「Private Simultaneous Message」 sp: 品川さん

10月25日

§1 イントロ to 暗号

§2 PSM

§3 通信量 $O(N)$ のプロトコル

§4 通信量 $O(\sqrt{n})$ のプロトコル

§5 平方剰余に基づくPSM.

- 通信量
- 通信回数
- 計算時間 + メモリ

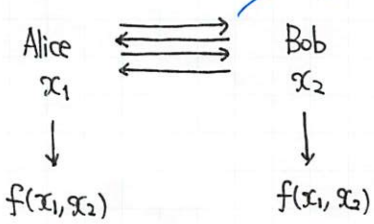
§1: Craptgraphy = Computational Conplexity + Secrecy (計算量+秘匿性)

- 情報理論的 安全
  計算能力 ∞
  攻撃者に対しても安全
  - 暗号
  - 秘密計算 — PSM
  - 秘密分散
- 計算量的 安全 — 暗号
  (計算量仮定が必要)
  - RSA
  - 楕円
  - 格子
  - 多変数

§2: PSM

- 通常の秘密計算

ラウンド数 = 4



- PMS

m_1, m_2 は x_1, x_2 と r から決まる量

Definition

$X_1, \dots, X_n, Y, R, M_1, \dots, M_n$: finite set

$f : X_1 \times X_2 \times \cdots \times X_n \longrightarrow Y$: a map

$\mathrm{Enc}_i : X_i \times R \longrightarrow M_i$: a map

$\mathrm{Dec} : M_1 \times \cdots \times M_n \longrightarrow Y$: a map

$\Pi = (R, M_1, \dots, M_n, \mathrm{Enc}_i, \mathrm{Dec})$ が f に対する PMS プロトコル であるとは 以下の 正当性 と 安全性 を満たすときをいう.

<u>正当性</u> : ${}^\forall x = (x_1, \dots, x_n) \in X_1 \times \cdots \times X_n$, ${}^\forall r \in R$ に対して

$$f(x_1, \dots, x_n) = \mathrm{Dec}(\mathrm{Enc}_1(x_1, r), \dots, \mathrm{Enc}_n(x_n, r))$$

<u>安全性</u> : ${}^\forall x, x' \in X_1 \times \cdots \times X_n$ で $f(x) = f(x')$ であるような任意の x, x' をとる.

${}^\forall \vec{m} \in M_1 \times \cdots \times M_n$ に に対して

$$\Pr_{r \leftarrow R}[(\mathrm{Enc}_1(x_1, r), \dots, \mathrm{Enc}_n(x_n, r)) = \vec{m}] = \Pr_{r \leftarrow R}[(\mathrm{Enc}(x_1', r), \dots, \mathrm{Enc}_n(x_n', r)) = \vec{m}]$$

↑ Rから一様ランダムにとって入れる.

§3 通信号 $O(n)$ の プロトコル. [Feige - Kilian - Naor '94]

・計算対象 $f : \underbrace{\mathbb{Z}/N\mathbb{Z}}_{= \mathbb{Z}_N} \times \mathbb{Z}/N\mathbb{Z} \longrightarrow \{0, 1\}$

・乱数空間 $R = \{(r, s) \mid r \in \{0,1\}^N, s \in \mathbb{Z}_N\}$

・暗号化関数

$m_1 = \mathrm{Enc}_1(x_1, (r,s))$ の計算

$$\begin{bmatrix} f(x_1, 0) \\ \vdots \\ f(x_1, N-1) \end{bmatrix} \oplus \begin{bmatrix} r_0 \\ \vdots \\ r_{N-1} \end{bmatrix} = \begin{bmatrix} y_0 \\ \vdots \\ y_{N-1} \end{bmatrix} \rightsquigarrow m_1 = \left.\begin{bmatrix} y_s \\ y_{s+1} \\ \vdots \\ y_N \\ y_1 \\ \vdots \\ y_{s-1} \end{bmatrix}\right\} N\text{ビット}$$

XOR = 足して mod 2 .

$m_2 = \mathrm{Enc}_2(x_2, (r, s))$ の計算

$$m_2 = (\underbrace{x_2 - s \pmod N}_{\log N \text{ ビット}}, \underbrace{r_{x_2}}_{1\text{ビット}})$$

◎ 復号関数

$$\begin{array}{ll} y_s & 0 \\ y_{s+1} & 1 \\ \vdots & \vdots \\ y_{x_2} & x_2 - s \end{array} \quad \rightsquigarrow \quad y_{x_2} \oplus r_{x_2} = (f(x_1, x_2) \oplus r_{x_2}) \oplus r_{x_2} = f(x_1, x_2)$$

通信量 $N + \log N + 1 = O(N)$ である.

§4 Omit.

§5 平方剰余に基づく PSM

大小比較プロトコル [FKN '94]

$$f(x_1, x_2) = \begin{cases} 1 & x_1 > x_2 \\ 0 & x_1 = x_2 \\ -1 & x_1 < x_2 \end{cases} \quad (x_i \in \{0,1,2\})$$

$r = (r_1, r_2)$, where $r_1 \in \{0, 1, 2, \dots, 6\} = \mathbb{F}_7$

$$r_2 \in QR_7^+ = \{x \in \mathbb{F}_7 \mid x = b^2 \text{ for some } b \in \mathbb{F}_7,\ x \neq 0\}$$
$$= \{1, 2, 7\}$$

$$Enc_1(x_1, (r_1, r_2)) = r_1 + r_2 x_1 \pmod 7 \quad =: m_1$$
$$Enc_2(x_2, (r_1, r_2)) = r_1 + r_2 x_1 \pmod 7 \quad =: m_2$$

$$\rightsquigarrow \quad Dec(m_1, m_2) = \left(\frac{m_1 - m_2}{7}\right) = \begin{cases} 1 \\ 0 \\ -1 \end{cases}$$

ルジャンドルの記号

$m_1 - m_2$ mod 7 の平方剰余 なら 1

zero なら 0

非平方剰余 なら -1

$$m_1 - m_2 = r_2(x_1 - x_2)$$
$$\left(\frac{r_2(x_1 - x_2)}{7}\right) = \left(\frac{r_2}{7}\right)\left(\frac{x_1 - x_2}{7}\right)$$

Lemma [Peralta]

$p \cdot \left(\frac{1}{2}\right)^n > n(\sqrt{p}+3) \Rightarrow$ pの平方剰余列は 任意の ビット列 $t \in \{0,1\}^n$ を 部分列として 含む.

$\rightsquigarrow$ $\vec{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$, $\vec{x} = (x_1, \dots, x_n) \in \{0,1\}^n$ を入力したときに
$\vec{x}' = (x_1', \dots, x_n') \in \{0,1\}^n$

$f(\vec{x}) \neq f(\vec{x}') \Rightarrow \langle \vec{a}, \vec{x} \rangle \neq \langle \vec{a}, \vec{x}' \rangle$ を満たす $\vec{a}$ を探す.

このような $\vec{a}$ の中で

$$\min_{\vec{a}} \left(\max_{\vec{x}} \langle \vec{a}, \vec{x} \rangle - \min_{\vec{x}} \langle \vec{a}, \vec{x} \rangle \right)$$

を満たすものをとりたい. ($\min_{\vec{a}}$ である必要はないが、小さい方がよい)

p:素数.

$r \in QR_p^+$

$r_1, \dots, r_n \in \mathbb{F}_p$ (s.t.) $\sum r_i = 0 \pmod p$

$\mathrm{Enc}_i(x_i, (r, r_1, \dots, r_n)) = r_i + r \cdot x_i a_i \pmod p$ if $i \neq 1$

$\mathrm{Enc}_1(x_1, (r, r_1, \dots, r_n)) = r_1 + r(a_1 x_1 + \underset{\text{shift量}}{a_0}) \pmod p$

$\mathrm{Dec}(m_1, m_2, \dots, m_n)$ $\sum m_i = r(\langle \vec{a}, \vec{x} \rangle + a_0)$

$$= \begin{cases} 0 & \text{otherwise} \\ 1 & \text{if } \left(\frac{\sum m_i}{p}\right) = 1 \end{cases}$$