Quantum security of the Fujisaki-Okamoto transform *

Ehsan Ebrahimi Targhi, Dominique Unruh

University of Tartu

April 25, 2015

Abstract

In this paper, we present a hybrid encryption scheme that is chosen ciphertext secure in the quantum random oracle model. Our scheme is a combination of an asymmetric and a symmetric encryption scheme that are secure in a weak sense. It is a slight modification of Fujisaki and Okamoto's transformation that is secure against classical adversaries.

keywords: Quantum, Random Oracle, Indistinguishability against chosen ciphertext attack.

Motivation: The interest in verifying the security of cryptosystems in the presence of a quantum adversary increased after the celebrated paper of Shor [Sho97]. Shor showed that any cryptosystem based on factoring problem and discrete logarithm problem is breakable in the existence of a quantum adversary. Also, many efficient classical cryptosystems are proved to be secure in the random oracle model [BR93] and many of them still lack equivalent proof in the quantum setting. Therefore to construct an efficient cryptosystem secure against quantum adversaries, even if we find a cryptographic primitive immune to quantum attacks, we may have to consider its security in the quantum random oracle model in which adversary has quantum access to the random oracle.

Fujisaki and Okamoto [FO99] constructed a hybrid encryption scheme that is secure against chosen ciphertext attack in the random oracle model. Their scheme is combination of a symmetric and an asymmetric encryption scheme using two hash functions where the symmetric and asymmetric encryption schemes are secure in a very weak sense. However, their proof of security works against a classical adversary and it is not clear how one can fix their proof in the quantum setting. Following, we mention the parts of the classical proof that may not follow against quantum adversaries. The classical proof uses the record list of random oracles to simulate the decryption algorithm without possessing the secret key of the asymmetric encryption scheme. In the quantum case, where adversary has quantum access to random oracles and submits queries in superpositions, there is no such a list. Also, the classical proof uses the fact that changing output of random oracle on one random input does not make it distinguishable from the original random oracle and this may not occur in the quantum case as long as adversary can query the random oracle in superposition of all inputs and see all corresponding outputs in one query. Finally, the classical proof uses the fact that finding a collision for a function whose outputs have a high min-entropy is difficult with classical access to the function and polynomial number of queries. However, this may not happen when adversary has quantum access to the function. Consequently, the quantum security of the scheme is left as an open problem in the related works of Boneh et al.[BDF+11] and Zhandry [Zha12].

Our Contribution: We modify the hybrid encryption scheme presented by Fujisaki and Okamoto using an extra hash function. We prove that our scheme is indistinguishable secure against chosen ciphertext attack in the quantum random oracle model. For message m, the encryption algorithm of our scheme, Enc^{hy}_{pk}, works as follows:

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

where pk and sk are the public key and the secret key of the asymmetric encryption scheme. Enc^{asy}_{pk} and Enc^{sy}_{sk} are the asymmetric and symmetric encryption algorithms respectively. δ is a random element

*Full paper: `http://www.cs.ut.ee/~unruh/qro.pdf`

from message space of the asymmetric encryption scheme. H, G and H' are random oracles with proper domain and co-domain. The asymmetric encryption scheme is One-Way secure, that is, adversary can not decrypt the encryption of a random message. The symmetric encryption scheme is One-Time secure, that is, adversary can not distinguish between encryption of two messages when a fresh key is used for every encryption. In addition, the asymmetric encryption scheme is well-spread in which any message can lead to at least $2^{\omega(\log n)}$ potential ciphertexts.

Following, we present an overview of our quantum security proof and explain how we overcome the challenges that appear in the quantum case. In the security proof, we introduce a sequence of games and compute the difference between their success probability. The first game presents the chosen ciphertext attack. Let (m_0, m_1) be the challenge message and (e^*, c^*, d^*) be the challenge ciphertext where e^* is the asymmetric encryption of δ^* that is chosen randomly from the message space of the asymmetric encryption scheme, c^* is the symmetric encryption of m_b using key $G(\delta^*)$ and d^* is output of H' on input δ^*. In the second game, we change the decryption algorithm. The new algorithm outputs $\perp$ if the first coordinate of the ciphertext is e^*. We show that the difference between the success probability of these two games can be bounded by the probability of finding a quantum collision for a function with a specific min-entropy. Here we use the existing result to find a quantum collision for non-uniformly distributed functions presented in [ETTU15]. Note that we use the well-spread assumption of the asymmetric encryption scheme to show that the bound is negligible. In the third game, we use a random key from the key space of the symmetric encryption scheme to encrypt m_b and also replace the third coordinate of challenge ciphertext with a random element chosen from the message space of the asymmetric encryption scheme. Now, we can obtain an upper bound for the difference between the success probability of the second game and the third game using the One-way to Hiding Lemma presented in [Unr14b]. Unruh gives an upper bound for any quantum adversary that is trying to distinguish between two random oracles that have different output on only one random input. We only need to show that the upper bound is negligible since the success probability of the third game can be reduced to the One-Time security of the symmetric encryption scheme for the reason that the key is chosen randomly. Therefore, we introduce the fourth game such that the success probability of the game is the upper bound obtained by the One-way to Hiding Lemma. In the fifth game, we replace the random oracle H' with a random polynomial in order to force the adversary to submit which input of δ has been used to obtain the ciphertext. This can be done due to result by Zhandry [Zha12] that shows a random oracle is indistinguishable from a $2q$-wise independent function where q is the number of quantum queries that adversary makes to the oracle function. Note that random polynomials of degree $2q-1$ are $2q$-wise independent. By calculating the roots of polynomial $H' - d$ where d is the third coordinate of ciphertext, we can find which element of the message space of the asymmetric encryption scheme is used to obtain the ciphrtext. Therefore, in the next game we replace the decryption algorithm with a new decryption algorithm that does not use the secret key of the asymmetric encryption scheme. In the seventh game, we replace $H(\delta^*, c^*)$ (this is the randomness that is used to obtain the first coordinate of challenge ciphertext, e^*) with a random element from the coin space of the asymmetric encryption scheme in order to be able to use the One-Way security of asymmetric encryption scheme in our proof. Finally, we use the adaptive One-way to Hiding Lemma presented in [Unr14a] to get an upper bound for the difference between the success probability of the sixth game and the seventh game. We introduce the eighth game such that the success probability of the game is this upper bound. We are able to reduce the success probability of the seventh game and the eighth game to the One-Way security of the asymmetric encryption scheme for the reason that we use a fresh randomness to get ciphertext e^* and also the decryption algorithm in these two games does not use the secret key of the asymmetric encryption scheme. This completes our proof.

Related Works: Boneh et al. [BDF+11] present a scheme that is secure in the random oracle model, but insecure in the quantum random oracle model. They also analyze in which condition a classical random oracle proof entails security in quantum random oracle model. Zhandry [Zha12] gives a proof of security for an identity-based encryption scheme in the quantum random oracle model. However, they techniques are not sufficient to prove the security of the scheme analyzed in this paper and they leave it as an open problem.

Unruh [Unr14a] present position verification scheme that is secure in the quantum random oracle model and avoids the assumption in prior works. Unruh [Unr15] construct a non-interactive zero-knowledge proof system in the quantum random oracle model.

References

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993.*, pages 62–73. ACM, 1993.

[ETTU15] Ehsan Ebrahimi Targhi, Gelo Tabia, and Dominique Unruh. Quantum collision-resistance of non-uniformly distributed functions. 2015. Available at `http://www.cs.ut.ee/~unruh/collision.pdf`.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '99, pages 537–554, London, UK, UK, 1999. Springer-Verlag.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[Unr14a] Dominique Unruh. Quantum position verification in the random oracle model. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II*, volume 8617 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2014.

[Unr14b] Dominique Unruh. Revocable quantum timed-release encryption. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 129–146. Springer, 2014.

[Unr15] Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 755–784. Springer, 2015.

[Zha12] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 758–775. Springer, 2012.