個人識別方式

廣瀬勝一

はじめに

太郎はどのようにして太郎自身であることを証明すればよいか？
「私は太郎しか知らない秘密の情報を知っているので太郎本人です.」

秘密情報を知っていることを開示することなく証明したい

質問応答型 (challenge-and-response) プロトコル

以下の技術を利用する

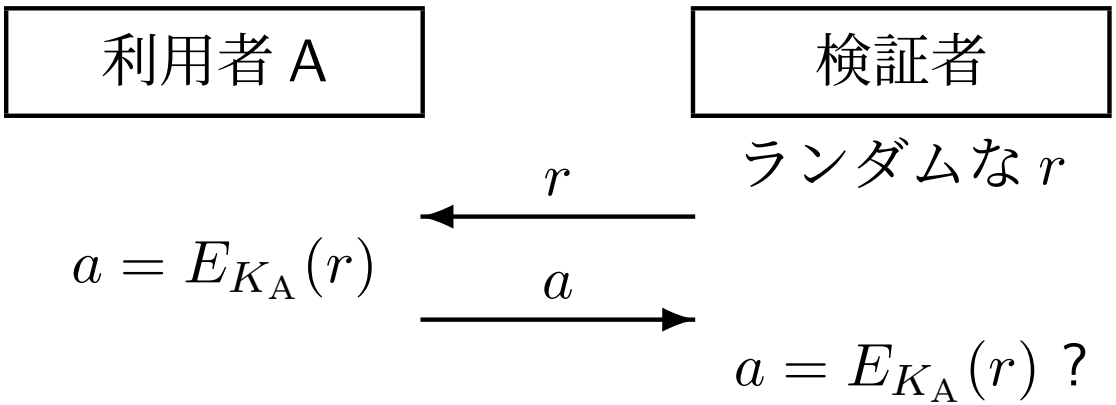
- 共通鍵暗号（ブロック暗号）
- ディジタル署名
- ゼロ知識対話証明 (zero-knowledge interactive proof)
  - Fiat-Shamir 方式
  - Schnorr 方式
  - ...

共通鍵暗号を用いた方式

秘密鍵を知る者のみが暗号化できるという性質を利用

E　暗号化手続き
K_{A}　利用者 A の秘密鍵

認証方式



利　点　盗聴に対して安全
問題点　検証者側での秘密鍵の管理が必要

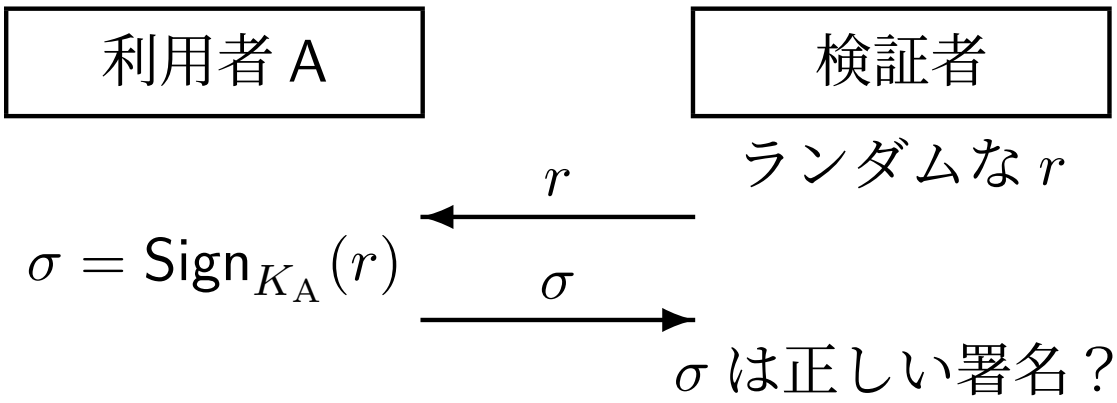
注意　不正なサーバは選択平文（暗号文）攻撃を実行可能

ディジタル署名を用いた方式

秘密鍵を知る者のみが署名でき，誰もが署名を検証できる．

Sign　ディジタル署名の手続き
K_{A}　利用者 A の秘密鍵

認証方式



利点

- 盗聴に対して安全
- 検証者側での秘密鍵の管理が不要

注意　不正なサーバは選択文書攻撃を実行可能

ゼロ知識証明に基づく方式

Schnorr 方式

- 1989 年に提案された
- 離散対数に基づく

Fiat-Shamir 方式

- 1986 年に提案された
- 素因数分解に基づく
- ID に基づく (identity-based) 方式

Schnorr 方式 (1/2)

公開鍵 p, q, g, y

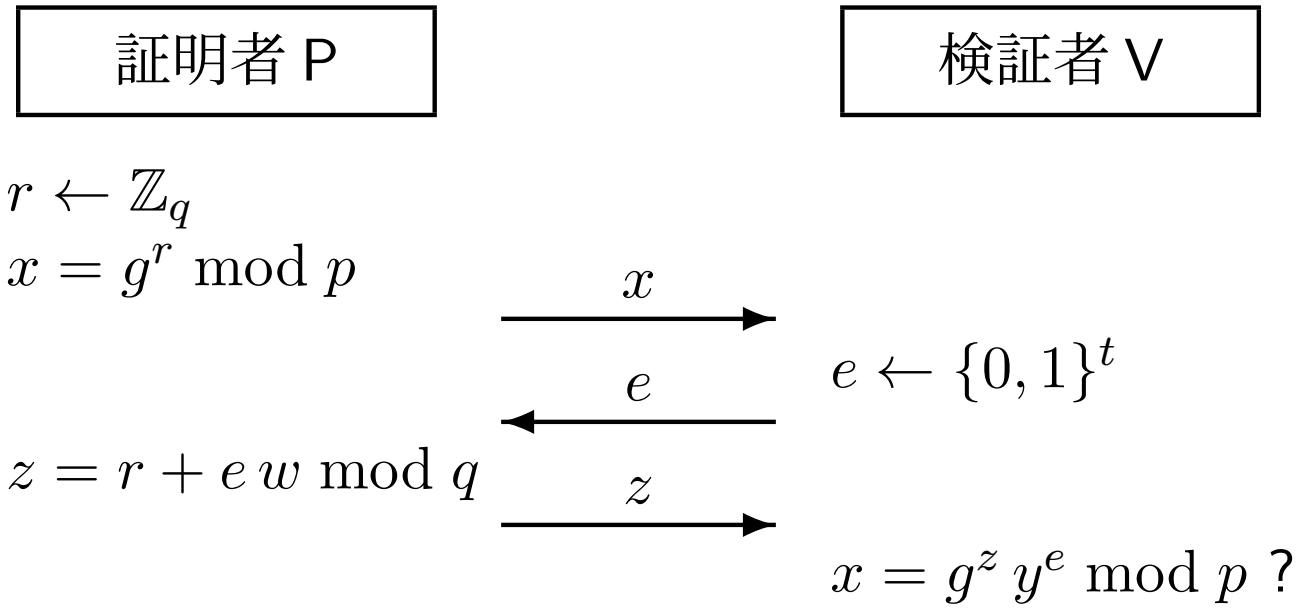
- p, q は素数で，$q \mid p-1$
- g は乗法群 $\mathbb{Z}_p^*$ の位数 q の元．すなわち，$g^q \equiv 1 \pmod{p}$
- $y = g^{-w} \bmod p$

秘密鍵 $w \in \mathbb{Z}_q$

プロトコル 証明者 P と検証者 V の対話

1. P は無作為に $r \in \mathbb{Z}_q$ を選び，$x = g^r \bmod p$ を計算して V に送る．
2. V は x を受け取った後，$e \in \{0,1\}^t$ を無作為に選んで P に送る．
3. P は e を受け取った後，$z = r + e\,w \bmod q$ を計算して V に送る．
4. V は z を受け取った後，$x = g^z\, y^e \bmod p$ が成立するかどうかを検証する．成立する場合は正しい証明者である．

Schnorr 法 (2/2)



注意

- 同じ r を複数回用いてはならない.
- e は無作為に選択されなければならない.

Fiat-Shamir 法 (1/2)

利用者の ID を公開鍵として利用する方式.

この方式では信頼できるセンタの存在を仮定する.

センタは各利用者の ID からその利用者の秘密鍵を生成する.

システムパラメータ $n, k, t; f_1, \ldots, f_k$

- $n = p\,q$. p, q は秘密の素数
- k, t はセキュリティパラメータ
- $f_i : \{0,1\}^* \to \{v \mid \text{ある } s \in \mathbb{Z}_n \text{ について } v = s^2 \bmod n\}$

利用者 P の公開鍵 ID_{P}

利用者 P の秘密鍵 $s_1, \ldots, s_k$

- $s_i = {v_i}^{-\frac{1}{2}} \bmod n$. ここで $v_i = f_i(ID_{\mathrm{P}})$

Fiat-Shamir 法 (2/2)

プロトコル 以下の手続きが t 回繰り返される．

1. 利用者 P は $r \in \mathbb{Z}_n$ を無作為に選び，$x = r^2 \bmod n$ を計算する．P は ID_{P}, x を検証者 V に送る．
2. V は x を受け取った後，$e_1, e_2, \ldots, e_k$ を無作為に選んで P に送る．ここで，$i = 1, \ldots, k$ について $e_i \in \{0, 1\}$．
3. P は $e_1, \ldots, e_k$ を受け取った後，$z = r \prod_{i=1}^{k} {s_i}^{e_i} \bmod n$ を計算して V に送る．
4. V は z を受け取った後，$x = z^2 \prod_{i=1}^{k} {v_i}^{e_i} \bmod n$ が成立するかどうかを検証する．

ゼロ知識対話証明

証明者が検証者と対話して行う証明

完全性

証明者と検証者が共に正直な時，検証者は証明を受理する．

健全性

秘密情報を知らない証明者は，検証者に証明を受理させることができない．

ゼロ知識性

ある情報を知っていることのみ示す．　それ以外の情報は全く漏れない．

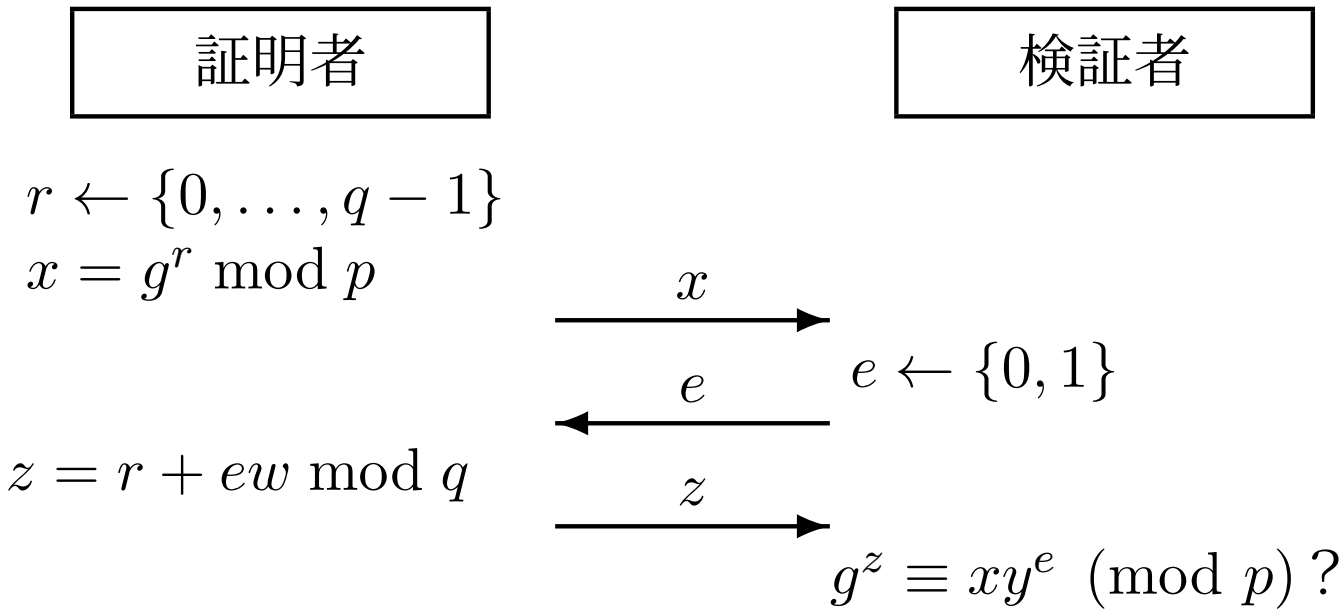
離散対数問題のゼロ知識対話証明

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

$y = g^w \bmod p,\ w \in \{0, \ldots, q-1\}$

w を知っていることのゼロ知識対話証明

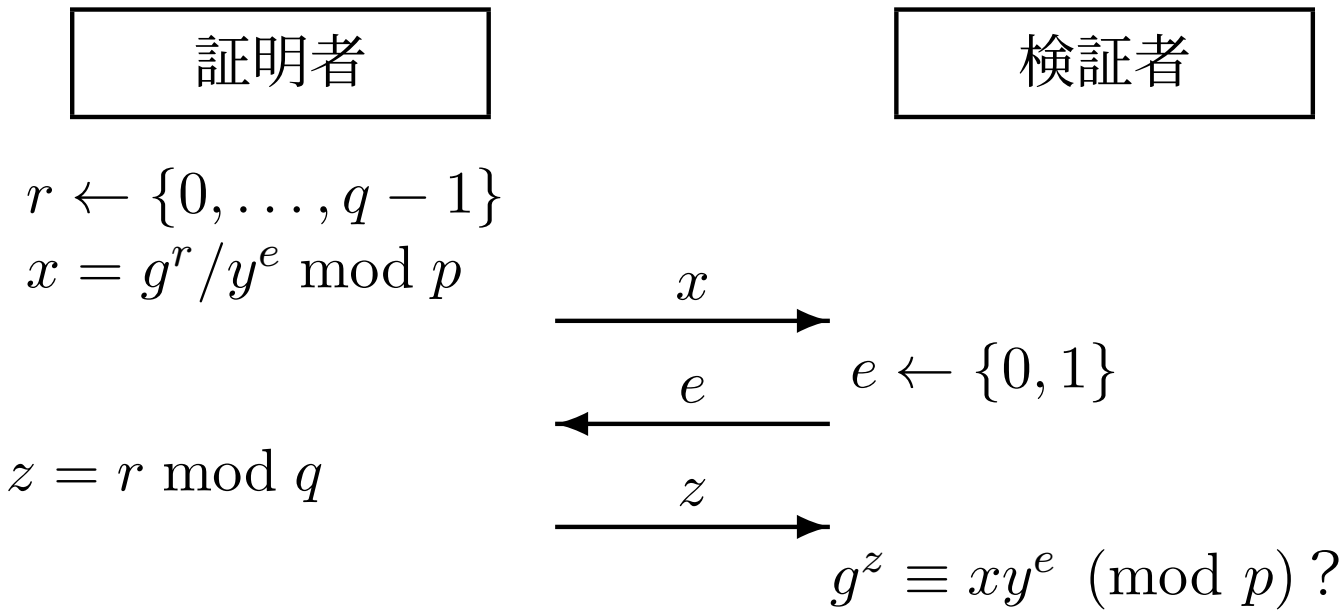
以下の対話を繰り返す



注意　$\leftarrow$ は無作為選択を表す.

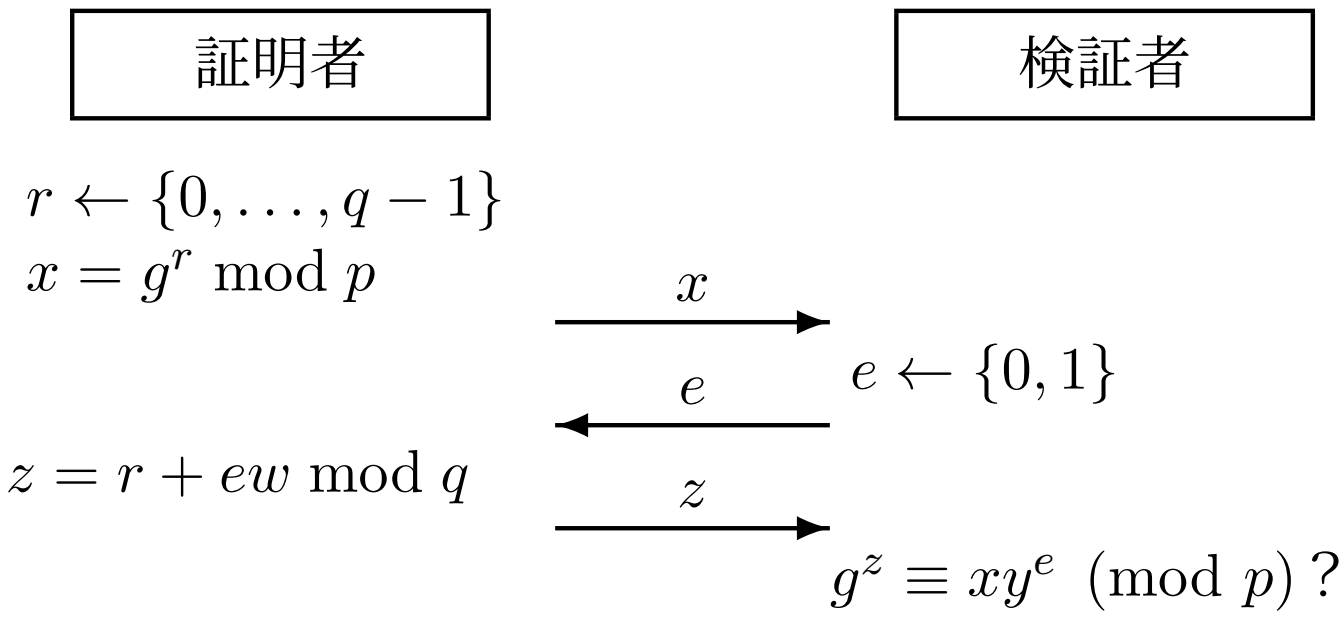
ゼロ知識対話証明の健全性 (1/2)

w を知らない証明者でも，e を正しく予測できれば，以下のようにして，証明に成功できる．



ただし，$\Pr[e \text{ を } k \text{ 回正しく予測}] = 1/2^k$

ゼロ知識対話証明の健全性 (2/2)



証明に成功する確率 $> 1/2^k$ ならば，少なくとも 1 回の対話については，$e = 0, 1$ どちらの質問にも答えられる．

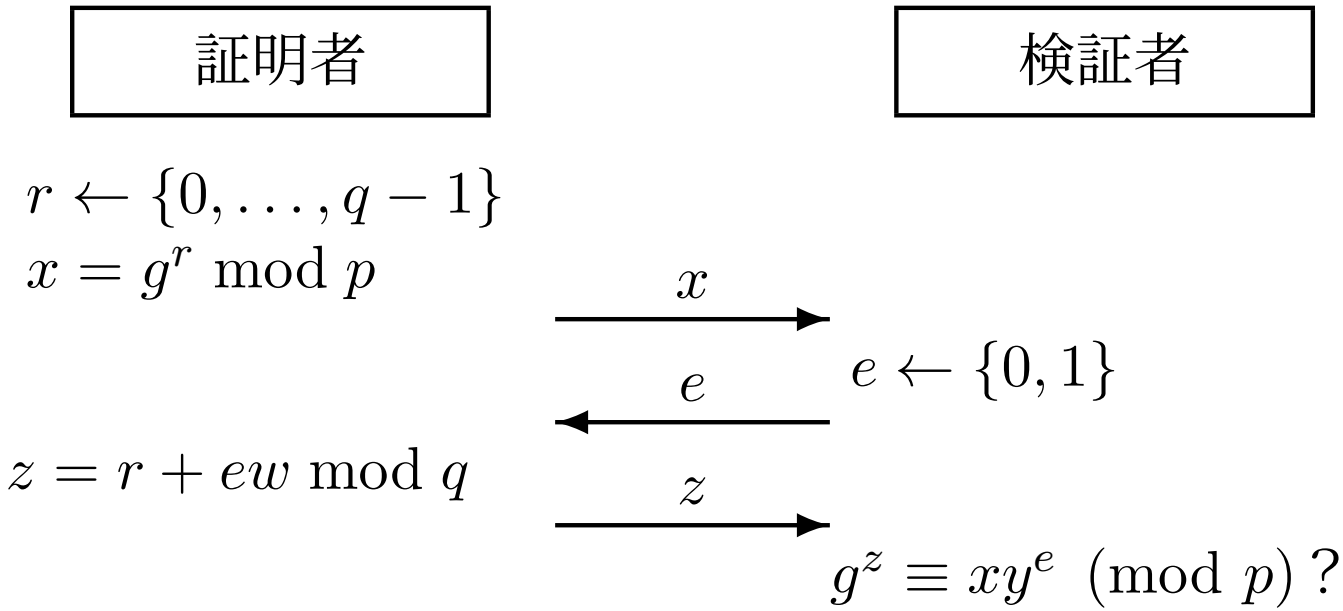
- $e = 0$ のとき，$z_0 = r$
- $e = 1$ のとき，$z_1 = r + w \bmod q$

したがって，両方の質問に答えられるとき

$$z_1 - z_0 \bmod q = w$$

により w が得られる．

ゼロ知識対話証明のゼロ知識性



- $e = 0$ のとき，$z = r$
  w に関する情報は全く伝送されない
- $e = 1$ のとき，$z = r + w \bmod q$
  検証者には r の値がわからないので，w もわからない．

Schnorr 法の安全性の証明

補題 1　$0 \leq \varepsilon \leq 1$ なる任意の ε について,

$$\Pr[\text{P が合格}] \geq \delta \Rightarrow \sum_{\Pr[\text{P が合格} \mid x=\alpha] \geq \varepsilon\delta} \Pr[x = \alpha] \geq (1 - \varepsilon)\delta.$$

定理 1　$\delta \geq 2^{-(t-2)}$ とする．高々T ステップで成功確率 δ のなりすまし者 P が存在するならば，高々$2T + \ell^{O(1)}$ ステップで成功確率 $\delta^3/8$ 以上で P の秘密鍵を計算するアルゴリズムが存在する．ここで ℓ はセキュリティパラメータである．

補題 1 の証明

$$
\begin{aligned}
\Pr[\text{P が合格}] &= \sum_{\alpha} \Pr[x = \alpha \wedge \text{P が合格}] \\
&= \sum_{\alpha} \Pr[x = \alpha] \Pr[\text{P が合格} \mid x = \alpha] \\
&= \sum_{\Pr[\text{P が合格} \mid x=\alpha] < \varepsilon\delta} \Pr[x = \alpha] \Pr[\text{P が合格} \mid x = \alpha] \\
&\quad + \sum_{\Pr[\text{P が合格} \mid x=\alpha] \geq \varepsilon\delta} \Pr[x = \alpha] \Pr[\text{P が合格} \mid x = \alpha] \\
&\leq \varepsilon\,\delta + \sum_{\Pr[\text{P が合格} \mid x=\alpha] \geq \varepsilon\delta} \Pr[x = \alpha]
\end{aligned}
$$

□

演習問題

1. 補題 1 の証明を完成させよ.
2. Schnorr 法でいつも同じ e を使用するとどうなるか.
3. $g, y, g\,y$ を利用して以下の単純な方法よりも効率よく $g^z y^e \bmod p$ を計算する方法を述べよ.

   $c_1 = g^z \bmod p, c_2 = y^e \bmod p$ を計算して $c_1 c_2 \bmod p$ を計算する.