Towards Automated Proofs for Asymmetric Encryption Schemes in the Random Oracle Model

J. Courant M. Daubignard C. Ene **Y. Lakhnech** P. Lafourcade

University of Grenoble (France), CNRS
VERIMAG

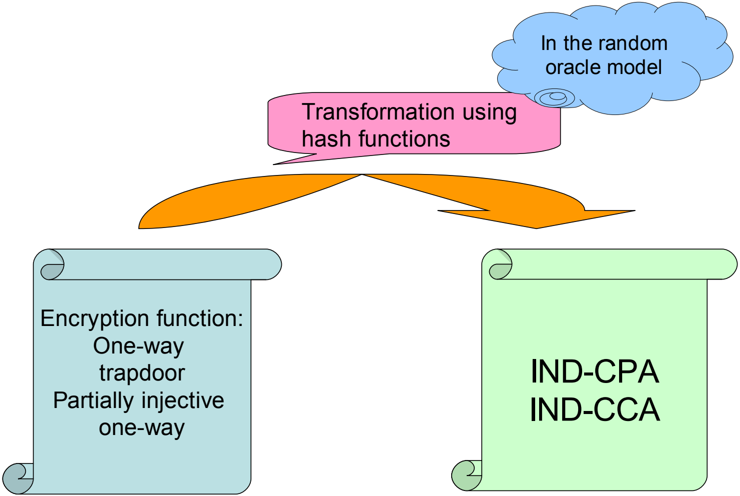
Cosyproofs'09 - Japan
Based on CCS'08

Introduction

Goal

A sound autmated proof method for IND-CCA security of generic encryption schemes.

Generic Encryption Schemes



Examples of Generic Encryption Schmes

- Bellare & Rogaway'93: $f(r)||\mathsf{in}_e \oplus G(r)||H(\mathsf{in}_e||r)$
- Zheng & Seberry'93: $f(r)||G(r) \oplus (\mathsf{in}_e||H(\mathsf{in}_e))$
- OAEP'94 (Bellare & Rogaway): $f(s||r \oplus H(s))$ where $s = \mathsf{in}_e 0^k \oplus G(r)$
- OAEP+'02 (Shoup): $f(s||r \oplus H(s))$ where $s = \mathsf{in}_e \oplus G(r)||H'(r||\mathsf{in}_e)$.
- Fujisaki & Okamoto'99: $\mathcal{E}((\mathsf{in}_e||r); H(\mathsf{in}_e||r))$. where $\mathcal{E}$ is IND-CPA.
- Pointcheval's transformer PKC'00 : $f(r||H(\mathsf{in}_e||s))||(\mathsf{in}_e||s) \oplus G(r)$
- REACT (Rapid enhanced asymmetric cryptosystem) 2001: $f(R||r)||\mathsf{in}_e \oplus G(R)||H(R||\mathsf{in}_e||f(R||r)||\mathsf{in}_e \oplus R)$

Security notions for Asymmetric Encryption

Adversarial goal

- OW: when the attacker finds a plaintext matching a ciphertext
- RR-C: when the attacker distinguishes a cipher from a random bit-string
- RR-P: when the attacker distinguishes the cipher of a given plaintext from that of a random one
- IND: when the attacker decides to which plaintext does a ciphertext correspond

Attack models

- CPA: chosen plaintext - no oracle
- CCA: chosen cipher text - decryption oracle

Plaintext awareness

Intuition

A condition that ensures that decryption oracle is not useful for the adversary.
The adversary cannot produce a meaningful ciphertext without knowing the corresponding plaintext.

- Introduced by Bellare & Rogaway with OAEP in a weaker form.
- Refined by Desai, Bellare, Rogaway and Pointcheval with a proof that : IND-CPA + PA $\rightarrow$ IND-CCA

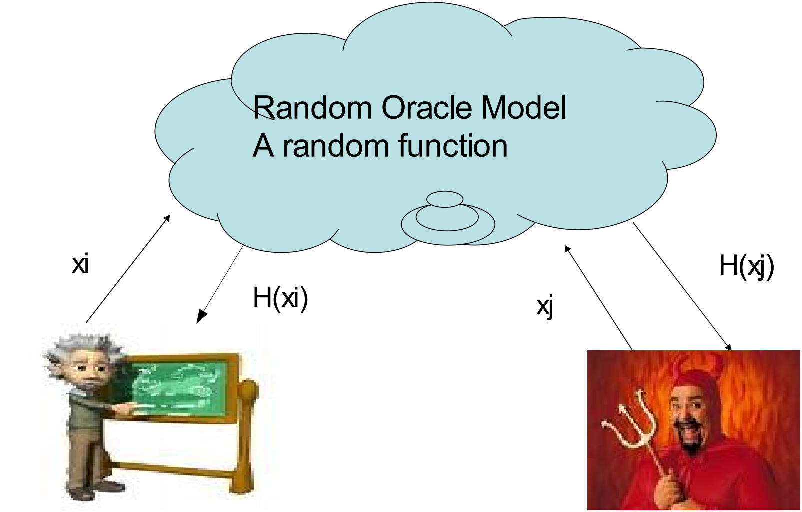
Relations Between Security Notions for PK Encryption

$$\begin{tikzcd}
\text{RR-C} \arrow[d, shift right=2] \\
\text{RR-P} \arrow[u, shift right=2, "/" marking] \arrow[r, shift right] & \text{IND-CPA} \arrow[l, shift right]
\end{tikzcd}$$

$$\left.\begin{array}{c}\text{IND-CPA}\\ + \\ \text{PA}\end{array}\right\}\ \text{IND-CCA}$$

The random oracle model

Hash functions are idealized: truly random functions.



Results

RR-X

An automated sound verification method for RR-P and RR-C for schemes based on:

- One-way trapdoor permutations (e.g. RSA)
- Injective partially one-way functions
- OW-PCA, hard to invert even in presence of a plaintext checking oracle

Plaintext awareness

An easy syntactic condition that ensures plaintext awareness.
RR-X + PA $\Rightarrow$ IND-CCA

Implementation and Applications

Implementation

- A CAML program, about 300 loc. for RR-X
- Trivial to implement.

- Bellare & Rogaway'93: $f(r)||\mathsf{in}_e \oplus G(r)||H(\mathsf{in}_e||r)$ - IND-CCA
- Zheng & Seberry'93: $f(r)||G(r) \oplus (\mathsf{in}_e||H(\mathsf{in}_e))$ - IND-CPA (and not IND-CCA as claimed in the paper)
- Pointcheval's transformer PKC'00 : $f(r||H(\mathsf{in}_e||s))||(\mathsf{in}_e||s) \oplus G(r)$ - IND-CCA
- REACT (Rapid enhanced asymmetric cryptosystem) 2001: $f(R||r)||\mathsf{in}_e \oplus G(R)||H(R||\mathsf{in}_e||f(R||r)||\mathsf{in}_e \oplus R)$ - IND-CCA
- Fujisaki & Okamoto'99: $\mathcal{E}((\mathsf{in}_e||r); H(\mathsf{in}_e||r))$. where $\mathcal{E}$ is IND-CPA - IND-CCA
- OAEP+: plaintext awareness.

Overview of the method for proving RR-X

- A simple probabilistic imperative programming language for describing the encryption and decryption algorithms
- An assertion language based on three atomic predicates:
  1. Indistinguishability w.r.t. a randomly sampled value
  2. One-way secrecy - values that cannot be easily computed by an adversary
  3. Book keeping of hashed values
- A Hoare-style calculus, axioms and rules, to establish triples of the form $\{\varphi\}\mathsf{c}\{\psi\}$

Remarks

- The calculus is compositional - easy to adapt for new primitives
- The axioms and rules can be interpreted forward or backward to obtain an automated analysis.

The language by an Example

Bellare-Rogaway'93:

$$f(r)||\mathsf{in}_e \oplus G(r)||H(\mathsf{in}_e||r)$$

Encryption $\mathcal{E}(\mathsf{in}_e, \mathsf{out}_e) =$
$r \xleftarrow{r} \mathcal{U}$;
$a = f(r)$;
$g := G(r)$;
$b := \mathsf{in}_e \oplus g$;
$t := \mathsf{in}_e||r$
$c := H(t)$;
$\mathsf{out}_e := a||b||c$

Decryption $\mathcal{D}(\mathsf{in}_d, \mathsf{out}_d)$
match in_d with $a^*||b^*||c^*$;
$r^* := f^{-1}(a^*)$;
$g^* := G(r^*)$;
$m^* := b^* \oplus g^*$;
$t^* := m^*||r^*$;
$h^* := H(t^*)$;
if $h^* = c^*$ then $\mathsf{out}_d := m^*$
else $\mathsf{out}_d := error$

The assertion Language

States facts about randomness of the values of the variables, their secrecy and the randomness of their hashed values.

$$\begin{array}{lcl} \psi & ::= & \mathsf{Indis}(\nu x; V_1; V_2) \mid \mathsf{WS}(x; V) \mid \mathsf{H}(H, e) \\ \varphi & ::= & \mathsf{true} \mid \psi \mid \varphi \wedge \varphi \end{array}$$

- $\mathsf{Indis}(\nu x; V_1; V_2)$: x is indistinguishable from a uniformly sampled value, even when the adversary is given the values in V_1 and the f-images of those in V_2.
- $\mathsf{WS}(x; V)$: the value of x is hard to compute given the values in V.
- $\mathsf{H}(H, e)$: the value of the expression e has not been queried to H.

Indistinguishability - Example

Let f be a one-way permutation.

- Distribution D1:
  - Uniformly sample x in $\{0,1\}^\eta$.
  - Return $x, H(x)$
- Distribution D2:
  - Uniformly sample x in $\{0,1\}^\eta$.
  - Uniformly sample x' in $\{0,1\}^\eta$.
  - Return $x', H(x)$
- D1 $\not\sim$ D2
-

$$x \xleftarrow{r} \mathcal{U};$$
$$y := H(x);$$
$$z := x$$

Indis($z; y$) does not hold

Indistinguishability - Example

Let f be a one-way permutation.

- Distribution D1:
  - Uniformly sample x in $\{0,1\}^\eta$.
  - Return $f(x), H(x)$
- Distribution D2:
  - Uniformly sample x in $\{0,1\}^\eta$.
  - Uniformly sample x' in $\{0,1\}^\eta$.
  - Return $f(x'), H(x)$
- D1 $\sim$ D2
-

$$x \xleftarrow{r} \mathcal{U};$$
$$y := H(x);$$
$$z := f(x)$$

Indis($z; y$) holds

The Calculus

- Standard rules: Sequential composition and consequence rule
- A set of axioms for each command - this provides a semantic characterization for one-way functions, hash functions in the ROM, etc....

- $\{true\}\ x \xleftarrow{r} \mathcal{U}\ \{\mathsf{Indis}(\nu x) \wedge \mathsf{H}(H, x)\}$,

The Calculus

- Standard rules: Sequential composition and consequence rule
- A set of axioms for each command - this provides a semantic characterization for one-way functions, hash functions in the ROM, etc....

- $\{true\}\ x \stackrel{r}{\leftarrow} \mathcal{U}\ \{\mathsf{Indis}(\nu x) \wedge \mathsf{H}(H, x)\}$,

- $\{\mathsf{Indis}(\nu y; V \cup \{y\}; \emptyset)\}\ x := f(y)\ \{\mathsf{WS}(y; V \cup \{x\})\}$
  if $y \notin V \cup \{x\}$

The Calculus

- Standard rules: Sequential composition and consequence rule
- A set of axioms for each command - this provides a semantic characterization for one-way functions, hash functions in the ROM, etc....

- $\{true\}\ x \stackrel{r}{\leftarrow} \mathcal{U}\ \{\mathsf{Indis}(\nu x) \wedge \mathsf{H}(H, x)\}$,
- $\{\mathsf{Indis}(\nu y; V \cup \{y\}; \emptyset)\}\ x := f(y)\ \{\mathsf{WS}(y; V \cup \{x\})\}$
  if $y \notin V \cup \{x\}$
- $\{\mathsf{WS}(y; V) \wedge \mathsf{H}(H, y)\}\ x := H(y)\ \{\mathsf{Indis}(\nu x; V \cup \{x\}; \emptyset)\}$
  etc...

Example

Bellare & Rogaway's 1993 generic construction.

$r \xleftarrow{r} \{0,1\}^{n_0}$ –

–

$a := f(r)$ –

–

$g := G(r)$ –

–

$e := \mathsf{in}_e \oplus g$ –

–

$d := \mathsf{in}_e || r$ –

–

$c := H(d)$ –

–

$\mathsf{out}_e := a||e||c$ – $\mathsf{Indis}(\nu\ \mathsf{out}_e; \mathsf{in}_e, \mathsf{out}_e, s)$

–

Example

Bellare & Rogaway's 1993 generic construction.

$r \xleftarrow{r} \{0,1\}^{n_0}$	–	$\mathsf{Indis}(\nu r) \wedge \mathsf{H}(G, r)$
	–	$\wedge\ \mathsf{H}(H, \mathsf{in}_e \Vert r)$
$a := f(r)$	–	
	–	
$g := G(r)$	–	
	–	
$e := \mathsf{in}_e \oplus g$	–	
	–	
$d := \mathsf{in}_e \Vert r$	–	
	–	
$c := H(d)$	–	
	–	
$\mathsf{out}_e := a \Vert e \Vert c$	–	$\mathsf{Indis}(\nu\ \mathsf{out}_e; \mathsf{in}_e, \mathsf{out}_e, s)$
	–	

Example

Bellare & Rogaway's 1993 generic construction.

$r \xleftarrow{r} \{0,1\}^{n_0}$	$-$	$\mathsf{Indis}(\nu r) \wedge \mathsf{H}(G, r)$
	$-$	$\wedge\ \mathsf{H}(H, \mathsf{in}_e \vert\vert r)$
$a := f(r)$	$-$	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{H}(G, r) \wedge$
	$-$	$\mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \vert\vert r)$
$g := G(r)$	$-$	
	$-$	
$e := \mathsf{in}_e \oplus g$	$-$	
	$-$	
$d := \mathsf{in}_e \vert\vert r$	$-$	
	$-$	
$c := H(d)$	$-$	
	$-$	
$\mathsf{out}_e := a \vert\vert e \vert\vert c$	$-$	$\mathsf{Indis}(\nu\ \mathsf{out}_e; \mathsf{in}_e, \mathsf{out}_e, s)$
	$-$	

Example

Bellare & Rogaway's 1993 generic construction.

$r \xleftarrow{r} \{0,1\}^{n_0}$	$-$	$\mathsf{Indis}(\nu r) \wedge \mathsf{H}(G, r)$
	$-$	$\wedge\, \mathsf{H}(H, \mathsf{in}_e \vert\vert r)$
$a := f(r)$	$-$	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{H}(G, r) \wedge$
	$-$	$\mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \vert\vert r)$
$g := G(r)$	$-$	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{Indis}(\nu g; \mathsf{Var} - r) \wedge$
	$-$	$\mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \vert\vert r)$
$e := \mathsf{in}_e \oplus g$	$-$	
	$-$	
$d := \mathsf{in}_e \vert\vert r$	$-$	
	$-$	
$c := H(d)$	$-$	
	$-$	
$\mathsf{out}_e := a \vert\vert e \vert\vert c$	$-$	$\mathsf{Indis}(\nu\, \mathsf{out}_e; \mathsf{in}_e, \mathsf{out}_e, s)$
	$-$	

Example

Bellare & Rogaway's 1993 generic construction.

$r \xleftarrow{r} \{0,1\}^{n_0}$	$-$	$\mathsf{Indis}(\nu r) \wedge \mathsf{H}(G, r)$
	$-$	$\wedge\, \mathsf{H}(H, \mathsf{in}_e \| r)$
$a := f(r)$	$-$	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{H}(G, r) \wedge$
	$-$	$\mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \| r)$
$g := G(r)$	$-$	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{Indis}(\nu g; \mathsf{Var} - r) \wedge$
	$-$	$\mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \| r)$
$e := \mathsf{in}_e \oplus g$	$-$	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{Indis}(\nu e; \mathsf{Var} - g, r) \wedge$
	$-$	$\wedge\, \mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \| r)$
$d := \mathsf{in}_e \| r$	$-$	
	$-$	
$c := H(d)$	$-$	
	$-$	
$\mathsf{out}_e := a \| e \| c$	$-$	$\mathsf{Indis}(\nu\, \mathsf{out}_e; \mathsf{in}_e, \mathsf{out}_e, s)$
	$-$	

Example

Bellare & Rogaway's 1993 generic construction.

$r \xleftarrow{r} \{0,1\}^{n_0}$	$-$	$\mathsf{Indis}(\nu r) \wedge \mathsf{H}(G, r)$
	$-$	$\wedge\, \mathsf{H}(H, \mathsf{in}_e \Vert r)$
$a := f(r)$	$-$	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{H}(G, r) \wedge$
	$-$	$\mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \Vert r)$
$g := G(r)$	$-$	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{Indis}(\nu g; \mathsf{Var} - r) \wedge$
	$-$	$\mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \Vert r)$
$e := \mathsf{in}_e \oplus g$	$-$	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{Indis}(\nu e; \mathsf{Var} - g, r) \wedge$
	$-$	$\wedge\, \mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \Vert r)$
$d := \mathsf{in}_e \Vert r$	$-$	$\mathsf{Indis}(\nu a; \mathsf{Var} - r, d) \wedge \mathsf{Indis}(\nu e; \mathsf{Var} - r, d, g) \wedge$
	$-$	$\mathsf{WS}(d; \mathsf{Var} - r, d) \wedge \mathsf{H}(H, d)$
$c := H(d)$	$-$	
	$-$	
$\mathsf{out}_e := a \Vert e \Vert c$	$-$	$\mathsf{Indis}(\nu\, \mathsf{out}_e; \mathsf{in}_e, \mathsf{out}_e, s)$
	$-$	

Example

Bellare & Rogaway's 1993 generic construction.

$r \xleftarrow{r} \{0,1\}^{n_0}$	–	$\mathsf{Indis}(\nu r) \wedge \mathsf{H}(G, r)$
	–	$\wedge\, \mathsf{H}(H, \mathsf{in}_e \vert\vert r)$
$a := f(r)$	–	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{H}(G, r) \wedge$
	–	$\mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \vert\vert r)$
$g := G(r)$	–	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{Indis}(\nu g; \mathsf{Var} - r) \wedge$
	–	$\mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \vert\vert r)$
$e := \mathsf{in}_e \oplus g$	–	$\mathsf{Indis}(\nu a; \mathsf{Var} - r) \wedge \mathsf{Indis}(\nu e; \mathsf{Var} - g, r) \wedge$
	–	$\wedge\, \mathsf{WS}(r; \mathsf{Var} - r) \wedge \mathsf{H}(H, \mathsf{in}_e \vert\vert r)$
$d := \mathsf{in}_e \vert\vert r$	–	$\mathsf{Indis}(\nu a; \mathsf{Var} - r, d) \wedge \mathsf{Indis}(\nu e; \mathsf{Var} - r, d, g) \wedge$
	–	$\mathsf{WS}(d; \mathsf{Var} - r, d) \wedge \mathsf{H}(H, d)$
$c := H(d)$	–	$\mathsf{Indis}(\nu a; \mathsf{Var} - r, d) \wedge \mathsf{Indis}(\nu e; \mathsf{Var} - r, d, g) \wedge$
	–	$\mathsf{Indis}(\nu c, \mathsf{Var} - r, d)$
$\mathsf{out}_e := a \vert\vert e \vert\vert c$	–	$\mathsf{Indis}(\nu\ \mathsf{out}_e; \mathsf{in}_e, \mathsf{out}_e, s)$
	–	

Soundness of the analysis

Proposition

Let X be distribution that is computable in polyt-time with oracle access to hash functions and given the function f.
Then, for every rule $\{\varphi\}c\{\varphi'\}$, we have

$$X \models \varphi \textit{ implies } [\![c]\!]X \models \varphi'.$$

Theorem

Let $GE = (\mathbb{F}, \mathcal{E}(\mathit{in}_e, \mathit{out}_e) : c, \mathcal{D}(\mathit{in}_d, \mathit{out}_d) : c')$ be an asymmetric encryption scheme.
If $\{\mathit{true}\}c\{\mathit{Indis}(\nu \mathit{out}_e; \mathit{in}_e, \mathit{out}_e, s; \emptyset)\}$ then $\mathcal{E}$ is RR-C.

Plaintext Syntactic Condition: The idea

Bellare & Rogaway: $f(r)||\mathsf{in}_e \oplus G(r)||H(\mathsf{in}_e||r)$.
Consider a variation: $f(r)||\mathsf{in}_e \oplus G(r)$.
One can prove, e.g. using our automatic analysis, that this variation is IND-CPA.
It is, however, easy to see that it is malleable, and hence, not IND-CCA. E.g,
$f(r)||\mathsf{in}_e \oplus G(r) \rightsquigarrow f(r)||1 \oplus G(r) = f(r)||(\mathsf{in}_e \oplus \bar{\mathsf{in}}_e) \oplus G(r)$.
Problem: nothing binds in_e and r.
Solution: add a hash of $\mathsf{in}_e||r$ to the cipher

In the paper, we prove (actually a more general result)

If the cipher includes as a substring the hash $H(\mathsf{in}_e||r)$ of the plaintext in_e and the random seed of the encryption algorithm r then the scheme is plaintext aware.

Concluding remarks

- An automated method for proving strong security properties of generic asymmetric encryption schemes in the ROM.
- A CAML-implementation is available.
- Proofs for:
  - Bellare & Rogaway '93
  - Pointcheval PKC'00
  - REACT...

Future work:

- Exact Security
- Reasoning about oracles and conditional reasoning:
  A logic for reasoning about

  $$A \rightarrow s \sim t \text{ and } A \rightarrow s : E$$

  Addition examples: OAEP, FDH, Hash ElGamal in the standard model and in the ROM

Related Work

- Game-based approach Bellare'04, Shoup'04, Halevi.
- CryptoVerif (B. Blanchet & D. Pointcheval'06) supports security proofs within the game-based, based on observational equivalence.
- Barthe et al.: Coq-formalization of the Game based approach.
- Hoare-style proof system by R. Corin and J. Den Hartog'06 for game-based cryptographic proofs.
- Datta et al. : A computationally sound compositional logic for key exchange protocols.
- R. Impagliazzo and B.M. Kapron, Logics for reasoning about cryptographic constructions, FOCS'03.