ディジタル署名

廣瀬勝一

ディジタル署名の要件

- 「誰が何に署名したか」を誰もが確認できる.
- 偽造できない.

ディジタル署名方式

鍵生成アルゴリズム Gen（確率アルゴリズム）

$$(pk, sk) \leftarrow \mathsf{Gen}(1^{\ell})$$

ℓ はセキュリティパラメータ
(pk, sk) は公開鍵（検証鍵）と秘密鍵（署名鍵）の組

署名アルゴリズム Sign（決定的または確率アルゴリズム）

$$\sigma \leftarrow \mathsf{Sign}(pk, sk, M)$$

M はメッセージ，σ は M の署名

検証アルゴリズム Verif（決定的アルゴリズム）

$$d \leftarrow \mathsf{Verif}(pk, M, \sigma)$$

$d \in \{\mathtt{true}, \mathtt{false}\}$

RSA 方式

公開鍵 n, e

- $n = p\,q$. ここで p, q は相異なる奇素数
- e は $\gcd(e, \phi(n)) = 1$ を満たす

秘密鍵 d

- $d\,e \equiv 1 \pmod{\phi(n)}$

署名 σ はメッセージ $M \in \mathbb{Z}_n$ の署名である

$$\sigma = M^d \bmod n$$

検証 以下が成立するとき，σ は M の正しい署名である

$$M \equiv \sigma^e \pmod{n}$$

ElGamal 方式

公開鍵 p, g, y

- p は素数
- g は乗法群 $\mathbb{Z}_p^*$ の原始元
- $y = g^x \bmod p$

秘密鍵 $x \in \mathbb{Z}_{p-1}$

署名 (a, b) はメッセージ $M \in \mathbb{Z}_{p-1}$ の署名である

1. $k \in \mathbb{Z}_{p-1}^*$ を無作為に選ぶ．$\gcd(k, p-1) = 1$ が成立する．
2. $a = g^k \bmod p$
3. $b = (M - xa)k^{-1} \bmod p - 1$

検証 以下が成立するとき，(a, b) は M の正しい署名である

$$g^M \equiv y^a a^b \pmod{p}$$

ElGamal 方式の誤用 (1/2)

複数のメッセージの署名に同一の k を使用しない

k を二つのメッセージ M_1, M_2 の署名に用いたとする.

$$M_1 \text{ の署名 } (a, b_1) \qquad M_2 \text{ の署名 } (a, b_2)$$

このとき，署名アルゴリズムより

$$\begin{cases} M_1 = a\,x + k\,b_1 \bmod p-1 \\ M_2 = a\,x + k\,b_2 \bmod p-1 \end{cases}$$

$$M_1 - M_2 \equiv k(b_1 - b_2) \pmod{p-1}$$

$\gcd(b_1 - b_2, p-1) = 1$ のときは,

$$k = (M_1 - M_2)(b_1 - b_2)^{-1} \bmod p-1$$

ElGamal 方式の誤用 (2/2)

$$M_1 - M_2 \equiv k(b_1 - b_2) \pmod{p-1}$$

について，$\gcd(b_1 - b_2, p-1) = d \neq 1$ のとき

$$\tilde{M} = \frac{M_1 - M_2}{d},\ \tilde{b} = \frac{b_1 - b_2}{d},\ \tilde{p} = \frac{p-1}{d}$$

とすると

$$\tilde{M} \equiv k\,\tilde{b} \pmod{\tilde{p}}$$

$\tilde{k} = \tilde{M}\,\tilde{b}^{-1} \bmod \tilde{p}$ とすると，ある $i \in \mathbb{Z}_d$ について $k = i\,\tilde{p} + \tilde{k}$.
k の正しい値は $a = g^k \bmod p$ が成立するかどうかで確認できる.

k の値が分かれば，$\gcd(a, p-1) = 1$ のとき

$$x = (M_1 - k\,b_1)a^{-1} \bmod p - 1$$

$\gcd(a, p-1) \neq 1$ のときも，上記と同様にして x が計算できる.

Digital Signature Algorithm (DSA)

- ElGamal 方式の改良版
- 1991 年 8 月に（米国）標準技術局 (NIST: National Institute of Standards and Technology) によって提案された.
- 1994 年に米国情報処理規格 (FIPS: Federal Information Processing Standard) に制定された (FIPS 186). Digital Signature Standard (DSS) と呼ばれている.
  - FIPS 186-2 (2000 年 6 月)
  - FIPS 186-3 (2009 年 6 月)

Digital Signature Algorithm (DSA)

公開鍵 p, q, g, y

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

秘密鍵 $x \in \mathbb{Z}_q$

署名 (a, b) はメッセージ $M \in \mathbb{Z}_q$ の署名である

1. $k \in \mathbb{Z}_q^*$ を無作為に選ぶ．
2. $a = (g^k \bmod p) \bmod q$
3. $b = (M + x\,a)k^{-1} \bmod q$

検証 以下が成立するとき，(a, b) は M の正しい署名である．

$$(g^{u_1} y^{u_2} \bmod p) \bmod q = a$$

ここで

$$u_1 = M\,b^{-1} \bmod q \qquad u_2 = a\,b^{-1} \bmod q$$

鍵の長さ

- $2^{L-1} < p < 2^{L}$
- $2^{N-1} < q < 2^{N}$

L は公開鍵の長さ，N は秘密鍵の長さ

L	1024	2048	2048	3072
N	160	224	256	256

検証式がどのようにはたらくか

検証式　　$(g^{u_1} y^{u_2} \bmod p) \bmod q = a$

$$u_1 = M\, b^{-1} \bmod q \qquad u_2 = a\, b^{-1} \bmod q$$

署名アルゴリズムより

$$k = (M + x\, a)\, b^{-1} \bmod q$$

したがって,

$$\begin{aligned} g^k &\equiv g^{(M+x\,a)\,b^{-1}} \pmod p \\ &\equiv g^{M\,b^{-1}}\, g^{x\,a\,b^{-1}} \pmod p \\ &\equiv g^{M\,b^{-1}}\, y^{a\,b^{-1}} \pmod p \end{aligned}$$

Schnorr 方式

公開鍵 p, q, g, y

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

秘密鍵 $x \in \mathbb{Z}_q$

署名 以下の (e, s) は M の署名である．

1. $k \in \mathbb{Z}_q^*$ を無作為に選ぶ．
2. $e = H(r, M)$．ここで $r = g^k \bmod p$
3. $s = k - e\,x \bmod q$

検証 以下が成立するとき (e, s) は M の正しい署名である．

$$r' = g^s y^e \bmod p \text{ について } e = H(r', M)$$

$H : \{0,1\}^* \to \mathbb{Z}_q^*$ は衝突計算困難なハッシュ関数

ディジタル署名とメッセージダイジェスト

任意長のメッセージ M への署名

1. ハッシュ関数 H により M のダイジェスト $H(M)$ を計算する.
2. $H(M)$ に署名する.

ハッシュ関数 H は衝突計算困難でなければならない.

ハッシュ関数 $H : D \to R$ が衝突計算困難 (collision resistant)

$$\Updownarrow$$

$H(x) = H(x')$ かつ $x \neq x'$ を満たす $x, x' \in D$ を見つけることが困難

署名方式の安全性 (1/2)

攻撃者の目標

完全解読 (total break) 攻撃者は任意のメッセージに対して正しい署名を作成できる.

選択的偽造 (selective forgery) 攻撃者は与えられたメッセージに対して正しい署名を作成できる.

存在的偽造 (existential forgery) 攻撃者は少なくとも一つのメッセージに対して正しい署名を作成できる.

- 攻撃者がメッセージを自由に選べる.

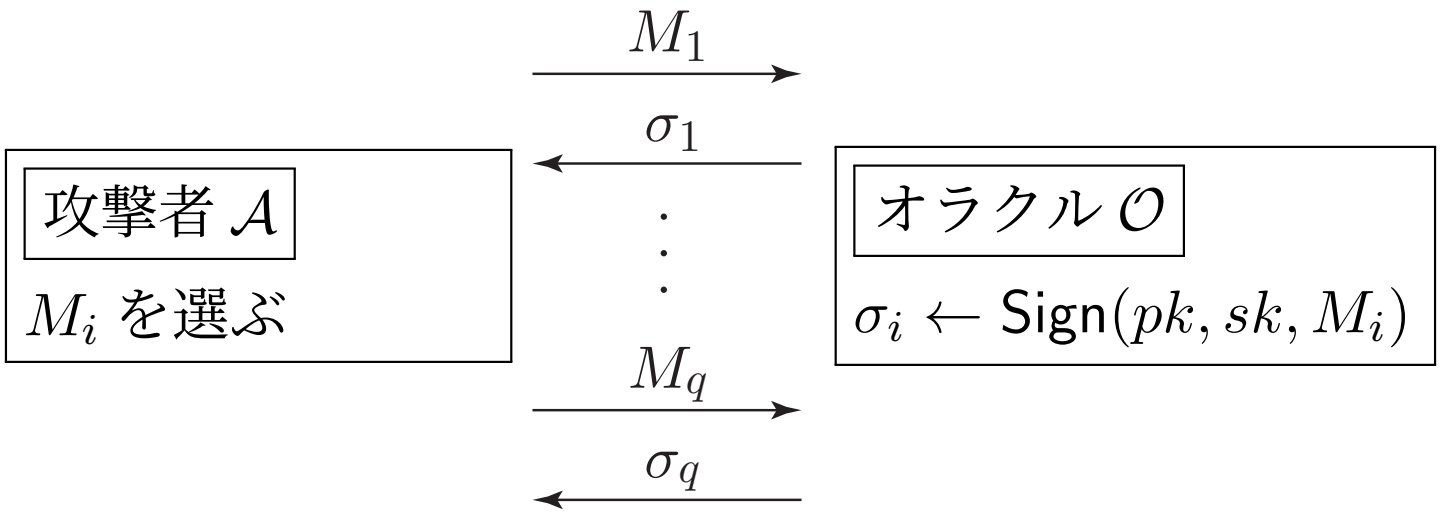
攻撃法（攻撃者に与えられる情報）

鍵単独攻撃 (key-only attack) 署名者の公開鍵のみ

既知文書攻撃 (known message attack) 複数の文書とそれらの署名の組

選択文書攻撃 (chosen message attack) 攻撃者自身の選んだ複数の文書とそれらの署名の組

選択文書攻撃



$\mathcal{A}$ は σ_i を得た後に M_{i+1} を選ぶことができる.

証明可能安全性を有する (provably secure) 署名方式

証明可能安全性を有する効率の良い署名方式が提案されている.

- ランダムオラクルモデルで
- 整数論の問題の困難性に基づいて

これらの方式については,

選択文書攻撃によっても存在的偽造が不可能である

ことが証明されている.

Schnorr 方式の証明可能安全性

Theorem

離散対数問題が困難であると仮定する．このとき，*Schnorr* 方式はランダムオラクルモデルで選択文書攻撃によっても存在的偽造が困難である．

(証明の概要) ランダムオラクルモデルでは

- 署名オラクルは，秘密鍵を持たなくても，署名者を模倣できる．
- 攻撃者が無視できない確率で正しい署名を偽造できるならば，攻撃者をサブルーチンとして用いることにより，公開鍵の離散対数を無視できない確率で容易に計算できるアルゴリズムを構成できる．

ランダムオラクルモデルでの署名者の模倣

公開鍵 p, q, g, y

秘密鍵 $x \in \mathbb{Z}_q$. ここで $y = g^x \bmod p$

攻撃者が M に対する署名を要求したとき，シミュレータは以下のようにして署名 (e, s) を計算して攻撃者に渡す.

1. $e, s \in \mathbb{Z}_q^*$ を無作為に選び，$\tilde{r} = g^s y^e \bmod p$ を計算する.
2. $e = H(\tilde{r}, M)$ とする.

攻撃者は以下の二つを識別できない.