鍵共有法

廣瀬勝一

話題

鍵事前配布法 (key pre-distribution scheme)

- Blom 法
- Diffie-Hellman 法

オンライン鍵共有法 (on-line key establishment protocol)

- Diffie-Hellman プロトコル
- 認証付 Diffie-Hellman プロトコル

Blom の鍵事前配布法

Blom, 1985 年

信頼できるセンタ (TA) の存在を仮定する

k 人以下の利用者の結託に対して無条件に安全

利用者を $U_1, U_2, \ldots, U_n$ とする

- p は素数で $n \leq p$
- 配布される鍵は $\mathbb{Z}_p$ の要素
- 各利用者 U_i は $r_i \in \mathbb{Z}_p$ を割り当てられる.

  $i \neq j$ のとき $r_i \neq r_j$. U_i の ID を r_i として利用できる.
- p と $r_1, \ldots, r_n$ は公開される.

Blom の鍵事前配布法

TA によるセットアップ

1. $0 \leq i \leq k$, $0 \leq j \leq k$ について $a_{i,j} \in \mathbb{Z}_p$ を無作為に選ぶ.
   - すべての i, j について $a_{i,j} = a_{j,i}$ を満たすように選ぶ.
   - $a_{i,j}$ は TA のみが知る秘密情報

   多項式 $f(x, y)$ を以下のように定める.

$$f(x, y) = \sum_{i=0}^{k} \sum_{j=0}^{k} a_{i,j}\, x^i y^j \bmod p$$

2. 多項式 $f_{U_s}(x) = f(x, r_s) \bmod p$ を計算し，安全な通信路を用いて U_s に送る.

Blom の鍵事前配布法

鍵共有

U_s は U_t との間の秘密鍵 $K_{s,t}$ を以下のように計算する．

$$K_{s,t} = f_{U_s}(r_t) \bmod p$$

ここで

$$K_{s,t} = f_{U_s}(r_t) \bmod p = f(r_t, r_s) \bmod p$$

である．一方，U_t が計算する U_s との間の秘密鍵 $K_{t,s}$ は

$$K_{t,s} = f_{U_t}(r_s) \bmod p = f(r_s, r_t) \bmod p$$

である．次に述べるとおり $K_{s,t} = K_{t,s}$ である．

Blom の鍵事前配布法

$$
\begin{aligned}
f(x,y) &= \sum_{i=0}^{k}\sum_{j=0}^{k} a_{i,j}\, x^i y^j \\
&= \sum_{i=0}^{k}\sum_{j=0}^{k} a_{j,i}\, y^j x^i \qquad (a_{i,j} = a_{j,i} \text{より}) \\
&= \sum_{v=0}^{k}\sum_{u=0}^{k} a_{u,v}\, y^u x^v \qquad ((i,j) \to (v,u)) \\
&= \sum_{u=0}^{k}\sum_{v=0}^{k} a_{u,v}\, y^u x^v \qquad (\text{加算の順序を変更}) \\
&= f(y,x)
\end{aligned}
$$

例（$k = 1$ のとき）

TA は $a_{0,0}, a_{0,1}, a_{1,0}, a_{1,1} \in \mathbb{Z}_p$ を無作為に選ぶ．ただし $a_{0,1} = a_{1,0}$.

- 簡単のため $a_0 = a_{0,0}, a_1 = a_{0,1} = a_{1,0}, a_2 = a_{1,1}$ と書く．
- a_0, a_1, a_2 は TA のみが知る秘密情報.

$$f(x, y) = a_0 + a_1(x + y) + a_2\, x\, y \bmod p$$

U_s は TA から以下の多項式を受け取る．

$$f_{U_s}(x) = (a_0 + a_1\, r_s) + (a_1 + a_2\, r_s)\, x \bmod p$$

U_s と U_t の共有する秘密鍵は

$$\begin{aligned} K_{s,t} &= f_{U_s}(r_t) \bmod p = f_{U_t}(r_s) \bmod p \\ &= a_0 + a_1(r_s + r_t) + a_2\, r_s\, r_t \bmod p \end{aligned}$$

例（$k = 1$ のときの方式の安全性）

単一の第三者 U_u は，秘密鍵 $K_{s,t}$ の情報を一切得ることが出来ない．

$$K_{s,t} = a_0 + a_1(r_s + r_t) + a_2\, r_s\, r_t$$

$$f_{U_u}(x) = (a_0 + a_1\, r_u) + (a_1 + a_2\, r_u)\, x \stackrel{\text{def}}{=} c_{u,0} + c_{u,1}x$$

このとき

$$\begin{pmatrix} K_{s,t} \\ c_{u,0} \\ c_{u,1} \end{pmatrix} = \begin{pmatrix} 1 & r_s + r_t & r_s\, r_t \\ 1 & r_u & 0 \\ 0 & 1 & r_u \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} \stackrel{\text{def}}{=} M \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$$

$r_u \neq r_s, r_t$ なので，$\det(M) = (r_u - r_s)(r_u - r_t) \neq 0$
したがって，(a_0, a_1, a_2) と $K_{s,t}$ とは 1 対 1 対応

例（$k = 1$ のときの方式の結託に対する非安全性）

U_s と U_t が結託して互いの秘密情報を教えあったと仮定すると

$$f_{U_s}(x) = (a_0 + a_1\, r_s) + (a_1 + a_2\, r_s)\, x \stackrel{\text{def}}{=} c_{s,0} + c_{s,1}\, x$$
$$f_{U_t}(x) = (a_0 + a_1\, r_t) + (a_1 + a_2\, r_t)\, x \stackrel{\text{def}}{=} c_{t,0} + c_{t,1}\, x$$

したがって，U_s と U_t は，

$$a_0 + a_1\, r_s = c_{s,0} \qquad a_1 + a_2\, r_s = c_{s,1}$$
$$a_0 + a_1\, r_t = c_{t,0} \qquad a_1 + a_2\, r_t = c_{t,1}$$

により a_0, a_1, a_2 を計算できる．

Diffie-Hellman 鍵事前配布法

Diffie & Hellman, 1976 年

盗聴のある安全でない通信路を介して秘密鍵を共有する方式

- Diffie-Hellman 問題を解くことが現実的に不可能であれば安全
- 信頼できるセンタを必要としない

Diffie-Hellman 問題 (DHP)
p は素数
g は乗法群 $\mathbb{Z}_p^*$ の位数 q の元

$\alpha = g^x \bmod p$. ただし $x \in \mathbb{Z}_q$
$\beta = g^y \bmod p$. ただし $y \in \mathbb{Z}_q$

DHP
入力　p, q, g, α, β
出力　$g^{x\,y} \bmod p$

仮定　x, y が無作為に選択されるならば DHP を解くことは困難

Diffie-Hellman 鍵事前配布法

p は素数
g は乗法群 $\mathbb{Z}_p^*$ の位数 q の元

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

Alice と Bob とが共有する秘密鍵

$$\begin{aligned} K = g^{s_{\mathrm{A}} s_{\mathrm{B}}} \bmod p &= {v_{\mathrm{B}}}^{s_{\mathrm{A}}} \bmod p \\ &= {v_{\mathrm{A}}}^{s_{\mathrm{B}}} \bmod p \end{aligned}$$

オンライン Diffie-Hellman プロトコル

p は素数
g は乗法群 $\mathbb{Z}_p^*$ の位数 q の元

Alice		Bob
$r_{\mathrm{A}} \in \mathbb{Z}_q$		$r_{\mathrm{B}} \in \mathbb{Z}_q$
$u_{\mathrm{A}} = g^{r_{\mathrm{A}}} \bmod p$	$\xrightarrow{u_{\mathrm{A}}}$	$u_{\mathrm{B}} = g^{r_{\mathrm{B}}} \bmod p$
	$\xleftarrow{u_{\mathrm{B}}}$	

Alice と Bob とが共有する秘密鍵（セッション鍵と呼ばれる）

$$K = g^{r_{\mathrm{A}} r_{\mathrm{B}}} \bmod p = {u_{\mathrm{B}}}^{r_{\mathrm{A}}} \bmod p$$
$$= {u_{\mathrm{A}}}^{r_{\mathrm{B}}} \bmod p$$

オンライン Diffie-Hellman プロトコルの安全性

DHP が解けなければ，オンライン DH プロトコルは受動的な攻撃者に対して安全である．
しかし，能動的な攻撃者に対しては安全ではない．

受動的な攻撃者はやり取りされるメッセージの盗聴のみを行う．
能動的な攻撃者はメッセージの改竄なども行う．

オンライン DH プロトコルへの man-in-the-middle 攻撃

Eve を能動的な攻撃者とする．
Eve は以下のようにして，Alice，Bob のそれぞれとセッション鍵を共有できる．

Alice		Eve		Bob
$r_{\mathrm{A}} \in \mathbb{Z}_q$		$r_{\mathrm{E}} \in \mathbb{Z}_q$		$r_{\mathrm{B}} \in \mathbb{Z}_q$
$u_{\mathrm{A}} = g^{r_{\mathrm{A}}} \bmod p$	$\xrightarrow{u_{\mathrm{A}}}$	$u_{\mathrm{E}} = g^{r_{\mathrm{E}}} \bmod p$	$\xrightarrow{u_{\mathrm{E}}}$	$u_{\mathrm{B}} = g^{r_{\mathrm{B}}} \bmod p$
	$\xleftarrow{u_{\mathrm{E}}}$		$\xleftarrow{u_{\mathrm{B}}}$	

$$K_{\mathrm{AE}} = g^{r_{\mathrm{A}} r_{\mathrm{E}}} \bmod p$$
$$K_{\mathrm{BE}} = g^{r_{\mathrm{B}} r_{\mathrm{E}}} \bmod p$$

認証つき DH プロトコル

Alice		Bob
$r_{\mathrm{A}} \in \mathbb{Z}_q$		$r_{\mathrm{B}} \in \mathbb{Z}_q$
$u_{\mathrm{A}} = g^{r_{\mathrm{A}}} \bmod p$	$\xrightarrow{ID_{\mathrm{A}}, s, u_{\mathrm{A}}}$	$u_{\mathrm{B}} = g^{r_{\mathrm{B}}} \bmod p$
	$\xleftarrow{ID_{\mathrm{B}}, s, u_{\mathrm{B}}, \beta}$	$\beta = \mathsf{Sign}_{\mathrm{B}}(ID_{\mathrm{B}}, ID_{\mathrm{A}}, s, u_{\mathrm{B}}, u_{\mathrm{A}})$
$\mathsf{Ver}_{\mathrm{B}}(\beta, (ID_{\mathrm{B}}, ID_{\mathrm{A}}, s, u_{\mathrm{B}}, u_{\mathrm{A}})) = \mathtt{true}?$		
$\alpha = \mathsf{Sign}_{\mathrm{A}}(ID_{\mathrm{A}}, ID_{\mathrm{B}}, s, u_{\mathrm{A}}, u_{\mathrm{B}})$	$\xrightarrow{ID_{\mathrm{A}}, s, \alpha}$	
		$\mathsf{Ver}_{\mathrm{A}}(\alpha, (ID_{\mathrm{A}}, ID_{\mathrm{B}}, s, u_{\mathrm{A}}, u_{\mathrm{B}})) = \mathtt{true}?$

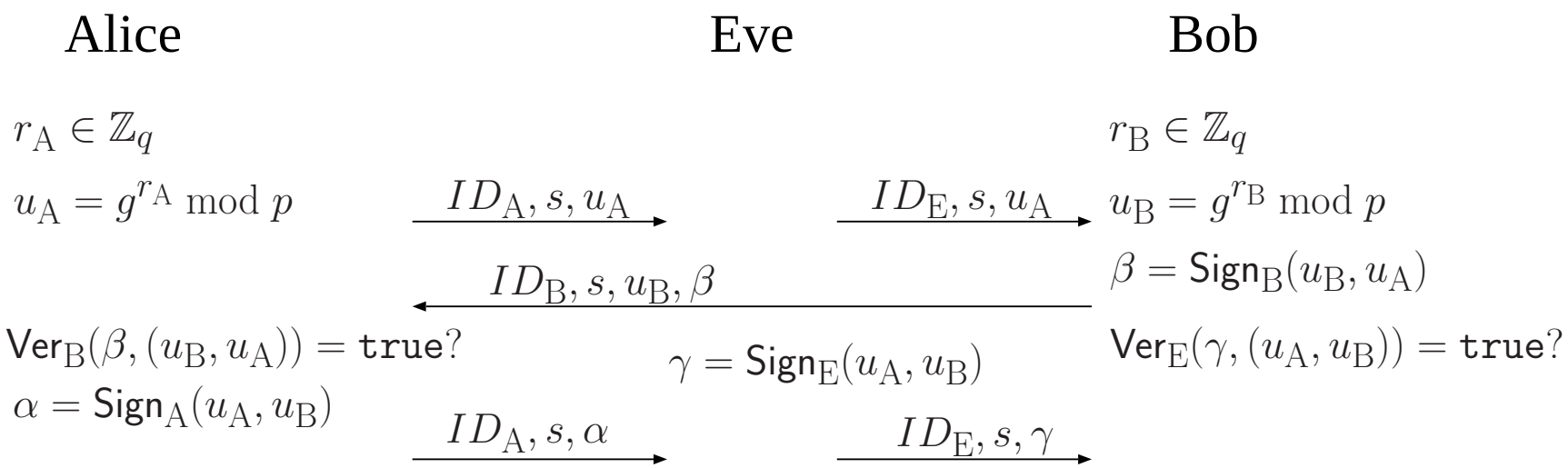
- $ID_{\mathrm{A}}, ID_{\mathrm{B}}$ はそれぞれ Alice, Bob の ID を表す.
- s はセッション ID である.

似ているが安全でないプロトコル

Alice		Bob
$r_{\mathrm{A}} \in \mathbb{Z}_q$		$r_{\mathrm{B}} \in \mathbb{Z}_q$
$u_{\mathrm{A}} = g^{r_{\mathrm{A}}} \bmod p$	$\xrightarrow{ID_{\mathrm{A}}, s, u_{\mathrm{A}}}$	$u_{\mathrm{B}} = g^{r_{\mathrm{B}}} \bmod p$
	$\xleftarrow{ID_{\mathrm{B}}, s, u_{\mathrm{B}}, \beta}$	$\beta = \mathsf{Sign}_{\mathrm{B}}(u_{\mathrm{B}}, u_{\mathrm{A}})$
$\mathsf{Ver}_{\mathrm{B}}(\beta, (u_{\mathrm{B}}, u_{\mathrm{A}})) = \mathtt{true}?$		
$\alpha = \mathsf{Sign}_{\mathrm{A}}(u_{\mathrm{A}}, u_{\mathrm{B}})$	$\xrightarrow{ID_{\mathrm{A}}, s, \alpha}$	
		$\mathsf{Ver}_{\mathrm{A}}(\alpha, (u_{\mathrm{A}}, u_{\mathrm{B}})) = \mathtt{true}?$

異なる点
署名されるメッセージに ID が含まれていない.

攻撃



- Alice と Bob のみがセッション鍵 $K_{\mathrm{AB}} = g^{r_{\mathrm{A}} r_{\mathrm{B}}} \bmod p$ を知っている.
- Alice は Bob と K_{AB} を共有したと信じている.
- Bob は Eve と K_{AB} を共有したと信じている.

演習問題

1. $k = 2$ の場合の Blom 方式を示し，任意の二人の利用者が秘密鍵を共有できることを確認せよ.
2. Diffie-Hellman 問題を利用して，3 人以上の利用者がセッション鍵を共有する方法を考えよ.