秘密分散方式

廣瀬勝一

内容

- しきい値法 (threshold scheme)
- 検証可能な秘密分散方式 (verifiable secret sharing (VSS) scheme)
- 一般の秘密分散方式
- しきい値暗号 (threshold cryptography)

(t, n) しきい値法

n 人の利用者の内の任意の t 人が秘密を復元できる.
t 人未満の利用者が結託しても秘密に関するいかなる情報も得られない.

1979 年に Blakley と Shamir が独立に提案した

- Blakley の方式はベクトル空間に基づく
- Shamir の方式は多項式補間に基づく

準備

n 人の利用者を $U_1, U_2, \ldots, U_n$ とする
p は素数で，$n < p$
秘密 s は $\mathbb{Z}_p$ の要素

各 U_i には $d_i \in \mathbb{Z}_p$ が割り当てられる．なお，$i \neq j$ のとき $d_i \neq d_j$
例えば，U_i の ID を d_i として利用できる．

p と $d_1, \ldots, d_n$ は公開

ディーラー $D \notin \{U_1, U_2, \ldots, U_n\}$ の存在を仮定する
D は秘密情報 s から部分情報 (share) s_i を計算し，U_i に配る

簡単な例

$(1, n)$ しきい値法

1. ディーラー D は，各 $1 \leq i \leq n$ について，$s_i = s$ とする
2. D は安全な通信路を介して s_i を U_i に送る

(n, n) しきい値法

1. D は，各 $1 \leq i \leq n-1$ について，s_i を無作為に選ぶ
2. $s_n = s - (s_1 + \cdots + s_{n-1}) \bmod p$
3. D は安全な通信路を介して s_i を U_i に送る

注意

- 「安全な通信路」は盗聴，改ざんのない通信路を意味する
- これらの方式では d_i は不要

Shamir の (t, n) しきい値法

1. D は，各 $1 \leq j \leq t-1$ について，秘密かつ無作為に $a_j \in \mathbb{Z}_p$ を選び，多項式 $f(x)$ を以下のように定める

$$f(x) = s + a_1\, x + a_2\, x^2 + \cdots + a_{t-1}\, x^{t-1} \bmod p$$

   このとき，秘密 s について，$s = f(0)$ である
2. D は安全な通信路を介して $s_i = f(d_i)$ を U_i に送る

任意の t 人の利用者 $U_{i_1}, U_{i_2}, \ldots, U_{i_t}$ は以下の式で s を復元できる

$$s = \sum_{k=1}^{t} s_{i_k} \prod_{1 \leq \ell \leq t, \ell \neq k} \frac{d_{i_\ell}}{d_{i_\ell} - d_{i_k}} \bmod p$$

検証可能な秘密分散法

各利用者は，自分の部分情報が正しいことを確認できる

- Feldman 1987
- Pedersen 1991

離散対数問題に基づく方式

Feldman の VSS (1/2)

p, q は素数で $q \,|\, p-1$ を満たす．g を $\mathbb{Z}_p^*$ の位数 q の元とする．

1. D は，各 $1 \leq j \leq t-1$ について，秘密かつ無作為に $a_j \in \mathbb{Z}_q$ を選び，多項式 $f(x)$ を以下のように定める

$$f(x) = s + a_1\, x + a_2\, x^2 + \cdots + a_{t-1}\, x^{t-1} \bmod q$$

2. D は，各 $0 \leq j \leq t-1$ について，$G_j = g^{a_j} \bmod p$ を計算して公開する．ここで，$a_0 = s$ である
3. D は安全な通信路を介して $s_i = f(d_i)$ を U_i に送る

Feldman の VSS (2/2)

U_i は以下の合同式を確認することにより，自分の部分情報が正しいかどうかを確認できる

$$
\begin{aligned}
g^{s_i} &\equiv g^{f(d_i)} \\
&\equiv g^{s+a_1 d_i + a_2 {d_i}^2 + \cdots + a_{t-1} {d_i}^{t-1}} \\
&\equiv g^s g^{a_1 d_i} g^{a_2 {d_i}^2} \cdots g^{a_{t-1} {d_i}^{t-1}} \\
&\equiv G_0 {G_1}^{d_i} {G_2}^{{d_i}^2} \cdots {G_{t-1}}^{{d_i}^{t-1}} \\
&\equiv ((\cdots((({G_{t-1}}^{d_i}) G_{t-2})^{d_i} \cdots) G_1)^{d_i} G_0 \pmod{p}
\end{aligned}
$$

この方式では，$G_0 = g^s$ が公開されるので，離散対数問題が解けないという仮定の下でのみ，s は安全

Pedersen の VSS (1/2)

p, q は素数で $q \,|\, p-1$ を満たす．g, h を $\mathbb{Z}_p^*$ の位数 q の元とする．

1. D は，各 $0 \le j \le t-1$ について，秘密かつ無作為に $a_j, b_j \in \mathbb{Z}_q$ を選び，多項式 $f_1(x)$, $f_2(x)$ を以下のように定める．ただし，$a_0 = s$ である．

$$f_1(x) = s + a_1\, x + a_2\, x^2 + \cdots + a_{t-1}\, x^{t-1} \bmod q$$
$$f_2(x) = b_0 + b_1\, x + b_2\, x^2 + \cdots + b_{t-1}\, x^{t-1} \bmod q$$

2. D は，各 $0 \le j \le t-1$ について，$G_j = g^{a_j} h^{b_j} \bmod p$ を計算して公開する．
3. D は安全な通信路を介して $s_i = f_1(d_i)$, $r_i = f_2(d_i)$ を U_i に送る

Pedersen の VSS (2/2)

U_i は以下の合同式を確認することにより，自分の部分情報が正しいかどうかを確認できる

$$
\begin{aligned}
g^{s_i} h^{r_i} &\equiv g^{f_1(d_i)} h^{f_2(d_i)} \\
&\equiv g^{a_0 + a_1 d_i + a_2 {d_i}^2 + \cdots + a_{t-1} {d_i}^{t-1}} h^{b_0 + b_1 d_i + b_2 {d_i}^2 + \cdots + b_{t-1} {d_i}^{t-1}} \\
&\equiv (g^{a_0} h^{b_0})(g^{a_1 d_i} h^{b_1 d_i})(g^{a_2 {d_i}^2} h^{b_2 {d_i}^2}) \cdots (g^{a_{t-1} {d_i}^{t-1}} h^{b_{t-1} {d_i}^{t-1}}) \\
&\equiv (g^{a_0} h^{b_0})(g^{a_1} h^{b_1})^{d_i} (g^{a_2} h^{b_2})^{{d_i}^2} \cdots (g^{a_{t-1}} h^{b_{t-1}})^{{d_i}^{t-1}} \\
&\equiv G_0 {G_1}^{d_i} {G_2}^{{d_i}^2} \cdots {G_{t-1}}^{{d_i}^{t-1}} \\
&\equiv ((\cdots((({G_{t-1}}^{d_i}) G_{t-2})^{d_i} \cdots) G_1)^{d_i} G_0 \pmod{p}
\end{aligned}
$$

$G_0 = g^s h^{b_0}$ が公開されるが，s に関する情報は全く漏れない

一般の秘密分散法 (1/4)

$\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ を利用者の集合とする

定義（アクセス構造）秘密を復元できる $\mathcal{U}$ の部分集合の集合

例　(t, n) しきい値法のアクセス構造は，$\Gamma = \{\mathcal{P} \,|\, \mathcal{P} \subseteq \mathcal{U} \wedge |\mathcal{P}| \geq t\}$

$n = 4$, $t = 2$ のとき

$$\Gamma = \left\{ \begin{array}{l} \{U_1, U_2\}, \{U_1, U_3\}, \{U_1, U_4\}, \{U_2, U_3\}, \{U_2, U_4\}, \{U_3, U_4\}, \\ \{U_1, U_2, U_3\}, \{U_1, U_2, U_4\}, \{U_1, U_3, U_4\}, \{U_2, U_3, U_4\}, \\ \{U_1, U_2, U_3, U_4\} \end{array} \right\}$$

任意のアクセス構造 Γ は単調である，すなわち

$$\mathcal{P} \subseteq \mathcal{P}' \wedge \mathcal{P} \in \Gamma \Rightarrow \mathcal{P}' \in \Gamma$$

一般の秘密分散法 (2/4)

任意のアクセス構造 Γ はブール関数で表現できる

$$\alpha_\Gamma : \{0,1\}^n \to \{0,1\}$$

$\mathcal{P} \subseteq \{U_1, U_2, \ldots, U_n\}$ について，$z^{\mathcal{P}} \in \{0,1\}^n$ を以下のように定める

$$z_i^{\mathcal{P}} = \begin{cases} 1 & U_i \in \mathcal{P} \text{ のとき} \\ 0 & U_i \notin \mathcal{P} \text{ のとき} \end{cases}$$

α_Γ は以下のように定義される

$$\alpha_\Gamma(z^{\mathcal{P}}) = 1 \Leftrightarrow \mathcal{P} \in \Gamma$$

一般の秘密分散法 (3/4)：アクセス構造を表すブール関数の例

$\mathcal{U} = \{U_1, U_2, U_3, U_4\}$ とする

- $\Gamma_1 = \{\{U_1, U_2\}, \{U_1, U_3, U_4\}, \{U_2, U_3, U_4\}\}$ とすると

$$\alpha_{\Gamma_1}(z_1, z_2, z_3, z_4) = z_1 z_2 \vee z_1 z_3 z_4 \vee z_2 z_3 z_4 = z_1 z_2 \vee (z_1 \vee z_2) z_3 z_4$$

- Γ_2 を $(2, 4)$ しきい値法のアクセス構造とすると

$$\begin{aligned}\alpha_{\Gamma_2}(z_1, z_2, z_3, z_4) = {} & z_1 z_2 \vee z_1 z_3 \vee z_1 z_4 \vee z_2 z_3 \vee z_2 z_4 \vee z_3 z_4 \\ & \vee z_1 z_2 z_3 \vee z_1 z_2 z_4 \vee z_1 z_3 z_4 \vee z_2 z_3 z_4 \\ & \vee z_1 z_2 z_3 z_4 \\ = {} & z_1 z_2 \vee z_1 z_3 \vee z_1 z_4 \vee z_2 z_3 \vee z_2 z_4 \vee z_3 z_4\end{aligned}$$

一般の秘密分散法 (4/4)

任意のアクセス構造 Γ について $\alpha_\Gamma : \{0,1\}^n \to \{0,1\}$ は単調

定義（半順序関係）$z = (z_1, z_2, \ldots, z_n) \in \{0,1\}^n$ とする．

$$\text{各 } 1 \le i \le n \text{ について，} \ z_i = 1 \Rightarrow z'_i = 1$$

のとき $z \preceq z'$ と表記する．

定義（単調ブール関数）ブール関数 $\alpha : \{0,1\}^n \to \{0,1\}$ について

$$z \preceq z' \Rightarrow \alpha(z) \le \alpha(z')$$

のとき，α は単調．

すべての単調ブール関数は AND 素子と OR 素子のみで計算できる

しきい値暗号

Desmedt 1987

- 利用者は秘密分散法で秘密鍵を共有している
- 秘密鍵を復元することなく，復号や署名などを行うことができる

しきい値 Diffie-Hellman 法 (1/3)

p, q は素数で，g は $\mathbb{Z}_p^*$ の位数 q の元であるとする

	秘密鍵	公開鍵
Alice	$s_{\mathrm{A}} \in \mathbb{Z}_q$	$v_{\mathrm{A}} = g^{s_{\mathrm{A}}} \bmod p$
Bob	$s_{\mathrm{B}} \in \mathbb{Z}_q$	$v_{\mathrm{B}} = g^{s_{\mathrm{B}}} \bmod p$

Diffie-Hellman 法で Alice と Bob が得る鍵は

$$K = g^{s_{\mathrm{A}} s_{\mathrm{B}}} \bmod p = {v_{\mathrm{B}}}^{s_{\mathrm{A}}} \bmod p$$

今，s_{A} が Shamir の (t, n) しきい値法で共有されているとする

$$f(x) = s_{\mathrm{A}} + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \bmod q$$

さらに，$i = 1, 2, \ldots, n$ について，$s_i = f(d_i)$

しきい値 Diffie-Hellman 法 (2/3)

任意の t 個の部分情報 $s_{i_1}, s_{i_2}, \ldots, s_{i_t}$ について

$$s_{\mathrm{A}} = \sum_{k=1}^{t} s_{i_k} \prod_{1 \le \ell \le t, \ell \neq k} \frac{d_{i_\ell}}{d_{i_\ell} - d_{i_k}} \bmod q = \sum_{k=1}^{t} c_k \, s_{i_k} \bmod q$$

ここで

$$c_k = \prod_{1 \le \ell \le t, \ell \neq k} \frac{d_{i_\ell}}{d_{i_\ell} - d_{i_k}} \bmod q$$

したがって

$$K = {v_{\mathrm{B}}}^{s_{\mathrm{A}}} \bmod p = {v_{\mathrm{B}}}^{\sum_{k=1}^{t} c_k s_{i_k}} \bmod p = \prod_{k=1}^{t} {v_{\mathrm{B}}}^{c_k \, s_{i_k}} \bmod p$$

U_{i_k} のみが ${v_{\mathrm{B}}}^{c_k s_{i_k}} \bmod p$ を計算できる

しきい値 Diffie-Hellman 法 (3/3)

アルゴリズム

1. 各 U_{i_k} は $K_k = {v_{\mathrm{B}}}^{c_k\, s_{i_k}} \bmod p$ を計算して他の利用者に配布する
2. 各 U_{i_k} は $K = \prod_{k=1}^{t} K_k \bmod p$ を計算する

安全性

- s_{A} は復元されない
- $K_k = {v_{\mathrm{B}}}^{c_k\, s_{i_k}} \bmod p$ から s_{i_k} を得るのは困難（離散対数問題）

演習問題

1. $t = 2$ をしきい値とする Shamir 秘密分散の部分情報を持ち寄ったところ，$(1, 2), (2, 0), (3, 2)$ であった．秘密を復元せよ．なお，法は $q = 11$ である．