New security notions and feasibility results for authentication of quantum data

Sumegha Garg Princeton

Henry Yuen MIT

Mark Zhandry MIT

Authenticating messages is one of the fundamental operations in classical cryptography. A sender Alice wishes to send a message m over an insecure channel to Bob, while ensuring that the message was not tampered with in transit. She does this by affixing a "signature" σ to m using a key k shared with Bob. Bob can then verify the signature he receives to ensure the message came from Alice. Such a (symmetric key) authentication protocol is usually referred to as a Message Authentication Code (MAC). As long as k is only used to authenticate a single message, information-theoretic security can be achieved [10].

Just as authentication is fundamental to classical cryptography, it will continue to be an important tool in the coming age of quantum computers. In this work, we investigate authentication in the quantum setting.

Quantum Attacks on Classical Protocols. A recent series of works [3, 6, 4, 5, 11, 9] have studied quantum superposition attacks on classical cryptosystems. In the case of message authentication codes, an adversary in such an attack is able to trick the sender into signing a superposition of messages. Clearly, the adversary can tamper with the signed state: he can, for example, measure the entire state in the standard basis. Because the scheme is classical, the measured state will still pass verification, but will be different from the signed state the adversary received.

Boneh and Zhandry [4] argue that, at a minimum, the adversary given a single signed superposition should only be able to produce a single signed message; he should not be able to produce both valid signed messages m, σ_m and $m', \sigma_{m'}$ for $m \neq m'$. In the classical setting, this requirement is equivalent to the traditional MAC security definition. However, the Boneh-Zhandry definition in the quantum setting has some unsatisfying properties. For example, consider the case where the sender only signs messages that start with the email address of some intended recipient, say, `bob@gmail.com`. Suppose the adversary tricks the sender into a signing a superposition of messages that all begin with `bob@gmail.com`, but then manipulates the signed superposition into a different superposition that includes valid signed messages that *do not* start with `bob@gmail.com`. Clearly, this is an undesirable outcome. Unfortunately, the Boneh-Zhandry definition does not rule out such attacks — it only rules out the possibility of an adversary producing $q + 1$ valid signed messages when given q signed superpositions. The situation illustrated here, however, is that the adversary is given *one* signed superposition, and now wants to produce *one* valid signed message that was not part of the original superposition.

Quantum Authentication of Quantum Data. Barnum et al. [2] investigate the possibility of authenticating quantum data using a quantum protocol. They present a definition of quantum authentication where, conditioned on the protocol succeeding, the sender has effectively teleported a quantum state to the receiver. They then give a scheme which attains this definition. Interestingly, they show that quantum state authentication also implies quantum state *encryption*.

Follow up works [8] showed that the protocol actually has *universal composable security*, which implies that it remains secure in the presence of side information. However, no general definition for authentication with quantum side information was given. Furthermore, [8] show that the secret key used in the Barnum, et al. protocol can be partially *re-used* in further applications without compromising their security. When authenticating classical information, the key can even be re-used in its entirety [7].

However, existing definitions have some shortcomings. For example, the key re-usability property does not follow from the general security definition alone, but follows from an analysis of the particular [2] protocol. Moreover, it has been an open question of whether there is a quantum authentication scheme to allow for full re-usability of the key upon successful verification.

1 This Work

In this work, we address the above limitations by giving new security notions for authentication in the quantum setting. We present an abstract framework of security for both classical and quantum authentication schemes that not only captures the existing security definitions, but also is more powerful in that it strongly *characterizes* the (effective) behavior of an adversary. The adversary can even have access to quantum side information with the message state that is being authenticated. The characterization of the adversary's admissable actions is what allows us to easily deduce many desirable security properties (such as unforgeability, key reuse, and more). Furthermore, we will show that various natural authentication protocols satisfy our security definitions.

A new security definition for classical authentication. We think of a classical protocol giving rise to a weak form of authentication of quantum messages, where a state is authenticated by running the classical signing algorithm in superposition. The state is similarly verified in superposition. More generally, we think of the protocol acting on messages states that may be entangled with an adversary, and even consider signing mixed states. By thinking of the protocol in this way, we are able to give security definitions that actually consider the relationship between the sender's signed state and the final state the adversary produces.

Clearly, such a classical scheme cannot fully protect the quantum state. An adversary could, for example measure the signed state or any subset of bits of the state. The adversary can also replace the signed state with junk if the outcome of some measurement is 1, forwarding the signed state otherwise. None of these actions would be detected by the classical verification procedure.

Our security definition for classical protocols says that, roughly, an arbitrary adversary can be simulated by an ideal adversary that can only do operations such as those above. Thus, our definition is essentially the best one could hope for, since is disallows the adversary from doing anything other than operations that are trivially possible on *any* classical protocol. Our definition readily implies the Boneh-Zhandry security definition for one-time MACs[1], and does not suffer from the weakness of their definition. Finally, we show that the classical Carter-Wegman MAC that uses three-universal hashing is sufficient for achieving this strong security definition.

Definitions for Quantum Authentication. We next turn to quantum protocols for authenticating quantum messages, and similarly give a "best possible" definition of quantum authentication — which we call *total authentication* — that more or less states that the adversary cannot do anything but simply forward the state.

Our definition strengthens Barnum et al.'s definition, and due to the fact that we consider side information about the plaintext state, we obtain security guarantees that are similar to the universally composable variant of their definition [8]. However, our definition is actually strictly stronger, due to the fact that we consider the receiver's view to include the authentication key as well as whatever information the adversary may learn about the key. The ideal adversary must approximate the real adversary, even considering the entire key. Our security definition of total authentication thus rules out the possibility of the adversary learning anything about the key (because the ideal adversary does not interact with the authenticated state at all), a feature not present in prior definitions.

This fact has interesting consequences. For example, our definition immediately implies that, upon successful verification by the receiver, the key can actually be completely recycled to authenticate a new message. We note that key recycling from quantum authentication was studied before by [8], but they were only able to demonstrate that *part* of the key in the Barnum, et al. protocol is reusable. Furthermore, no prior definition for authentication of quantum data directly implies key re-usability, and no prior protocol for quantum messages gets full key re-usability upon successful verification. Our definition also gives a conceptually simple, though not practical, QKD protocol, illustrating the power of our definitions.

Next, we exhibit a protocol meeting our strong security notion. We present an authentication scheme based on *unitary designs*, which are efficiently sampleable distributions over unitary matrices that behave much like the uniform distribution over unitaries when only considering low degree moments. The protocol is simple, and is basically the *non-malleable quantum encryption* scheme based on unitary 2-designs that was proposed by Ambainis, Bouda, and Winter [1], except with some extra padding before encryption.

[1] Except that we consider a slightly different model of the adversary queries the signer.

We note that their scheme without padding does not provide any authentication, their analysis does not consider quantum side information, and we therefore require a much more careful analysis.

Finally, we also give a definition of *total authentication with key leakage*, where some of the key might leak to the adversary. This is slightly weaker notion of security than total authentication, but it still implies simple QKD and some amount of key reuse. We note that the work of [8] essentially show that the Barnum et al. protocol satisfies total authentication with (minor) key leakage. We give a simple authentication scheme that achieves this: first, one classically authenticates, performs the quantum Fourier transform, and classically authenticates again using a fresh key. We call this the "Auth-QFT-Auth" protocol, and show that it achieves total authentication where the key used in the second authentication may leak. This illustrates the surprising versatility of classical authentication schemes: combined with one quantum step (the Fourier transform), it can give full quantum authentication. This also gives a conceptually simple alternative to [2].

Acknowledgments. We thank Debbie Leung for kindly sharing a manuscript of [8].

References

[1] A. Ambainis, J. Bouda, and A. Winter. Nonmalleable encryption of quantum information. *Journal of Mathematical Physics*, 50(4):042106, 2009.

[2] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *The Proceedings of the 43rd Annual IEEE Foundations of Computer Science, 2002.*, pages 449–458. IEEE, 2002.

[3] D. Boneh, O. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random Oracles in a Quantum World. In *Proceedings of ASIACRYPT*, 2011.

[4] D. Boneh and M. Zhandry. Quantum-secure message authentication codes. In *Advances in Cryptology–EUROCRYPT 2013*, pages 592–608. Springer, 2013.

[5] D. Boneh and M. Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *Advances in Cryptology–CRYPTO 2013*, pages 361–379. Springer, 2013.

[6] I. Damgård, J. Funder, J. B. Nielsen, and L. Salvail. Superposition attacks on cryptographic protocols. In *Information Theoretic Security*, pages 142–161. Springer, 2013.

[7] I. Damgård, T. B. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. In *Proceedings of the 25th Annual International Conference on Advances in Cryptology*, CRYPTO'05, pages 494–510, Berlin, Heidelberg, 2005. Springer-Verlag.

[8] P. M. Hayden, D. W. Leung, and D. Mayers. The universal composable security of quantum message authentication with key recycling. *In preparation*, 2011.

[9] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. *arXiv preprint arXiv:1602.05973*, 2016.

[10] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22(3):265–279, 1981.

[11] M. Zhandry. How to Construct Quantum Random Functions. In *Proceedings of the 53rd IEEE Symposium on Foundations of Computer Science (FOCS)*, 2012.