RUB

RUHR-UNIVERSITÄT BOCHUM

Replacing a Random Oracle

Full Domain Hash From Indistinguishabilitly Obfuscation

UbiCrypt Seminar Lecture Series, 22.01.2015

Felix Heuer
Horst Görtz Institute for IT Security
Ruhr University Bochum

hgi
Horst Görtz Institut
für IT-Sicherheit

Recap: RSA Full Domain Hash Signatures

- Gen: $(N, e, d) \leftarrow \text{RSAGen}$ s.t. $N = p \cdot q$ and $e \cdot d = 1 \mod \Phi(N)$.
  $pk = (N, e)$, $sk = (N, d)$.

Recap: RSA Full Domain Hash Signatures

§ Gen: $(N, e, d) \leftarrow \text{RSAGen}$ s.t. $N = p \cdot q$ and $e \cdot d = 1 \mod \Phi(N)$.
$pk = (N, e)$, $sk = (N, d)$.

§ Sign(m):

$$\sigma = H(m)^d \mod N.$$

$H : \{0,1\}^* \to \mathbb{Z}_N^*$ is modeled as a Random Oracle.

Recap: RSA Full Domain Hash Signatures

- Gen: $(N, e, d) \leftarrow \text{RSAGen}$ s.t. $N = p \cdot q$ and $e \cdot d = 1 \mod \Phi(N)$.
  $pk = (N, e)$, $sk = (N, d)$.

- Sign(m):

$$\sigma = H(m)^d \mod N.$$

- Vrfy(m, σ):

$$\sigma^e \stackrel{?}{=} H(m) \mod N.$$

$H : \{0,1\}^* \to \mathbb{Z}_N^*$ is modeled as a Random Oracle.

Proof idea

Theorem 1 (Bellare, Rogaway '93)

RSA FDH Hash is selectively secure in the Random Oracle Model if the RSA Assumption holds.

$\mathcal{A}$ has to commit to the message m^* for which he is going to provide a forgery in advance.

Proof idea

Theorem 1 (Bellare, Rogaway '93)

RSA FDH Hash is selectively secure in the Random Oracle Model if the RSA Assumption holds.

$\mathcal{A}$ has to commit to the message m^* for which he is going to provide a forgery in advance.
Given (N, e) and $y = x^e \mod N$ for some $x \xleftarrow{\$} \mathbb{Z}_N^*$, find x.

Proof idea

Theorem 1 (Bellare, Rogaway '93)

RSA FDH Hash is selectively secure in the Random Oracle Model if the RSA Assumption holds.

$\mathcal{A}$ has to commit to the message m^* for which he is going to provide a forgery in advance.

Given (N, e) and $y = x^e \mod N$ for some $x \xleftarrow{\$} \mathbb{Z}_N^*$, find x.

Answer Hash queries $H(m_i)$ with σ_i^e for random $\sigma_i \xleftarrow{\$} \mathbb{Z}_N^*$.

Proof idea

Theorem 1 (Bellare, Rogaway '93)

RSA FDH Hash is selectively secure in the Random Oracle Model if the RSA Assumption holds.

$\mathcal{A}$ has to commit to the message m^* for which he is going to provide a forgery in advance.
Given (N, e) and $y = x^e \mod N$ for some $x \xleftarrow{\$} \mathbb{Z}_N^*$, find x.
Answer Hash queries $H(m_i)$ with σ_i^e for random $\sigma_i \xleftarrow{\$} \mathbb{Z}_N^*$.
Program $H(m^*) := y$ and hope $\mathcal{A}$ provides a valid forgery σ^*, then σ^* solves the RSA Challenge:

$$\sigma^* = H(m^*)^d = y^d = x \mod N.$$

EUROCRYPT '14 (Hohenberger, Sahai and Waters)

Replacing a Random Oracle:
Full Domain Hash From Indistinguishability Obfuscation

EUROCRYPT '14 (Hohenberger, Sahai and Waters)

Replacing a Random Oracle:
Full Domain Hash From Indistinguishability Obfuscation

Theorem

Let F be a (punctured) PRF, $i\mathcal{O}$ be an Indistinguishability Obfuscator. RSA FDH is selectively secure in the Standard Model if the RSA Assumption holds.

Indistinguishability Obfuscators

A ppt algorithm $i\mathcal{O}$ that obfuscates a given program $\mathtt{P}$ such that

- Given $\mathtt{P}$, $i\mathcal{O}$ outputs a program $\boxed{\mathtt{P}}$ such that $\mathtt{P}(x) = \boxed{\mathtt{P}}(x)$ for all possible inputs x.
- Given Programs $\mathtt{P}_1$ and $\mathtt{P}_2$ such that $\mathtt{P}_1(x) = \mathtt{P}_2(x)$ for all possible inputs x,

$$\boxed{\mathtt{P}_1} \approx_c \boxed{\mathtt{P}_2}.$$

Proof in the Standard Model

G_0

$$H(\cdot) := \boxed{\begin{cases} F_k(\cdot)^e \\ \\ \end{cases}}$$

We can sign messages without knowing d since $\sigma_i = (H(m_i))^d = F_k(m_i)$ and k is known.

Proof in the Standard Model

$G_0 \rightsquigarrow G_1$

$$H(\cdot) := \boxed{\begin{cases} F_k(\cdot)^e & \text{for } m \neq m^* \\ z^* & \text{for } m = m^* \end{cases}}$$

We can sign messages without knowing d since $\sigma_i = (H(m_i))^d = F_k(m_i)$ and k is known.
Let $z^* := F_k(m^*)^e$

Proof in the Standard Model

$$G_0 \rightsquigarrow G_1 \rightsquigarrow G_2$$

$$H(\cdot) := \boxed{\begin{cases} F_k(\cdot)^e & \text{for } m \neq m^* \\ z^* & \text{for } m = m^* \end{cases}}$$

We can sign messages without knowing d since $\sigma_i = (H(m_i))^d = F_k(m_i)$ and k is known.
Let $z^* := x^e$ for uniformly random x.

Proof in the Standard Model

$$G_0 \rightsquigarrow G_1 \rightsquigarrow G_2$$

$$H(\cdot) := \boxed{\begin{cases} F_k(\cdot)^e & \text{for } m \neq m^* \\ z^* & \text{for } m = m^* \end{cases}}$$

We can sign messages without knowing d since $\sigma_i = (H(m_i))^d = F_k(m_i)$ and k is known.
Let $z^* := x^e$ for uniformly random x.
We can embed a given RSA Challenge by setting $z^* := y = x^e$ for unknown x.

RUB

RUHR-UNIVERSITÄT BOCHUM

Many thanks for your attention!

QUESTIONS?

hgi
Horst Görtz Institut
für IT-Sicherheit