

Computer-aided security proofs for the working cryptographer

Gilles Barthe
Sylvain Heraud

Benjamin Grégoire
Santiago Zanella Béguelin



CRYPTO'11, August 15 2011

A plea for computer-aided cryptographic proofs

A plausible approach to computer-aided cryptographic proofs. Halevi, 2005

Code-Based Game-Playing Proofs and the Security of Triple Encryption. Bellare and Rogaway, 2004-2006

A plea for computer-aided cryptographic proofs

A plausible approach to computer-aided cryptographic proofs. Halevi, 2005

Code-Based Game-Playing Proofs and the Security of Triple Encryption. Bellare and Rogaway, 2004-2006

A problem with security proofs

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

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

A plea for computer-aided cryptographic proofs

A plausible approach to computer-aided cryptographic proofs. Halevi, 2005

Code-Based Game-Playing Proofs and the Security of Triple Encryption. Bellare and Rogaway, 2004-2006

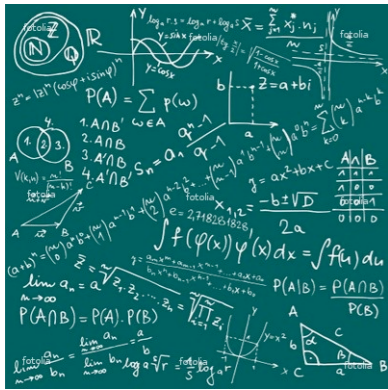
A problem with security proofs: a plausible solution

I advocate creating an automated tool to help us [...] writing and checking [...] our proofs—Halevi, 2005

The possibility for tools [to help write and verify proofs] has always been one of our motivations, and one of the reasons why we focused on code-based games—Bellare and Rogaway, 2004-2006

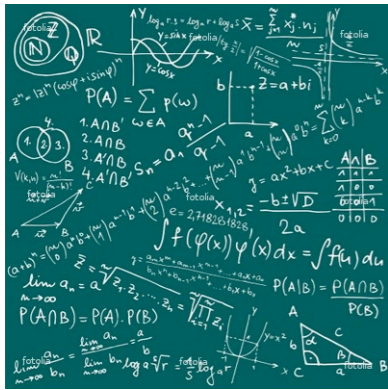
A primer on computer-aided proofs

A primer on computer-aided proofs

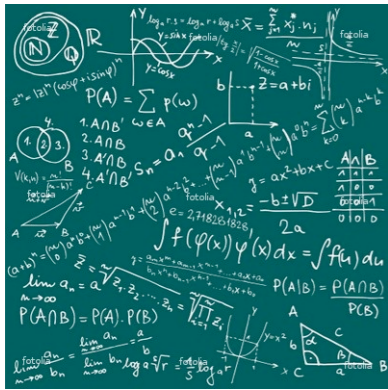


A primer on computer-aided proofs

Lemma : $\forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$



A primer on computer-aided proofs



Lemma : $\forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$

Proof.

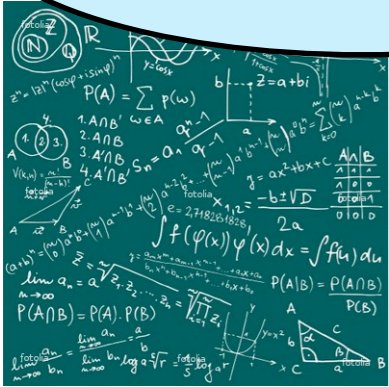
intros r ; exists $(\lceil r \rceil + 1)$.

destruct $(nceil_spec\ r)$ as $(-, H)$; exact H .

Qed.

A primer on computer-aided proofs

Manual review



Lemma : $\forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$

Proof.

intros r ; exists $(\lceil r \rceil + 1)$.

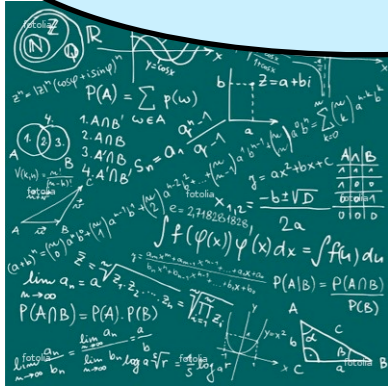
destruct $(nceil_spec\ r)$ as $(-, H)$; exact H .

Qed.



A primer on computer-aided proofs

Manual review



Lemma : $\forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$

Proof.

intros r ; exists $(\lceil r \rceil + 1)$.

destruct $(nceil_spec\ r)$ as $(-, H)$; exact H .

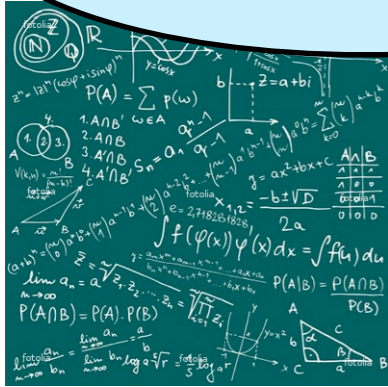
Qed.

Automated checking



A primer on computer-aided proofs

Manual review



Lemma : $\forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$

Proof.

intros r ; exists ($\lceil r \rceil + 1$).

destruct (n ceil_spec r) as ($-$, H); exact H .

Qed.

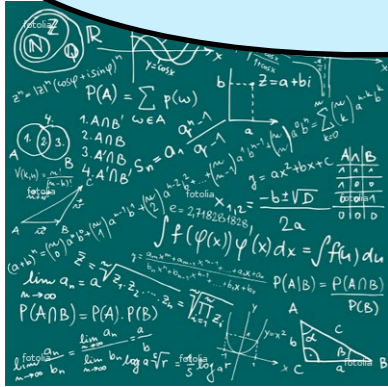
Correctness from first principles

Automated checking



A primer on computer-aided proofs

Manual review



Lemma : $\forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$

Proof.

intros r ; exists $(\lceil r \rceil + 1)$.

destruct $(n\text{ceil_spec } r)$ as $(-, H)$; exact H .

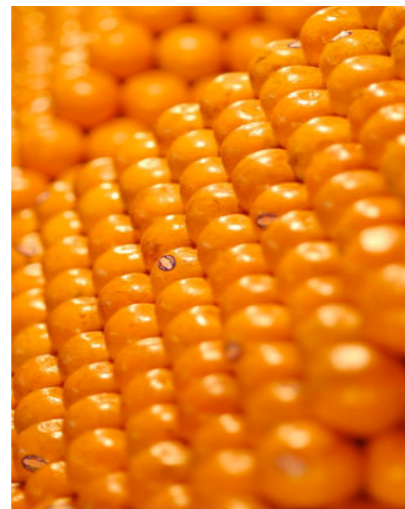
Qed.

Correctness from first principles

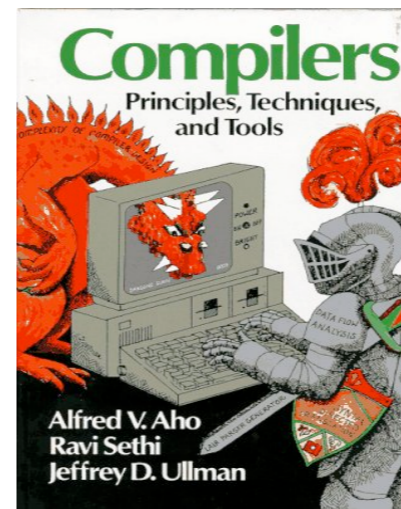
Automated checking



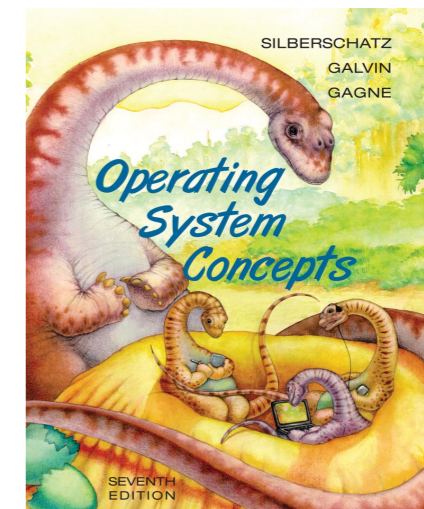
4 colour theorem



Kepler conjecture



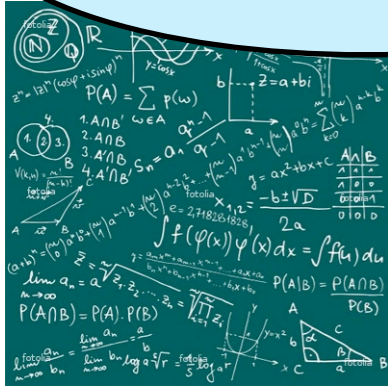
C compiler



seL4
HyperV

A primer on computer-aided proofs

Manual review



Lemma : $\forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$

Proof.

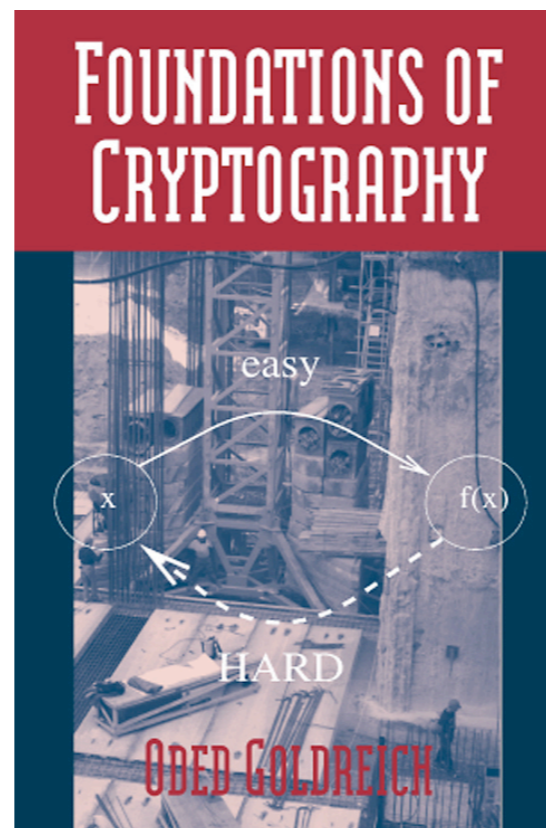
intros r ; exists ($\lceil r \rceil + 1$).

destruct (nceil_spec r) as ($-$, H); exact H .

Qed.

Correctness from first principles

Automated checking



CertiCrypt

Formal framework for security proofs:

- Code-based game-based technique
- Independently verifiable proofs
- Applied to FDH, OAEP, Sigma-Protocols, IBE



CertiCrypt

Formal framework for security proofs:

- Code-based game-based technique
- Independently verifiable proofs
- Applied to FDH, OAEP, Sigma-Protocols, IBE

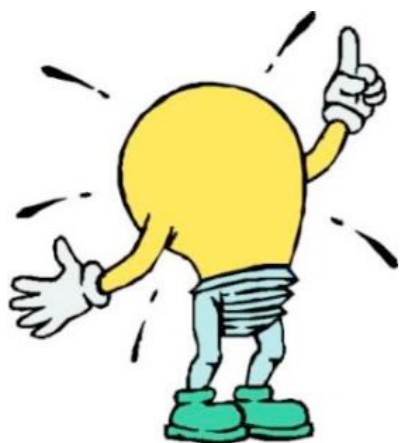


High level of Coq expertise and a lot of time

CertiCrypt

Formal framework for security proofs:

- Code-based game-based technique
- Independently verifiable proofs
- Applied to FDH, OAEP, Sigma-Protocols, IBE



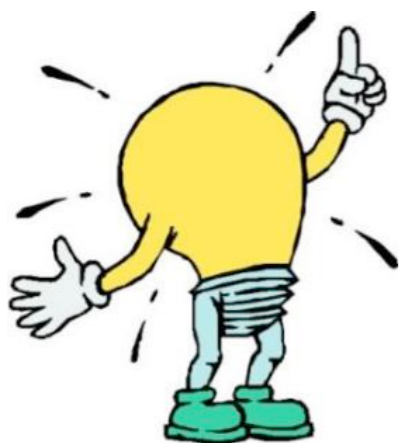
High level of Coq expertise and a lot of time

Exploit state-of-the-art program verification tools!

From CertiCrypt to EasyCrypt

Formal framework for security proofs:

- Code-based game-based technique
- Independently verifiable proofs
- Applied to FDH, OAEP, Sigma-Protocols, IBE

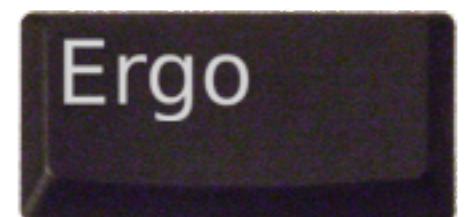


High level of Coq expertise and a lot of time

Exploit state-of-the-art program verification tools!

Computer-assisted security proofs

- With moderate effort
- Using off-the-shelf tools



The essence of game-based proofs

Game IND – CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
return $(b = b')$



Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
return $(b = b')$



Game G_2 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
return $(b = b')$



Game G_3 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h);$
return $(b = b')$



Game LCDH :
 $x \xleftarrow{\$} \mathbb{Z}_q; y \xleftarrow{\$} \mathbb{Z}_q;$
 $L \leftarrow \mathcal{B}(g^x, g^y);$
return $(g^{xy} \in L)$
Adversary $\mathcal{B}(\alpha, \beta)$:
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $\gamma \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
return L

The essence of game-based proofs

Game IND – CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$



Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



Game G_2 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



$$\Pr[\text{IND – CPA} : b = b'] = \Pr[G_1 : b = b']$$

Game G_3 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h);$
 return $(b = b')$



Game LCDH :
 $x \xleftarrow{\$} \mathbb{Z}_q; y \xleftarrow{\$} \mathbb{Z}_q;$
 $L \leftarrow \mathcal{B}(g^x, g^y);$
 return $(g^{xy} \in L)$
Adversary $\mathcal{B}(\alpha, \beta)$:
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $\gamma \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return L

The essence of game-based proofs

Game IND – CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$



Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



Game G_2 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



$$\Pr[\text{IND – CPA} : b = b'] = \Pr[G_1 : b = b']$$

$$|\Pr[G_1 : b = b'] - \Pr[G_2 : b = b']| \leq \Pr[G_2 : \hat{y} \in L]$$

Game G_3 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h);$
 return $(b = b')$



Game LCDH :
 $x \xleftarrow{\$} \mathbb{Z}_q; y \xleftarrow{\$} \mathbb{Z}_q;$
 $L \leftarrow \mathcal{B}(g^x, g^y);$
 return $(g^{xy} \in L)$
Adversary $\mathcal{B}(\alpha, \beta)$:
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $\gamma \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return L

The essence of game-based proofs

Game IND – CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$



Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



Game G_2 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



$$\Pr[\text{IND – CPA} : b = b'] = \Pr[G_1 : b = b']$$

$$|\Pr[G_1 : b = b'] - \Pr[G_2 : b = b']| \leq \Pr[G_2 : \hat{y} \in L]$$

$$\Pr[G_2 : b = b'] = \Pr[G_3 : b = b'] = \frac{1}{2}$$

$$\Pr[G_2 : \hat{y} \in L] = \Pr[G_3 : \hat{y} \in L]$$

Game G_3 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h);$
 return $(b = b')$



Game LCDH :
 $x \xleftarrow{\$} \mathbb{Z}_q; y \xleftarrow{\$} \mathbb{Z}_q;$
 $L \leftarrow \mathcal{B}(g^x, g^y);$
 return $(g^{xy} \in L)$
Adversary $\mathcal{B}(\alpha, \beta)$:
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $\gamma \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return L

The essence of game-based proofs

Game IND – CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$



Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



Game G_2 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



$$\Pr[\text{IND – CPA} : b = b'] = \Pr[G_1 : b = b']$$

$$|\Pr[G_1 : b = b'] - \Pr[G_2 : b = b']| \leq \Pr[G_2 : \hat{y} \in L]$$

$$\Pr[G_2 : b = b'] = \Pr[G_3 : b = b'] = \frac{1}{2}$$

$$\Pr[G_2 : \hat{y} \in L] = \Pr[G_3 : \hat{y} \in L]$$

Game G_3 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h);$
 return $(b = b')$



Game LCDH :
 $x \xleftarrow{\$} \mathbb{Z}_q; y \xleftarrow{\$} \mathbb{Z}_q;$
 $L \leftarrow \mathcal{B}(g^x, g^y);$
 return $(g^{xy} \in L)$
Adversary $\mathcal{B}(\alpha, \beta)$:
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $\gamma \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return L

$$\Pr[G_3 : \hat{y} \in L] = \Pr[\text{LCDH} : g^{xy} \in L]$$

The essence of game-based proofs

Game IND – CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$



Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



Game G_2 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



$$\Pr[\text{IND – CPA} : b = b'] = \Pr[G_1 : b = b']$$

$$|\Pr[G_1 : b = b'] - \Pr[G_2 : b = b']| \leq \Pr[G_2 : \hat{y} \in L]$$

$$\Pr[G_2 : b = b'] = \Pr[G_3 : b = b'] = \frac{1}{2}$$

$$\Pr[G_2 : \hat{y} \in L] = \Pr[G_3 : \hat{y} \in L]$$

Game G_3 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h);$
 return $(b = b')$



Game LCDH :
 $x \xleftarrow{\$} \mathbb{Z}_q; y \xleftarrow{\$} \mathbb{Z}_q;$
 $L \leftarrow \mathcal{B}(g^x, g^y);$
 return $(g^{xy} \in L)$
Adversary $\mathcal{B}(\alpha, \beta)$:
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $\gamma \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return L

$$\Pr[G_3 : \hat{y} \in L] = \Pr[\text{LCDH} : g^{xy} \in L]$$

$$\Pr[\text{IND – CPA} : b = b'] - \frac{1}{2} \leq \Pr[\text{LCDH} : g^{xy} \in L]$$

The essence of game-based proofs

Game IND – CPA :

$(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$



Game G₁ :

$x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



Game G₂ :

$x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



$$\Pr[\text{IND – CPA} : b = b'] = \Pr[\text{G}_1 : b = b']$$

$$|\Pr[\text{G}_1 : b = b'] - \Pr[\text{G}_2 : b = b']| \leq \Pr[\text{G}_2 : \hat{y} \in L]$$

$$\Pr[\text{G}_2 : b = b'] = \Pr[\text{G}_3 : b = b'] = \frac{1}{2}$$

$$\Pr[\text{G}_2 : \hat{y} \in L] = \Pr[\text{G}_3 : \hat{y} \in L]$$

Game G₃ :

$$\models \text{IND – CPA} \sim \text{G}_1 : \text{true} \implies (b = b') \langle 1 \rangle = (b = b') \langle 2 \rangle$$

$b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h);$
 return $(b = b')$

Game LCDH :

$x \xleftarrow{\$} \mathbb{Z}_q; y \xleftarrow{\$} \mathbb{Z}_q;$
 $\mathcal{B}(g^x, g^y);$
 return $(g^{xy} \in L)$

Adversary $\mathcal{B}(\alpha, \beta)$:

$(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $\gamma \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return L

$$\Pr[\text{G}_3 : \hat{y} \in L] = \Pr[\text{LCDH} : g^{xy} \in L]$$

$$\Pr[\text{IND – CPA} : b = b'] - \frac{1}{2} \leq \Pr[\text{LCDH} : g^{xy} \in L]$$

The essence of game-based proofs

Game IND – CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$

$$\Pr[\text{IND – CPA} : b = b'] = \Pr[\text{G}_1 : b = b']$$

Game G₁ :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$

$$|\Pr[\text{G}_1 : b = b'] - \Pr[\text{G}_2 : b = b']| \leq \Pr[\text{G}_2 : \hat{y} \in L]$$

Game G₂ :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$

$$\Pr[\text{G}_2 : b = b'] = \Pr[\text{G}_3 : b = b'] = \frac{1}{2}$$

$$\Pr[\text{G}_2 : \hat{y} \in L] = \Pr[\text{G}_3 : \hat{y} \in L]$$

Game G₃ :
 $\models \text{IND – CPA} \sim \text{G}_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

$b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h);$
 return $(b = b')$

$$\Pr[\text{G}_3 : \hat{y} \in L] = \Pr[\text{LCDH} : g^{xy} \in L]$$

Game LCDH:

$y \xleftarrow{\$} \mathbb{Z}_q; y$
 $\leftarrow \mathcal{B}(g^x, y)$
 return (g^{xy})

Adversary $\mathcal{B}(\alpha, \beta)$:
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $\gamma \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return L

$\models \text{G}_1 \sim \text{G}_2 : \text{true} \implies (\hat{y} \in L)\langle 1 \rangle \leftrightarrow (\hat{y} \in L)\langle 2 \rangle \wedge$
 $(\hat{y} \notin L)\langle 1 \rangle \rightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

$$\Pr[\text{IND – CPA} : b = b'] - \frac{1}{2} \leq \Pr[\text{LCDH} : g^{xy} \in L]$$

The essence of game-based proofs

Game IND – CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$



Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



Game G_2 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



$$\Pr[\text{IND – CPA} : b = b'] = \Pr[G_1 : b = b']$$

$$|\Pr[G_1 : b = b'] - \Pr[G_2 : b = b']| \leq \Pr[G_2 : \hat{y} \in L]$$

$$\Pr[G_2 : b = b'] = \Pr[G_3 : b = b'] = \frac{1}{2}$$

$$\Pr[G_2 : \hat{y} \in L] = \Pr[G_3 : \hat{y} \in L]$$

Game G_3 :

$$\models \text{IND – CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

$$b \xleftarrow{\$} \{0, 1\};$$

Game LCDH :

$x \xleftarrow{\$} \mathbb{Z}_q; y \xleftarrow{\$} \mathbb{Z}_q;$
 $\mathcal{B}(g^x, g^y);$
 return (g^{xy})

$$\models G_1 \sim G_2 : \text{true} \implies (\hat{y} \in L)\langle 1 \rangle \leftrightarrow (\hat{y} \in L)\langle 2 \rangle \wedge (\hat{y} \notin L)\langle 1 \rangle \rightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

Adversary $\mathcal{B}(\alpha, \beta)$:
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$

$$\models G_2 \sim G_3 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle \wedge (\hat{y} \in L)\langle 1 \rangle = (\hat{y} \in L)\langle 2 \rangle$$

$$\Pr[G_3 : \hat{y} \in L] = \Pr[\text{LCDH} : g^{xy} \in L]$$

$$\Pr[\text{IND – CPA} : b = b'] - \frac{1}{2} \leq \Pr[\text{LCDH} : g^{xy} \in L]$$

The essence of game-based proofs

Game IND – CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$



Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



Game G_2 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$



$$\Pr[\text{IND – CPA} : b = b'] = \Pr[G_1 : b = b']$$

$$|\Pr[G_1 : b = b'] - \Pr[G_2 : b = b']| \leq \Pr[G_2 : \hat{y} \in L]$$

$$\Pr[G_2 : b = b'] = \Pr[G_3 : b = b'] = \frac{1}{2}$$

$$\Pr[G_2 : \hat{y} \in L] = \Pr[G_3 : \hat{y} \in L]$$

Game G_3 :

$$\models \text{IND – CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

$b \xleftarrow{\$} \{0, 1\};$

Game LCDH :

$x \xleftarrow{\$} \mathbb{Z}_q; y \xleftarrow{\$} \mathbb{Z}_q;$
 $\mathcal{B}(g^x, g^y)$
 return (g^{xy})

$$\models G_1 \sim G_2 : \text{true} \implies (\hat{y} \in L)\langle 1 \rangle \leftrightarrow (\hat{y} \in L)\langle 2 \rangle \wedge (\hat{y} \notin L)\langle 1 \rangle \rightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

Adversary $\mathcal{B}(\alpha, \beta)$:

$(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$

$$\models G_2 \sim G_3 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle \wedge (\hat{y} \in L)\langle 1 \rangle = (\hat{y} \in L)\langle 2 \rangle$$

$$\models G_3 \sim \text{LCDH} : \text{true} \implies (\hat{y} \in L)\langle 1 \rangle = (g^{xy} \in L)\langle 2 \rangle$$

$$\Pr[G_3 : \hat{y} \in L] = \Pr[\text{LCDH} : g^{xy} \in L]$$

$$\Pr[\text{IND – CPA} : b = b'] - \frac{1}{2} \leq \Pr[\text{LCDH} : g^{xy} \in L]$$

The essence of game-based proofs

Game IND – CPA :

$(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
return $(b = b')$



Game LCDH :

$x \xleftarrow{\$} \mathbb{Z}_q; y \xleftarrow{\$} \mathbb{Z}_q;$
 $L \leftarrow \mathcal{B}(g^x, g^y);$
return $(g^{xy} \in L)$

Adversary $\mathcal{B}(\alpha, \beta)$:

$(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $\gamma \xleftarrow{\$} \{0, 1\}^k;$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
return L

$$\Pr[\text{IND – CPA} : b = b'] - \frac{1}{2} \leq \Pr[\text{LCDH} : g^{xy} \in L]$$

Automated verification of proof sketches

Game IND – CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
return $(b = b')$

$\models \text{IND – CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

$$\Pr[\text{IND – CPA} : b = b'] \\ = \Pr[G_1 : b = b']$$

Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
return $(b = b')$

Automated verification of proof sketches

$$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

Game IND - CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
return $(b = b')$

Inline

Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
return $(b = b')$

Automated verification of proof sketches

$$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

Game IND - CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_1);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
return $(b = b')$

Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
return $(b = b')$

Inline

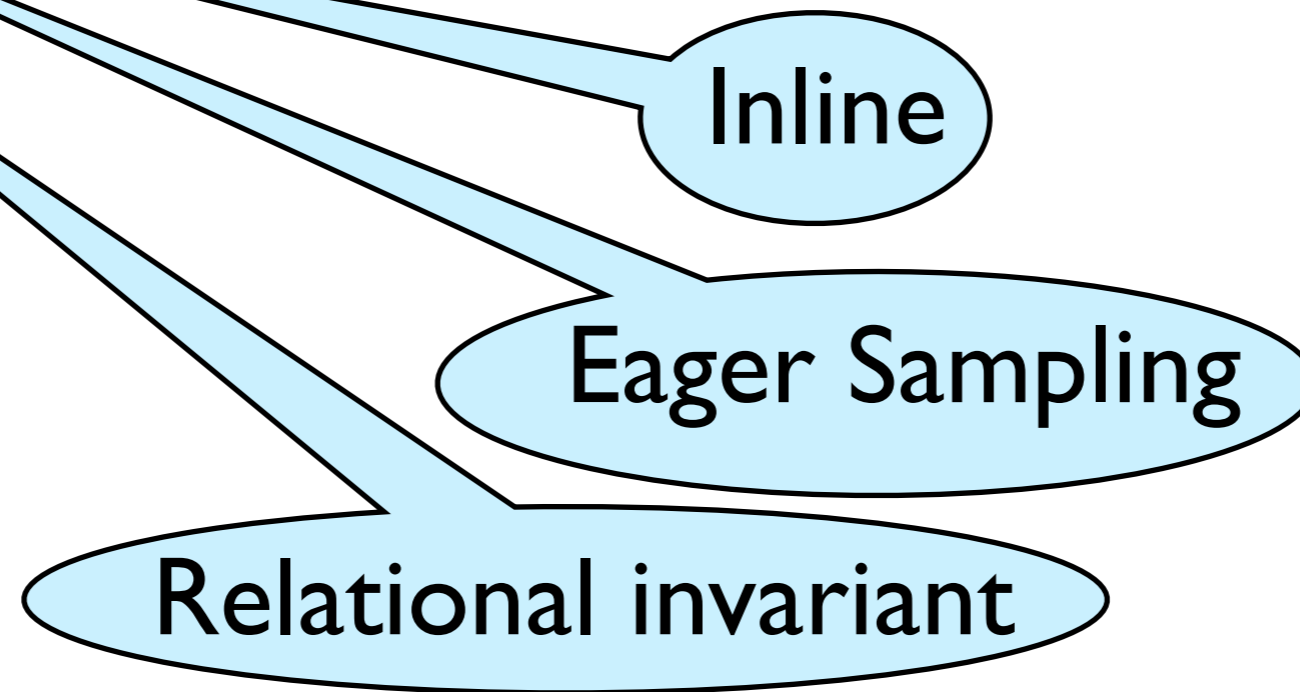
Eager Sampling

Automated verification of proof sketches

$$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

Game IND - CPA :
 $(x, \alpha) \leftarrow \text{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_1);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
return $(b = b')$

Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
return $(b = b')$

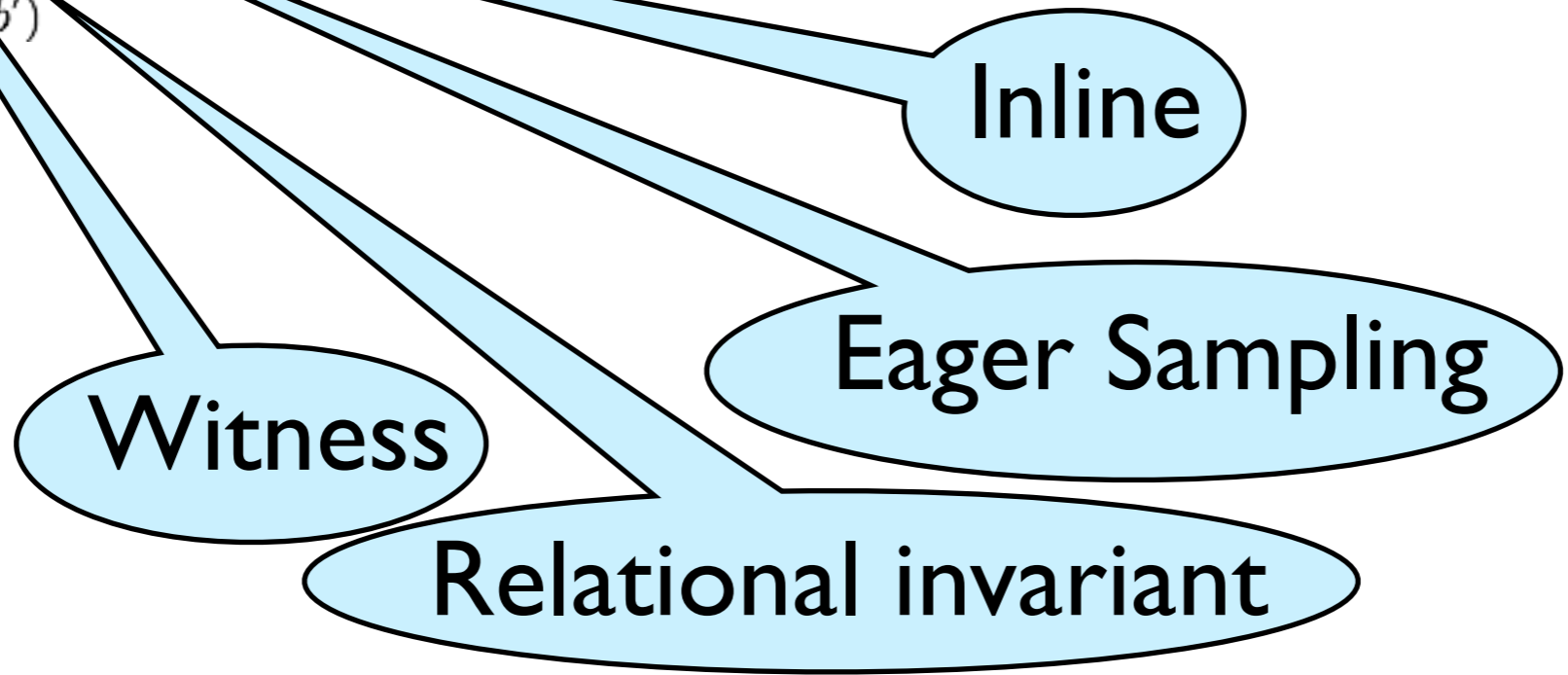


Automated verification of proof sketches

$$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

```
Game IND - CPA :  
(x, alpha) ← KG();  
(m0, m1) ← A1(alpha);  
b ← S {0, 1};  
(beta, gamma) ← E(alpha, m1);  
b' ← A2(beta, gamma);  
return (b = b')
```

```
Game G1 :  
x ← S Zq; alpha ← g^x;  
y ← S Zq; y-hat ← alpha^y;  
(m0, m1) ← A1(alpha);  
b ← S {0, 1};  
h ← H(y-hat);  
b' ← A2(g^y, h ⊕ mb);  
return (b = b')
```



Automated verification of proof sketches

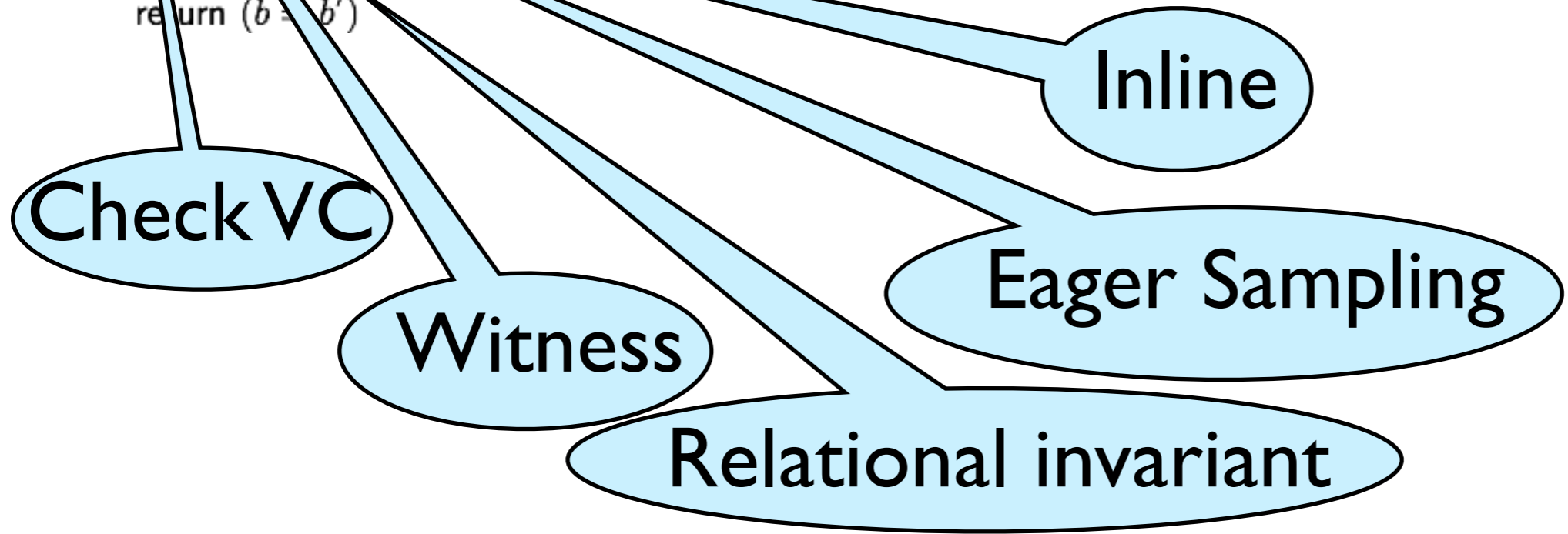
$$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

```

Game IND - CPA :
(x, α) ← KG();
(m0, m1) ← A1(α);
b ← S {0, 1};
(β, γ) ← E(α, mb);
b' ← A2(β, γ);
return (b = b')
    
```

```

Game G1 :
x ← S Zq; α ← gx;
y ← S Zq; ŷ ← αy;
(m0, m1) ← A1(α);
b ← S {0, 1};
h ← H(ŷ);
b' ← A2(gy, h ⊕ mb);
return (b = b')
    
```



Automated verification of proof sketches



Simplify

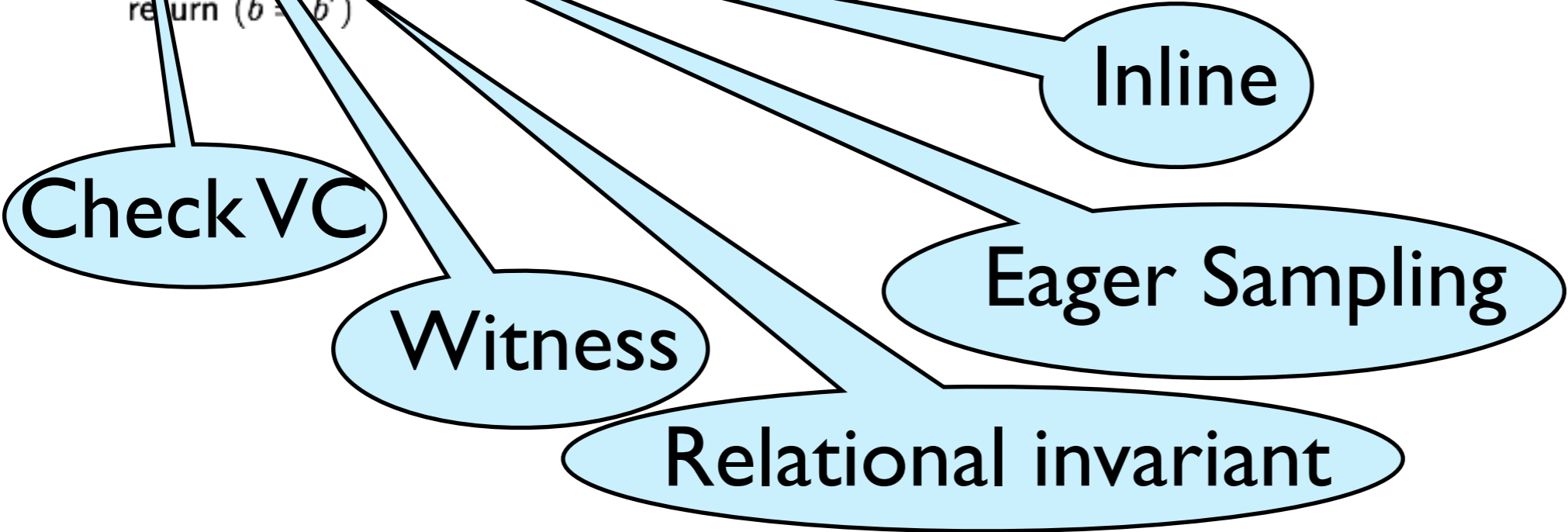
$$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

```

Game IND - CPA :
(x, α) ← KG();
(m₀, m₁) ← A₁(α);
b ← S {0, 1};
(β, γ) ← E(α, m₁);
b' ← A₂(β, γ);
return (b = b')
    
```

```

Game G₁ :
x ← S Z_q; α ← g^x;
y ← S Z_q; ŷ ← α^y;
(m₀, m₁) ← A₁(α);
b ← S {0, 1};
h ← H(ŷ);
b' ← A₂(g^y, h ⊕ m_b);
return (b = b')
    
```



Automated verification of proof sketches



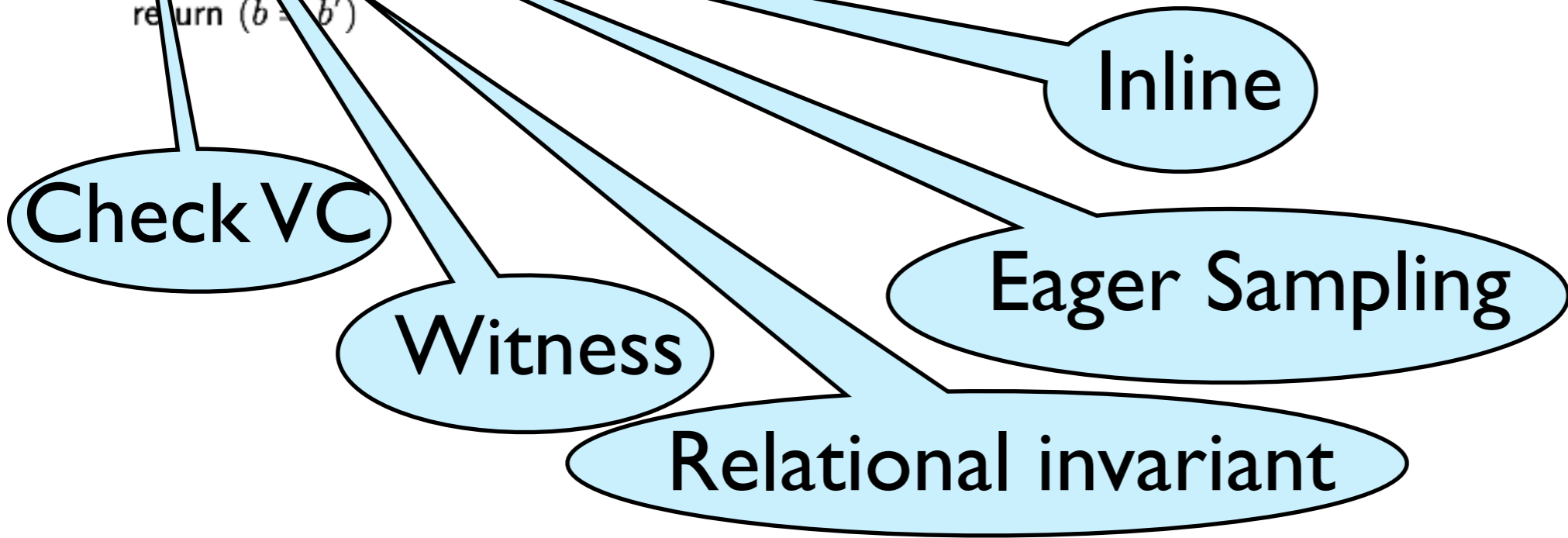
```
equiv FactI : INDCPA.Main ~ G1.Main : {true} ==> = {res}
inline KG, Enc; derandomize; auto inv = {L, LA}; pop{2} I; repeat rnd; trivial;;
save;;
```

Simplify

$$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

```
Game IND - CPA :
(x, alpha) ← KG();
(m0, m1) ← A1(alpha);
b ← {0, 1};
(beta, gamma) ← E(alpha, m1);
b' ← A2(beta, gamma);
return (b = b')
```

```
Game G1 :
x ← Zq; alpha ← g^x;
y ← Zq; y-hat ← alpha^y;
(m0, m1) ← A1(alpha);
b ← {0, 1};
h ← H(y-hat);
b' ← A2(g^y, h ⊕ mb);
return (b = b')
```



Automated verification of proof sketches



```
equiv FactI : INDCPA.Main ~ G1.Main : {true} ==> = {res}  
inline KG, Enc; derandomize; auto inv = {L, LA}; pop{2} 1; repeat rnd; trivial;;  
save;;
```

Simplify

$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

Game IND - CPA :
 $(x, \alpha) \leftarrow \text{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
return $(b = b')$

Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
return $(b = b')$

Automated verification of proof sketches



Simplify

```
equiv FactI : INDCPA.Main ~ G1.Main : {true} ==> = {res}
inline KG, Enc; derandomize; auto inv = {L, LA}; pop{2} I; repeat rnd; trivial;;
save;;

claim PrI : INDCPA.Main[res] == G1.Main[res] using FactI;;
```

$$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

Game IND - CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$

$$\Pr[\text{IND - CPA} : b = b'] = \Pr[G_1 : b = b']$$

Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$

Automated verification of proof sketches



```
equiv FactI : INDCPA.Main ~ G1.Main : {true} ==> = {res}
inline KG, Enc; derandomize; auto inv = {L, LA}; pop{2} I; repeat rnd; trivial;;
save;;

claim PrI : INDCPA.Main[res] == G1.Main[res] using FactI;;
```

Simplify

$$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

Game IND - CPA :

```
(x, alpha) ← KG();
(m0, m1) ← A1(alpha);
b ←S {0, 1};
(beta, gamma) ← E(alpha, mb);
b' ← A2(beta, gamma);
return (b = b')
```

$$\Pr[\text{IND - CPA} : b = b'] = \Pr[G_1 : b = b']$$

Game G₁ :

```
x ←S Zq; alpha ← g^x;
y ←S Zq; y-hat ← alpha^y;
(m0, m1) ← A1(alpha);
b ←S {0, 1};
h ← H(y-hat);
b' ← A2(g^y, h ⊕ mb);
return (b = b')
```

- Bridging steps
- Lazy sampling
- Code motion
- Algebraic equivs
- Failure events
- Reduction steps

Automated verification of proof sketches



```
equiv FactI : INDCPA.Main ~ G1.Main : {true} ==> = {res}
inline KG, Enc; derandomize; auto inv = {L, LA}; pop{2} I; repeat rnd; trivial;;
save;;

claim PrI : INDCPA.Main[res] == G1.Main[res] using FactI;;
```

Simplify

$$\models \text{IND - CPA} \sim G_1 : \text{true} \implies (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

Game IND - CPA :
 $(x, \alpha) \leftarrow \mathcal{KG}();$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $(\beta, \gamma) \leftarrow \mathcal{E}(\alpha, m_b);$
 $b' \leftarrow \mathcal{A}_2(\beta, \gamma);$
 return $(b = b')$

$$\Pr[\text{IND - CPA} : b = b'] = \Pr[G_1 : b = b']$$

Game G_1 :
 $x \xleftarrow{\$} \mathbb{Z}_q; \alpha \leftarrow g^x;$
 $y \xleftarrow{\$} \mathbb{Z}_q; \hat{y} \leftarrow \alpha^y;$
 $(m_0, m_1) \leftarrow \mathcal{A}_1(\alpha);$
 $b \xleftarrow{\$} \{0, 1\};$
 $h \leftarrow H(\hat{y});$
 $b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b);$
 return $(b = b')$

- Bridging steps
- Lazy sampling
- Code motion
- Algebraic equivs
- Failure events
- Reduction steps



Case studies

Cramer-Shoup encryption system:

$$\text{Adv}_{\text{CCA}}(\mathcal{A}) \leq \text{Adv}_{\text{DDH}}(\mathcal{B}) + \text{Adv}_{\text{TCR}}(\mathcal{C}) + \frac{q_D^4}{q^4} + \frac{q_D + 2}{q}$$

10 games, 1650 lines of EasyCrypt, ~100 lines of Coq

	CertiCrypt	EasyCrypt
ElGamal	565	190
Hashed ElGamal	1255	243
Full-Domain Hash	2035	509
Cramer-Shoup	n/a	1637
OAEP	11162	n/a

Significant reduction in:

- script size (from $\times 2$ to $\div 5$ wrt sequence of games)
- development time (~10 times faster)
- learning time

Perspectives

Computer-assisted security proofs

- Can be built with moderate effort
- Using off-the-shelf tools
- Producing independently verifiable evidence
- Work for challenging example: Cramer-Shoup encryption

Perspectives

Computer-assisted security proofs

- Can be built with moderate effort
- Using off-the-shelf tools
- Producing independently verifiable evidence
- Work for challenging example: Cramer-Shoup encryption



- Distribute (<http://certicrypt.gforge.inria.fr/>)
- Improve and extend
- More examples: SHA3, differential privacy