3. 署名

Def 署名は 鍵生成, 署名生成 署名検証の

3つの関数からなる.

鍵生成: セキュリティパラメータ $\{0,1\}^*$ (鍵のビット長) に対して公開鍵と秘密鍵を 出力する 関数

署名検証: メッセージ $m \in \{0,1\}^*$ と 秘密鍵の入力に対して. 署名 σ を出力する 関数

署名検証: メッセージ $m \in \{0,1\}^*$ と 公開鍵の入力に対して. 署名 σ を用いて. 署名が正しければ 1. 正しくなければ 0 を出力する関数.

RSA署名

鍵生成: コーザA は (p, q, d) 秘密鍵と (n, e) 公開鍵を生成

1. 素数 p, q を生成
2. $n = pq$ を計算
3. $\lambda(n) = LCM(p-1, q-1)$ とし, $e \in (\mathbb{Z}/\lambda(n)\mathbb{Z})^*$ を生成し. $ed \equiv 1 \pmod{\lambda(n)}$ を求める.

(復習) $U(\mathbb{Z}/\lambda(n)\mathbb{Z}) = \{\mathbb{Z}/\lambda(n)\mathbb{Z} \ni a \mid a^{-1} \in \mathbb{Z}/\lambda(n)\mathbb{Z}\}$
$= (\mathbb{Z}/\lambda(n)\mathbb{Z})^*$

4. $H: \{0,1\}^* \longrightarrow \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ ハッシュ関数

署名生成 $m \in \{0,1\}^*$

1 $m' = H(m) \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$

2. $\sigma = (m')^d \pmod n$ σが署名

署名検証 $(m, \sigma) \in \{0,1\}^* \times \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$

1 $m' = H(m)$

2, $\sigma^e = m'$ のとき. 署名は 正しいと出力

$\neq m'$ のとき は NG と出力

(注) 正しい署名のとき. $\sigma = (m')^d$

$\sigma^e = (m')^{de} = m'$

3.1 安全性

安全性 = 攻撃 レベル × 偽造 レベル

攻撃レベル

(弱) 直接攻撃 : 公開情報のみ

既知平文攻撃: メッセージ $\{m_1, \dots, m_n\}$ に対する署名文 $\{\sigma_1, \dots, \sigma_n\}$ を入手可能. ($m_1, \dots, m_n$ は選択できない)

能動的攻撃 : 一般的 選択平文攻撃: 事前に選択した メッセージ $\{m_1, \dots, m_n\}$ に対する署名 $\{\sigma_1, \dots, \sigma_n\}$ が入手可

(強) 適応的選択平文攻撃 (chosen message attack) 適応的にメッセージ $\{m_1, \dots, m_n\}$ を選択して その署名を入手可

偽造レベル

全面的解読：秘密鍵がわかる

RSA署名 d

- 一般的偽造：任意のメッセージの偽造可 $\forall m \to H(m)^d$

選択的偽造：攻撃者の選択したメッセージの偽造可 $\exists m \to H(m)^d$

存在的偽造：少なくとも1つのメッセージの偽造可 $\exists (m, H(m)^d)$

⊙ RSA署名でHash関数がないとき偽造できるか？

- m: message → $m^d = \sigma$ 署名
- (検証) $\sigma^e = m$ となる (σ, m) が作れると偽造ができる

存在的偽造可になる（直接攻撃の下）

1. $\sigma \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$
2. $m \leftarrow \sigma^e \pmod n$ とする.
3. (m, σ) は正しい署名となる.

4 Hash関数：$H: \{0,1\}^* \to \{0,1\}^l$ (l固定長)

① 容易に計算可

② 衝突困難性：$\{0,1\}^* \to m, m'$ で $H(m) = H(m')$ をみたす m, m' をみつけることは困難である.

③ 不可逆性

$\forall y$ に $H(x) = y$ とするとき, $x \in \{0,1\}^*$ で $H(x) = y$ となる x をみつけることが困難

5. RSA署名の応用.

ユーザAの署名鍵：d

検証鍵：e

⊙ ユーザVはメッセージmをAに隠してAの署名を入手する.

1 メッセージの秘匿化

1. 乱数 $\in r \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$

$t = H(m) r^e \pmod n$

2. tをAに送付

2, Aのブラインド署名

1. $\sigma = (H(m) r^e)^d \pmod n$

((注1) $= H(m)^d r^{ed} \pmod n$ と同じ)

σをVに送付

3. 署名の入手

$\sigma = H(m)^d r^{ed}$

$= H(m)^d r$

$\sigma' = \sigma / r \pmod n$

でAの署名σ'を入手.