CryptoVerif のための Authenticated Encryption の安全性の定式化に関する考察

2008/3/8

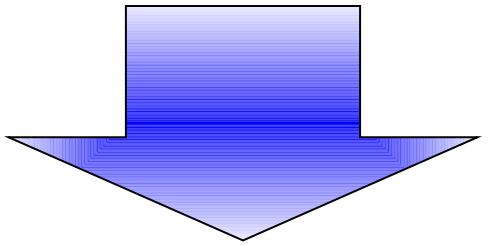
○*荒井　研一，**岡崎　裕之，**不破　泰

*信州大学大学院総合工学系研究科
**信州大学大学院工学系研究科

CryptoVerifとゲーム について

CryptoVerif

- CryptoVerif とは
  - Blanchetが作成
    (http://www.cryptoverif.ens.fr/) version 1.06pl3
  - ゲームによる安全性の検証を自動で行うプログラム
  - Observational Equivalence



Full Domain Hash署名方式が選択メッセージ攻撃のもとで偽造不可能性を満たすことを自動で検証

ゲームによる安全性証明

- ゲームとは

攻撃者と挑戦者との間で行われる攻撃ゲーム

V. Shoup, "Sequences of Games : A Tool for Taming Complexity in Security Proofs," In Cryptology ePrint Archive, Report 2004/332, Available at http://eprint.iacr.org/2004/332, 2004.

ゲームによる安全性証明

- ゲームによる安全性証明とは

  初期ゲームを次々に変換しながら

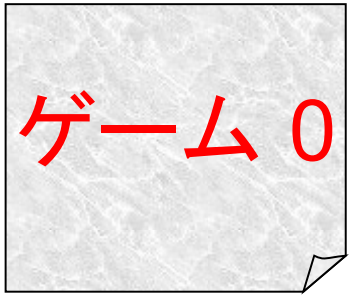
  1. 攻撃者の勝つ確率は各ステップでほとんど変わらない
  2. 最終ゲームでは攻撃者が勝つ確率が十分に小さい

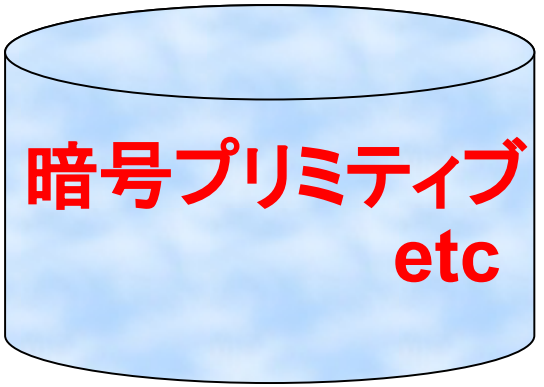
  を証明する

CryptoVerifによる検証

初期ゲーム

条件





与えられた条件から最終ゲームに到達できるか判定

Authenticated Encryption について

Authenticated Encryption

- Authenticated Encryptionとは

  Authenticated Encryption(AE) : $AE=(AE\text{-}K, AE\text{-}\varepsilon, AE\text{-}D)$

共通鍵暗号方式

メッセージ秘匿　メッセージ認証

秘匿　完全性

秘匿の安全性

共通鍵暗号方式：$S\varepsilon = (\varepsilon, D, K)$

Proc Initialize　$K \xleftarrow{R} K$; $b \xleftarrow{R} \{0,1\}$

Proc LR(M_0,M_1)　$C \xleftarrow{R} \varepsilon_K(M_b)$;

Return C

Proc Finalize(d)　Return(d = b)

IND-CPA$_{S\varepsilon}$ ゲーム

Proc Initialize　$K \xleftarrow{R} K$; $b \xleftarrow{R} \{0,1\}$; $S \leftarrow \phi$

Proc LR(M_0,M_1)　$C \xleftarrow{R} \varepsilon_K(M_b)$; $S \leftarrow S \cup \{C\}$;

Return C

Proc Dec(C)　If $C \notin S$ then $M \leftarrow D_K(C)$

else $M \leftarrow \perp$

Proc Finalize(d)　Return(d = b)

IND-CCA$_{S\varepsilon}$ ゲーム

MAC(Message Authentication Code)の安全性

MAC(Message Authentication Code)：MAC=(MAC-ε, MAC-V, MAC-K)

Proc Initialize　$K \xleftarrow{R} K$; $S \leftarrow \phi$
Proc Tag(M)　$Tag \xleftarrow{R} MAC\text{-}\varepsilon_K(M)$; $S \leftarrow S \cup \{M\}$;
Return Tag
Proc VF(M,Tag)
$b \leftarrow MAC\text{-}V_K(M,Tag)$
If $b = 1$ and $M \notin S$ then $Win \leftarrow true$
Return b
Proc Finalize　Return Win

WUF-CMA$_{MAC}$ ゲーム

Proc Initialize　$K \xleftarrow{R} K$; $S \leftarrow \phi$
Proc Tag(M)　$Tag \xleftarrow{R} MAC\text{-}\varepsilon_K(M)$; $S \leftarrow S \cup \{(M,Tag)\}$;
Return Tag
Proc VF(M,Tag)
$b \leftarrow MAC\text{-}V_K(M,Tag)$
If $b = 1$ and $(M,Tag) \notin S$ then $Win \leftarrow true$
Return b
Proc Finalize　Return Win

SUF-CMA$_{MAC}$ ゲーム

完全性(Integrity)

共通鍵暗号方式:$S\varepsilon = (\varepsilon, D, K)$

Proc Initialize　$K \xleftarrow{R} K$; $S \leftarrow \phi$
Proc ENC(M)　$C \xleftarrow{R} \varepsilon_K(M)$; $S \leftarrow S \cup \{M\}$;
Return C
Proc VF(C)
$M \leftarrow D_K(C)$
If $M \neq \perp$ and $M \notin S$ then Win $\leftarrow$ true
Return $(M \neq \perp)$
Proc Finalize　Return Win

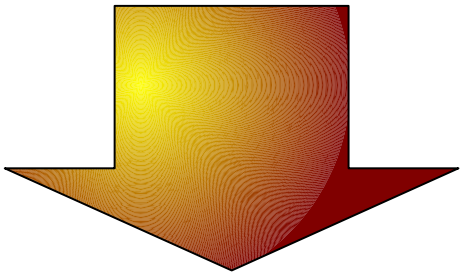
INT-PTXT$_{S\varepsilon}$ ゲーム

Proc Initialize　$K \xleftarrow{R} K$; $S \leftarrow \phi$
Proc ENC(M)　$C \xleftarrow{R} \varepsilon_K(M)$; $S \leftarrow S \cup \{C\}$;
Return C
Proc VF(C)
$M \leftarrow D_K(C)$
If $M \neq \perp$ and $C \notin S$ then Win $\leftarrow$ true
Return $(M \neq \perp)$
Proc Finalize　Return Win

INT-CTXT$_{S\varepsilon}$ ゲーム

Authenticated Encryptionの一般的な構成

- Authenticated Encryptionの一般的な構成について
  - Encrypt-and-MAC （E&M）
  - MAC-then-Encrypt （MtE）
  - Encrypt-then-MAC （EtM）



CryptoVerifにおける安全性の定式化及び評価

Encrypt-and-MAC (E&M)

Authenticated Encryption(AE) : $\mathrm{AE}=(\mathrm{AE\text{-}K}, \mathrm{AE\text{-}\varepsilon}, \mathrm{AE\text{-}D})$

$K_e \xleftarrow{R} K_e$
$K_m \xleftarrow{R} K_m$
Return $K_e \| K_m$

Algorithm AE-K

$C' \xleftarrow{R} \varepsilon_{Ke}(M)$, $Tag \xleftarrow{R} MAC\text{-}\varepsilon_{Km}(M)$
$C \leftarrow C' \| Tag$
Return C

Algorithm AE-$\varepsilon(K_e \| K_m)(M)$

Parse C as $C' \| Tag$
$M \xleftarrow{R} D_{Ke}(C')$, $b \leftarrow MAC\text{-}V_{Km}(M, Tag)$
If b=1 then Return M else Return $\perp$

Algorithm AE-D$(K_e \| K_m)(C)$

MAC-then-Encrypt (MtE)

Authenticated Encryption(AE) : $\mathrm{AE}=(\mathrm{AE\text{-}K}, \mathrm{AE\text{-}\varepsilon}, \mathrm{AE\text{-}D})$

$K_e \xleftarrow{R} K_e$
$K_m \xleftarrow{R} K_m$
Return $K_e \| K_m$

Algorithm AE-K

$Tag \xleftarrow{R} MAC\text{-}\varepsilon_{K_m}(M)$
$C \xleftarrow{R} \varepsilon_{K_e}(M \| Tag)$
Return C

Algorithm AE-$\varepsilon(K_e \| K_m)(M)$

$M' \xleftarrow{R} D_{K_e}(C)$, Parse M' as $M \| Tag$
$b \leftarrow MAC\text{-}V_{K_m}(M, Tag)$
If b=1 then Return M else Return $\perp$

Algorithm AE-D$(K_e \| K_m)(C)$

Encrypt-then-MAC (EtM)

Authenticated Encryption(AE) : $\mathrm{AE}=(\mathrm{AE\text{-}K}, \mathrm{AE\text{-}\varepsilon}, \mathrm{AE\text{-}D})$

$K_e \xleftarrow{R} K_e$
$K_m \xleftarrow{R} K_m$
Return $K_e \| K_m$

Algorithm AE-K

$C' \xleftarrow{R} \varepsilon_{Ke}(M)$, $Tag' \xleftarrow{R} MAC\text{-}\varepsilon_{Km}(C')$
$C \leftarrow C' \| Tag'$
Return C

Algorithm AE-$\varepsilon(K_e \| K_m)(M)$

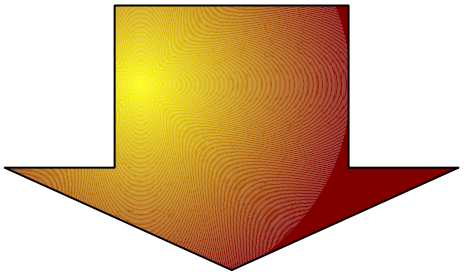
Parse C as $C' \| Tag'$
$M \xleftarrow{R} D_{Ke}(C')$, $b \leftarrow MAC\text{-}V_{Km}(C', Tag')$
If b=1 then Return M else Return $\perp$

Algorithm AE-D$(K_e \| K_m)(C)$

CryptoVerifにおける Authenticated Encryption の安全性の評価

Authenticated Encryptionの安全性の評価

- Encrypt-and-MAC （E&M）
- MAC-then-Encrypt （MtE）
- Encrypt-then-MAC （EtM）



IND-CPA　IND-CCA　INT-PTXT　INT-CTXT

Authenticated Encryptionの安全性の評価

- 各構成で利用される共通鍵暗号方式

IND-CPA

- 各構成で利用されるMAC

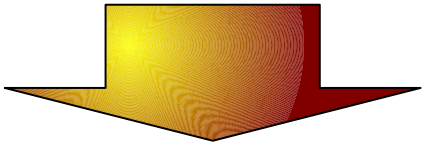
WUF-CMA 又は SUF-CMA

安全性の根拠

CryptoVerifで取り扱うための定式化

Blanchetにより既に与えられている暗号プリミティブ

- 共通鍵暗号方式の IND-CPA
- MACの WUF-CMA



与えられていない暗号プリミティブ

Observational Equivalence を満たす式として定式化
(ただし，人間による評価が必要)

- MACの SUF-CMA

MACのSUF-CMAをCryptoVerifで取り扱うための定式化

一般的な定式化

$$\mathrm{Succ}_p^{\mathrm{SUF}}(A) = \Pr\left[\begin{array}{l} r \xleftarrow{R} \mathrm{seed}; k \leftarrow \mathrm{mkgen}(r); \\ (M, \mathrm{Tag}) \leftarrow A^{\mathrm{mac}(.,k),\mathrm{check}(.,k,.)} \\ \mathrm{check}(M, k, \mathrm{Tag}) \end{array} : \left(M,\mathrm{Tag}\right) \notin \{(M_1,\mathrm{Tag}_1),\ldots,(M_i,\mathrm{Tag}_i)\}\right]$$

CryptoVerifで取り扱うための定式化

攻撃が成功するかもしれない一般的なモデルを定式化

$\approx_p$

絶対に攻撃が成功しない理想的なモデルを定式化

MACのSUF-CMAをCryptoVerifで取り扱うための定式化

一般的な定式化

$$\mathrm{Succ}_p^{\mathrm{SUF}}(A) = \Pr\left[\begin{array}{l} r \xleftarrow{R} \mathrm{seed};\ k \leftarrow \mathrm{mkgen}(r); \\ (M, \mathrm{Tag}) \leftarrow A^{\mathrm{mac}(.,k),\mathrm{check}(.,k,.)} \\ \mathrm{check}(M, k, \mathrm{Tag}) \end{array} : \left(M,\mathrm{Tag}\right) \notin \{(M_1,\mathrm{Tag}_1),\ldots,(M_i,\mathrm{Tag}_i)\}\right]$$

CryptoVerifで取り扱うための定式化

```
! N3 new r: mkeyseed;(
(x: bitstring) N ->
    mac(x, mkgen(r)),
(m: bitstring, ma: macs) N2 ->
    check(m, mkgen(r), ma))
```

$\approx_p$ (N3 * Psmac(time, N, N2))

```
! N3 new r: mkeyseed;(
(x: bitstring) N ->
  let x2:macs = mac2(x, mkgen2(r)) in x2,
(m: bitstring, ma: macs) N2 ->
  find j <= N suchthat defined(x[j],x2[j])
  && (m = x[j]) && (ma = x2[j]) &&
  check2(x[j], mkgen2(r), mac2(x[j],mkgen2(r)))
  then true else false).
```

Encrypt-and-MAC (E&M)の安全性の評価

- 共通鍵暗号方式 = IND−CPA
- MAC = WUF−CMA

	IND-CPA	IND-CCA	INT-PTXT	INT-CTXT
E&M	insecure	insecure	secure	insecure

IND-CPA & WUF-CMA

- 共通鍵暗号方式 = IND−CPA
- MAC = SUF−CMA

	IND-CPA	IND-CCA	INT-PTXT	INT-CTXT
E&M	insecure	insecure	secure	insecure

IND-CPA & SUF-CMA

MAC-then-Encrypt (MtE)の安全性の評価

- 共通鍵暗号方式 = IND−CPA
- MAC = WUF−CMA

	IND-CPA	IND-CCA	INT-PTXT	INT-CTXT
MtE	secure	insecure	secure	insecure

IND-CPA & WUF-CMA

- 共通鍵暗号方式 = IND−CPA
- MAC = SUF−CMA

	IND-CPA	IND-CCA	INT-PTXT	INT-CTXT
MtE	secure	insecure	secure	insecure

IND-CPA & SUF-CMA

Encrypt-then-MAC (EtM)の安全性の評価

- 共通鍵暗号方式 = IND−CPA
- MAC = WUF−CMA

	IND-CPA	IND-CCA	INT-PTXT	INT-CTXT
EtM	secure	insecure	secure	insecure

IND-CPA & WUF-CMA

- 共通鍵暗号方式 = IND−CPA
- MAC = SUF−CMA

	IND-CPA	IND-CCA	INT-PTXT	INT-CTXT
EtM	secure	secure	secure	secure

IND-CPA & SUF-CMA

論文[BN2000]の安全性評価

Composition Method	Privacy		Integrity	
	IND-CPA	IND-CCA	INT-PTXT	INT-CTXT
Encrypt-and-MAC	insecure	insecure	secure	insecure
MAC-then-encrypt	secure	insecure	secure	insecure
Encrypt-then-MAC	secure	insecure	secure	insecure

IND-CPA & WUF-CMA

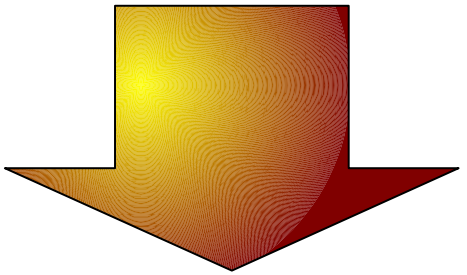
Composition Method	Privacy		Integrity	
	IND-CPA	IND-CCA	INT-PTXT	INT-CTXT
Encrypt-and-MAC	insecure	insecure	secure	insecure
MAC-then-encrypt	secure	insecure	secure	insecure
Encrypt-then-MAC	secure	secure	secure	secure

IND-CPA & SUF-CMA

[BN2000] M.Bellare and C.Namprempre, “Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm” Advances in Cryptology – ASIACRYPTO 2000.

CryptoVerifと論文[BN2000]の安全性評価の比較

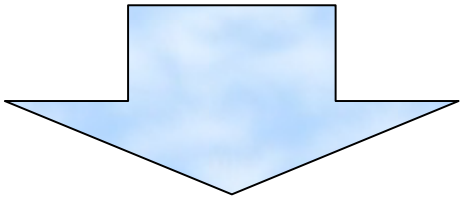
- Encrypt-and-MAC （E&M）
- MAC-then-Encrypt （MtE）
- Encrypt-then-MAC （EtM）



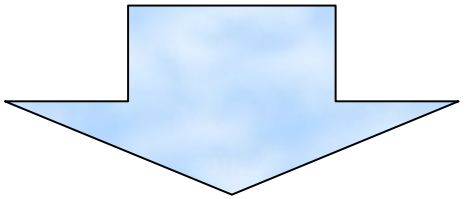
CryptoVerifにおいて，論文[BN2000]と同様の評価を得られた

まとめ

Authenticated Encryptionの一般的な構成に対するCryptoVerifにおける安全性の評価



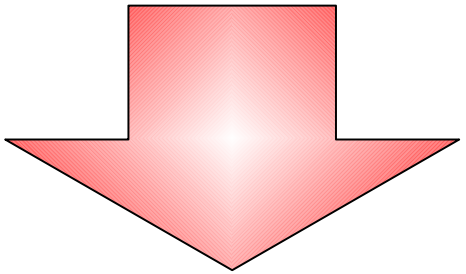
MACの SUF-CMA を CryptoVerifで扱うための定式化



安全性の評価が論文[BN2000]と一致

今後

- Signatureにおける強偽造不可能性(SUF-CMA)



- SignatureのSUF-CMAを利用したCryptoVerifを用いた安全性の評価