ランプセッション発表原稿

EPOC-2: CRYPTREC'01提出版とROMでの証明可能安全性との関係

藤崎@NTT

‘EPOC-2’ = OU**暗号** + ROM**変換**

(EUROCRYPT’98) (CRYPTO’99)

$c = g^m h^r \bmod n,$

$n = p^2 q.$

OW ⟷ FACT(n)

OW ⟶ IND-CCA2

ROM**変換**

提案者の主張：FACT(n) + ROM => EPOC-2: IND-CCA2.

CREC'01**版の仕様**

証明可能なパラメータ

1. h **の選び方**：

$$h_0 \in_R (Z/nZ)^{\times};$$

$$h = h_0^n \bmod n.$$

$\longrightarrow$

$$h = g^n \bmod n.$$

(NESSIE'01, EUROCRYPT'98)

2. r **の範囲** (hLen)：

$$|r| \geq 2k + 32.$$

$$\begin{pmatrix} k = |p|, |q|, \\ n = p^2 q. \end{pmatrix}$$

$\longrightarrow$

$$|r| \geq 2k + \text{const.}$$

$$\text{const} \geq 1.$$

で証明可能。

(NESSIE'01)

EUROCRYPT'98**では**

$$|r| \geq 3k.$$

http://info.isl.ntt.co.jp/epoc/nessie/index-j.html or
http://info.isl.ntt.co.jp/
参照。

[帰着証明の中で]

[Adversary's real view]

$$p^{real}(z^*) = \Pr[\sigma \leftarrow_R \{0,1\}^{k-1}; r \leftarrow_R \{0,1\}^{2k+\text{const}} : z^* = \sigma + nr \bmod ord(g)],$$

where $c = g^{\sigma} h^{r} (= g^{\sigma+nr})$.

[Simulation view]

$$p^{sim}(z^*) = \Pr[z \leftarrow_R [0,\ldots,n^2-1] : z^* = z \bmod ord(g)],$$

where $c = g^{z}$.

$$\frac{p^{sim}(z^*)}{p^{real}(z^*)} \geq \frac{1}{2}\left(1-\frac{1}{n}\right)\left(1-\frac{1}{2^{\text{const}}+1}\right)$$

EPOC-2のFACTからの帰着(結論)

$$A^{epoc}: \quad (t, q_G, q_H, q_D, \varepsilon) - \text{break},$$

$$B^{fact}: \quad (t_B, \varepsilon_B) - \text{break} \quad \text{where}$$

- $t_B = t + (q_G + q_H)\, T_{\text{gcd},n} + q_D q_H (T_{Enc,q} + T_{\text{gcd},n})$,
- $\varepsilon_B = \frac{\varepsilon}{3}\left(1 - 2^{-3k+1}\right)\left(1 - 2^{-\gamma}\right)^{q_D}$.

備考:

$$\frac{p^{sim}(z^*)}{p^{real}(z^*)} \geq \frac{1}{2}\left(1 - \frac{1}{n}\right)\left(1 - \frac{1}{2^{\text{const}} + 1}\right) \geq \frac{1}{3}\left(1 - 2^{-3k+1}\right)$$

結論

1. h の選び方。

$$h = h_0^n \longrightarrow h = g^n$$

に今後変更希望。

2. r の範囲 (hLen) 。

変更なし。