COPS: The Curious Case of PPEnc

Sanjit Chatterjee and M. Prem Laxman Das

Rump Session, Asiacrypt 2013
Eurocrypt 2012

- Pandey-Rouselakis [PR] Property Preserving Encryption.
COPS \textit{meets} PPEnc

Eurocrypt 2012

- **Menezes**: Cryptanalysis Of Provable Security.
- **Pandey-Rouselakis [PR]** Property Preserving Encryption.
  1. Definition and Security Notions of PPEnc.
  2. Separation results.
  3. Provably secure scheme for testing orthogonality.
Eurocrypt 2012

- Pandey-Rouselakis [PR] Property Preserving Encryption.
  1. Definition and Security Notions of PPEnc.
  2. Separation results.
  3. Provably secure scheme for testing orthogonality.
  4. Three theorems.
COPS meets PPENC

Eurocrypt 2012

- Pandey-Rouselakis [PR] Property Preserving Encryption.
  1. Definition and Security Notions of PPENC.
  2. Separation results.
  3. Provably secure scheme for testing orthogonality.
  4. Three theorems.

COPS Philosophy: Concrete analysis of concrete situation
PPTag to Test Orthogonality of Vectors

Given ciphertext of \( \overrightarrow{x} = (x_1, x_2) \) and \( \overrightarrow{y} = (y_1, y_2) \)

Check: \( \overrightarrow{x} \cdot \overrightarrow{y} \neq 0 \) (and no other meaningful information)
PPTag to Test Orthogonality of Vectors

Given ciphertext of $\vec{x} = (x_1, x_2)$ and $\vec{y} = (y_1, y_2)$

Check: $\vec{x} \cdot \vec{y} \neq 0$ (and no other meaningful information)

Setup $e : G \times G \rightarrow G_T$, $|G| = |G_T| = N = pq$

Select $(\gamma_1, \gamma_2) \in \mathbb{Z}_q$ s.t. $\gamma_1^2 + \gamma_2^2 = \delta^2$ (mod $q$)

$G_p = \langle g_0 \rangle$, $G_q = \langle g_1 \rangle$, $M = (\mathbb{Z}_N^* \cup \{0\})^2$

$$PP = \langle N, G, G_T, e \rangle, \quad SK = \langle g_0, g_1, \gamma_1, \gamma_2, \delta \rangle,$$

Encrypt $M = (m_1, m_2)$

Select $\phi, \psi \in \mathbb{R} \mathbb{Z}_N$

$$CT = (ct_0, ct_1, ct_2) = \left( g_1^\psi \delta, g_0^{\phi m_1} \cdot g_1^{\psi \gamma_1}, g_0^{\phi m_2} \cdot g_1^{\psi \gamma_2} \right).$$

Test($PP, CT^{(1)}, CT^{(2)}$): outputs 1 iff

$$\prod_{i=1}^{2} e(ct_i^{(1)}, ct_i^{(2)}) = e(ct_0^{(1)}, ct_0^{(2)}).$$
Hey...What’s the Magic?

Test checks

\[ e(g_1, g_1)^{\phi(1) \phi(2) \delta^2} = e(g_1, g_1)^{\phi(1) \phi(2) (\gamma_1^2 + \gamma_2^2)} e(g_0, g_0)^{\psi(1) \psi(2) (m_1^1 m_1^2 + m_2^1 m_2^2)} \]

Recall

\[ \gamma_1^2 + \gamma_2^2 = \delta^2 \pmod{q} \]
Hey...What’s the Magic?

Test checks

\[ e(g_1, g_1)^{\phi(1) \phi(2) \delta^2} \equiv e(g_1, g_1)^{\phi(1) \phi(2) (\gamma_1^2 + \gamma_2^2)} e(g_0, g_0)^{\psi(1) \psi(2) (m_1(1) m_1(2) + m_2(1) m_2(2))} \]

Recall

\[ \gamma_1^2 + \gamma_2^2 = \delta^2 \pmod{q} \]

Theorem [PR]: Advantage of \( \mathcal{A} \) in the strongest security game (LoR) is at most \( O((nQ + W)^2 \cdot 2^{-\lambda}) \).
Hey...What’s the Magic?

Test checks

\[ e(g_1, g_1)^{\phi(1) \phi(2) \delta^2} = e(g_1, g_1)^{\phi(1) \phi(2) (\gamma_1^2 + \gamma_2^2)} e(g_0, g_0)^{\psi(1) \psi(2) (m_1^1 m_1^2 + m_2^1 m_2^2)} \]

Recall

\[ \gamma_1^2 + \gamma_2^2 = \delta^2 \pmod{q} \]

**Theorem [PR]:** Advantage of \( \mathcal{A} \) in the strongest security game (LoR) is at most \( O((nQ + W)^2 \cdot 2^{-\lambda}) \).

**Proof:** Full Version.
Hey...What’s the Magic?

Test checks

\[ e(g_1, g_1)^{\phi(1)\phi(2)\delta^2} \overset{?}{=} e(g_1, g_1)^{\phi(1)\phi(2)(\gamma_1^2 + \gamma_2^2)} e(g_0, g_0)^{\psi(1)\psi(2)(m_1^1 m_1^2 + m_2^1 m_2^2)} \]

Recall

\[ \gamma_1^2 + \gamma_2^2 = \delta^2 \pmod{q} \]

Theorem [PR]: Advantage of \( \mathcal{A} \) in the strongest security game (LoR) is at most \( O((nQ + W)^2 \cdot 2^{-\lambda}) \).

Proof: Full Version.

COPS Recall what your Guru once said:

Never be fooled by a zero-knowledge proof!
Hey...What’s the Magic?

Test checks

\[ e(g_1, g_1)^{\phi(1)\phi(2)\delta^2} \equiv e(g_1, g_1)^{\phi(1)\phi(2)(\gamma_1^2 + \gamma_2^2)} e(g_0, g_0)^{\psi(1)\psi(2)(m_1^1 m_1^2 + m_2^1 m_2^2)} \]

Recall

\[ \gamma_1^2 + \gamma_2^2 = \delta^2 \pmod{q} \]

**Theorem [PR]:** Advantage of \( A \) in the strongest security game (LoR) is at most \( O((nQ + W)^2 \cdot 2^{-\lambda}) \).

**Proof:** Full Version.

COPS Recall what your *Guru* once said:

Never be fooled by a zero-knowledge proof!

\[ \delta^2 = \gamma_1^2 + \gamma_2^2 = \]
Hey...What’s the Magic?

Test checks

\[ e(g_1, g_1)^{\phi(1)\phi(2)\delta^2} \equiv e(g_1, g_1)^{\phi(1)\phi(2)(\gamma_1^2 + \gamma_2^2)} e(g_0, g_0)^{\psi(1)\psi(2)(m_1(1)m_2(2) + m_1(2)m_2(1))} \]

Recall

\[ \gamma_1^2 + \gamma_2^2 = \delta^2 \pmod{q} \]

**Theorem [PR]:** Advantage of \( A \) in the strongest security game (LoR) is at most \( O((nQ + W)^2 \cdot 2^{-\lambda}) \).

**Proof:** Full Version.

COPS Recall what your *Guru* once said:

Never be fooled by a zero-knowledge proof!

\[ \delta^2 = \gamma_1^2 + \gamma_2^2 = \gamma_1(\gamma_1 + \gamma_2) + \gamma_2(\gamma_2 - \gamma_1) \pmod{q} \]
(i) COPS sends challenges $\mathbf{m}_0^* = (1, 0)$ and $\mathbf{m}_1^* = (0, 1)$.

COPS has to decide which $\mathbf{m}_b^*$ is encrypted as challenge cipher.

Lo and behold: COPS has a (pseudo)-ciphertext for $(2, 0)$ and $(2, 0)$ is orthogonal to $(0, 1)$ but not to $(1, 0)$.

The public Test allows COPS to distinguish an encryption of $(0, 1)$ from $(1, 0)$. 
(i) COPS sends challenges \( \overrightarrow{m}^*_0 = (1, 0) \) and \( \overrightarrow{m}^*_1 = (0, 1) \). COPS has to decide which \( \overrightarrow{m}^*_b \) is encrypted as challenge cipher.

(ii) COPS asks for the encryption of \( \overrightarrow{m} = (1, 1) \) and receives:

\[
(C_0, C_1, C_2) = (g_1^{\psi \delta}, g_0^{1 \cdot \phi} g_1^{\psi \gamma_1}, g_0^{1 \cdot \phi} g_1^{\psi \gamma_2})
\]
The Assault

(i) COPS sends challenges $\overrightarrow{m_0^*} = (1, 0)$ and $\overrightarrow{m_1^*} = (0, 1)$. COPS has to decide which $\overrightarrow{m_b}$ is encrypted as challenge cipher.

(ii) COPS asks for the encryption of $\overrightarrow{m} = (1, 1)$ and receives:

$$(C_0, C_1, C_2) = (g_1^{\psi\delta}, g_0^{1\cdot\phi} g_1^{\gamma_1}, g_0^{1\cdot\phi} g_1^{\gamma_2})$$

(iii) COPS does some juggling:

$$(C_0, C_1 \cdot C_2, C_2/C_1) = \langle g_1^{\psi\delta}, g_0^{2\phi} g_1^{\psi(\gamma_1+\gamma_2)}, g_1^{\psi(\gamma_2-\gamma_1)} \rangle.$$
(i) COPS sends challenges $\overrightarrow{m_0^*} = (1, 0)$ and $\overrightarrow{m_1^*} = (0, 1)$. COPS has to decide which $\overrightarrow{m_b^*}$ is encrypted as challenge cipher.

(ii) COPS asks for the encryption of $\overrightarrow{m} = (1, 1)$ and receives:

$$(C_0, C_1, C_2) = (g_1^{\psi \delta}, g_0 1^{\phi} g_1^{\psi \gamma_1}, g_0 1^{\phi} g_1^{\psi \gamma_2})$$

(iii) COPS does some juggling:

$$(C_0, C_1 \cdot C_2, C_2/C_1) = \langle g_1^{\psi \delta}, g_0 2^{\phi} g_1^{\psi (\gamma_1 + \gamma_2)}, g_1^{\psi (\gamma_2 - \gamma_1)} \rangle.$$ 

**Lo and behold:** COPS has a (pseudo)-ciphertext for $(2, 0)$ and $(2, 0)$ is orthogonal to $(0, 1)$ but not to $(1, 0)$.

The public Test allows COPS to distinguish an encryption of $(0, 1)$ from $(1, 0)$. 

Chatterjee and Das

COPS: Property Preserving Encryption

Rump Session, Asiacrypt 2013
PR-PPEnc is not secure even in the *weaker* selective-FtG definition.
The story continues...

...assuming I’m able to bribe DANJA!

1. Spicy home-made Bengali food!
2. Wild elephants at Bandipur forest!
The story continues...

...assuming I’m able to bribe Danja!

1. Spicy home-made Bengali food!
2. Wild elephants at Bandipur forest!

- PR states two separation results of security notions of PPEnc.
  - Assumes the existence of a particular type of PPEnc secure under certain notions of security.
  - The theorems stand vacuous in the absence of a concrete scheme.

- We fill this gap by showing the existence of such scheme.
- For details:
  
  **Property Preserving Symmetric Encryption: Revisited**