Quantum security of the Fiat-Shamir transform

Dominique Unruh

University of Tartu

Quantum computers threaten classical cryptography. With a quantum computer, an attacker would be able to break all schemes based on the hardness of factoring, or on the hardness of discrete logarithms [8]. This would affect most public key encryption and signature schemes is use today. For symmetric ciphers and hash functions, longer key and output lengths will be required due to considerable improvements in brute force attacks [5,3]. These threats lead to the question: how can classical cryptography be made secure against quantum attacks? Much research has been done towards cryptographic schemes based on hardness assumptions not known to be vulnerable to quantum computers, e.g., lattice-based cryptography. (This is called *post-quantum cryptography*.) Yet, identifying useful quantum-hard assumptions is only half of the problem. Even if the underlying assumption holds against quantum attackers, for many classically secure protocols it is not clear if they also resist quantum attacks: the proof techniques used in the classical setting often cannot be applied in the quantum world.

An example of such a protocol is the popular Fiat-Shamir transform [4], a transformation that takes a so-called sigma-protocol (i.e., a simple kind of zero-knowledge proof) and transforms it into a highly efficient *non-interactive* zero-knowledge proof. This in turn also yields a highly efficient signature scheme. In the classical setting, the security of Fiat-Shamir is well-studied; the "forking lemma" [7] allows us to deal with the interaction of rewinding[1] and random oracles in the proof. Unfortunately, both rewinding and random oracles are notoriously difficult in the quantum setting. Rewinding, when done naively, contradicts the no-cloning theorem (but in some cases it can be done [11,9]), and the random oracle can be queried in superposition [2], moving the proofs into the realm of quantum query complexity.

Indeed, [1] shows that the Fiat-Shamir transform is insecure in general.[2]

This is unfortunate, since no other general construction of comparable efficiency is known. (The construction from [10] is a quantum secure non-interactive zero-knowledge proof from any sigma-protocol, but it is much less efficient.) In this work, we set out to save Fiat-Shamir. In [9], an extra condition on sigma-protocols was introduced, "strict soundness" and shown to circumvent the impossibility results from [1] for *interactive* protocols. . (Roughly, strict soundness means that the third message is determined by the first two.) We give evidence that the same holds for Fiat-Shamir. In particular, our contributions are:

- We formalize the security notions achieved by Fiat-Shamir in the quantum case. (Zero-knowledge and simulation-sound extractability.) These turn out to be non-trivial, because a one-to-one translation of the classical definitions leads to trivially unachievable definitions.
- We prove: If the "quantum forking lemma" (see below) holds, then Fiat-Shamir is secure (zero-knowledge and simulation-sound extractable; assuming strict soundness of the underlying sigma-protocol).
- And we show that these security notions imply the existence of signatures, like in the classical case.

What is the (conjectured) quantum forking lemma? Rougly, it states:

[1] This refers to a proof technique where the state of the adversary is stored and reproduced later.

[2] Relative to some oracle.

Conjecture (Quantum forking lemma – informal) Let M^H be a *projective* measurement that can be implemented by a quantum circuit making polynomially many queries to a random function H. Measure some quantum system X using M^H, this leads an outcome x. Change the function H at input x: $H(x) := \mathit{random}$. Measure the quantum system X again using M^H (but with the changed H), this leads an outcome x'.
Then $x = x'$ with non-negligible probability.

Intuitively this means: A projective measurement cannot find an input x for H so that the post-measurement state encodes much information about $H(x)$.[3]

Summarizing, we have reduced the security of Fiat-Shamir to a self-contained query complexity question. Proving the quantum forking lemma will show the security of Fiat-Shamir.

References

1. A. Ambainis, A. Rosmanis, and D. Unruh. Quantum attacks on classical proof systems (the hardness of quantum rewinding). In *FOCS 2014*, pages 474–483. IEEE, October 2014.
2. D. Boneh, O. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In *ASIACRYPT 2011*, pages 41–69, Berlin, Heidelberg, 2011. Springer-Verlag.
3. G. Brassard, P. Høyer, and A. Tapp. Quantum algorithm for the collision problem. *ACM SIGACT News*, 28:14–19, 1997. Full version at arXiv:quant-ph/9705002.
4. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. M. Odlyzko, editor, *Advances in Cryptology, Proceedings of CRYPTO '86*, number 263 in Lecture Notes in Computer Science, pages 186–194. Springer-Verlag, 1987.
5. L. K. Grover. A fast quantum mechanical algorithm for database search. In *STOC*, pages 212–219, 1996.
6. R. Koenig, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. `http://arxiv.org/abs/0807.1338`.
7. D. Pointcheval and J. Stern. Security proofs for signature schemes. In U. Maurer, editor, *Eurocrypt 96*, volume 1070 of *LNCS*, pages 387–398. Springer, 1996.
8. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *FOCS 1994*, pages 124–134. IEEE, 1994.
9. D. Unruh. Quantum proofs of knowledge. In *Eurocrypt 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, April 2012. Preprint on IACR ePrint 2010/212.
10. D. Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *Eurocrypt 2015*, volume 9057, pages 755–784. Springer, 2015. IACR ePrint 2014/587.
11. J. Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009.

[3] Formally, if x is the outcome of the measurement M^H, the max-entropy [6] of $H(x)$ is superlogarithmic given x, X, and all values $H(x')$ except for $H(x)$.