Post-Quantum Security of Fiat-Shamir

Dominique Unruh
University of Tartu

Abstract. We show the post-quantum security of the Fiat-Shamir construction (Crypto 1986), both as a proof system, and as a signature scheme. We circumvent the impossibility results from Ambainis, Rosmanis, and Unruh (FOCS 2014) by strengthening the assumptions about the underlying sigma-protocol.

A full version of this paper can be found at [19].

Fiat-Shamir signatures. Signatures are (next to encryption) probably one of the most important constructs in modern cryptography. In the search for efficient signature schemes, Fiat-Shamir [10] gave a construction for transforming many three-round identification schemes into signatures, using the random oracle. The Fiat-Shamir transform and variations thereof have since been used in a large number of constructions (signatures [17, 15], group signatures [5], anonymous credentials [8], e-voting [1], anonymous attestation [7], etc.) The benefit of the Fiat-Shamir transform is that it combines efficiency with universality: The underlying identification scheme can be any so-called sigma-protocol, this allows for great flexibility in how public and secret key are related and enables the construction of more advanced signature schemes and related schemes such as group signatures, etc.

Non-interactive zero-knowledge proofs. At the first glance unrelated, but upon closer inspection intimately connected to signatures are non-interactive zero-knowledge proof of knowledge in the random oracle model. In fact, Fiat-Shamir can also be seen as a highly efficient construction for NIZKPoKs in the random oracle model [9]. Basically, a NIZKPoKs allows a prover to show his knowledge of a witness sk that stands in a given relation to a publicly known statement pk. From a NIZKPoK, we can derive a signature scheme: To sign a message m, the signer constructs a proof that he knows the secret key corresponding to the public key pk. (Of course, the message m needs to be included in the proof as well, we omit the details in this discussion.) For this construction to work, the NIZKPoK needs to satisfy certain advanced security notions ("simulation-sound extractability"); Fiat-Shamir satisfies this notion in the classical setting [9]. Thus Fiat-Shamir doubles both as a signature scheme and as a NIZKPoK, leading to simple and highly efficient constructions of both.

The construction. A sigma-protocol Σ is a three-message protocol: The prover (given a statement x and a corresponding valid witness w) sends a message com, called "commitment", to the verifier. The verifier (who knowns only the statement x) responds with a uniformly random "challenge" ch. Then the prover answers with his "response" $resp$, and the verifier checks whether $(com, ch, resp)$ is a valid interaction. If so, he accepts the proof of the statement x.

Given the sigma-protocol Σ, the Fiat-Shamir transform yields a non-interactive proof system: The Fiat-Shamir prover P_{FS} internally executes the prover of the sigma-protocol to get the commitment com. Then he computes the challenge as $ch := H(x\|com)$ where H is a hash function, modeled as a random oracle. That is, instead of letting the verifier generate a random challenge, the prover produces it by hashing. This guarantees, at least on an intuitively level, that the prover does not have any control over the challenge, it is as if it was chosen randomly. Then the prover internally produces the response *resp* corresponding to *com* and sends the non-interactive proof $com\|resp$ to the verifier. The Fiat-Shamir verifier V_{FS} computes $ch := H(x\|com)$ and checks whether $(com, ch, resp)$ is a valid interaction of the sigma-protocol.

Post-quantum security. In this paper we are interested in the post-quantum security of Fiat-Shamir. That is, under what conditions is Fiat-Shamir secure if the adversary has a quantum computer? In the post-quantum setting, the random oracle has to be modeled as a random function that can be queried in superposition since a normal hash function can be evaluated in superposition as well (see [6]). Ambainis, Rosmanis, and Unruh [2] showed that in this model, Fiat-Shamir is insecure in general. More precisely, they showed that relative to certain oracles, there are sigma-protocols such that: The sigma-protocol satisfies the usual security properties. (Such as zero-knowledge and computational special soundness. These are sufficient for security in the classical case.) But when applying the Fiat-Shamir transform to it, the resulting NIZKPoK is not sound (and thus, as a signature, not unforgeable). Since this negative result is relative to specific oracles, it does not categorically rule out a security proof. However, it shows that no relativizing security proof exists, and indicates that it is unlikely that Fiat-Shamir can be shown post-quantum secure in general.

A number of papers have used Fiat-Shamir to construct post-quantum secure signature schemes (e.g., [11, 14, 13, 3, 12, 4]). The negative results by Ambainis et al. show that the post-quantum security of these schemes is hard to justify.[1] Thus the post-quantum security of Fiat-Shamir would be of great interest, both from a practical and theoretical point of view.

Fortunately, the results from [2] only imply that it is difficult to prove the security of Fiat-Shamir under comparable assumptions as in the classical setting. In this paper, we show that under suitably strengthened (but still realistic) assumptions, Fiat-Shamir is post-quantum secure. Concretely, we have the following contributions:

Security of Fiat-Shamir as a proof system. We prove that Fiat-Shamir is post-quantum secure as a proof system. More precisely, we prove that it is zero-knowledge (using random-oracle programming techniques from [18]), and that it is sound (i.e., a proof of knowledge, using a reduction to quantum search). In addition, we show that Fiat-Shamir is non-malleable, that is, given one valid proof, one cannot produce another valid proof (for a potentially related statement). This is modeled by the stronger simulation-soundness property from [16]. More precisely:

Theorem 1 (Post-quantum security of Fiat-Shamir) *Assume that Σ has: computational honest-verifier zero-knowledge,* perfect *special soundness, computationally unique responses,*[2] *completeness,*[3] *unpredictable commitments,*[4]*, and that the challenge ch has superlogarithmic length. Then the Fiat-Shamir proof system (P_{FS}, V_{FS}) is computationally zero-knowledge and computationally simulation-sound.*

The assumptions are the same as in the classical setting, except that instead of *computational* special soundness (in the classical case), we now need *perfect* special soundness (i.e., against unlimited adversaries). This is interesting, because it means that we need one of the properties of the sigma-protocol to hold unconditionally, even though we only want computational security in the end. However, [2] shows that this is necessary: when assuming only computational special soundness, they construct a counter-example against the soundness of Fiat-Shamir (relative to some oracle).

[1] We stress that the *classical* security of these schemes is not in question.

[2] This means that is it hard to find a commitment, a challenge, and two valid responses for that same commitment/challenge pair. Also known as "computational strict soundness".

[3] I.e., honest proofs are valid with overwhelming probability

[4] A technical condition that requires the commitment *com* to be randomized.

Signatures. Normally, the security of Fiat-Shamir signatures is shown by reducing it to the simulation-sound extractability of Fiat-Shamir (implicitly or explicitly). Unfortunately, we do not know whether extractability holds in the quantum case. Thus, we need a new proof of the security of Fiat-Shamir signatures that only relies on simulation-soundness. We can do so by making additional assumptions about the way the key generator works: We call an algorithm G a "dual-mode hard instance generator" if G outputs a key pair (pk, sk) in such a way that pk is computationally indistinguishable from an invalid pk (i.e., a pk that has no corresponding sk). An example of such an instance generator would be: sk is chosen uniformly at random, and $pk := F(sk)$ for a pseudo-random generator F. Then we have:

Theorem 2 (Fiat-Shamir signatures) *Assume that G is a dual-mode hard instance generator. Fix a sigma-protocol Σ (for showing that a given pk has an sk). Assume that Σ has the properties from Theorem 1. Then the Fiat-Shamir signature scheme is strongly unforgeable.*

Note that classically, we only require that G is a hard instance generator. That is, given pk, it is hard to find sk. We leave it as an open problem whether this is sufficient in the post-quantum setting, too.

References

[1] B. Adida. Helios: Web-based open-audit voting. In *USENIX Security Symposium 08*, pages 335–348. USENIX, 2008. Online at `http://www.usenix.org/events/sec08/tech/full_papers/adida/adida.pdf`.

[2] 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, 2014.

[3] R. E. Bansarkhani and A. E. Kaafarani. Post-quantum attribute-based signatures from lattice assumptions. IACR ePrint 2016/823, 2016.

[4] C. Baum, I. D. rd, S. Oechsner, and C. Peikert. Efficient commitments and zero-knowledge protocols from ring-SIS with applications to lattice-based threshold cryptosystems. IACR ePrint https://eprint.iacr.org/2016/997, 2016.

[5] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Crypto 2004*, volume 3152 of *LNCS*, pages 41–55. Springer, 2004.

[6] 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.

[7] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In *ACM CCS '04*, pages 132–145, New York, NY, USA, 2004. ACM.

[8] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Eurocrypt 2001*, pages 93–118. Springer, 2001.

[9] S. Faust, M. Kohlweiss, G. A. Marson, and D. Venturi. On the non-malleability of the Fiat-Shamir transform. In *Indocrypt 2012*, volume 7668 of *LNCS*, pages 60–79. Springer, 2012. Preprint is IACR ePrint 2012/704.

[10] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Crypto '86*, number 263 in Lecture Notes in Computer Science, pages 186–194. Springer-Verlag, 1987.

[11] S. D. Gordon, J. Katz, and V. Vaikuntanathan. A group signature scheme from lattice assumptions. In *Asiacrypt 2010*, volume 6477, pages 395–412. Springer, 2010.

[12] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. In *Asiacrypt 2016*, volume 10032 of *LNCS*, pages 373–403. Springer, 2016. Full version IACR ePrint 2016/101.

[13] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang. Zero-knowledge arguments for matrix-vector relations and lattice-based group encryption. In *Asiacrypt 2016*, volume 10032 of *LNCS*, pages 101–131. Springer, 2016.

[14] S. Ling, K. Nguyen, and H. Wang. Group signatures from lattices: Simpler, tighter, shorter, ring-based. In *PKC 2015*, volume 9020, pages 427–449. Springer, 2015.

[15] D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.

[16] A. Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *FOCS '99*. IEEE, 1999.

[17] C.-P. Schnorr. Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, 4(3):161–174, 1991.

[18] D. Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *Eurocrypt 2015*, volume 9057, pages 755–784. Springer, 2015. Full version IACR ePrint 2014/587.

[19] D. Unruh. Post-quantum security of Fiat-Shamir. IACR ePrint 2017/398, 2017.