共通鍵暗号の安全性

定義1: Left-or-Right(LOR)

Experiment $Exp_{SE}^{lor-cpa-b}(A)$:

$K \leftarrow \mathscr{K}$

$d \leftarrow A^{\mathscr{E}_K(LR(\cdot,\cdot,b))}$

return d

$\mathscr{E}_K(x_0, x_1, b)$:

return $C = \mathscr{E}_K(x_b)$

$$Adv_{SE}^{lor-cpa}(A) = |Pr[Exp_{SE}^{lor-cpa-1}(A) = 1] - Pr[Exp_{SE}^{lor-cpa-0}(A) = 1]|$$

定義2 : Real-or-Random(ROR)

Experiment $Exp_{SE}^{ror-cpa-1}(A)$:

$K \leftarrow \mathscr{K}$

$d \leftarrow A^{\mathscr{E}_K(\cdot)}$

return d

Experiment $Exp_{SE}^{ror-cpa-0}(A)$:

$K \leftarrow \mathscr{K}$

$d \leftarrow A^{\mathscr{E}(\{0,1\}^*)}$

return d

$$Adv_{SE}^{ror-cpa}(A) = |Pr[Exp_{SE}^{ror-cpa-1}(A) = 1] - Pr[Exp_{SE}^{ror-cpa-0}(A) = 1]|$$

定義3: Find-then-Guess(FTG)

Experiment $Exp_{SE}^{ftg-cpa-b}(A)$:

$K \leftarrow \mathscr{K}$

$(x_0, x_1, s) \leftarrow A^{\mathscr{E}_K(\cdot)}(find)$

$y \leftarrow \mathscr{E}_K(x_b)$

$d \leftarrow A^{\mathscr{E}_K(\cdot)}(guess, y, s)$

return d

$$Adv_{SE}^{ftg-cpa}(A) = |Pr[Exp_{SE}^{ftg-cpa-1}(A) = 1] - Pr[Exp_{SE}^{ftg-cpa-0}(A) = 1]|$$

定義4 : Semantic Security(SS)

Experiment $Exp_{SE}^{sem-cpa-b}(A)$:

$K \leftarrow \mathscr{K}$

$(\mathscr{M}, s) \leftarrow A^{\mathscr{E}_K(\cdot)}(select)$

$x_0, x_1 \leftarrow \mathscr{M}$

$y \leftarrow \mathscr{E}_K(x_1)$

$(f, \alpha) \leftarrow A^{\mathscr{E}_K(\cdot)}(predict, y, s)$

If $\alpha = f(x_b)$ then $d \leftarrow 1$, else $d \leftarrow 0$

return d

$$Adv_{SE}^{sem-cpa}(A) = |Pr[Exp_{SE}^{sem-cpa-1}(A) = 1] - Pr[Exp_{SE}^{sem-cpa-0}(A) = 1]|$$

A Concrete Security Treatment of Symmetric Encryption(1997)
https://web.cs.ucdavis.edu/~rogaway/papers/sym-enc.pdf

AEについて(1)

論文名	内容	nonceの有無	安全性
Integrity-aware PCBC encryption schemes. (2000) https://www.iacr.org/archive/eurocrypt2001/20450525.pdf	AEの方式IACBCとIAPMの考案	有り?無し?	FTG
Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm(2000) https://cseweb.ucsd.edu/~mihir/papers/oem.pdf	AEの安全性の関係性について (Privacy,Integrity)	無し	LOR
OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption (2001) https://web.cs.ucdavis.edu/~rogaway/papers/ocb-full.pdf	IAPMを発達させて、AEの方式 OCBを考案	有り	ROR
Authenticated-Encryption with Associated-Data(2002) https://web.cs.ucdavis.edu/~rogaway/papers/ad.pdf	AEADの定義・安全性の考察	有り	ROR
A Provable-Security Treatment of the Key-Wrap Problem(2006) https://www.iacr.org/archive/eurocrypt2006/40040377/40040377.pdf	Key-Wrap Problemの解決策を考察 DAEの定義・安全性の考察	無し?	ROR

AEについて(2)

論文名	内容	nonceの有無	安全性
A Simple and Generic Construction of Authenticated Encryption With Associated Data(2009) https://eprint.iacr.org/2009/215.pdf	固定長のnonceをもつAEから可変長のAE(AE+)を構成して、 AE+からAEADを構成	有り	ROR
Message Franking via Committing Authenticated Encryption(2017) https://eprint.iacr.org/2017/664.pdf	Message frankingの考察	無しと有り	ROR
Nonce-Based Symmetric Encryption(2006) https://web.cs.ucdavis.edu/~rogaway/papers/nonce.pdf	nonceを用いた共通鍵暗号方式の定義と安全性 nonceを使用に関する議論	有り	ROR

AEとAEADの表記について

AEとAEADの定義の違いは

Header H が含まれているかどうか

⇒AEの定義はAEADの定義において H がないものと考える

安全性における表記について

AEAD： $Adv_{\Pi}^{PRIV}(A)$, $Adv_{\Pi}^{AUTH}(A)$ [大文字]

AD : $Adv_{\Pi}^{priv}(A)$, $Adv_{\Pi}^{auth}(A)$ [小文字]

AEADの定義

AEAD $\Pi = (\mathscr{K}, \mathscr{E}, \mathscr{D})$

$\mathscr{K}$：鍵空間 , $Nonce = \{0,1\}^n$, $Header \subseteq \{0,1\}^*$, $Message \subseteq \{0,1\}^*$

$N \in Nonce,\ H \in Header,\ M \in Message,\ C \in \{0,1\}^*$

$K \ \leftarrow \mathscr{K}$

$\mathscr{C} \ \leftarrow \mathscr{E}(K, N, H, M) = \mathscr{E}_K(N, H, M) = \mathscr{E}_K^{N,H}(M)$：決定的アルゴリズム

$M \ \leftarrow \mathscr{D}(K, N, H, C) = \mathscr{D}_K(N, H, \mathscr{C}) = \mathscr{D}_K^{N,H}(\mathscr{C})$：決定的アルゴリズム

Correctness: $\forall K \in \mathscr{K},\ \forall N \in Nouce,\ \forall H \in Header,\ \forall M \in Message$

$$s.t.\ \ \mathscr{D}_K^{N,H}(\mathscr{E}_K^{N,H}(M)) = M$$

AEADの安全性(IND$-CPA)

$l(|M|) = |\mathscr{E}_K^{N,H}(M)|$：線形時間で計算可能な暗号文の長さを返す関数

$\{0,1\}^{l(|M|)} \leftarrow \$(N, H, M)$：入力 (N, H, M) に対してランダムな $l(|M|)$ ビットの文字列を出力

Experiment $Exp_{\Pi}^{IND\$-CPA-1}(A)$	Experiment $Exp_{\Pi}^{IND\$-CPA-0}(A)$
$K \leftarrow \mathscr{K}$	$K \leftarrow \mathscr{K}$
$b \leftarrow A^{\mathscr{E}_K(\cdot,\cdot,\cdot)}$	$b \leftarrow A^{\$(\cdot,\cdot,\cdot)}$
return b	return b

$$Adv_{\Pi}^{PRIV}(A) = |Pr[Exp_{\Pi}^{IND\$-CPA-1}(A) = 1] - Pr[Exp_{\Pi}^{IND\$-CPA-0}(A) = 1]|$$

AEADの安全性(Authenticity)

Experiment $Exp_{\Pi}^{AUTH}(A)$

$K \leftarrow \mathscr{K}$

$(N, H, \mathscr{C}) \leftarrow A^{\mathscr{E}_K(\cdot,\cdot,\cdot)}()$

If $\mathscr{D}_K^{N,H}(\mathscr{C}) \neq \perp$ and A didn't query (N, H, M) to $\mathscr{E}_K(\cdot, \cdot, \cdot)$

then return 1 else 0

$$Adv_{\Pi}^{AUTH}(A) = Pr[Exp_{\Pi}^{AUTH}(A) = 1]$$

擬似乱数関数

$F : \mathscr{K} \times \mathscr{X} \rightarrow \{0,1\}^{\tau}$：関数族

$Rand(\mathscr{X}, \tau)$：$\mathscr{X}$ から$\{0,1\}^{\tau}$ への関数の集合

$Adv_F^{pdf}(A) = |Pr[A^{F_K(\cdot)} = 1; K \leftarrow \mathscr{K}] - Pr[A^{\rho(\cdot)} = 1; \rho \leftarrow Rand(\mathscr{X}, \tau)]|$

$Adv_F^{pdf}(A) < \epsilon$ のとき F は擬似乱数関数

$Time_f(q, \sigma)$：関数 $f : \mathscr{K} \times \mathscr{X} \rightarrow \mathscr{Y}$ において

$A + B$ の最悪時の計算時間(worst-case time)

$A = \{$ $K \leftarrow \mathscr{K}$ の計算時間$\}$

$B = \{$ $f_K(X_1), f_K(X_2), \cdots, f_K(X_q)$の計算時間 [但し、$\Sigma|\mathscr{X}_q| \leq \sigma$]$\}$

Encrypt-then-MACの定義

AE $\Pi = (\mathscr{K}, \mathscr{E}, \mathscr{D})$, $F : \mathscr{K}' \times \{0,1\}^* \to \{0,1\}^\tau$ に対して

AEAD $[\Pi, F] = (\overline{\mathscr{K}}, \overline{\mathscr{E}}, \overline{\mathscr{D}})$

$\overline{\mathscr{K}} = \mathscr{K} \times \mathscr{K}' \to (K, K')$

$\overline{\mathscr{E}}^{N,H}_{K,K'}(M) \to \mathscr{E}^N_K(M) \,||\, F_{K'}(<N, H, C>) = C \,||\, T$

$$\overline{\mathscr{D}}^{N,H}_{K,K'}(C \,||\, T) = \begin{cases} \mathscr{D}^N_K(C) & (F_{K'}(<N, H, C>) = T) \\ INVALID & (otherwise) \end{cases}$$

$<X, Y>$: 文字列 X, Y を符号化したもの

Encrypt-then-MACの安全性

AE $\Pi = (\mathscr{K}, \mathscr{E}, \mathscr{D})$, $F : \mathscr{K}' \times \{0,1\}^* \to \{0,1\}^\tau$ に対して

t, t_1, t_2 : 実行時間 , q : 最大のクエリ数 , σ : 全体の最大のビット数

$$Adv^{PRIV}_{[\Pi,F]}(t, q, \sigma) \leq Adv^{priv}_{\Pi}(t_1, q, \sigma) + Adv^{prf}_{F}(t_2, q, \sigma)$$

$$Adv^{AUTH}_{[\Pi,F]}(t, q, \sigma, \zeta) \leq Adv^{prf}_{F}(t_3, q+1, \sigma+\zeta) + \frac{1}{2^\tau}$$

$$\begin{cases} t = t_1 + t_2 + Time_F(q,\sigma) + \mathscr{O}(\sigma + q) \\ t = t_3 + Time_F(q, \sigma+\zeta) + \mathscr{O}(\sigma+\zeta+q) \end{cases}$$ を満たす

<u>AEが安全であり、Fが擬似乱数関数であるならば安全となる</u>

Key-Evolving AEAD

Key-Evolving AEAD $\hat{\Pi} = (KeyGen, Upd, Enc, Dec)$

$\mathscr{K}$：鍵空間 , $Nonce = \{0,1\}^n$, $Header \subseteq \{0,1\}^*$, $Message \subseteq \{0,1\}^*$

$K_0 \in \mathscr{K}, N \in Nonce,\ H \in Header,\ M \in Message,\ C \in \{0,1\}^*$

$K_0 \leftarrow KeyGen(1^k, n)$

$K_i \leftarrow Upd(K_{i-1})$

$(\mathscr{C}, i) \leftarrow Enc(K_i, N, H, M) = Enc_{K_i}(N, H, M) = Enc_{K_i}^{N,H}(M)$

$M \leftarrow Dec(K_i, N, H, \mathscr{C}) = Dec_{K_i}(N, H, \mathscr{C}) = Dec_{K_i}^{N,H}(\mathscr{C})$

Forward Secure(IND$-CPA)

Experiment $Exp_{\hat{\Pi}}^{FSIND\$-CPA-1}(A)$

$K_0 \leftarrow KeyGen(1^K, n)$; $i \leftarrow 0$, $h \leftarrow \epsilon$

Repeat

$i \leftarrow i + 1$; $K_i \leftarrow Upd(K_{i-1})$

$(d, h) \leftarrow A^{Enc_{K_i}(\cdot,\cdot,\cdot)}(find, h)$

Until $(d = guess)$ or $(i = n)$

$b \leftarrow A(guess, h)$

return b

Experiment $Exp_{\hat{\Pi}}^{FSIND\$-CPA-0}(A)$

$K_0 \leftarrow KeyGen(1^K, n)$; $i \leftarrow 0$, $h \leftarrow \epsilon$

Repeat

$i \leftarrow i + 1$; $K_i \leftarrow Upd(K_{i-1})$

$(d, h) \leftarrow A^{\$(\cdot,\cdot,\cdot)}(find, h)$

Until $(d = guess)$ or $(i = n)$

$b \leftarrow A(guess, h)$

return b

$$Adv_{\hat{\Pi}}^{FSPRIV}(A) = |\, Pr[Exp_{\hat{\Pi}}^{FDIND\$-CPA-1}(A) = 1] - Pr[Exp_{\hat{\Pi}}^{FSIND\$-CPA-0}(A) = 1]\,|$$

Forward Secure(Authenticity)

Experiment $Exp_{\hat{\Pi}}^{FSAUTH}(A)$

$K_0 \leftarrow KeyGen(1^K, n)$; $i \leftarrow 0$, $h \leftarrow \epsilon$

Repeat

  $i \leftarrow i + 1$; $K_i \leftarrow Upd(K_{i-1})$

  $(d, h) \leftarrow A^{Enc_{K_i}(\cdot,\cdot,\cdot)}(find, h)$

Until $(d = forge)$ or $(i = n)$

$(N, H, \mathscr{C}, j) \leftarrow A(forge, K_i, h)$

If $Dec_{K_j}^{N,H}(\mathscr{C}) \neq \perp$ and A didn't query (N, H, M) to $Enc_{K_i}(\cdot, \cdot, \cdot)$ and $1 \leq j < i$

  then return 1 else 0

$Adv_{\hat{\Pi}}^{FSAUTH}(A) = Pr[Exp_{\hat{\Pi}}^{FSAUTH}(A) = 1]$

擬似乱数生成器(PRG)

$G : \{0,1\}^s \to \{0,1\}^{b+s}$

Experiment $Exp_G^{prg-1}(D)$

$y \leftarrow \{0,1\}^s \; ; \; x||y \leftarrow G(y)$

$g \leftarrow D(x||y)$

return g

Experiment $Exp_G^{prg-1}(D)$

$x||y \leftarrow \{0,1\}^{b+s}$

$g \leftarrow D(x||y)$

return g

$$Adv_G^{prg}(D) = |Pr[Exp_G^{prg-1}(D) = 1] - Pr[Exp_G^{prg-0}(D) = 1]|$$

$$Adv_G^{prg}(t) = \max_D \left\{ Adv_G^{prg}(D) \right\}$$

Stateful PRGとforward secure

$PRG = (PRG.key, PRG.next, b)$

$St_0 \leftarrow PRG.key()$ ：確率的アルゴリズム

$(Out_i, St_i) \leftarrow PRG.next(St_{i-1})$ ：決定的アルゴリズム $(i = 1, \cdots, n)$

Experiment $Exp^{fsprg-1}_{PRG}(A)$

$St_0 \leftarrow PRG.key()$

$i \leftarrow 0$; $h \leftarrow \epsilon$

Repeat

$i \leftarrow i + 1$

$(Out_i, St_i) \leftarrow PRG.next(St_{i-1})$

$(d, h) \leftarrow A(find, Out_i, h)$

Until $(d = guess)$ or $(i = n)$

$g \leftarrow A(guess, St_i, h)$

return g

Experiment $Exp^{fsprg-0}_{PRG}(A)$

$St_0 \leftarrow PRG.key()$

$i \leftarrow 0$; $h \leftarrow \epsilon$

Repeat

$i \leftarrow i + 1$

$(Out_i, St_i) \leftarrow PRG.next(St_{i-1})$

$Out_i \leftarrow \{0,1\}^b$

$(d, h) \leftarrow A(find, Out_i, h)$

Until $(d = guess)$ or $(i = n)$

$g \leftarrow A(guess, St_i, h)$

return g

$$Adv^{fsprg}_{PRG}(A) = |Pr[Exp^{fsprg-1}_{PRG}(A) = 1] - Pr[Exp^{fsprg-0}_{PRG}(A) = 1]|$$

$$Adv^{fsprg}_{PRG}(t) = \max_{A} \left\{ Adv^{fsprg}_{PRG}(A) \right\}$$

Forward Secure AEADの構成

AEAD $\Pi = (\mathscr{K}, \mathscr{E}, \mathscr{D})$

Forward secure PRG $PRG = (PRG.key, PRG.gen, b)$

$\Rightarrow$ Forward Secure AEAD $\hat{\Pi} = (KeyGen, Upd, Enc, Dec)$

Algorithm $KeyGen(1^k, n)$ $K_0 \leftarrow PRG.key()$ return K_0	Algorithm $Upd(K_{i-1})$ $K_i \leftarrow PRG.next(K_{i-1})$ return K_i
Algorithm $Enc(K_i, N, H, M)$ $\mathscr{C} \leftarrow \mathscr{E}(K_i, N.H, M)$ return $<\mathscr{C}, i>$	Algorithm $Dec(K_i, N, H, <\mathscr{C}, j>)$ If $j \neq i$ then return $\perp$ $M \leftarrow \mathscr{D}(K_i, N, H, \mathscr{C})$ return M

Forward Secure(証明)

AEAD $\Pi = (\mathscr{K}, \mathscr{E}, \mathscr{D})$:

$Adv_{\Pi}^{PRIV}(A) = |Pr[Exp_{\Pi}^{IND\$-CPA-1}(A) = 1] - Pr[Exp_{\Pi}^{IND\$-CPA-0}(A) = 1]|$

$Adv_{\Pi}^{AUTH}(A) = Pr[Exp_{\Pi}^{AUTH}(A) = 1]$

Forward secure PRG $PRG = (PRG.key, PRG.gen, b)$:

$Adv_{PRG}^{fsprg}(A) = |Pr[Exp_{PRG}^{fsprg-1}(A) = 1] - Pr[Exp_{PRG}^{fsprg-0}(A) = 1]|$

目標(予想)

$Adv_{\hat{\Pi}}^{FSPRIV}(A) \leq Adv_{PRG}^{fsprg}(A) + n \cdot Adv_{\Pi}^{PRIV}(A)$

$Adv_{\hat{\Pi}}^{FSAUTH}(A) \leq Adv_{PRG}^{fsprg}(A) + n \cdot Adv_{\Pi}^{AUTH}(A)$