TOSHIBA

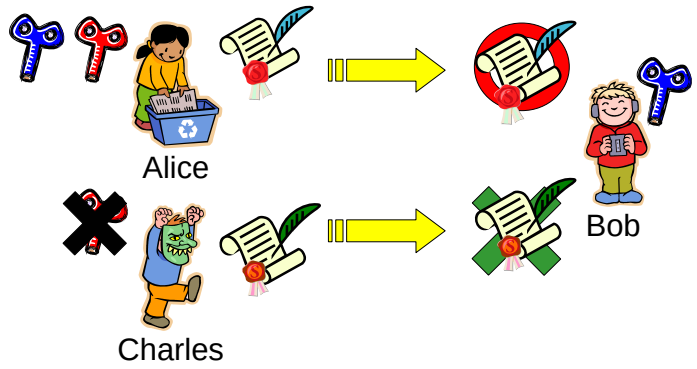
Tutorial「暗号技術の証明可能安全性」(2005.5.17)

デジタル署名の証明可能安全性

(株)東芝 研究開発センター
駒野 雄一

デジタル署名とは

・・・印鑑を電子的に実現したもの



誰 が どんな文書 を承認したかを検証できる

デジタル署名方式

プリミティブとして利用される方式

RSA署名(1978), Rabin署名(1979)

ElGamal署名(1985)

ランダムオラクルモデルで証明可能安全な方式 証明容易

Schnorr署名(1991)

FDH(1993), PFDH(2002), PSS(1996)

標準モデルで証明可能安全な方式 証明複雑

Cramer-Shoup署名(1999)

Gennaro-Halevi-Rabin署名(1999)

目次

TOSHIBA

準備

- 定義(署名)
- 定義(署名の安全性)
- 定義(一方向性関数)
- PFDHのアルゴリズム
- 定義(ランダムオラクル)

定義(署名方式)

定義1. 署名方式は次の3つのアルゴリズムで構成される

[鍵生成 $\mathcal{K}$] 安全性のパラメータ k を入力として，鍵の組

$$\mathcal{K}(1^k) = (\mathsf{pk}, \mathsf{sk})$$

を出力する確率的アルゴリズム

[署名生成 $\mathcal{S}$] 文書 Mと秘密鍵 sk を入力として，署名

$$\mathcal{S}_{\mathsf{sk}}(M) = \sigma$$

を出力する確率的アルゴリズム

[署名検証 $\mathcal{V}$] 文書 Mと署名 σ と公開鍵 pk を入力として，

$$\mathcal{V}_{\mathsf{pk}}(M,\sigma) = \begin{cases} 1 & (M,\sigma) \text{が正当な組} \\ 0 & (M,\sigma) \text{が不正な組} \end{cases}$$

を出力する確定的アルゴリズム

定義(デジタル署名方式の安全性の分類)

攻撃モデルと被害の程度による分類

	完全解読	一般的偽造	選択的偽造	存在的偽造
直接攻撃				
既知文書攻撃				
非適応的選択文書攻撃				
適応的選択文書攻撃				

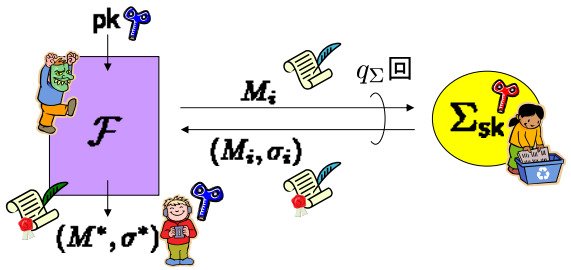
攻撃 容易

攻撃モデル 強

攻撃者に有利

定義(デジタル署名方式の安全性)

定義2. 署名方式 $(\mathcal{K},\mathcal{S},\mathcal{V})$に対して，以下の攻撃モデルを考える



実行時間 τ以内のすべての $\mathcal{F}$ について

$$\Pr[(\mathcal{V}_{\mathsf{pk}}(M^*,\sigma^*)=1) \wedge (M^* \neq M_i \text{ for } \forall i)] \leq \epsilon$$

となるとき $(\mathcal{K},\mathcal{S},\mathcal{V})$は EUF-ACMAの意味で $(\tau, q_\Sigma, \epsilon)$ 安全とよぶ

※Existential Un-Forgeability against Adaptive Chosen Message Attack

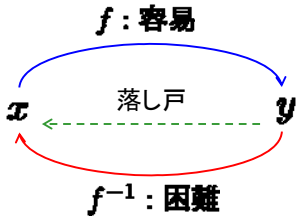
定義（一方向性関数）

定義3. $f : X \to Y$ を関数とする

実行時間 τ 以内のすべての $\mathcal{A}$ について

$$\Pr[f(x) = y | \mathcal{A}(y) = x] \leq \epsilon$$

となるとき f は (τ, ϵ) − 一方向 とよぶ



一方向性関数 と 落し戸付き一方向性関数

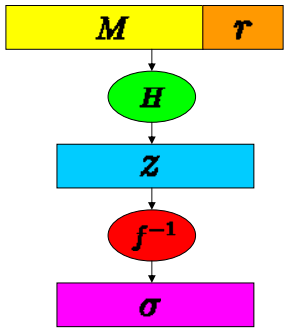
PFDH（Probabilistic Full Domain Hash）

Coron 2002

署名生成

f : k bit 落し戸付き乗法的置換* ($\mathrm{pk} = f, \mathrm{sk} = f^{-1}$ とみなす)

$H : \{0,1\}^* \to \{0,1\}^k$: ハッシュ関数



1. 文書 $M \in \{0,1\}^n$ を受け付ける
2. 乱数 $r \in \{0,1\}^{k_0}$ を選ぶ
3. $z = H(M, r)$ を計算する
4. $\sigma = f^{-1}(z)$ を計算する
5. (M, r, σ) を出力する

* 乗法性: $f(a)f(b) = f(ab)$
置換: 一対一関数

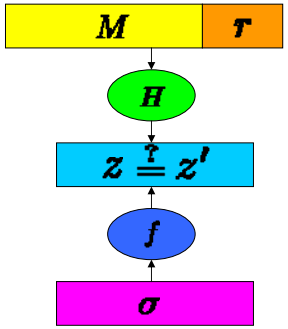
PFDH（Probabilistic Full Domain Hash）

Coron 2002

署名検証

f : k bit 落し戸付き乗法的置換

$H : \{0,1\}^* \to \{0,1\}^k$: ハッシュ関数



1. (M, r, σ) を受け付ける
2. $z = H(M, r)$ を計算する
3. $z' = f(\sigma)$ を計算する
4. $z = z'$ならば署名を受理し
   $z \neq z'$ならば署名を棄却する

定義（ランダムオラクル）

定義4. $H : \{0,1\}^\ell \to \{0,1\}^k$ が以下をみたすとき

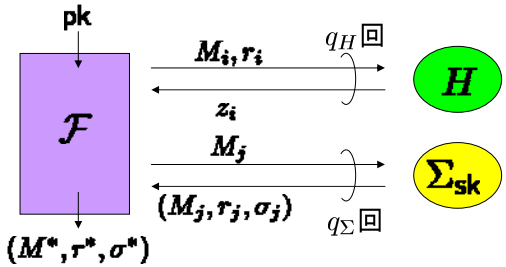
H をランダムオラクルとよぶ

1. 過去に定めた $H(x)$ は一意に決定され，
2. $H(x)$ が未定義のときには
   $\{0,1\}^k$ からランダムに値を決める

$\{0,1\}^l$	$\{0,1\}^k$	
000･･･001	100･･･110	← 値が確定
000･･･010	011･･･101	← 値が確定
･･･	･･･	
101･･･001	？？？	← 値が未確定
･･･	･･･	

ランダムオラクルモデルでの安全性

定義2'. 署名方式 $(\mathcal{K},\mathcal{S},\mathcal{V})$に対して，以下の攻撃モデルを考える



実行時間 τ以内のすべての $\mathcal{F}$について

$$\Pr[(\mathcal{V}_{pk}(M^*, r^*, \sigma^*) = 1) \wedge (M^* \neq M_j \text{ for } \forall j)] \leq \epsilon$$

となるとき $(\mathcal{K},\mathcal{S},\mathcal{V})$は EUF-ACMAの意味で $(\tau, q_H, q_\Sigma, \epsilon)$安全とよぶ

PFDHの安全性証明

- 安全性証明の方針
- 帰着アルゴリズムの構成戦略
- 帰着アルゴリズムの構成（ハッシュ依頼/署名依頼への回答）
- 帰着アルゴリズムの評価

安全性証明の方針

fが (τ', ϵ') − 一方向
⇒ PFDH は EUF-ACMA の意味で $(\tau, q_H, q_\Sigma, \epsilon)$ − 安全

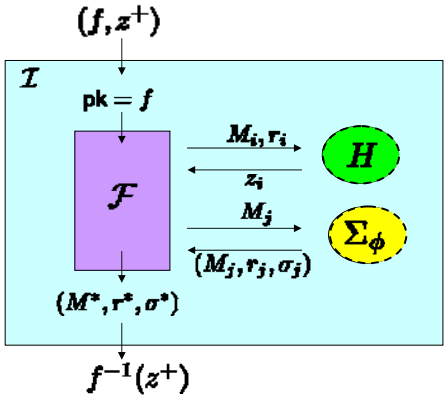
背理法

PFDH を EUF-ACMA の意味で偽造する$\mathcal{F}$が存在
⇒ f の一方向性を破るアルゴリズム $\mathcal{I}$が存在

$\mathcal{F}$をサブルーチンとして利用して
(f, z^+)を入力として $f^{-1}(z^+)$を出力する $\mathcal{I}$を構成する

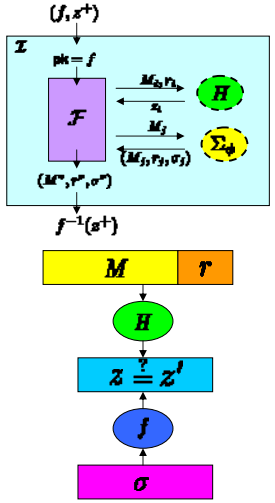
帰着アルゴリズム構成の戦略（1/2）

$\mathcal{F}$をサブルーチンとして利用して
(f, z^+)を入力として $f^{-1}(z^+)$を出力する $\mathcal{I}$を構成する



1. pk $= f$ と設定
2. H, Σ をシミュレート
   - Σ について
     sk $= f^{-1}$ を用いずに回答
   - H について
     Σ のシミュレートをサポート
     z^+ の埋め込み (次頁)

帰着アルゴリズム構成の戦略(2/2)



- H について

  z^+ の埋め込み

$\mathcal{F}^{H,\Sigma}(f) = (M^*, r^*, \sigma^*)$ を入手

$H(M^*, r^*) = f(\sigma^*)$ となるためには

$\mathcal{F}$ は (M^*, r^*) のハッシュ依頼するはず

$H(M^*, r^*) = z^+$ とシミュレートすれば

$\mathcal{I}$ は $\sigma^* = f^{-1}(z^+)$ を入手可能

H, Σ のシミュレート

$H(M_i, r_i)$ のシミュレート：

if $(*, M_i, r_i, *, z_i) \in$ List
  then return z_i
else then
  $a_i \leftarrow \{0,1\}^k$ z^+の埋め込み
  $(1, M_i, r_i, a_i, f(a_i)z^+) \rightarrow$ List
  return $f(a_i)z^+$

過去の回答と整合

詳細はCoron(EUROCRYPT'02)参照

$\Sigma(M_j)$ のシミュレート：

$r_j \leftarrow \{0,1\}^{k_0}$
if $(1, M_j, r_j, *, *) \in$ List
  then abort
else if $(0, M_j, r_j, a_j, z_j) \in$ List
  then return a_j
else then
  $a_i \leftarrow \{0,1\}^k$ z^+は埋め込まず
  $(0, M_i, r_i, a_i, f(a_i)) \rightarrow$ List
  return a_i

List $= \{($フラグ, H の入力 (2 成分), 中間情報, H の出力$)\}$

List の管理

フラグ	入力	中間情報	出力
1	M_1, r_1	a_1	$f(a_1)z^+$
0	M_2, r_2	a_2	$f(a_2)$
0	M_3, r_3	a_3	$f(a_3)$
⋮	⋮	⋮	⋮
1	M_i, r_i	a_i	$f(a_i)z^+$
⋮	⋮	⋮	⋮

H シミュレート時に設定

Σシミュレート時に設定

$\mathcal{F}^{H,\Sigma}(f) = (M^*, r^*, \sigma^*)$

偽造署名の定義から

$M^* \neq M_2, M_3$

無視できる確率を除いて

$\exists (1, M^*, r^*, a_i, f(a_i)z^+) \in$ List

$$\frac{\sigma^*}{a_i} = \frac{f^{-1}(f(a_i)z^+))}{a_i} = \frac{a_i f^{-1}(z^+)}{a_i} = f^{-1}(z^+)$$

帰着アルゴリズムの評価

$\epsilon' = \epsilon - \Pr[\mathcal{I}$ が証明に失敗$]$ $\therefore \epsilon' \geq \epsilon - \frac{q_H q_\Sigma}{2^{k_0}} - \frac{1}{2^k}$

Case 1

$\Sigma(M_j)$ のシミュレート：

$r_j \leftarrow \{0,1\}^{k_0}$
if $(1, M_j, r_j, *, *) \in$ List
  then abort
⋮

$\begin{cases} \sharp\{(1, M_i, r_i, a_i, f(a_i)z^+) \in \text{List}\} \leq q_H \\ r_j \leftarrow \{0,1\}^{k_0} \end{cases}$

より

$$\Pr[\text{Case 1}] = 1 - (1 - \frac{q_H}{2^{k_0}})^{q_\Sigma} \leq \frac{q_H q_\Sigma}{2^{k_0}}$$

Case 2

無視できる確率を除いて

$\exists (1, M^*, r^*, a_i, f(a_i)z^+) \in$ List

ランダムオラクルの定義より

$\Pr[\text{Case 2}] = \frac{1}{2^k}$

PFDHの安全性

定理(PFDHの安全性) 落し戸付き関数 f が (τ', ϵ') − 一方向ならば, PFDHは EUF-ACMA の意味で $(\tau, q_H, q_\Sigma, \epsilon)$ − 安全

ただし,

$$\begin{cases} \epsilon' \geq \epsilon - \frac{q_H q_\Sigma}{2^{k_0}} - \frac{1}{2^k} \\ \tau' \leq \tau + (q_H + q_\Sigma + 1)\mathrm{T}_f \end{cases}$$

がなりたつ. ここで T_f は f の1回の計算時間をあらわす.

緊密な安全性について

- 緊密な安全性
- FDHのアルゴリズム
- FDHが緊密な安全性をもたない理由

緊密な安全性

帰着アルゴリズム $\mathcal{I}$ を構成した結果, $\epsilon' \approx \epsilon, \tau' \approx \tau$ となるとき,

署名方式は(問題に対して)緊密な安全性をもつとよぶ

例. PFDHは f の一方向性に対して緊密な安全性をもつ

$$\begin{cases} \epsilon' \geq \epsilon - \frac{q_H q_\Sigma}{2^{k_0}} - \frac{1}{2^k} \\ \tau' \leq \tau + (q_H + q_\Sigma + 1)\mathrm{T}_f \end{cases}$$

例. FDHは f の一方向性に対して緊密な安全性をもたない

$$\begin{cases} \epsilon' \geq \frac{\epsilon}{q_\Sigma}\left(1 - \frac{1}{q_{\Sigma+1}}\right)^{q_{\Sigma+1}} \\ \tau' \leq \tau + (q_H + q_\Sigma + 1)\mathrm{T}_f \end{cases}$$

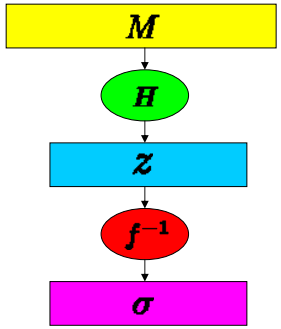
FDH(Full Domain Hash)

Bellare-Rogaway 1993

署名生成

f : k bit 置換 ($\mathrm{pk} = f, \mathrm{sk} = f^{-1}$ とみなす)

$H : \{0,1\}^* \to \{0,1\}^k$: ハッシュ関数



1. 文書 $M \in \{0,1\}^n$ を受け付ける
2. $z = H(M)$ を計算する
3. $\sigma = f^{-1}(z)$ を計算する
4. (M, σ) を出力する

FDHが緊密な安全性をもたない理由

$\Sigma(M_j)$ のシミュレート：

if $(1, M_j, \quad *, *) \in$ List
  then abort
else if $(0, M_j, \quad a_j, z_j) \in$ List
  then return a_j
else then
  $a_i \leftarrow \{0,1\}^k$
  $(0, M_i, \quad a_i, f(a_i)) \rightarrow$ List
  return a_i

過去に z^+ を埋め込んだ M_j が依頼されれば abort

↓

z^+ を確率的に埋め込む
$\left(\text{埋め込む確率} : \frac{1}{q_H+1}\right)$

↓

M^* が$(0, M_i, a_i, f(a_i)) \in$ List
と一致する確率が無視できない

↓

緊密な安全性をもたない

まとめ

- PFDHの安全性証明のご紹介
  - 一方向性関数を破る帰着アルゴリズムの構成
- 緊密な安全性
  - 乱数成分が緊密な安全性を保証 (PFDH)

ご清聴ありがとうございました

yuichi1.komano@toshiba.co.jp