Automatic Proofs for Symmetric Encryption Modes

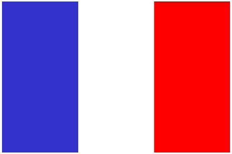
Martin Gagné[2] **Pascal Lafourcade**[1] Yassine Lakhnech[1]
Reihaneh Safavi-Naini[2]

[1] Université Grenoble 1, CNRS,VERIMAG, FRANCE

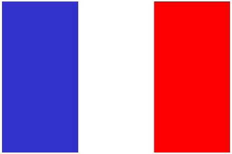
[2] Department of Computer Science, University of Calgary, Canada

ASIAN 2009, Seoul

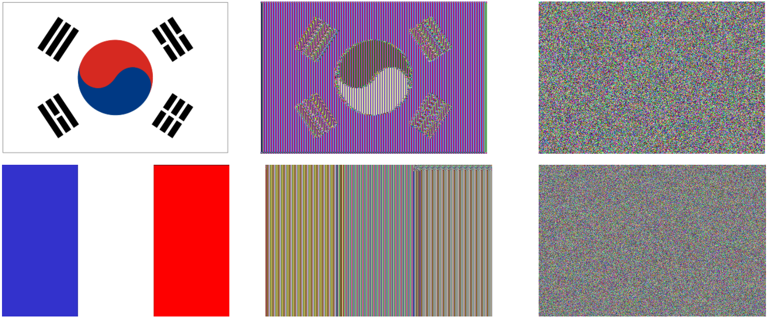
Indistinguishability and Symmetric Encryption Modes



Indistinguishability and Symmetric Encryption Modes



Indistinguishability and Symmetric Encryption Modes



ECB CBC, OFB ...

Block Cipher Modes

$$\text{PRP } \mathcal{E} \longrightarrow \boxed{\text{Encryption Mode}} \longrightarrow \text{ IND-CPA}$$

NIST standard

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher FeedBack mode (CFB)
- Output FeedBack (OFB), and
- Counter mode (CTR).

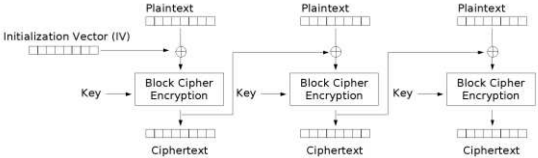
Others

DMC,CBC-MAC, IACBC, IAPM, XCB ,TMAC, HCTR, HCH, EME, EME*, PEP, OMAC, TET, CMC, GCM, EAX, XEX, TAE, TCH, TBC, CCM, ABL4

Block Cipher Modes

Example

Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

$$C_i = \mathcal{E}(P_i \oplus C_{i-1}), C_0 = IV$$

CBC and others

CBC	CTR	OFB	CFB
$IV \xleftarrow{\$} \mathcal{U};$	$IV \xleftarrow{\$} \mathcal{U};$	$IV \xleftarrow{\$} \mathcal{U};$	$IV \xleftarrow{\$} \mathcal{U};$
$z_1 := IV \oplus m_1;$	$z_1 := \mathcal{E}(IV + 1);$	$z_1 := \mathcal{E}(IV);$	$z_1 := \mathcal{E}(IV);$
$c_1 := \mathcal{E}(z_1);$	$c_1 := m_1 \oplus z_1;$	$c_1 := m_1 \oplus z_1;$	$c_1 := m_1 \oplus z_1;$
$z_2 := c_1 \oplus m_2;$	$z_2 := \mathcal{E}(IV + 2);$	$z_2 := \mathcal{E}(z_1);$	$z_2 := \mathcal{E}(c_1);$
$c_2 := \mathcal{E}(z_2);$	$c_2 := m_2 \oplus z_2;$	$c_2 := m_2 \oplus z_2;$	$c_2 := m_2 \oplus z_2;$
$z_3 := c_2 \oplus m_3;$	$z_3 := \mathcal{E}(IV + 3);$	$z_3 := \mathcal{E}(z_2);$	$z_3 := \mathcal{E}(c_2);$
$c_3 := \mathcal{E}(z_3);$	$c_3 := m_3 \oplus z_3;$	$c_3 := m_3 \oplus z_3;$	$c_3 := m_3 \oplus z_3;$

Outline

Outline

How to prove an encryption mode is IND-CPA ?

Our Approach

Automated method for proving correctness of encryption mode:

- Language: Generic Encryption Mode
- Predicates: F, E, Indis, Rcounter
- Hoare logic : 20 rules

RESULT:

If a Generic Encryption Mode $\mathcal{E}_M$ is correct according to our Hoare logic then $\mathcal{E}_M$ is IND-CPA.

Grammar

$$
\begin{aligned}
\mathsf{c} \quad ::= \quad & x \xleftarrow{\$} \mathcal{U} \mid x := \mathcal{E}(y) \mid x := y \oplus z \mid x := y \| z \mid \\
& x := y + 1 \mid c_1; c_2
\end{aligned}
$$

Generic Encryption Mode

Definition

A generic encryption mode M is represented by

$$\mathcal{E}_M(m_1|\ldots|m_p, c_0|\ldots|c_p) : \textbf{var } \vec{x}; \mathrm{c}$$

$$\begin{array}{l}
\mathcal{E}_{CBC}(m_1|m_2|m_3, IV|c_1|c_2|c_3) : \\
\textbf{var } z_1, z_2, z_3; \\
IV \xleftarrow{\$} \mathcal{U}; \\
z_1 := IV \oplus m_1; \\
c_1 := \mathcal{E}(z_1); \\
z_2 := c_1 \oplus m_2; \\
c_2 := \mathcal{E}(z_2); \\
z_3 := c_2 \oplus m_3; \\
c_3 := \mathcal{E}(z_3);
\end{array}$$

Predicates

$$\psi ::= \mathsf{Indis}(\nu x; V) \mid F(e) \mid \mathsf{E}(\mathcal{E}, e) \mid Rcounter(e)$$
$$\varphi ::= \mathsf{true} \mid \varphi \wedge \varphi \mid \psi,$$

$Indis(\nu x; V)$: The value of x is indistinguishable from a random value given the value of the variables in V.

$F(e)$: The value of e is indistinguishable from a random value that has not been used before.

$\mathsf{E}(\mathcal{E}, e)$: The probability that the value of e have been encrypted by $\mathcal{E}$ is negligible.

$RCounter(e)$: e is the most recent value of a monotone counter that started at a fresh random value.

How to generate $\mathsf{E}(\mathcal{E}, x)$?

Sampling a Random

(R1) $\{true\}\ x \xleftarrow{\$} \mathcal{U}\ \{F(x) \wedge \mathsf{Indis}(\nu x) \wedge \mathsf{E}(\mathcal{E}, x)\}$

How to generate $\mathsf{E}(\mathcal{E}, x)$?

Sampling a Random

(R1) $\{true\}\ x \xleftarrow{\$} \mathcal{U}\ \{F(x) \wedge \mathsf{Indis}(\nu x) \wedge \mathsf{E}(\mathcal{E}, x)\}$

PRP Encryption

(B1) $\{\mathsf{E}(\mathcal{E}, y)\}\ x := \mathcal{E}(y)\ \{F(x) \wedge \mathsf{Indis}(\nu x) \wedge \mathsf{E}(\mathcal{E}, x)\}$

How to generate $\mathsf{E}(\mathcal{E}, x)$?

Xor

(X4) $\{F(y)\}\ x := y \oplus z\ \{\mathsf{E}(\mathcal{E}, x)\}$ if $y \neq z$

How to generate $\mathsf{E}(\mathcal{E}, x)$?

Xor

(X4) $\{F(y)\}\ x := y \oplus z\ \{\mathsf{E}(\mathcal{E}, x)\}$ if $y \neq z$

Counter

- (I1) $\{F(y)\}\ x := y + 1\ \{RCounter(x) \wedge \mathsf{E}(\mathcal{E}, x)\}$
- (I2) $\{RCounter(y)\}\ x := y + 1\ \{RCounter(x) \wedge \mathsf{E}(E, x)\}$

20 Rules

$x \xleftarrow{\$} \mathcal{U}$	$x = y \| z$	$x := y+1$		$x := y \oplus z$	$x := \mathcal{E}(y)$
(R1)	(C1)	(I1)	(G1)	(X1)	(B1)
(R2)	(C2)	(I2)	(G2)	(X2)	(B2)
		(I3)	(G3)	(X3)	(B3)
			(G4)	(X4)	(B4)
					(B5)

Outline

How to prove that a Generic Encryption Mode is IND-CPA?

Theorem

Let $\mathcal{E}_M(m_1|\dots|m_p, c_0|\dots|c_p)$: **var** $\vec{x}$; c be a generic encryption mode, Then $\mathcal{E}_M$ is IND-CPA secure, if $\{\text{true}\}c \bigwedge_{i=0}^{i=p}\{\text{Indis}(\nu c_i; m_1, \dots, m_p, c_0, \dots, c_p)\}$ is valid.

Example: CBC

$$
\begin{array}{lll}
\multicolumn{3}{l}{\mathcal{E}_{CBC}(m_1|m_2|m_3, IV|c_1|c_2|c_3)} \\
\quad \textbf{var } IV, z_1, z_2, z_3; & & \\
\quad IV \xleftarrow{\$} \mathcal{U}; & \mathrm{Indis}(\nu IV; \mathrm{Var}) \wedge F(IV) & (\mathrm{R1}) \\
\quad z_1 := IV \oplus m_1; & \mathrm{Indis}(\nu IV; \mathrm{Var} - z_1) \wedge \mathrm{E}(\mathcal{E}, z_1, IV) & (\mathrm{X2})(\mathrm{X4}) \\
\quad c_1 := \mathcal{E}(z_1); & \mathrm{Indis}(\nu IV; \mathrm{Var} - z_1) & (\mathrm{B2}) \\
 & \wedge \mathrm{Indis}(\nu c_1; \mathrm{Var}) \wedge F(c_1) & (\mathrm{B1}) \\
\quad z_2 := c_1 \oplus m_2; & \mathrm{Indis}(\nu IV; \mathrm{Var} - z_1) & (\mathrm{G1}) \\
 & \wedge \mathrm{Indis}(\nu c_1; \mathrm{Var} - z_2) \wedge \mathrm{E}(\mathcal{E}, z_2) & (\mathrm{X2})(\mathrm{X4}) \\
\quad c_2 := \mathcal{E}(z_2); & \mathrm{Indis}(\nu IV; \mathrm{Var} - z_1) \wedge \mathrm{Indis}(\nu c_1; \mathrm{Var} - z_2) & (\mathrm{B2}) \\
 & \wedge Indis(\nu c_2; \mathrm{Var}) \wedge F(c_2) & (\mathrm{B1}) \\
\quad z_3 := c_2 \oplus m_3; & \mathrm{Indis}(\nu IV; \mathrm{Var} - z_1) \wedge \mathrm{Indis}(\nu c_1; \mathrm{Var} - z_2) & (\mathrm{G1}) \\
 & \wedge \mathrm{Indis}(\nu c_2; \mathrm{Var} - z_3) \wedge \mathrm{E}(\mathcal{E}, z_3) & (\mathrm{X2})(\mathrm{X4}) \\
\quad c_3 := \mathcal{E}(z_3); & \mathrm{Indis}(\nu IV; \mathrm{Var} - z_1) \wedge \mathrm{Indis}(\nu c_1; \mathrm{Var} - z_2) & (\mathrm{B2}) \\
 & \wedge Indis(\nu c_3; \mathrm{Var}) \wedge \mathrm{Indis}(\nu c_2; \mathrm{Var} - z_3) & (\mathrm{B1})
\end{array}
$$

Prototype

Implementation of a backward analysis in 1000 lines of Ocaml.

Examples

- CBC, FBC, OFB CFB are proved IND-CPA
- ECB and variants our tool fails: precondition is not true

All examples are immediate (less than one second)

Outline

Summary

- Generic Encryption Mode
- New predicats
- Hoare Logic for proving generic encryption mode IND-CPA
- Ocaml Prototype

Future Works

- Hybrid encryption
- using LSFR (Dual Encryption Mode)
- using Hash function
- using mathematics (GMC)
- IND-CCA ?
  Desai 2000: New Paradigms for Constructing Symmetric Encryption Schemes Secure against Chosen-Ciphertext Attack
- Considering : For loops

Thank you for your attention

Questions ?