Post-Quantum Security of the Fujisaki-Okamoto (FO) and OAEP Transforms

Made by:
Ehsan Ebrahimi

University of Tartu

Estonian-Latvian Theory Days, Lilaste, Latvia
13-16 October 2016
Joint work with **Dominique Unruh**

Motivation: Post-Quantum Cryptography

Users intend to use classical cryptographic schemes, however, the adversary has the **quantum computing power**.

[1] [Ambainis, Rosmanis and Unruh, Quantum attacks on classical proof systems (the hardness of quantum rewinding), FOCS 2014]

Motivation: Post-Quantum Cryptography

Users intend to use classical cryptographic schemes, however, the adversary has the **quantum computing power**.

1. Quantum hard problems are needed.

[1] [Ambainis, Rosmanis and Unruh, Quantum attacks on classical proof systems (the hardness of quantum rewinding), FOCS 2014]

Motivation: Post-Quantum Cryptography

Users intend to use classical cryptographic schemes, however, the adversary has the **quantum computing power**.

1. Quantum hard problems are needed.
2. Design cryptographic schemes based on them.

[1] [Ambainis, Rosmanis and Unruh, Quantum attacks on classical proof systems (the hardness of quantum rewinding), FOCS 2014]

Motivation: Post-Quantum Cryptography

Users intend to use classical cryptographic schemes, however, the adversary has the **quantum computing power**.

1. Quantum hard problems are needed.
2. Design cryptographic schemes based on them.
3. Prove quantum security: classical security may not work.

[1] [Ambainis, Rosmanis and Unruh, Quantum attacks on classical proof systems (the hardness of quantum rewinding), FOCS 2014]

Motivation: Post-Quantum Cryptography

Users intend to use classical cryptographic schemes, however, the adversary has the **quantum computing power**.

1. Quantum hard problems are needed.
2. Design cryptographic schemes based on them.
3. Prove quantum security: classical security may not work.
   - E.g. Security proofs in the Random Oracle Model.

[1] [Ambainis, Rosmanis and Unruh, Quantum attacks on classical proof systems (the hardness of quantum rewinding), FOCS 2014]

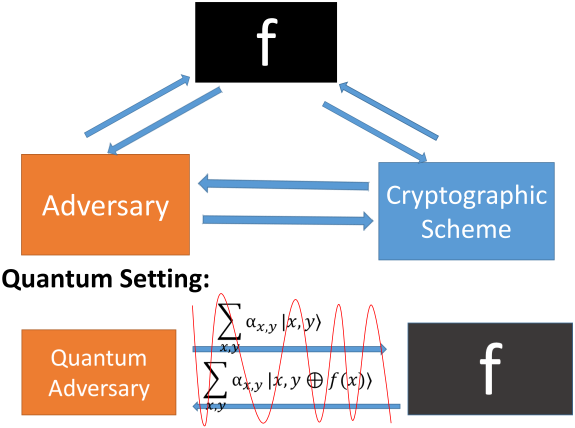
Motivation: Post-Quantum Cryptography

Users intend to use classical cryptographic schemes, however, the adversary has the **quantum computing power**.

1. Quantum hard problems are needed.
2. Design cryptographic schemes based on them.
3. Prove quantum security: classical security may not work.
   - E.g. Security proofs in the Random Oracle Model.
     - Relative to a specific oracle, the Fiat-Shamir transform is insecure in the quantum setting. [1]

[1] [Ambainis, Rosmanis and Unruh, Quantum attacks on classical proof systems (the hardness of quantum rewinding), FOCS 2014]

Random Oracle Model in quantum setting



[2] [Boneh et al. Random Oracles in a Quantum World. ASIACRYPT 2011]

Fujisaki-Okamoto (FO) transform

$$Enc^{hy}_{pk}(m;\delta) = \left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m)\right)$$

Fujisaki-Okamoto (FO) transform

$$Enc^{hy}_{pk}(m;\delta) = \left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m)\right)$$

Security goal: IND-CCA secure in the Random Oracle Model

Fujisaki-Okamoto (FO) transform

$$Enc^{hy}_{pk}(m;\delta) = \left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m)\right)$$

Security goal: IND-CCA secure in the Random Oracle Model

Properties of encryption schemes:

- The symmetric encryption scheme is One-time secure.
- The asymmetric encryption scheme is One-way secure.
- The asymmetric encryption scheme if Well-spread.

Fujisaki-Okamoto (FO) transform

$$Enc^{hy}_{pk}(m;\delta) = \left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m)\right)$$

Security goal: IND-CCA secure in the Random Oracle Model

Properties of encryption schemes:

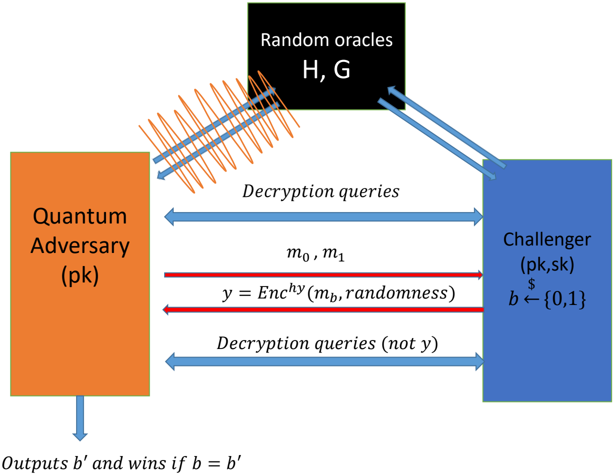
- The symmetric encryption scheme is One-time secure.
- The asymmetric encryption scheme is One-way secure.
- The asymmetric encryption scheme if Well-spread.

Question: What about security in the Quantum Random Oracle Model (QROM)?

Our contribution

Security of the slightly modified Fujisaki-Okamoto and OAEP transforms in the **Quantum** Random Oracle Model.

IND-CCA in the QROM



Challenges in the Quantum setting

$$Enc^{hy}_{pk}(m;\delta) = \left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m)\right)$$

Security techniques used in the classical proof:

1. List of $(\delta,\ H(\delta))$ and $(\delta, G(\delta))$ are needed!

Challenges in the Quantum setting

$$Enc^{hy}_{pk}(m;\delta) = \left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m)\right)$$

Security techniques used in the classical proof:

1. List of $(\delta,\ H(\delta))$ and $(\delta, G(\delta))$ are needed!
2. Reprogramme the random oracle: E.g. It uses a random element instead of a given output $G(\delta)$ and $H(\delta')$!

Challenges in the Quantum setting

$$Enc^{hy}_{pk}(m;\delta) = \left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m)\right)$$

Security techniques used in the classical proof:

1. List of $(\delta,\ H(\delta))$ and $(\delta, G(\delta))$ are needed!
2. Reprogramme the random oracle: E.g. It uses a random element instead of a given output $G(\delta)$ and $H(\delta')$!
3. Finding $x \neq x'$ st. $Enc^{asy}_{pk}(\delta; H(x)) = Enc^{asy}_{pk}(\delta; H(x'))$ is hard!

Challenges in the Quantum setting

$$Enc^{hy}_{pk}(m;\delta) = \left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m)\right)$$

Security techniques used in the classical proof:

1. List of $(\delta,\ H(\delta))$ and $(\delta, G(\delta))$ are needed!
2. Reprogramme the random oracle: E.g. It uses a random element instead of a given output $G(\delta)$ and $H(\delta')$!
3. Finding $x \neq x'$ st. $Enc^{asy}_{pk}(\delta; H(x)) = Enc^{asy}_{pk}(\delta; H(x'))$ is hard!

Solutions to the Challenges

1. List of $(x, H(x))$ and $(x, G(x))$ are needed!
   - Add $H'(\delta)$ to the ciphertext $\left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m), H'(\delta)\right)$.

[3] [Unruh, Revocable quantum timed-release encryption, Eurocrypt 2014]
[4] [Targhi, Tabia, Unruh. Quantum Collision-Resistance of Non-uniformly Distributed Functions. PQCrypto 2016]

Solutions to the Challenges

1. List of $(x, H(x))$ and $(x, G(x))$ are needed!
   - Add $H'(\delta)$ to the ciphertext
     $$\left(Enc_{pk}^{asy}\left(\delta; H\left(\delta \| Enc_{G(\delta)}^{sy}(m)\right)\right),\ Enc_{G(\delta)}^{sy}(m), H'(\delta)\right).$$
2. It uses a random element instead of a given output $H(\delta)$ or $G(\delta)$!
   - Using "One-way to hiding" Lemmas[3] as a tool to reprogramme the random oracle

[3] [Unruh, Revocable quantum timed-release encryption, Eurocrypt 2014]

[4] [Targhi, Tabia, Unruh. Quantum Collision-Resistance of Non-uniformly Distributed Functions. PQCrypto 2016]

Solutions to the Challenges

1. List of $(x, H(x))$ and $(x, G(x))$ are needed!
   - Add $H'(\delta)$ to the ciphertext $\left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m), H'(\delta)\right)$.
2. It uses a random element instead of a given output $H(\delta)$ or $G(\delta)$!
   - Using "One-way to hiding" Lemmas[3] as a tool to reprogramme the random oracle
3. Finding $x \neq x'$ st. $Enc^{asy}_{pk}(\delta; H(x)) = Enc^{asy}_{pk}(\delta; H(x'))$ is hard!
   - The collision resistance of random functions with outputs sampled from a non-uniform distribution [4]

[3] [Unruh, Revocable quantum timed-release encryption, Eurocrypt 2014]

[4] [Targhi, Tabia, Unruh. Quantum Collision-Resistance of Non-uniformly Distributed Functions. PQCrypto 2016]

Solutions to the Challenges

1. List of $(x, H(x))$ and $(x, G(x))$ are needed!
   - Add $H'(\delta)$ to the ciphertext $\left(Enc^{asy}_{pk}\left(\delta; H\left(\delta \| Enc^{sy}_{G(\delta)}(m)\right)\right),\ Enc^{sy}_{G(\delta)}(m), H'(\delta)\right)$.
2. It uses a random element instead of a given output $H(\delta)$ or $G(\delta)$!
   - Using "One-way to hiding" Lemmas[3] as a tool to reprogramme the random oracle
3. Finding $x \neq x'$ st. $Enc^{asy}_{pk}(\delta; H(x)) = Enc^{asy}_{pk}(\delta; H(x'))$ is hard!
   - The collision resistance of random functions with outputs sampled from a non-uniform distribution [4]

Comment: The same proof techniques work for OAEP transform

[3] [Unruh, Revocable quantum timed-release encryption, Eurocrypt 2014]

[4] [Targhi, Tabia, Unruh. Quantum Collision-Resistance of Non-uniformly Distributed Functions. PQCrypto 2016]

Question?

Thank you for listening!