Relational verification of probabilistic programs

Gilles Barthe
IMDEA Software Institute, Madrid, Spain

October 18, 2015

Probabilistic programs

$\mathcal{C}$	::=	skip	skip
	|	$\mathcal{V} \leftarrow \mathcal{E}$	assignment
	|	$\mathcal{V} \xleftarrow{\$} \mathcal{D}$	random sampling
	|	$\mathcal{C};\ \mathcal{C}$	sequence
	|	if $\mathcal{E}$ then $\mathcal{C}$ else $\mathcal{C}$	conditional
	|	while $\mathcal{E}$ do $\mathcal{C}$	while loop
	|	$\mathcal{V} \leftarrow \mathcal{P}(\mathcal{E}, \ldots, \mathcal{E})$	procedure call

Can be used to model

- Randomized algorithms
- Cryptography
- Privacy
- Networks
- Etc

Relational properties

- Stochastic dominance: let A be an ordered set.

μ *stochastically dominates* μ', written $\mu \geq_{sd} \mu'$, if for all $a \in A$,

$$\Pr_{x \sim \mu}[x \geq a] \geq \Pr_{x' \sim \mu'}\left[x' \geq a\right].$$

- Convergence:

μ_i and μ'_i converge iff their SD tends to 0

$$\lim_{i \to \infty} \left(\max_{Y \subseteq A} \left| \Pr_{x \sim \mu_i}[x \in Y] - \Pr_{x' \sim \mu'_i}\left[x' \in Y\right] \right| \right) = 0.$$

- Differential privacy

μ and μ' are ϵ, δ-differentially private iff

$$\max_{Y \subseteq A} \left(\Pr_{x \sim \mu}[x \in Y] - \exp(\epsilon) \Pr_{x' \sim \mu'}\left[x' \in Y\right] \right) \leq \delta.$$

More relational properties

- Continuity
- Probabilistic non-interference
- Computational indistinguishability
- Nash equilibria
- Truthfulness

Also: program equivalence, program improvement, etc

Probabilistic couplings

In the talk we always consider discrete sub-distributions.

- Frechet class of $\mu_1 \in \hat{\mathcal{D}}(A)$ and $\mu_2 \in \hat{\mathcal{D}}(B)$ is defined as:

$$\mathcal{F}_{\mu_1,\mu_2} = \left\{ \mu \in \hat{\mathcal{D}}(A \times B) \mid \pi_1(\mu) = \mu_1 \wedge \pi_2(\mu) = \mu_2 \right\}$$

  Elements of $\mathcal{F}_{\mu_1,\mu_2}$ are called couplings.
- The lifting $R^{\#}$ of a relation $R \subseteq A \times B$ is defined as:

$$\mu_1 R^{\#} \mu_2 \text{ iff } \exists \mu \in \mathcal{F}_{\mu_1,\mu_2}.\ \Pr_{y \sim \mu}[y \notin R] = 0$$

Application of probabilistic couplings

- Stochastic dominance:
  $\mu \geq_{sd} \mu'$ iff $\mu \geq^{\#} \mu'$
- Convergence:
  μ_i and μ'_i converge iff there exist P_i such that:
  - $\lim_{i \to \infty} \Pr_{x \sim \mu_i}[x \notin P_i] = 0$
  - $\mu_i \; R_i^{\#} \; \mu'_i$, where $R_i \; x \; y = P_i \; x \to x = y$
- Differential privacy: requires a more general notion of lifting

Convergence of random walks

```
pos := start; H := start::[]; i := 0;
while i<k do
  b := ${0,1};
  if b then pos++ else pos-- fi;
  H := pos :: H;
  i := i + 1;
end
return pos
```

- Two executions from start and start+2n converge.
- Coupling: the walks mirror each other until they meet
- Convergence: the probability that walk reaches start+n tends to one

A logic for probabilistic couplings

- Judgments
$$\models \{P\}\ c_1\ \sim\ c_2\ \{Q\}$$
- P and Q are relations on states
- $\models \{P\}\ c_1\ \sim\ c_2\ \{Q\}$ is valid iff for all $m_1, m_2 \in \mathcal{M}$, $P\ m_1\ m_2$ implies $Q^\sharp\ (\llbracket c_1 \rrbracket\ m_1)\ (\llbracket c_2 \rrbracket\ m_2)$
- If $\models \{P\}\ c_1\ \sim\ c_2\ \{A\langle 1\rangle \Rightarrow B\langle 2\rangle\}$ is valid then for all $m_1, m_2 \in \mathcal{M}$ s.t. $P\ m_1\ m_2$, we have
$$\Pr_{c_1,m_1}[A] \leq \Pr_{c_2,m_2}[B]$$
- If $\models \{P\}\ c_1\ \sim\ c_2\ \{A\langle 1\rangle \Rightarrow x\langle 1\rangle = x\langle 2\rangle\}$ is valid then for all $m_1, m_2 \in \mathcal{M}$ s.t. $P\ m_1\ m_2$ and B depends only on x, we have
$$|\Pr_{c_1,m_1}[B] - \Pr_{c_2,m_2}[B]| \leq \Pr_{c_1,m_1}[A]$$

pRHL rules: conditionals

$$\frac{P \;\Rightarrow\; e\langle 1\rangle = e'\langle 2\rangle \qquad \vDash \{P \wedge e\langle 1\rangle\}\ c_1 \sim c_1'\ \{Q\} \qquad \vDash \{P \wedge \neg e\langle 1\rangle\}\ c_2 \sim c_2'\ \{Q\}}{\vDash \{P\}\ \text{if } e \text{ then } c_1 \text{ else } c_2 \sim \text{if } e' \text{ then } c_1' \text{ else } c_2'\ \{Q\}}$$

$$\frac{\vDash \{P \wedge e\langle 1\rangle\}\ c_1 \sim c\ \{Q\} \qquad \vDash \{P \wedge \neg e\langle 1\rangle\}\ c_2 \sim c\ \{Q\}}{\vDash \{P\}\ \text{if } e \text{ then } c_1 \text{ else } c_2 \sim c\ \{Q\}}$$

pRHL rules: loops

$$\frac{\begin{array}{c} P \;\Rightarrow\; e\langle 1\rangle = e'\langle 2\rangle \\ \vDash \{P \wedge e\langle 1\rangle\}\ c\ \sim\ c'\ \{P\} \end{array}}{\vDash \{P\}\ \text{while } e \text{ do } c\ \sim\ \text{while } e' \text{ do } c'\ \{P \wedge \neg e\langle 1\rangle\}}$$

$$\frac{\vDash \{P \wedge e\langle 1\rangle\}\ c\ \sim\ \text{skip}\ \{P\} \qquad \text{while } e \text{ do } c \text{ lossless}}{\vDash \{P\}\ \text{while } e \text{ do } c\ \sim\ \text{skip}\ \{P\}}$$

Program transformation rules to alleviate incompleteness.

pRHL rules: samplings

$$\frac{h \text{ is 1-1 and } \forall a,\ \mu(a) = \mu'(h(a))}{\vDash \{\forall v \in \text{supp } \mu, Q\{v/x\langle 1\rangle\}\{h\, v/x\langle 2\rangle\}\}\ x \xleftarrow{\$} \mu \sim x \xleftarrow{\$} \mu'\ \{Q\}}$$

$$\frac{}{\vDash \{\forall v \in \text{supp } \mu, Q\{v/x\langle 1\rangle\}\}\ x \xleftarrow{\$} \mu \sim c\ \{Q\}}$$

Fall back on program semantics to alleviate incompleteness

Convergence revisited

Let Φ be $\mathrm{start}\langle 1\rangle + 2n = \mathrm{start}\langle 2\rangle$

$$\vDash \{\Phi\}\ RW\ \sim\ RW\ \{(\mathrm{start}\langle 1\rangle + n \in \mathrm{H}\langle 1\rangle) \Rightarrow \mathrm{pos}\langle 1\rangle = \mathrm{pos}\langle 2\rangle\}\,.$$

Invariant for the WHILE rule:

$$(\mathrm{pos}\langle 1\rangle \neq \mathrm{pos}\langle 2\rangle \Rightarrow \mathrm{pos}\langle 1\rangle - \mathrm{start}\langle 1\rangle = \mathrm{start}\langle 2\rangle - \mathrm{pos}\langle 2\rangle) \wedge$$
$$(\mathrm{start}\langle 1\rangle + n \in \mathrm{H}\langle 1\rangle) \Rightarrow \mathrm{pos}\langle 1\rangle = \mathrm{pos}\langle 2\rangle).$$

EasyCrypt

Next generation program verification environment

- full-fledged proof assistant (inspired from SSReflect)
- backend to SMT solvers and CAS
- native embedding of rich probabilistic language
- probabilistic Relational Hoare Logic for couplings
- probabilistic Hoare Logic for bounding probabilities

Modern cryptography

Shannon ’49

- Mathematical proof of security
- Perfect secrecy is impossible

Diffie & Hellman ’76

Goldwasser & Micali’82

Yao’82

- Computational security
- Asymptotic guarantees

PPT adversary has negligible advantage

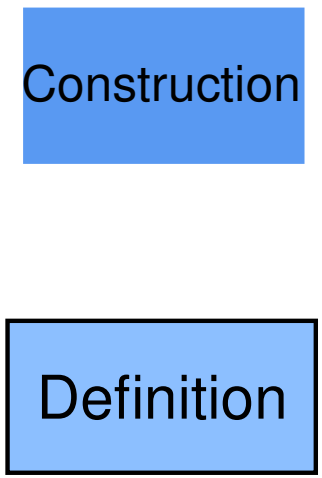
Bellare & Rogaway ’94

- Concrete bounds

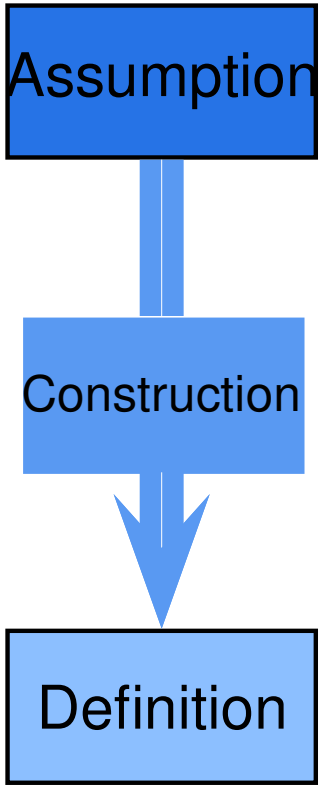
Aversary advantage to win in time t is $\leq p$

Pillars of provable security: Definitions

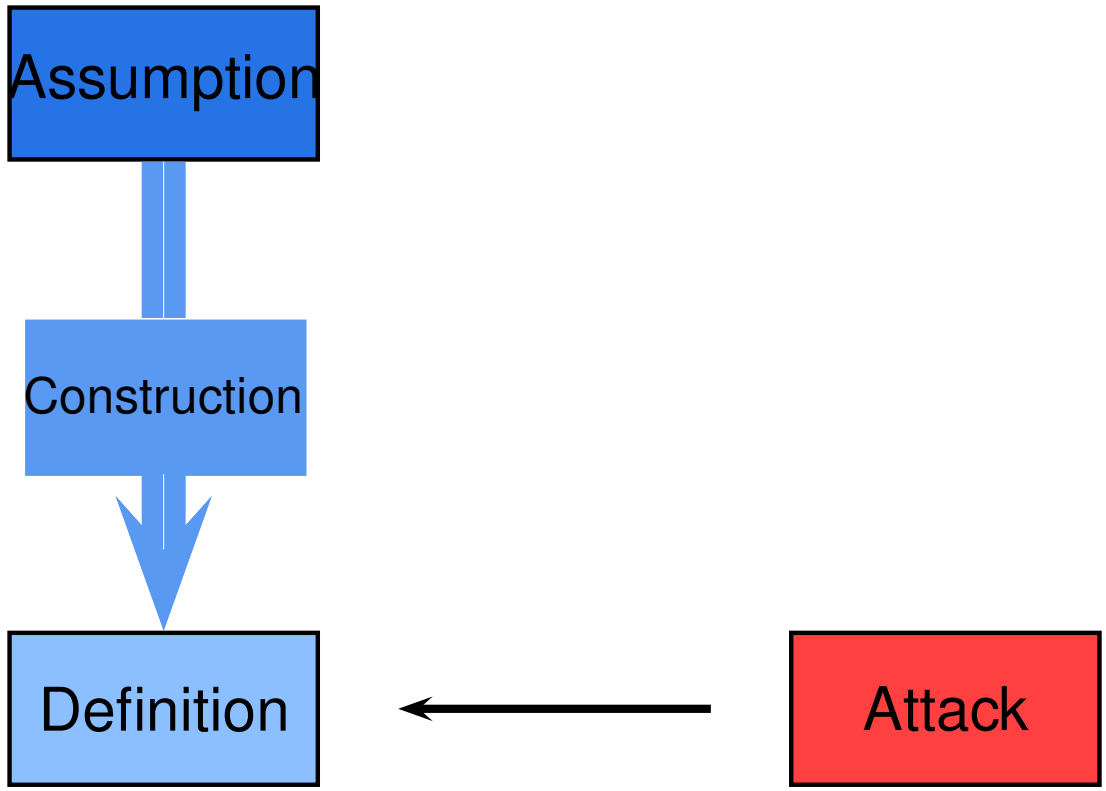
Pillars of provable security: Constructions



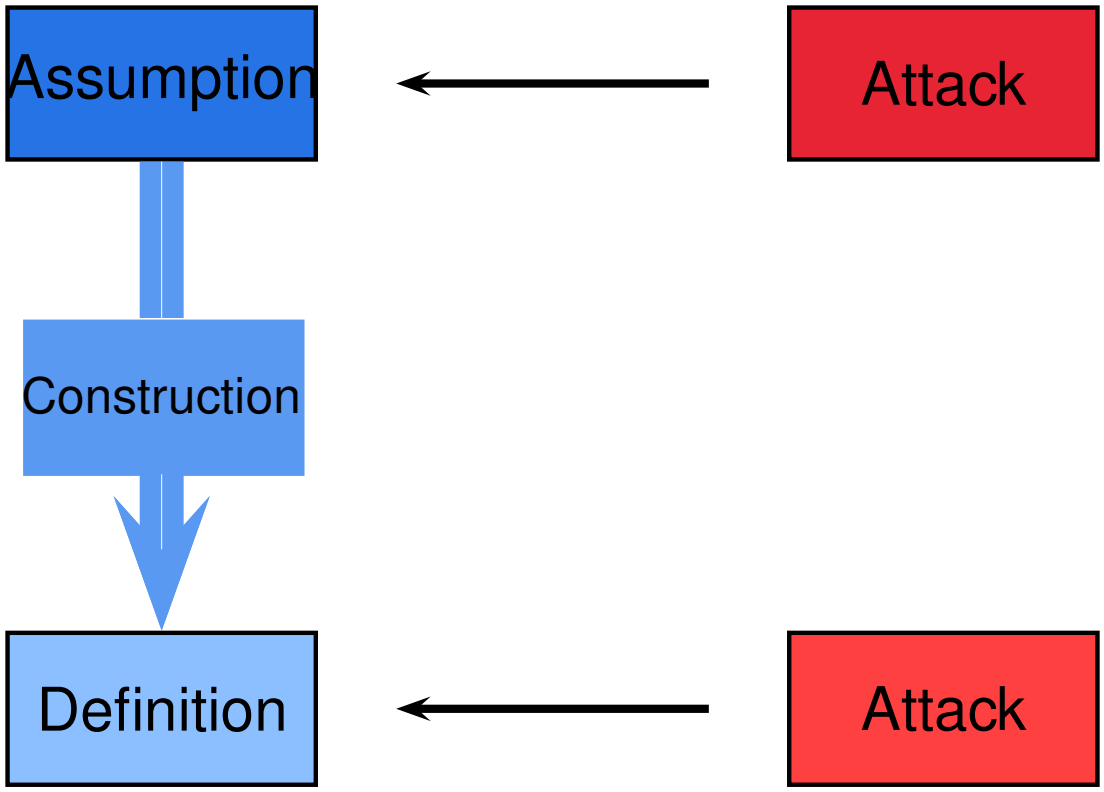
Pillars of provable security: Proofs



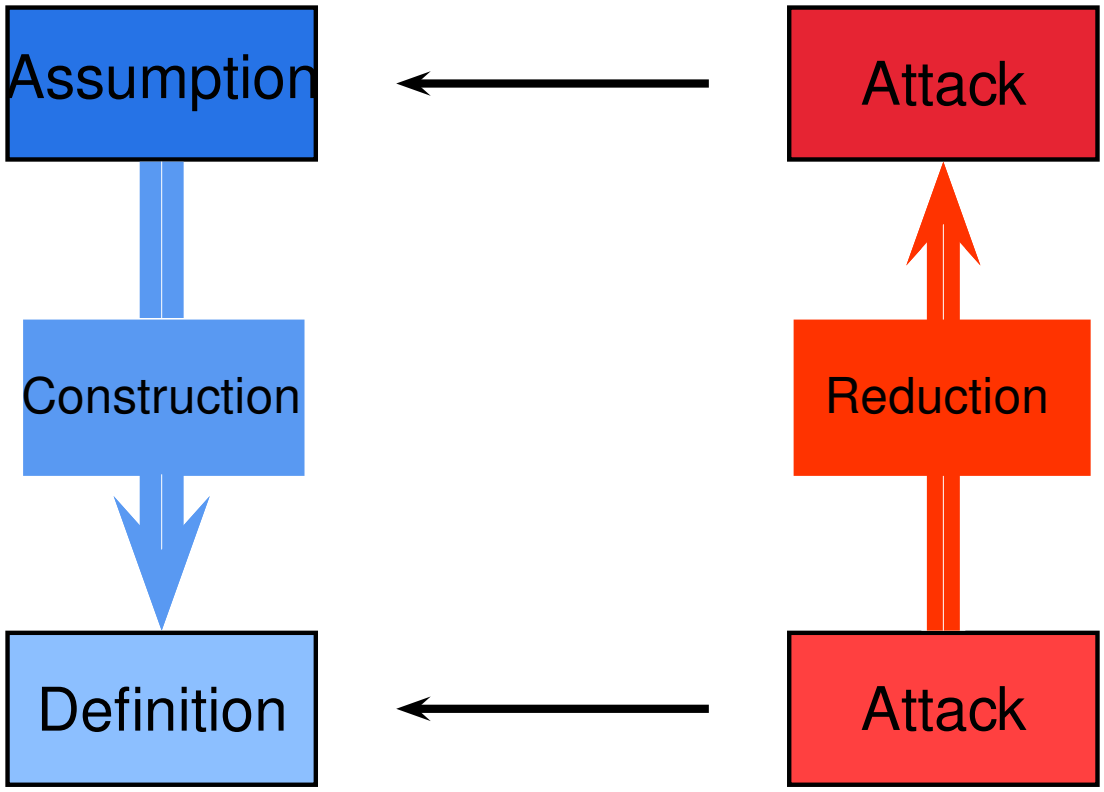
Pillars of provable security: Proofs



Pillars of provable security: Proofs



Pillars of provable security: Proofs



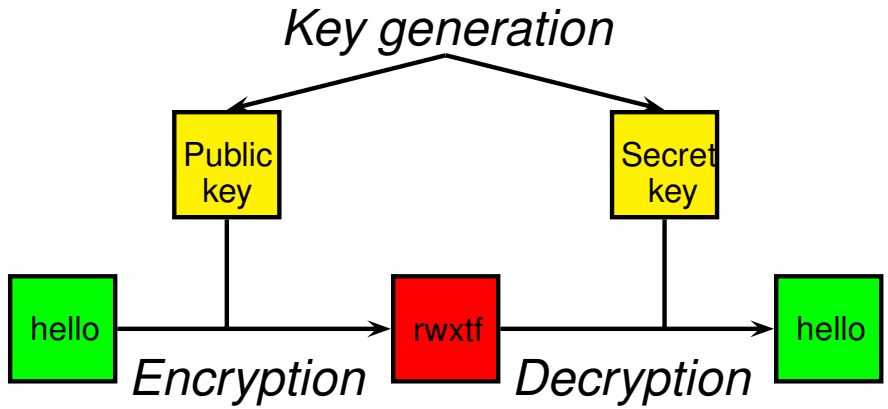
Public-key encryption

Algorithms $(\mathcal{K}, \mathcal{E}_{pk}, \mathcal{D}_{sk})$

- $\mathcal{E}$ probabilistic
- $\mathcal{D}$ deterministic and partial

If (sk, pk) is a valid key pair,

$$\mathcal{D}_{sk}(\mathcal{E}_{pk}(m)) = m$$

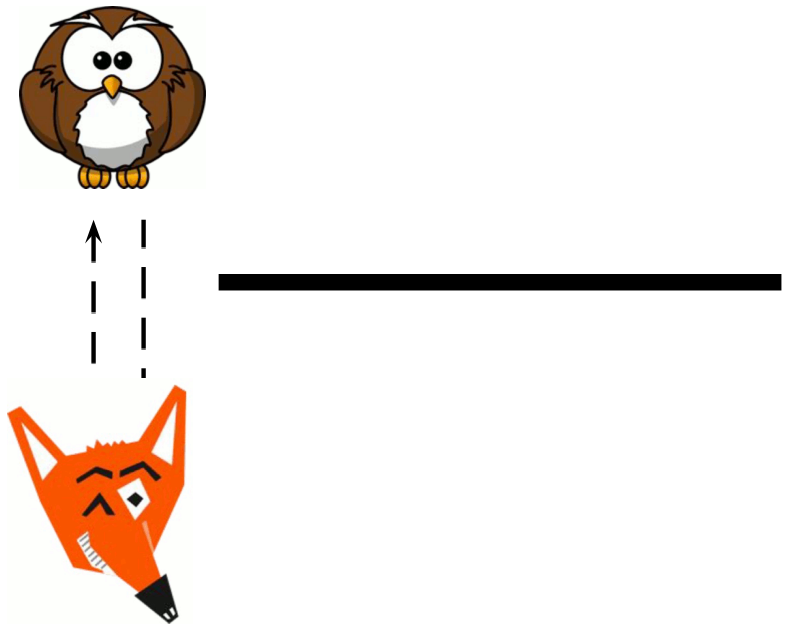


Indistinguishability

Game IND-CCA($\mathcal{A}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0, 1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$

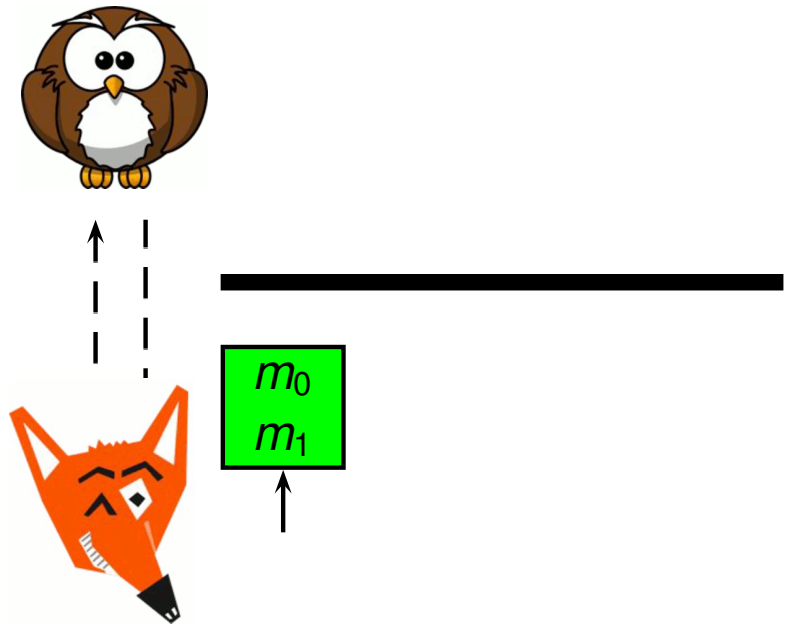
Indistinguishability

Game IND-CCA($\mathcal{A}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0,1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$



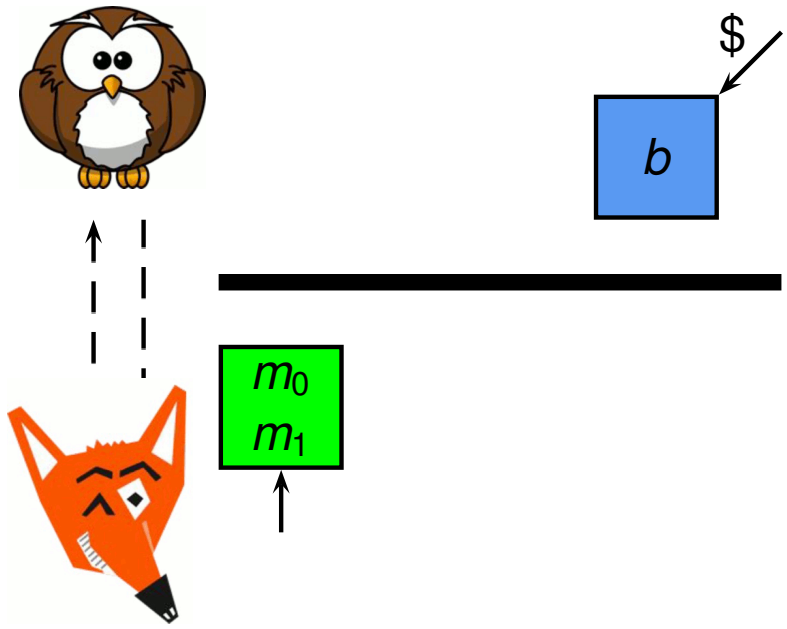
Indistinguishability

Game IND-CCA($\mathcal{A}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0, 1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$



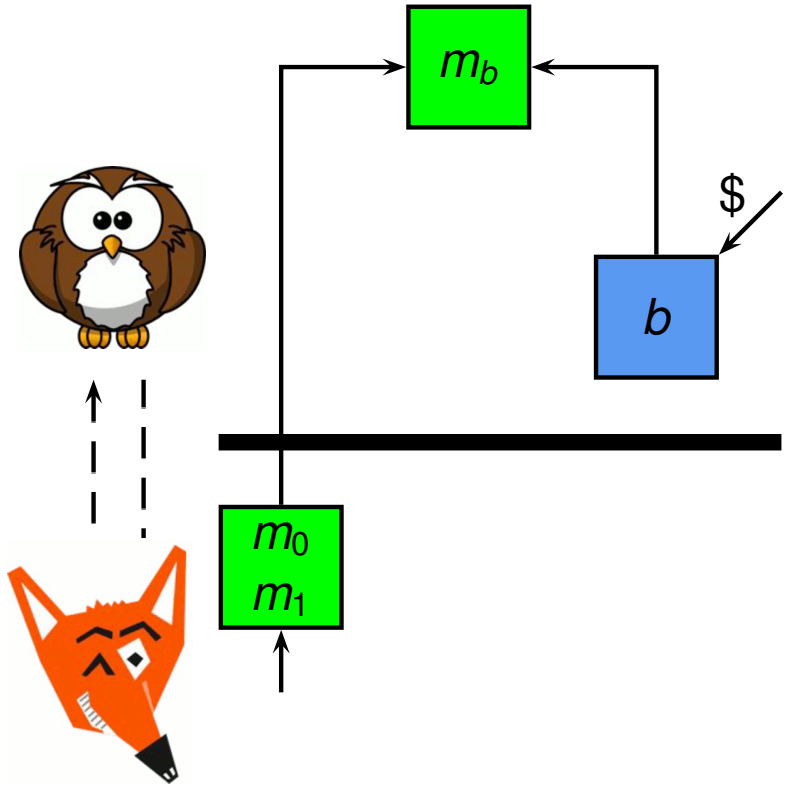
Indistinguishability

Game IND-CCA($\mathcal{A}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0,1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$



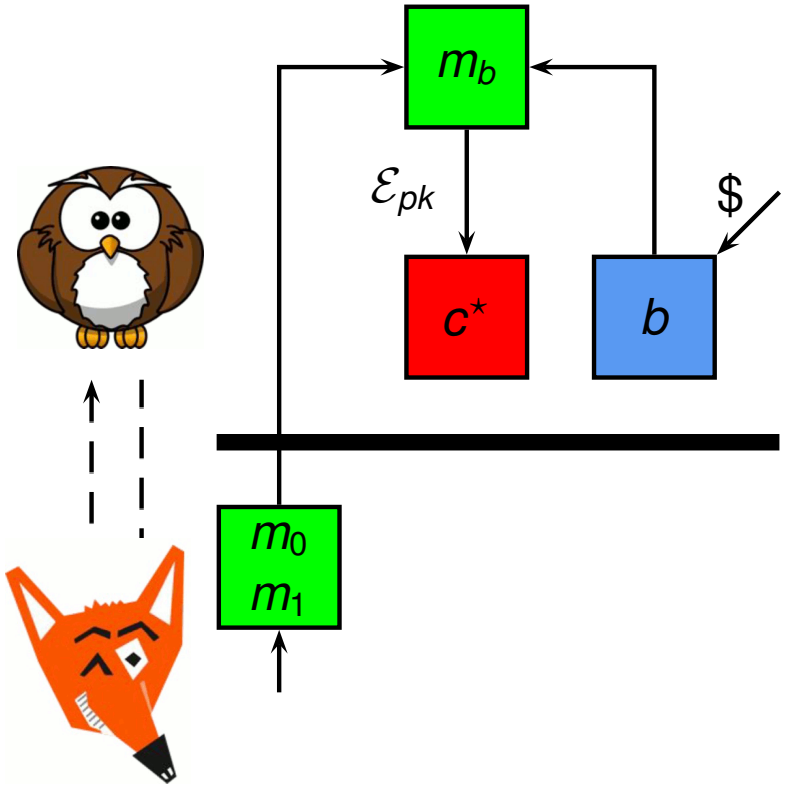
Indistinguishability

Game IND-CCA($\mathcal{A}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0,1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$



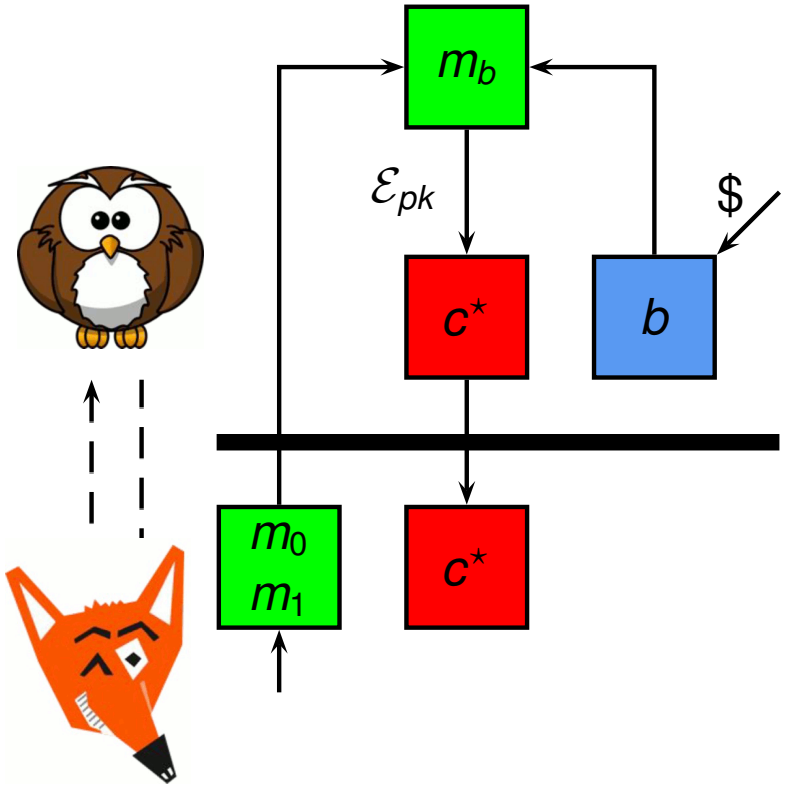
Indistinguishability

Game IND-CCA($\mathcal{A}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0,1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$



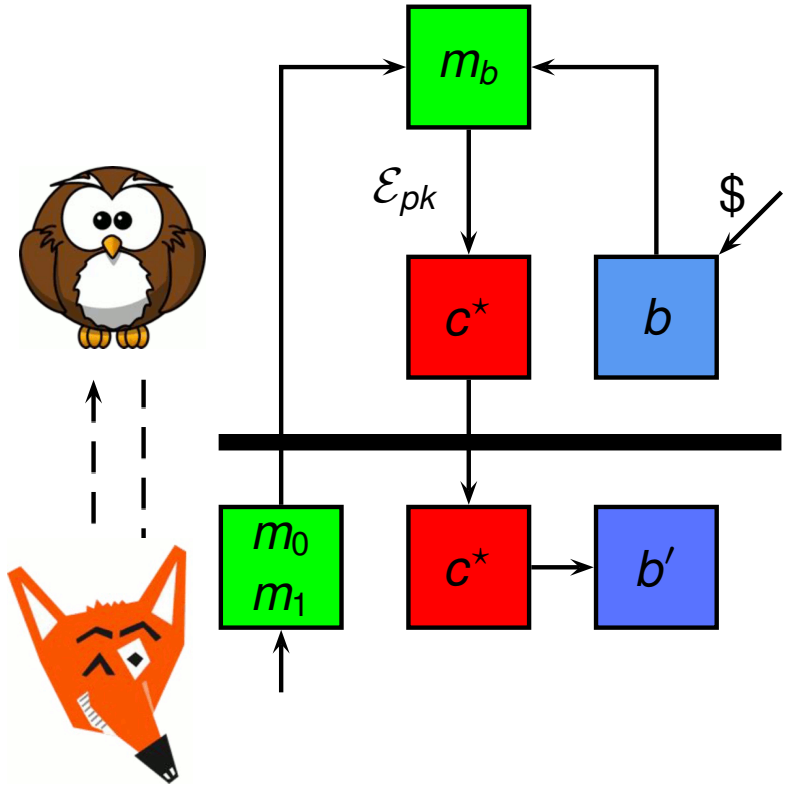
Indistinguishability

Game IND-CCA($\mathcal{A}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0,1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$



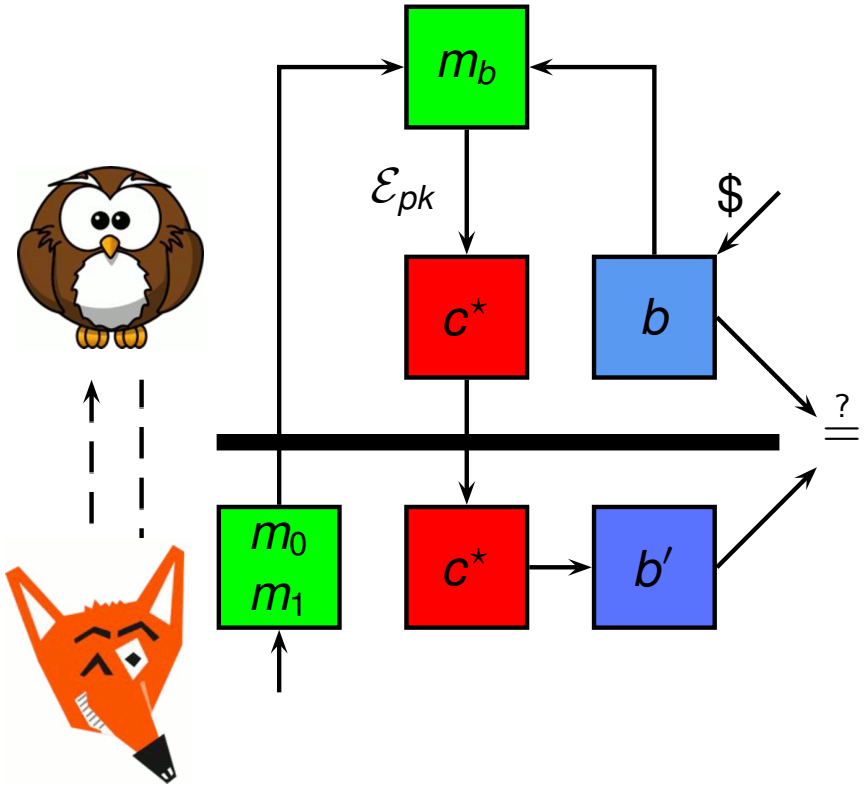
Indistinguishability

Game IND-CCA($\mathcal{A}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0,1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$



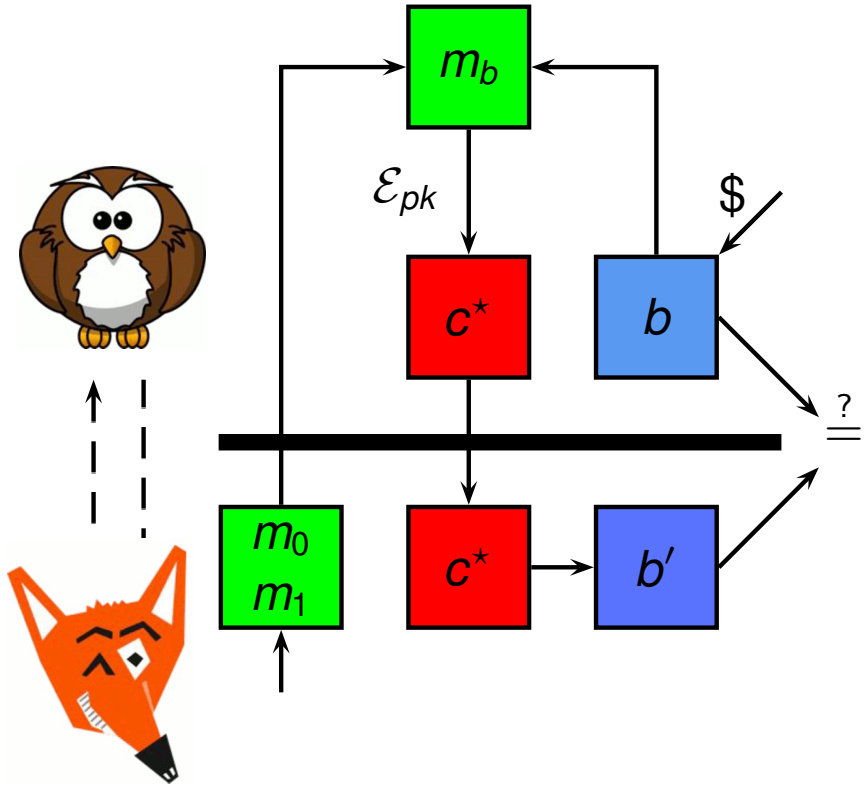
Indistinguishability

Game IND-CCA($\mathcal{A}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0,1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$



Indistinguishability

Game IND-CCA($\mathcal{A}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0,1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$



$$\Pr_{\text{IND-CCA}(\mathcal{A})}\left[b' = b\right] - \frac{1}{2} \quad \text{small}$$

Optimal Asymmetric Encryption Padding

Encryption $\mathcal{E}_{\mathrm{OAEP}(pk)}(m)$:
$r \xleftarrow{\$} \{0,1\}^{k_0}$;
$s \leftarrow G(r) \oplus (m \| 0^{k_1})$;
$t \leftarrow H(s) \oplus r$;
return $\mathsf{f}_{pk}(s \| t)$

Oracle $G(x)$:
if $x \notin L_G$ then
  $r \xleftarrow{\$} \{0,1\}^{k}$;
  $L_G \leftarrow (x, r) :: L_G$;
return $L_G[x]$;

Oracle $H(x)$:
if $x \notin L_H$ then
  $r \xleftarrow{\$} \{0,1\}^{k'}$;
  $L_H \leftarrow (x, r) :: L_H$;
return $L_H[x]$;

Decryption $\mathcal{D}_{\mathrm{OAEP}(sk)}(c)$:
$(s, t) \leftarrow \mathsf{f}_{sk}^{-1}(c)$;
$r \leftarrow t \oplus H(s)$;
if $([s \oplus G(r)]_{k_1} = 0^{k_1})$
  then $\{m \leftarrow [s \oplus G(r)]^{k}; \}$
  else $\{m \leftarrow \perp; \}$
return m

Game sPDOW($\mathcal{I}$)
$(sk, pk) \leftarrow \mathcal{K}()$;
$y_0 \xleftarrow{\$} \{0,1\}^{n_0}$;
$y_1 \xleftarrow{\$} \{0,1\}^{n_1}$;
$y \leftarrow y_0 \| y_1$;
$x^\star \leftarrow \mathsf{f}_{pk}(y)$;
$Y' \leftarrow \mathcal{I}(x^\star)$;
return $(y_0 \in Y')$

OAEP: provable security

FOR ALL IND-CCA adversary $\mathcal{A}$ against $(\mathcal{K}, \mathcal{E}_{\mathrm{OAEP}}, \mathcal{D}_{\mathrm{OAEP}})$,
THERE EXISTS a sPDOW adversary $\mathcal{I}$ against $(\mathcal{K}, \mathsf{f}, \mathsf{f}^{-1})$ st

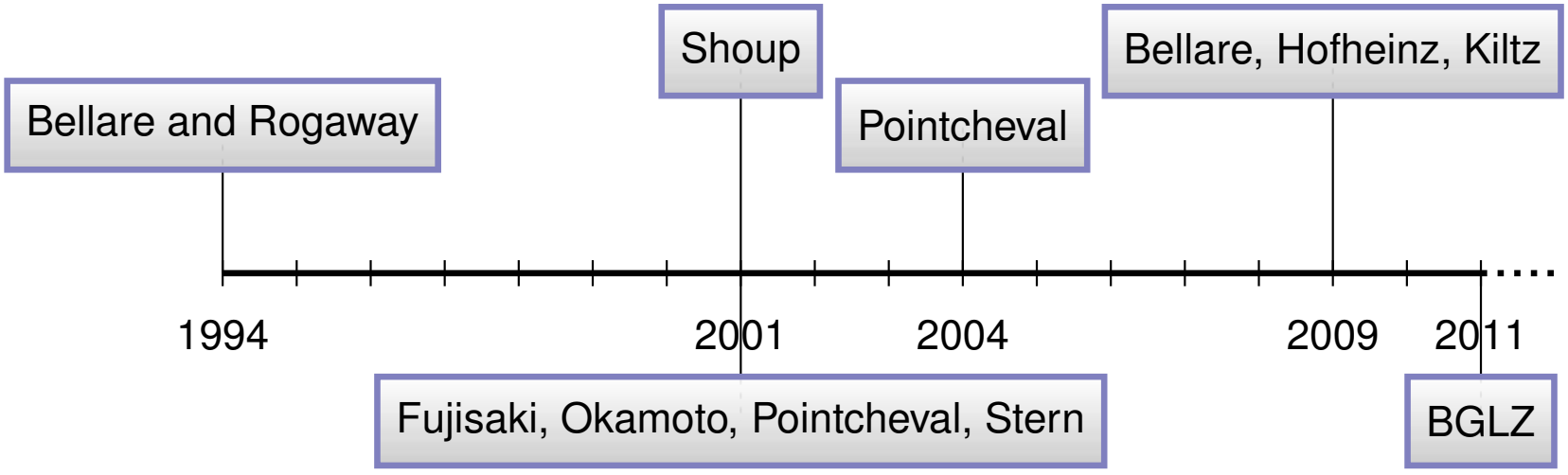
$$\left|\Pr_{\text{IND-CCA}(\mathcal{A})}[b' = b] - \tfrac{1}{2}\right| \leq$$

$$\Pr_{\text{PDOW}(\mathcal{I})}[y \in Y'] + \frac{3q_D q_G + q_D^2 + 4q_D + q_G}{2^{k_0}} + \frac{2q_D}{2^{k_1}}$$

and

$$t_{\mathcal{I}} \leq t_{\mathcal{A}} + q_D\, q_G\, q_H\, T_{\mathsf{f}}$$

OAEP: history



1994 Purported proof of chosen-ciphertext security

2001 1994 proof gives weaker security; desired security holds

- for a modified scheme
- under stronger assumptions

2004 Filled gaps in 2001 proof

2009 Security definition needs to be clarified

2011 Fills gaps in 2004 proof

An isolated problem?

- *In our opinion, many proofs in cryptography have become essentially unverifiable. Our field may be approaching a crisis of rigor*. Bellare and Rogaway, 2004-2006
- *Do we have a problem with cryptographic proofs? Yes, we do [...] We generate more proofs than we carefully verify (and as a consequence some of our published proofs are incorrect)*. Halevi, 2005

Computer-aided cryptographic proofs with EasyCrypt

- adhere to cryptographic practice
  - ☞ same guarantees
  - ☞ same level of abstraction
  - ☞ same proof techniques
- leverage existing verification techniques and tools

(code-based game-playing) provable security
=
deductive relational verification
of parametrized probabilistic programs

Applications

Emblematic examples

- encryption, signatures, hash designs, key exchange protocols, zero knowledge protocols, garbled circuits, secure function evaluation, verifiable computation
- (computational) differential privacy, mechanism design

Ongoing examples

- SHA3
- Voting

Example: Bellare and Rogaway 1993 encryption

Game IND-CPA($\mathcal{A}$) :
$(sk, pk) \leftarrow \mathcal{K}(\ )$;
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk)$;
$b \xleftarrow{\$} \{0,1\}$;
$c^\star \leftarrow \mathcal{E}_{pk}(m_b)$;
$b' \leftarrow \mathcal{A}_2(c^\star)$;
return $(b' = b)$

Encryption $\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^\ell$;
$s \leftarrow H(r) \oplus m$;
$y \leftarrow f_{pk}(r) \,\|\, s$;
return y

For every IND-CPA adversary $\mathcal{A}$, there exists an inverter $\mathcal{I}$ st

$$\Pr_{\text{IND-CPA}(\mathcal{A})}\left[b' = b\right] - \frac{1}{2} \leq \Pr_{\text{OW}(\mathcal{I})}\left[y' = y\right]$$

Proof

Game hopping technique

Game INDCPA :
$(sk, pk) \leftarrow \mathcal{K}();$
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk);$
$b \xleftarrow{\$} \{0,1\};$
$c^\star \leftarrow \mathcal{E}_{pk}(m_b);$
$b' \leftarrow \mathcal{A}_2(c^\star);$
return $(b' = b)$
Encryption $\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^\ell;$
$h \leftarrow H(r);$
$s \leftarrow h \oplus m;$
$c \leftarrow f_{pk}(r) \,\|\, s;$
return c

Game G :
$(sk, pk) \leftarrow \mathcal{K}();$
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk);$
$b \xleftarrow{\$} \{0,1\};$
$c^\star \leftarrow \mathcal{E}_{pk}(m_b);$
$b' \leftarrow \mathcal{A}_2(c^\star);$
return $(b' = b)$
Encryption $\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^\ell;$
$h \xleftarrow{\$} \{0,1\}^k;$
$s \leftarrow h \oplus m;$
$c \leftarrow f_{pk}(r) \,\|\, s;$
return c

Game G′ :
$(sk, pk) \leftarrow \mathcal{K}();$
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk);$
$b \xleftarrow{\$} \{0,1\};$
$c^\star \leftarrow \mathcal{E}_{pk}(m_b);$
$b' \leftarrow \mathcal{A}_2(c^\star);$
return $(b' = b)$
Encryption $\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^\ell;$
$s \xleftarrow{\$} \{0,1\}^k;$
$h \leftarrow s \oplus m;$
$c \leftarrow f_{pk}(r) \,\|\, s;$
return c

Game OW :
$(sk, pk) \leftarrow \mathcal{K}();$
$y \xleftarrow{\$} \{0,1\}^\ell;$
$y' \leftarrow \mathcal{I}(f_{pk}(y));$
return $y = y'$
Adversary $\mathcal{I}(x)$:
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk);$
$s \xleftarrow{\$} \{0,1\}^k;$
$c^\star \leftarrow x \,\|\, s;$
$b' \leftarrow \mathcal{A}_2(c^\star);$
$y' \leftarrow [z \in L_H^{\mathcal{A}} \,|\, f_{pk}(z) = x];$
return y'

1. For each hop
   - prove validity of pRHL judgment
   - derive probability claims
   - (possibly) resolve some probability expressions using pHL
2. Obtain security bound by combining claims
3. Check execution time of constructed adversary

Conditional equivalence

$\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^{\ell}$;
$h \leftarrow H(r)$;
$s \leftarrow h \oplus m$;
$c \leftarrow f_{pk}(r) \,\|\, s$;
return c

$\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^{\ell}$;
$h \xleftarrow{\$} \{0,1\}^{k}$;
$s \leftarrow h \oplus m$;
$c \leftarrow f_{pk}(r) \,\|\, s$;
return c

$$\models \{\top\} \text{ IND-CPA } \sim \mathbf{G} \left\{ (\neg r \in L_H^{\mathcal{A}}) \langle 2 \rangle \rightarrow =_{b,b'} \right\}$$

$$\Pr_{\text{IND-CPA}}\left[b' = b\right] - \Pr_{\mathbf{G}}\left[b' = b\right] \leq \Pr_{\mathbf{G}}\left[r \in L_H^{\mathcal{A}}\right]$$

Equivalence

$\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^{\ell}$;
$h \xleftarrow{\$} \{0,1\}^{k}$;
$s \leftarrow h \oplus m$;
$c \leftarrow f_{pk}(r) \| s$;
return c

$\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^{\ell}$;
$s \xleftarrow{\$} \{0,1\}^{k}$;
$h \leftarrow s \oplus m$;
$c \leftarrow f_{pk}(r) \| s$;
return c

$$\models \{\top\}\ \mathbf{G}\ \sim\ \mathbf{G}'\ \left\{=_{b,b',r,L_H^{\mathcal{A}}}\right\}$$

$$\Pr_{\mathbf{G}}\left[r \in L_H^{\mathcal{A}}\right] = \Pr_{\mathbf{G}'}\left[r \in L_H^{\mathcal{A}}\right] \qquad \Pr_{\mathbf{G}}[b' = b] = \Pr_{\mathbf{G}'}[b' = b] = \frac{1}{2}$$

Equivalence

$\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^{\ell}$;
$h \xleftarrow{\$} \{0,1\}^{k}$;
$s \leftarrow h \oplus m$;
$c \leftarrow f_{pk}(r) \| s$;
return c

$\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^{\ell}$;
$s \xleftarrow{\$} \{0,1\}^{k}$;
$h \leftarrow s \oplus m$;
$c \leftarrow f_{pk}(r) \| s$;
return c

$$\models \{\top\}\ \mathbf{G}\ \sim\ \mathbf{G}'\ \left\{=_{b,b',r,L_H^{\mathcal{A}}}\right\}$$

$$\Pr_{\text{IND-CPA}}[b' = b] - \tfrac{1}{2} \leq \Pr_{\mathbf{G}'}\left[r \in L_H^{\mathcal{A}}\right]$$

Reduction

Game INDCPA :
$(sk, pk) \leftarrow \mathcal{K}();$
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk);$
$b \xleftarrow{\$} \{0,1\};$
$c^\star \leftarrow \mathcal{E}_{pk}(m_b);$
$b' \leftarrow \mathcal{A}_2(c^\star);$
return $(b' = b)$

Encryption $\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^\ell;$
$s \xleftarrow{\$} \{0,1\}^k;$
$c \leftarrow f_{pk}(r) \,\|\, s;$
return c

Game OW :
$(sk, pk) \leftarrow \mathcal{K}();$
$y \xleftarrow{\$} \{0,1\}^\ell;$
$y' \leftarrow \mathcal{I}(f_{pk}(y));$
return $y = y'$

Adversary $\mathcal{I}(x)$:
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk);$
$b \xleftarrow{\$} \{0,1\};$
$s \xleftarrow{\$} \{0,1\}^k;$
$c^\star \leftarrow x \,\|\, s;$
$b' \leftarrow \mathcal{A}_2(c^\star);$
$y' \leftarrow [z \in L_H^{\mathcal{A}} \mid f_{pk}(z) = x];$
return y'

$$\models \{\top\}\ \mathbf{G}'\ \sim\ \mathrm{OW}\ \left\{(r \in L_H^{\mathcal{A}})\langle 1\rangle \rightarrow (y' = y)\langle 2\rangle\right\}$$

$$\Pr_{\mathbf{G}'}\left[r \in L_H^{\mathcal{A}}\right] \leq \Pr_{\mathrm{OW}(\mathcal{I})}[y' = y]$$

Reduction

Game INDCPA :
$(sk, pk) \leftarrow \mathcal{K}();$
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk);$
$b \xleftarrow{\$} \{0,1\};$
$c^\star \leftarrow \mathcal{E}_{pk}(m_b);$
$b' \leftarrow \mathcal{A}_2(c^\star);$
return $(b' = b)$

Encryption $\mathcal{E}_{pk}(m)$:
$r \xleftarrow{\$} \{0,1\}^\ell;$
$s \xleftarrow{\$} \{0,1\}^k;$
$c \leftarrow f_{pk}(r) \,\|\, s;$
return c

Game OW :
$(sk, pk) \leftarrow \mathcal{K}();$
$y \xleftarrow{\$} \{0,1\}^\ell;$
$y' \leftarrow \mathcal{I}(f_{pk}(y));$
return $y = y'$

Adversary $\mathcal{I}(x)$:
$(m_0, m_1) \leftarrow \mathcal{A}_1(pk);$
$b \xleftarrow{\$} \{0,1\};$
$s \xleftarrow{\$} \{0,1\}^k;$
$c^\star \leftarrow x \,\|\, s;$
$b' \leftarrow \mathcal{A}_2(c^\star);$
$y' \leftarrow [z \in L_H^{\mathcal{A}} \mid f_{pk}(z) = x];$
return y'

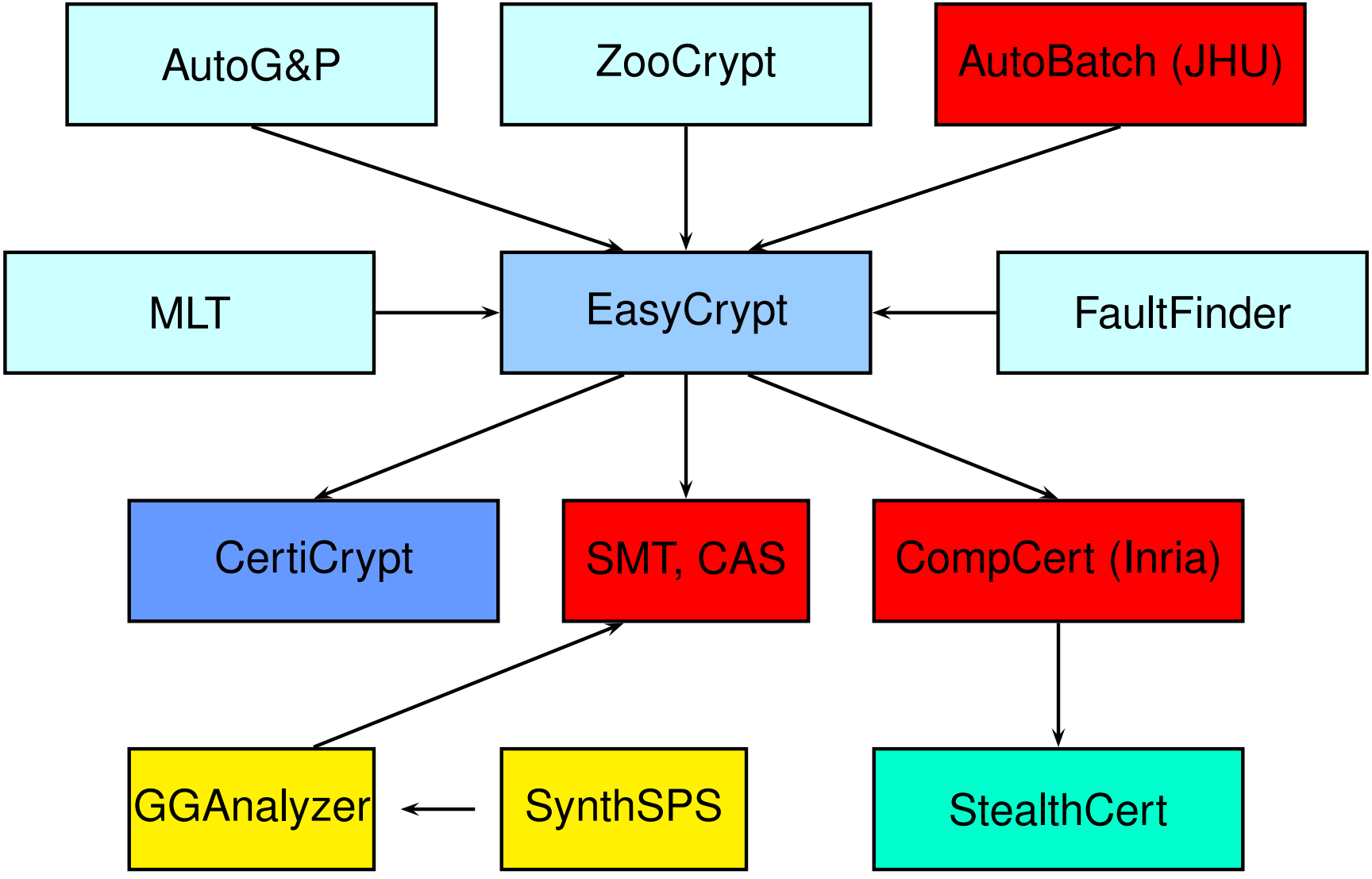
$$\models \{\top\}\ \mathbf{G}'\ \sim\ \mathrm{OW}\ \left\{(r \in L_H^{\mathcal{A}})\langle 1\rangle \rightarrow (y' = y)\langle 2\rangle\right\}$$

$$\Pr_{\text{IND-CPA}(\mathcal{A})}[b' = b] - \tfrac{1}{2} \leq \Pr_{\text{OW}(\mathcal{I})}[y' = y]$$

Other directions

- High-level logics
- Synthesis of cryptographic constructions
  Do the cryptosystems reflect [...] the situations that are being catered for? Or are they accidents of history and personal background that may be obscuring fruitful developments? [...] We must systematize their design so that a new cryptosystem is a point chosen from a well-mapped space, rather than a laboriously devised construction. Adapted from Landin, 1966. The next 700 programming languages
- Verified implementations
  Real-world crypto is breakable; is in fact being broken; is one of many ongoing disaster areas in security. Bernstein, 2013
- Side-channel and fault attacks
- Automated analysis in generic group model

Tools


AutoG&P
ZooCrypt
AutoBatch (JHU)
MLT
EasyCrypt
FaultFinder
CertiCrypt
SMT, CAS
CompCert (Inria)
GGAnalyzer
SynthSPS
StealthCert

Conclusion

Formal methods provide solid and practical foundations for (reconciling) provable security and practical crypto

Our tools allow to

- formally prove security of cryptographic constructions
- generate correct, secure, and optimized code, which can resist implementation-level adversaries

Challenges

- verified compilers and static analyses for implementations
- formalized mathematics
- automated deduction

`http://www.easycrypt.info`