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

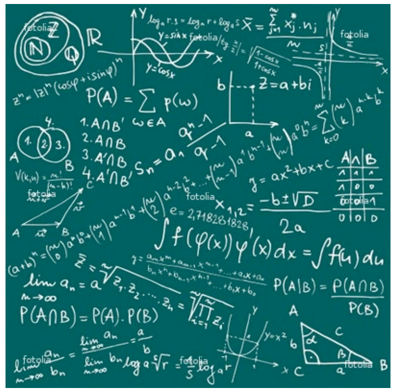
A problem with security proofs: a plausible solution

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

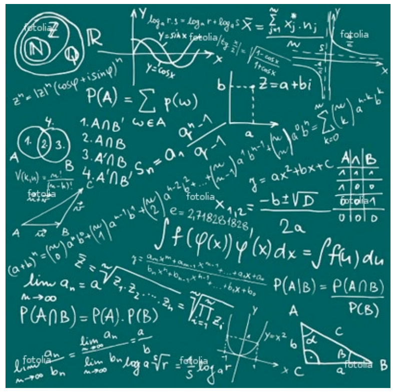
A primer on computer-aided proofs

A primer on computer-aided proofs

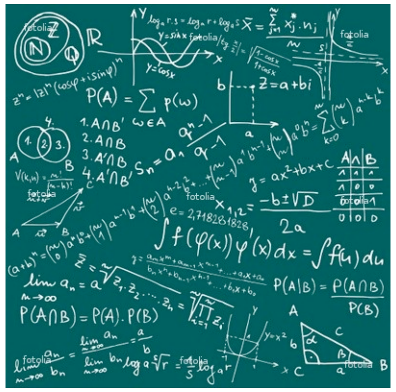


A primer on computer-aided proofs

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



A primer on computer-aided proofs

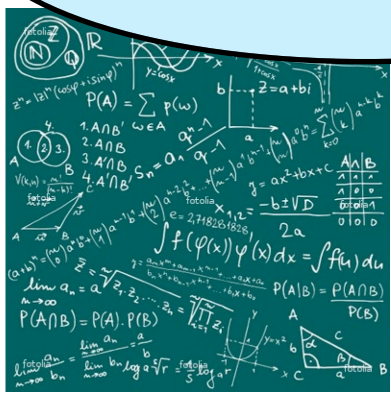


$$\text{Lemma} : \forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$$

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

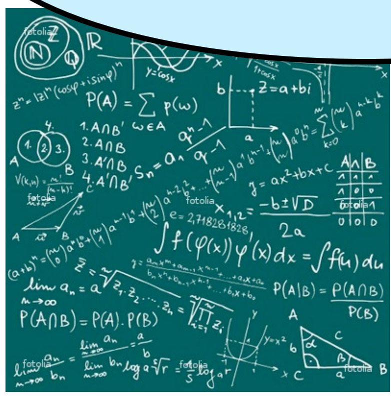


Lemma : $\forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$

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



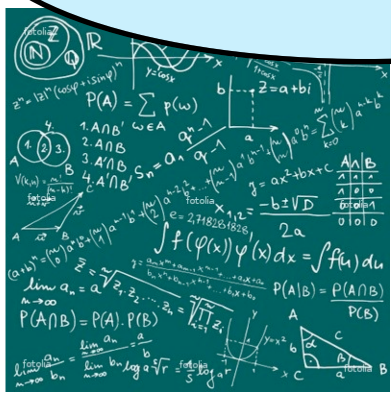
$$\text{Lemma} : \forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$$

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

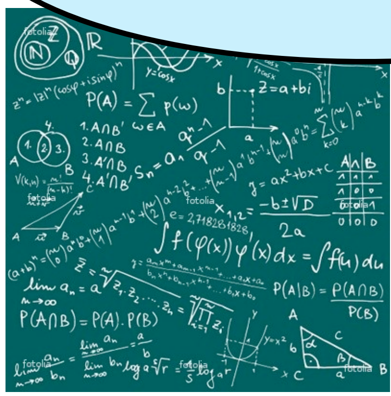
Proof.
intros r; exists $(\lceil r \rceil + 1)$.
destruct $(nceil\_spec\ r)$ as $(\_, H)$; exact H.
Qed.

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 $(\lceil r \rceil + 1)$.

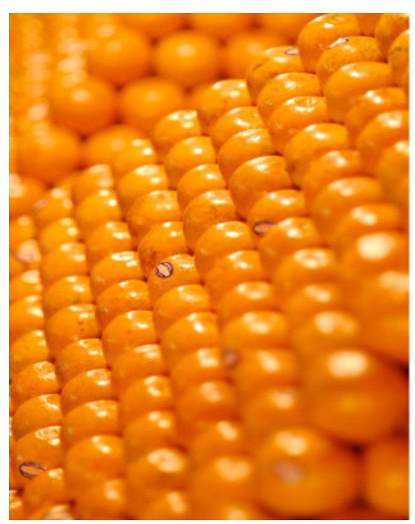
destruct $(nceil\_spec\ r)$ as $(\_, H)$; exact H.

Qed.

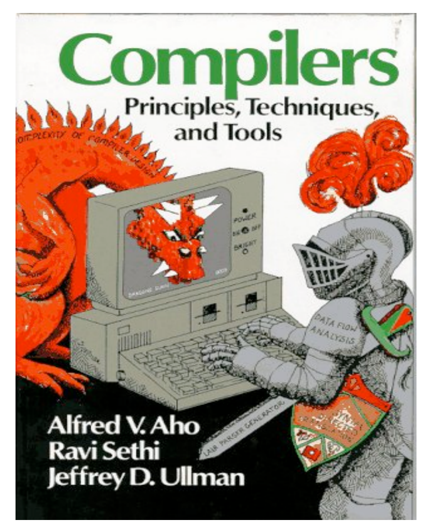
Correctness from first principles

Automated checking

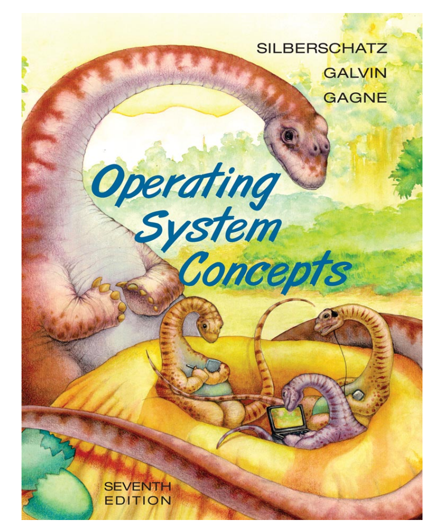
4 colour theorem



Kepler conjecture



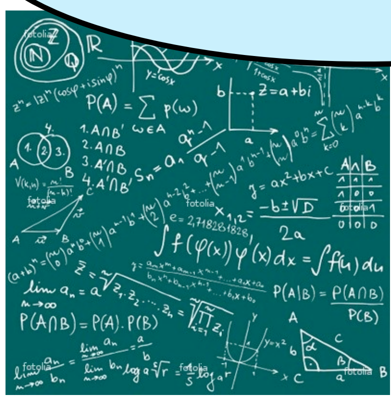
C compiler



seL4 HyperV

A primer on computer-aided proofs

Manual review

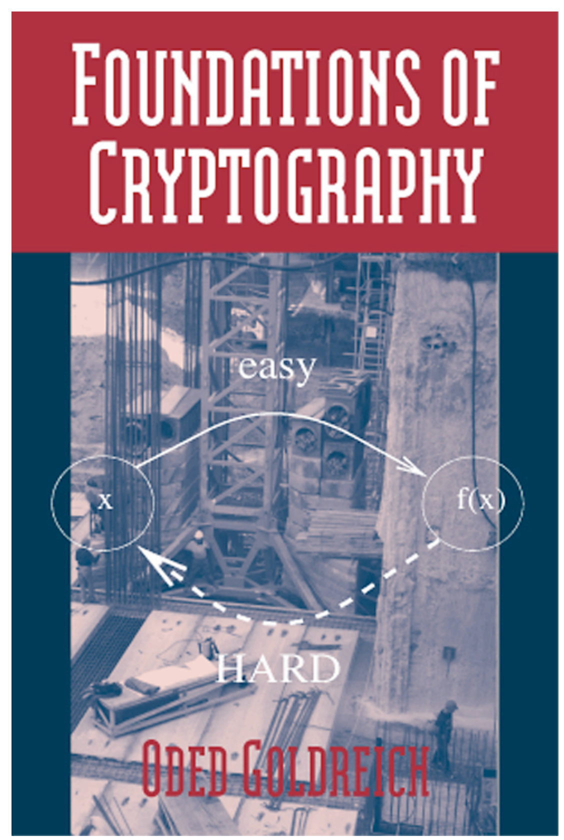


Lemma : $\forall r : \mathbb{R}, \exists n : \mathbb{N}. r < n$

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:

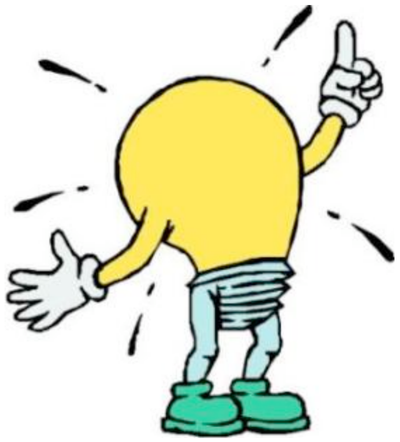
- Code-based game-based technique
- Independently verifiable proofs
- Applied to FDH, OAEP, Sigma-Protocols, IBE

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



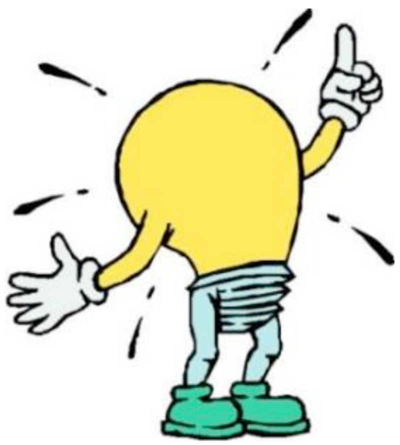
High level of Coq expertise and a lot of time

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

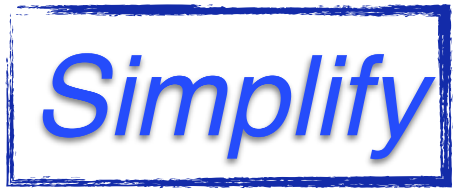


High level of Coq expertise and a lot of time

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

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

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

$\Pr[\mathsf{IND-CPA} : b = b']$
$= \Pr[\mathsf{G}_1 : b = b']$

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

Game LCDH :
$x \stackrel{\$}{\leftarrow} \mathbb{Z}_q;\ y \stackrel{\$}{\leftarrow} \mathbb{Z}_q;$
$L \leftarrow \mathcal{B}(g^x, g^y);$
$\mathsf{return}\ (g^{xy} \in L)$

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

The essence of game-based proofs

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

→

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

→

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

→

$\Pr[\mathsf{IND-CPA} : b = b']$
$= \Pr[\mathsf{G}_1 : b = b']$

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

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

→

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

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

The essence of game-based proofs

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

$\longrightarrow$

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

$\longrightarrow$

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

$\longrightarrow$

$\Pr[\mathsf{IND-CPA} : b = b']$
$= \Pr[\mathsf{G}_1 : b = b']$

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

$\Pr[\mathsf{G}_2 : b = b'] = \Pr[\mathsf{G}_3 : b = b'] = \dfrac{1}{2}$
$\Pr[\mathsf{G}_2 : \hat{y} \in L] = \Pr[\mathsf{G}_3 : \hat{y} \in L]$

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

$\longrightarrow$

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

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

The essence of game-based proofs

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

→

$$\Pr[\mathsf{IND-CPA} : b=b'] = \Pr[\mathsf{G}_1 : b=b']$$

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

$$\Pr[\mathsf{G}_2 : b=b'] = \Pr[\mathsf{G}_3 : b=b'] = \frac{1}{2}$$
$$\Pr[\mathsf{G}_2 : \hat{y} \in L] = \Pr[\mathsf{G}_3 : \hat{y} \in L]$$

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

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

The essence of game-based proofs

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

$$\Pr[\mathsf{IND-CPA} : b = b'] = \Pr[\mathsf{G}_1 : b = b']$$

→

$$
\begin{array}{l}
\textbf{Game } \mathsf{G}_1: \\
x \stackrel{\$}{\leftarrow} \mathbb{Z}_q;\ \alpha \leftarrow g^x; \\
y \stackrel{\$}{\leftarrow} \mathbb{Z}_q;\ \hat{y} \leftarrow \alpha^y; \\
(m_0,m_1) \leftarrow \mathcal{A}_1(\alpha); \\
b \stackrel{\$}{\leftarrow} \{0,1\}; \\
h \leftarrow H(\hat{y}); \\
b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b); \\
\mathsf{return}\ (b=b')
\end{array}
$$

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

→

$$
\begin{array}{l}
\textbf{Game } \mathsf{G}_2: \\
x \stackrel{\$}{\leftarrow} \mathbb{Z}_q;\ \alpha \leftarrow g^x; \\
y \stackrel{\$}{\leftarrow} \mathbb{Z}_q;\ \hat{y} \leftarrow \alpha^y; \\
(m_0,m_1) \leftarrow \mathcal{A}_1(\alpha); \\
b \stackrel{\$}{\leftarrow} \{0,1\}; \\
h \stackrel{\$}{\leftarrow} \{0,1\}^k; \\
b' \leftarrow \mathcal{A}_2(g^y, h \oplus m_b); \\
\mathsf{return}\ (b=b')
\end{array}
$$

$$\Pr[\mathsf{G}_2 : b = b'] = \Pr[\mathsf{G}_3 : b = b'] = \frac{1}{2}$$
$$\Pr[\mathsf{G}_2 : \hat{y} \in L] = \Pr[\mathsf{G}_3 : \hat{y} \in L]$$

→

$$
\begin{array}{l}
\textbf{Game } \mathsf{G}_3: \\
x \stackrel{\$}{\leftarrow} \mathbb{Z}_q;\ \alpha \leftarrow g^x; \\
y \stackrel{\$}{\leftarrow} \mathbb{Z}_q;\ \hat{y} \leftarrow \alpha^y; \\
(m_0,m_1) \leftarrow \mathcal{A}_1(\alpha); \\
b \stackrel{\$}{\leftarrow} \{0,1\}; \\
h \stackrel{\$}{\leftarrow} \{0,1\}^k; \\
b' \leftarrow \mathcal{A}_2(g^y, h); \\
\mathsf{return}\ (b=b')
\end{array}
$$

→

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

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

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

The essence of game-based proofs

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

$\longrightarrow$

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 $(b=b')$

$\longrightarrow$

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 $(b=b')$

$\longrightarrow$

$\Pr[\mathsf{IND-CPA} : b=b']$
$= \Pr[\mathsf{G}_1 : b=b']$

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

$\Pr[\mathsf{G}_2 : b=b'] = \Pr[\mathsf{G}_3 : b=b'] = \frac{1}{2}$
$\Pr[\mathsf{G}_2 : \hat{y} \in L] = \Pr[\mathsf{G}_3 : \hat{y} \in L]$

Game G_3 :

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b=b')\langle 1\rangle = (b=b')\langle 2\rangle$

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

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

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

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

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

The essence of game-based proofs

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

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

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

$\Pr[\mathsf{IND-CPA} : b = b']$
$= \Pr[\mathsf{G}_1 : b = b']$

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

$\Pr[\mathsf{G}_2 : b = b'] = \Pr[\mathsf{G}_3 : b = b'] = \frac{1}{2}$
$\Pr[\mathsf{G}_2 : \hat{y} \in L] = \Pr[\mathsf{G}_3 : \hat{y} \in L]$

Game G_3 :

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

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

Game LCDH :
$\stackrel{\$}{\leftarrow} \mathbb{Z}_q;\ y$
$\leftarrow \mathcal{B}(g^x,$
urn $(g^{xy}$

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

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

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

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

The essence of game-based proofs

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

→

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

→

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

→

$$\Pr[\mathsf{IND-CPA} : b = b'] = \Pr[\mathsf{G}_1 : b = b']$$

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

$$\Pr[\mathsf{G}_2 : b = b'] = \Pr[\mathsf{G}_3 : b = b'] = \frac{1}{2}$$
$$\Pr[\mathsf{G}_2 : \hat{y} \in L] = \Pr[\mathsf{G}_3 : \hat{y} \in L]$$

Game G_3 :

Game LCDH :
$\stackrel{\$}{\leftarrow} \mathbb{Z}_q;\ y$
$\leftarrow \mathcal{B}(g^x,$
urn $(g^{xy}$

$$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1\rangle = (b = b')\langle 2\rangle$$

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

$b \stackrel{\$}{\leftarrow} \{0,1\};$

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

$$\models \mathsf{G}_2 \sim \mathsf{G}_3 : \mathsf{true} \Longrightarrow (b = b')\langle 1\rangle = (b = b')\langle 2\rangle \wedge (\hat{y} \in L)\langle 1\rangle = (\hat{y} \in L)\langle 2\rangle$$

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

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

The essence of game-based proofs

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

→

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

→

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

→

$\Pr[\mathsf{IND-CPA} : b = b']$
$= \Pr[\mathsf{G}_1 : b = b']$

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

$\Pr[\mathsf{G}_2 : b = b'] = \Pr[\mathsf{G}_3 : b = b'] = \frac{1}{2}$
$\Pr[\mathsf{G}_2 : \hat{y} \in L] = \Pr[\mathsf{G}_3 : \hat{y} \in L]$

Game G_3 :

Game LCDH :

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

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

$b \stackrel{\$}{\leftarrow} \{0,1\};$

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

$\models \mathsf{G}_2 \sim \mathsf{G}_3 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle \wedge (\hat{y} \in L)\langle 1 \rangle = (\hat{y} \in L)\langle 2 \rangle$

$\models \mathsf{G}_3 \sim \mathsf{LCDH} : \mathsf{true} \Longrightarrow (\hat{y} \in L)\langle 1 \rangle = (g^{xy} \in L)\langle 2 \rangle$

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

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

The essence of game-based proofs

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

$\longrightarrow$

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

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

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

Automated verification of proof sketches

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1\rangle = (b = b')\langle 2\rangle$

Game $\mathsf{IND-CPA}$:

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

$\Pr[\mathsf{IND-CPA} : b = b']$
$= \Pr[\mathsf{G}_1 : b = b']$

Game G_1 :

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

Automated verification of proof sketches

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

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

Inline

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

Automated verification of proof sketches

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1\rangle = (b = b')\langle 2\rangle$

Game IND − CPA :

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

Inline

Eager Sampling

Game G_1 :

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

Automated verification of proof sketches

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

Game IND − CPA :

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

Game G_1 :

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

Inline

Eager Sampling

Relational invariant

Automated verification of proof sketches

$$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$$

Game IND − CPA :

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

Game G_1 :

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

Inline

Eager Sampling

Witness

Relational invariant

Automated verification of proof sketches

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

Game IND − CPA :

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

Game G_1 :

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

Inline

Check VC

Eager Sampling

Witness

Relational invariant

Automated verification of proof sketches

Alt Ergo

Simplify

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

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

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

Inline

Eager Sampling

Check VC

Witness

Relational invariant

Automated verification of proof sketches

Simplify

```
equiv Fact1 : INDCPA.Main ~ G1.Main : {true} ==> ={res}
 inline KG, Enc; derandomize; auto inv ={L,LA}; pop{2} 1; repeat rnd; trivial;;
save;;
```

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

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

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

Inline

Check VC

Eager Sampling

Witness

Relational invariant

Automated verification of proof sketches

Alt Ergo

Simplify

```
equiv Fact1 : INDCPA.Main ~ G1.Main : {true} ==> ={res}
 inline KG, Enc; derandomize; auto inv ={L,LA}; pop{2} 1; repeat rnd; trivial;;
save;;
```

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

Game IND − CPA :

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

Game G_1 :

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

Automated verification of proof sketches

Simplify

```
equiv Fact1 : INDCPA.Main ~ G1.Main : {true} ==> ={res}
 inline KG, Enc; derandomize; auto inv ={L,LA}; pop{2} 1; repeat rnd; trivial;;
save;;

   claim Pr1 : INDCPA.Main[res] == G1.Main[res]  using Fact1;;
```

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1 \rangle = (b = b')\langle 2 \rangle$

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 $(b = b')$

$$\Pr[\mathsf{IND-CPA} : b = b'] = \Pr[\mathsf{G}_1 : b = b']$$

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 Fact1 : INDCPA.Main ~ G1.Main : {true} ==> ={res}
 inline KG, Enc; derandomize; auto inv ={L,LA}; pop{2} 1; repeat rnd; trivial;;
save;;

  claim Pr1 : INDCPA.Main[res] == G1.Main[res]  using Fact1;;
```

Simplify

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1\rangle = (b = b')\langle 2\rangle$

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

$$\Pr[\mathsf{IND-CPA} : b = b'] = \Pr[\mathsf{G}_1 : b = b']$$

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

Automated verification of proof sketches


```
equiv Fact1 : INDCPA.Main ~ G1.Main : {true} ==> ={res}
 inline KG, Enc; derandomize; auto inv ={L,LA}; pop{2} 1; repeat rnd; trivial;;
save;;

   claim Pr1 : INDCPA.Main[res] == G1.Main[res]  using Fact1;;
```

Simplify

$\models \mathsf{IND-CPA} \sim \mathsf{G}_1 : \mathsf{true} \Longrightarrow (b = b')\langle 1\rangle = (b = b')\langle 2\rangle$

Game $\mathsf{IND-CPA}$:

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

$\Pr[\mathsf{IND-CPA} : b = b']$
$= \Pr[\mathsf{G}_1 : b = b']$

Game G_1 :

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

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

Case studies

Cramer-Shoup encryption system:

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

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 ×2 to ÷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