに計算. 結果、$(M_{P_i} \otimes M_{P_i})(\boldsymbol{r_a} \otimes \boldsymbol{r_b}) \in K^{(t+1)^2}$ のシェア（列ベクトル）をローカルに保持. これは、

$$\boldsymbol{c} = (M \otimes M)(\boldsymbol{r_a} \otimes \boldsymbol{r_b})$$

  とした時、P_i が、$\{c_j\}_{\phi(j)=i}$ をローカルに保持しているのと同じである。
- 各 P_i が自らの $\boldsymbol{c_j}$ $(\phi(j) = i)$ を全て $P_1, \ldots, P_n$ 間で線型秘密分散し、結果 $[c_j; \boldsymbol{r_{c_j}}]_S$ $(j = 1, \ldots, m^2)$ という状態になる。
- $\boldsymbol{u}^T = (u_1, \ldots, u_{m^2})$ とすると、

$$\sum_j u_j [c_j; \boldsymbol{r_{c_j}}]_S = \left[\sum_j u_j c_j; \sum_j u_j \boldsymbol{r_{c_j}}\right]_S = \left[ab; \sum_j u_j \boldsymbol{r_{c_j}}\right]_S$$

  となるので、各 P_i のローカルな計算により、$\left[ab; \sum_j u_j \boldsymbol{r_{c_j}}\right]_S$ という状態が作られる。

参考文献

[CDN15] Ronald Cramer, Ivan Damgård, and Jesper Nielsen.
Secure Multiparty Computation and Secret Sharing.
Cambridge University Press, 2015.