# Automated Verification of Asymmetric Encryption

V.C. Ngo  C. Ene  Y. Lakhnech

VERIMAG, Grenoble

ESORICS 2009

# Outline

- Formal Model
- Formal Non-Deducibility and Indistinguishability Relations (FNDR and FIR)
- Automated Verification Framework
- Application

# Objectives and Approach

Objectives

- Use symbolic (hence it is more simple and automated) proofs
- And enjoy computational soundness
  (formal indistinguishability implies computational indistinguishability)

A possible approach

- Represent encryption schemes as *frame* in cryptographic $\pi - calculus$
- Use formal relations to prove security property (IND-CPA in our case)

# Example

- Bellare-Rogaway encryption scheme:
  $\mathcal{E}(m,r) = f(r)||(m \oplus G(r))||H(m||r)$
- As a frame: $\phi(m) = \nu r.\{x_a = f(r), x_b = m \oplus G(r), x_c = H(m \parallel r)\}$
- Prove: $\phi(m); \nu r_1.r_2.r_3.\{x_a = r_1, x_b = r_2, x_c = r_3\}$(ideal frame) are formally indistinguishable
- Thus, $\forall m_1, m_2, \phi(m_1)$ and $\phi(m_2)$ are formally indistinguishable

# Terms, Frames, Equational Theory

- Represent messages(plain-text, cipher-text or parts,..) as formal notions like terms, frames
- A signature is a pair $\Sigma = (\mathcal{S}, \mathcal{F}), \mathcal{S}$, set of *sorts*, $\mathcal{F}$, set of function symbols with arity of the form $arity(f) = s_1 \times s_2 \times ... \times s_k \to s, k \geq 0$
- A term $T ::= x|a|f(T_1, T_2, ..., T_k), f \in \mathcal{F}$
- A substitution $\sigma = \{x_1 = T_1, ..., x_n = T_n\}$, is *well-sorted* if $\forall i, x_i$ and $T_i$ have the same sort. And $names(\sigma) = \bigcup_i names(T_i), var(\sigma) = \bigcup_i var(T_i)$
- A frame $\phi = \nu\tilde{n}.\sigma$ and $names(\phi) = \nu\tilde{n}$, $fvar(\phi) = var(\sigma) \backslash dom(\phi)$ the set of free variables in $\phi$

# Deducibility and Equational Theory

Deducibility

- $T$ is *deducible* from a frame $\phi$, written as $\phi \vdash T$ iff $\exists M$ s.t $M\phi =_E T$

An equational theory is an equivalence relation $E \subseteq \mathcal{T} \times \mathcal{T}$ (written as $=_E$) s.t.

- $T_1 =_E T_2$ implies $T_1\sigma =_E T_2\sigma$ for every $\sigma$
- $T_1 =_E T_2$ implies $T\{x = T_1\} =_E T\{x = T_2\}$ for every $\sigma, x$
- $T_1 =_E T_2$ implies $\tau(T_1) =_E \tau(T_2)$ for every $\sigma$

# Concrete semantics

Each frame $\phi = \nu\tilde{n}.\{x_1 = T_1, \ldots, x_k = T_k\}$ is given a concrete semantic, written as $[[\phi]]_A$ based on a *computational algebra A* which consists of

- a non-empty set of bit strings $[[s]]_A$ for each sort
- a function $f_A : [[s_1]]_A \times [[s_2]]_A \times \ldots \times [[s_k]]_A \rightarrow [[s]]_A$
- polynomial time algorithms to check the equality $(=_A, s)$ and to draw random elements from $x \xleftarrow{R} [[s]]_A$

# Distribution and Formal Indistinguishability

Distribution $\psi = [[\phi]]_A$ (of which the drawings $\hat{\phi} \leftarrow^R \psi$) are computed:

- for each name $a \in T_i$ draw a value $\hat{a} \leftarrow^R [[s]]_A$
- for each $x_i$ compute $\hat{T}_i$ recursively of the structure of the term $T_i$, $\widehat{f(T'_1, ..., T'_m)} = f_A(\hat{T}'_1, ..., \hat{T}'_m)$
- Two distributions are *indistinguishable*, written $(\psi_\eta) \approx (\psi'_\eta)$ iff for every ppt adversary $\mathcal{A}$, the *advantage* $Adv^{IND}(\mathcal{A}, \eta, \psi_\eta, \psi'_\eta) = P[\hat{\phi} \leftarrow \psi_\eta ; \mathcal{A}(\eta, \hat{\phi}) = 1] - P[\hat{\phi} \leftarrow \psi'_\eta ; \mathcal{A}(\eta, \hat{\phi}) = 1]$ is negligible
- $=_E$*-sound* iff $\forall T_1, T_2, T_1 =_E T_2$ implies that $P[\hat{e}_1, \hat{e}_2 \leftarrow^R [[T_1, T_2]]_{A_\eta} ; \hat{e}_1 \neq_{A_\eta} \hat{e}_2]$ is negligible

# Formal Non-Deducibility and Indistinguishability Relations

- The formal relation deducibility is not appropriate and to reason about what "can not be deduced" by the adversary
- For example, consider a one-way function $f$, $\nu a.b.\{x = f(a||b)\}$, it is very hard to say that what can be deduced
- Static equivalence sometimes does not imply computational soundness
- And we would like to preserve the soundness from an initial set and some closure rules
- It requires a new formal relation that is more flexible and finer, called FNDR and FIR(denoted $\not\models, \cong$), respectively

# Definition

A FNDR is a relation ($\subseteq \mathcal{F} \times \mathcal{T}$) w.r.t an equational theory $E$, written as $\not\models$ such that for every $(\phi, M) \in FNDR$

- if $\phi \not\models M$ then $\tau(\phi) \not\models \tau(M)$, for any renaming function $\tau$
- if $\phi \not\models M$ and $M =_E N$ then $\phi \not\models N$
- if $\phi \not\models M$ and $\phi =_E \phi'$ then $\phi' \not\models M$
- for any frame $\phi'$ s.t. $var(\phi') \subseteq dom(\phi)$ and $names(\phi') \cap names(\phi) = \emptyset$, $\phi \not\models M$ then $\phi'\phi \not\models M$

*Remark:* If two frames $\phi, \phi'$ s.t. $dom(\phi) \cap dom(\phi') = \emptyset$, $names(\phi) \cap names(\phi') = \emptyset, \phi \not\models M$, and $\phi' \not\models M$ then $\{\phi|\phi'\} \not\models M$

# Soundness and FNDR Generation

$\not\models -$*sound* iff for every $\phi$ and $M$ s.t. $\phi \not\models M$ implies for any polynomial-time adversary $\mathcal{A}$, the advantage

- $P[\hat{\phi}, \hat{e} \xleftarrow{R} [[\phi, M]]_{A_\eta} : \mathcal{A}(\eta, \hat{\phi}) =_{A_\eta} \hat{e}]$ is negligible

*Theorem*

$S_d \subseteq \mathcal{F} \times \mathcal{T}$, there exists a unique smallest set(denoted as $\langle S_d \rangle_{FNDR}$) such that:

- $S_d \subseteq \langle S_d \rangle_{FNDR}$
- is a FNDR
- is sound if $=_E$ and $S_d$ are sound

$$\langle S \rangle_{FNDR} := \left\{ \begin{array}{l} (\phi', M') \in \mathcal{F} \times \mathcal{T} \mid \exists \phi, \psi, M \text{ such that } (\phi, M) \in S_d, \\ \phi' =_E \tau(\psi\phi), M' =_E \tau(M) \text{ where} \\ names(\psi) \cap names(\phi) = \phi, var(\psi) \subseteq dom(\phi) \end{array} \right.$$

# Definition

A FIR is an equivalent relation ($\subseteq \mathcal{F} \times \mathcal{F}$) w.r.t an equational theory $E$, written as $\cong$ such that for every $(\phi_1, \phi_2) \in FIR$

- $\phi_1 \cong \phi_2$ if $dom(\phi_1) = dom(\phi_2)$
- for any frame $\phi$ s.t. $var(\phi) \subseteq dom(\phi_i)$, $names(\phi) \cap names(\phi_i) = \emptyset$, and $\phi_1 \cong \phi_2$ then $\phi\phi_1 \cong \phi\phi_2$
- if $\phi_1 =_E \phi_2$ then $\phi_1 \cong \phi_2$
- for any renaming $\tau$, $\tau(\phi) \cong \phi$

*Remark:* If four frames $\phi_1, \phi_2, \phi'_1, \phi'_2$ s.t. $dom(\phi_1) \cap dom(\phi_2) = \emptyset$, $dom(\phi'_1) \cap dom(\phi'_2) = \emptyset$, $names(\phi_1) \cap names(\phi_2) = \emptyset$, $names(\phi'_1) \cap names(\phi'_2) = \emptyset$, and $\phi_i \cong \phi'_i$, then $\{\phi_1 | \phi_2\} \cong \{\phi'_1 | \phi'_2\}$

# Soundness and FIR Generation

$\cong -$*sound* iff for $\phi_1$ and $\phi_2$ s.t. $\phi_1 \cong \phi_2$ implies for any polynomial-time adversary $\mathcal{A}$, the advantage

- $Adv^{IND}(\mathcal{A}, \eta, \phi_{1\eta}, \phi_{2\eta})$ is negligible

*Theorem*

$S_i \subset \mathcal{F} \times \mathcal{F}$, there exists a unique smallest set(denoted as $\langle S_i \rangle_{FIR}$) such that:

- $S_i \subseteq \langle S_i \rangle_{FIR}$
- is a FIR
- is sound if $=_E$ and $S_i$ are sound

# FIR Generation

$\langle S_i \rangle_{FIR}$ can be generated in the following way. Let

$$S' := \left\{ \begin{array}{l} (\phi', \phi'') \in \mathcal{F} \times \mathcal{F} \,|\, \phi' = \phi\{\phi'_1|\ldots|\phi'_n\}, \phi'' = \phi\{\phi''_1|\ldots|\phi''_n\} \\ \text{such that } names(\phi) = \emptyset \, \forall i = 1, \ldots, n, \\ (\phi'_i, \phi''_i) \in S_i, \text{ or } (\phi''_i, \phi'_i) \in S_i, \text{ or } \phi''_i =_E \tau_i(\phi'_i) \end{array} \right.$$

Then $\langle S_i \rangle_{FIR}$ is the transitive closure of $S'$

# Verification Framework

A general verification framework consists of

- basis axioms for encryption primitives(Radom, Xor, Concatenation, Hash, One-way functions)
- the generation of FNDR and FIR

# Basis Axioms

Random

- (RD1) $\nu a.\emptyset \not\models a$
- (RE1) $\nu a.\{x = a\} \cong \nu r.\{x = r\}$

Xor

- (XD1) $\nu\tilde{n}.\sigma \not\models M$, then $\nu\tilde{n}.a.\{\sigma, x = a \oplus M\} \not\models M$
- (XE1) $\nu\tilde{n}.a.\{\sigma, x = a \oplus M\} \cong \nu\tilde{n}.a.\{\sigma, x = a\}$

Concatenation

- (CD1) $\nu\tilde{n}.\sigma \not\models M$, then $\nu\tilde{n}.\sigma \not\models M||M'$
- (CE1) $\nu a.b.\{x = a||b\} \cong \nu r.\{x = r\}$

# Basis Axioms

Hash function

- (HD1) $\nu\tilde{n}.\sigma \not\models M$, $H(T) \notin st(\sigma)$ then $\nu\tilde{n}.\{\sigma, x = H(M)\} \not\models M$
- (HE1) $\nu\tilde{n}.\sigma \not\models M$, $H(T) \notin st(\sigma)$ then $\nu\tilde{n}.\{\sigma, x = H(M)\} \cong \nu\tilde{n}.r.\{\sigma, x = r\}$

One-way function

- (OD1) $\nu a.\{x = f(a)\} \not\models a$
- (OE1) $\nu a.\{x = f(a)\} \cong \nu r.\{x = r\}$

# Verification Framework

It works as following

- take representation frame as input. Generate the initial set $(S_d, S_i)$ based on the set of basis axioms above
- construct a pair of FNDR and FIR $(\langle S_d \rangle_{FNDR}, \langle S_i \rangle_{FIR})$ according to the generation theorems
- perform two steps above recursively of the structure of the representation frame
- if a pair of the representation frame and the ideal frame is in $\langle S_i \rangle_{FIR}$ then output “yes”

# B-R's Frame and Proof

- $\phi_{br}(m) = \nu r.\{x_1 = f(r), x_2 = G(r) \oplus m, x_3 = H(m||r)\}$, where $m$ is the adaptive plaintext that an adversary has chosen
- proof. $\phi_{br}(m) \cong \nu a.b.c.\{x_1 = a, x_2 = b, x_3 = c\}$

The FNDR and FIR are generated from the B-R's frame as following.
Denote $\phi_1 = \nu r.\{x_1 = f(r)\}, \phi_2 = \nu r.\{x_1 = f(r), x_2 = G(r)\}$,
$\phi_2' = \nu r.\{x_1 = f(r), x_2 = G(r) \oplus m\}$, and $\phi_3 = \nu r.\{x_1 = f(r), x_2 = G(r) \oplus m, x_3 = H(m||r)\}$

# B-R's FNDR

- $\nu r.\emptyset \not\models r$ (RD1)
- $\nu r.\{x_1 = f(r)\} \not\models r$ (OD1)
- $\nu r.\{x_1 = f(r), x_2 = G(r)\} \not\models r$ (HD1)
- $\nu r.\{x_1 = f(r), x_2 = G(r) \oplus m\} \not\models r$ (Generation rule) $\phi' = \{x_1 = x_1, x_2 = x_2 \oplus m\}$ $\phi'\phi_2 \not\models r$
- $\nu r.\{x_1 = f(r), x_2 = G(r) \oplus m\} \not\models m||r$ (CD1)
- $\nu r.\{x_1 = f(r), x_2 = G(r) \oplus m, x_3 = H(m||r)\} \not\models m||r$ (HD1)

# B-R's FIR

- $\nu r.\{x_1 = f(r)\} \cong \nu a.\{x_1 = a\}$ (OE1)
- $\nu r.b.\{x_1 = f(r), x_2 = b\} \cong \nu a.\{x_1 = a, x_2 = b\}$ (Generation rule) $\phi' = \nu b.\{x_1 = x_1, x_2 = b\}$
  $\phi'\phi_1 \cong \phi'\nu a.\{x_1 = a\}$
- $\nu r.\{x_1 = f(r), x_2 = G(r)\} \cong \nu r.b.\{x_1 = f(r), x_2 = b\}$ (HE1)
- $\nu r.\{x_1 = f(r), x_2 = G(r)\} \cong \nu r.b.\{x_1 = a, x_2 = b\}$ (Transitive rule)
- $\nu a.b.\{x_1 = a, x_2 = b\} \cong \nu a.b.\{x_1 = a, x_2 = b \oplus m\}$ (XE1)
- $\nu r.\{x_1 = f(r), x_2 = G(r) \oplus m\} \cong \nu a.b.\{x_1 = a, x_2 = b \oplus m\}$ (Generation rule)
  $\phi' = \{x_1 = x_1, x_2 = x_2 \oplus m\}$
  $\phi'\phi_2 \cong \phi'\nu a.b.\{x_1 = a, x_2 = b\}$
- $\nu r.\{x_1 = f(r), x_2 = G(r) \oplus m\} \cong \nu a.b.\{x_1 = a, x_2 = b\}$ (Transitive rule)

# B-R's FIR

- $\phi_3 \cong \nu r.c.\{x_1 = f(r), x_2 = G(r) \oplus m, x_3 = c\}$ (HE1)
- $\nu r.c.\{x_1 = f(r), x_2 = G(r) \oplus m, x_3 = c\} \cong \nu a.b.c.\{x_1 = a, x_2 = b, x_3 = c\}$ (Generation rule)
  $\phi' = \nu c.\{x_1 = x_1, x_2 = x_2, x_3 = c\}$
  $\phi' \phi'_2 \cong \phi' \nu a.b.\{x_1 = a, x_2 = b\}$
- $\phi_3 \cong \nu a.b.c.\{x_1 = a, x_2 = b, x_3 = c\}$ (Transitive rule)

Thank you!