# Quantum authentication with key recycling

Christopher Portmann*[1]

[1]Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.

April 21, 2017

**Abstract**

We show that a family of quantum authentication protocols introduced in [Barnum et al., FOCS 2002] can be used to construct a secure quantum channel and additionally recycle all of the secret key if the message is successfully authenticated, and recycle part of the key if tampering is detected. We give a full security proof that constructs the secure channel given only insecure noisy channels and a shared secret key. We also prove that the number of recycled key bits is optimal for this family of protocols, i.e., there exists an adversarial strategy to obtain all non-recycled bits. Previous works recycled less key and only gave partial security proofs, since they did not consider all possible distinguishers (environments) that may be used to distinguish the real setting from the ideal secure quantum channel and secret key resource.

A full version of this work can be found on the arXiv [Por17].

## 1 Reusing a one-time pad

A one-time pad can famously be used only once [Sha49], i.e., a secret key as long as the message is needed to encrypt it with information-theoretic security. But this does not hold anymore if the honest players can use quantum technologies to communicate. A quantum key distribution (QKD) protocol [BB84, SBPC+09] allows players to expand an initial short secret key, and thus encrypt messages that are longer than the length of the original key. Instead of first expanding a key, and then using it for encryption, one can also swap the order if the initial key is long enough: one first encrypts a message, then recycles the key. This is possible due to the same physical principles as QKD: quantum states cannot be cloned, so if the receiver holds the exact cipher that was sent, the adversary cannot have a copy, and thus does not have any information about the key either, so it may be reused. This requires the receiver to verify the authenticity of the message received, and if this process fails, a net key loss occurs — the same happens in QKD: if an adversary tampers with the communication, the players have to abort and also lose some of the initial secret key.

## 2 Quantum authentication and key recycling

Some ideas for recycling encryption keys using quantum ciphers were already proposed in 1982 [BBB82]. Many years later, Damgård et al. [DPS05] (see also [DPS14, FS17]) showed how to encrypt a classical message in a quantum state and recycle the key. At roughly the same time, the first protocol for authenticating quantum messages was proposed by Barnum et al. [BCG+02], who also proved that quantum authentication necessarily encrypts the message as well. Gottesman [Got03] then showed that after the message is successfully authenticated by the receiver, the key can be leaked to the adversary without compromising the confidentiality of the message. And Oppenheim and Horodecki [OH05] adapted the protocol of [BCG+02] to recycle key. But the security definitions

*chportma@.ethz.ch

in these initial works on quantum authentication have a major flaw: they do not consider the possibility that an adversary may hold a purification of the quantum message that is encrypted. This was corrected by Hayden, Leung and Mayers [HLM11], who give a composable security definition for quantum authentication with key recycling. They then show that the family of protocols from [BCG+02] are secure, and prove that one can recycle part of the key if the message is accepted.

The security proof from [HLM11] does however not consider all possible environments. They restrict their analysis to so-called *substitution attacks* — where the adversary obtains a valid pair of message and cipher and attempts to substitute the cipher with one that will decode to a different message — but ignore *impersonation attacks* — where the adversary directly sends a forged cipher to the receiver, without knowledge of a valid message-cipher pair. To the best of our knowledge, there is no proof showing that security against impersonation attacks follows from security against substitution attacks, hence the literature analyzes both attacks separately.[1] This is particularly important in the case of composable security, which aims to prove the security of the protocol when used in any arbitrary environment, therefore also in an environment that first sends a forged cipher to the receiver, learns wether it is accepted or rejected, then provides a message to the sender to be authenticated, and finally obtains the cipher for this message. This is all the more crucial when key recycling is involved, since the receiver will already recycle (part of) the key upon receiving the forged cipher, which is immediately given to the environment. The work of Hayden et al. [HLM11] thus does not provide a complete composable security proof of quantum authentication, which prevents the protocol from being composed in an arbitrary environment.[2]

More recently, alternative security definitions for quantum authentication have been proposed, both without [DNS12, BW16] and with [GYZ16] key recycling (see also [AM16]). These still only consider substitution attacks, and furthermore, they are, strictly speaking, not composable. While it is possible to prove that these definitions imply security in a composable framework (if one restricts the environment to substitution attacks), the precise way in which the error $\varepsilon$ carries over to the framework has not been worked out in any of these papers. If two protocols with composable errors $\varepsilon$ and $\delta$ are run jointly (e.g., one is a subroutine of the other), the error of the composed protocol is bounded by the sum of the individual errors, $\varepsilon + \delta$. If a security definition does not provide a bound on the composable error, then one cannot evaluate the new error after composition.[3] For example, quantum authentication with key recycling requires a backwards classical authentic channel, so that the receiver may tell the sender that the message was accepted, and allow her to recycle the key. The error of the complete protocol is thus the sum of errors of the quantum authentication and classical authentication protocols. Definitions such as those of [DNS12, BW16, GYZ16] are not sufficient to directly obtain a bound on the error of such a composed protocol.

## 3 Contributions

In this work we use the Abstract Cryptography (AC) framework [MR11] to model the composable security of quantum authentication with key recycling. AC views cryptography as a resource theory: a protocol constructs a (strong) resource given some (weak) resources. For example, the quantum authentication protocols that we analyze construct two resources: a secure quantum channel — a channel that provides both *confidentiality* and *authenticity* — and a secret key resource that shares a fresh key between both players. In order to construct these resources, we require shared secret key, an insecure (noiseless) quantum channel and a backwards authentic classical channel. These are

[1] In fact, one can construct examples where the probability of a successful impersonation attack is higher than the probability of a successful substitution attack. This can occur, because any valid cipher generated by the adversary is considered a successful impersonation attack, whereas only a cipher that decrypts to a different message is considered a successful substitution attack.

[2] For example, QKD can be broken if the underlying authentication scheme is vulnerable to impersonation attacks, because Eve could trick Alice into believing that the quantum states have been received by Bob so that she releases the basis information.

[3] In an asymptotic setting, one generally does not care about the exact error, as long as it is negligible. But for any (finite) implementation, the exact value is crucial, since without it, it is impossible to set the parameters accordingly, e.g., how many qubits should one send to get an error $\varepsilon \leq 10^{-18}$.

all resources, that may in turn be constructed from weaker resources, e.g., the classical authentic channel can be constructed from a shared secret key and an insecure channel, and noiseless channels are constructed from noisy channels.

We thus first formally define the ideal resources constructed by the quantum authentication protocol with key recycling — the secure channel and key resource mentioned in this introduction — as well as the resources required by this construction. We then prove that a family of quantum authentication protocols proposed by Barnum et al. [BCG+02] satisfy this construction, i.e., no distinguisher (called environment in UC) can distinguish the real system from the ideal resources and simulator except with an advantage $\varepsilon$ that is exponentially small in the security parameter. This proof considers all distinguishers allowed by quantum mechanics, including those that perform impersonation attacks.

We show that in the case where the message is accepted, every bit of key may be recycled. And if the message is rejected, one may recycle all the key except the bits used to one-time pad the cipher.[4] We prove that this is optimal for the family of protocols considered, i.e., an adversary may obtain all non-recycled bits of key. This improves on previous results, which recycled less key and only considered a subset of possible environments. More specifically, Hayden et al. [HLM11], while also analyzing protocols from [BCG+02], only recycle part of the key in case of an accept, and lose all the key in case of a reject. Garg et al. [GYZ16] propose a new protocol, which they prove can recycle all of the key in the case of an accept, but do not consider key recycling in the case of a reject either. The protocols we analyze are also more key efficient than that of [GYZ16]. We give two instances which need $\Theta(m + \log 1/\varepsilon)$ bits of initial secret key, instead of the $\Theta((m + \log 1/\varepsilon)^2)$ required by [GYZ16], where $m$ is the length of the message and $\varepsilon$ is the error. Independently from this work, Alagic and Majenz [AM16] proved that one of the instances analyzed here satisfies the weaker security definition of [GYZ16].

We then give two explicit instantiations of this family of quantum authentication protocols. The first is the construction used in [BCG+02], which requires an initial key of length $2m + 2n$, where $m$ is the length of the message and $n$ is the security parameter, and has error $\varepsilon \leq 2^{-n/2+1}\sqrt{2m/n + 2}$. The second is an explicit unitary 2-design [Dan05, DCEL09] discovered by Chau [Cha05], which requires $5m + 4n$ bits of initial key[5] and has error $\varepsilon \leq 2^{-n/2+1}$. Both constructions have a net loss of $2m + n$ bits of key if the message fails authentication. Since several other explicit quantum authentication protocols proposed in the literature are instances of this family of schemes, our security proof is a proof for these protocols as well.

Finally, we show how to construct the resources used by the protocol from nothing but insecure noisy channels and shared secret key, and calculate the joint error of the composed protocols. We also show how to compensate for the bits of key lost in the construction of the backwards authentic channel, so that the composed protocol still has a zero net key consumption if no adversary jumbles the communication.

A full version of this work can be found on the arXiv [Por17].

## References


[AM16] Gorjan Alagic and Christian Majenz. Quantum non-malleability and authentication. Eprint, 2016. [arXiv:1610.04214].

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.


[4] Key recycling in the case of a rejected message is not related to any quantum advantage. A protocol does not leak more information about the key than (twice) the length of the cipher, so the rest may be reused. The same holds for classical authentication [Por14].

[5] The complete design would require $5m + 5n$ bits of key, but we show that some of the unitaries are redundant when used for quantum authentication and can be dropped.

[BBB82] Charles H. Bennett, Gilles Brassard, and Seth Breidbart. Quantum cryptography II: How to re-use a one-time pad safely even if P=NP. Original unpublished manuscript uploaded to arXiv in 2014, 1982. [arXiv:1407.0451].

[BCG+02] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *Proceedings of the 43rd Symposium on Foundations of Computer Science, FOCS '02*, pages 449–458. IEEE, 2002. [doi:10.1109/SFCS.2002.1181969, arXiv:quant-ph/0205128].

[BW16] Anne Broadbent and Evelyn Wainewright. Efficient simulation for quantum message authentication. In *Proceedings of the 9th International Conference on Information Theoretic Security, ICITS 2016*, pages 72–91. Springer, 2016. [doi:10.1007/978-3-319-49175-2_4, arXiv:1607.03075].

[Cha05] Hoi Fung Chau. Unconditionally secure key distribution in higher dimensions by depolarization. *IEEE Transactions on Information Theory*, 51(4):1451–1468, April 2005. [doi:10.1109/TIT.2005.844076, arXiv:quant-ph/0405016].

[Dan05] Christoph Dankert. Efficient simulation of random quantum states and operators. Master's thesis, University of Waterloo, 2005. [arXiv:quant-ph/0512217].

[DCEL09] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A*, 80:012304, July 2009. [doi:10.1103/PhysRevA.80.012304, arXiv:quant-ph/0606161].

[DNS12] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Actively secure two-party evaluation of any quantum operation. In *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 794–811. Springer, 2012. [doi:10.1007/978-3-642-32009-5_46, IACR e-print: 2012/304].

[DPS05] Ivan Damgård, Thomas Brochmann Pedersen, and Louis Salvail. A quantum cipher with near optimal key-recycling. In *Advances in Cryptology – CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 494–510. Springer, 2005. [doi:10.1007/11535218_30].

[DPS14] Ivan Damgård, Thomas Brochmann Pedersen, and Louis Salvail. How to re-use a one-time pad safely and almost optimally even if P = NP. *Natural Computing*, 13(4):469–486, December 2014. [doi:10.1007/s11047-014-9454-5].

[FS17] Serge Fehr and Louis Salvail. Quantum authentication and encryption with key recycling. In *Advances in Cryptology – EUROCRYPT 2017, Proceedings, Part III*, volume 10212 of *Lecture Notes in Computer Science*, pages 311–338. Springer, 2017. [doi:10.1007/978-3-319-56617-7_11, arXiv:1610.05614].

[Got03] Daniel Gottesman. Uncloneable encryption. *Quantum Information and Computation*, 3:581, 2003. [arXiv:quant-ph/0210062].

[GYZ16] Sumegha Garg, Henry Yuen, and Mark Zhandry. New security notions and feasibility results for authentication of quantum data. Eprint, 2016. [arXiv:1607.07759].

[HLM11] Patrick Hayden, Debbie Leung, and Dominic Mayers. The universal composable security of quantum message authentication with key recycling. Eprint, presented at QCrypt 2011, 2011. [arXiv:1610.09434].

[MR11] Ueli Maurer and Renato Renner. Abstract cryptography. In *Proceedings of Innovations in Computer Science, ICS 2011*, pages 1–21. Tsinghua University Press, 2011.

[OH05] Jonathan Oppenheim and Michał Horodecki. How to reuse a one-time pad and other notes on authentication, encryption, and protection of quantum information. *Physical Review A*, 72:042309, October 2005. [doi:10.1103/PhysRevA.72.042309, arXiv:quant-ph/0306161].

[Por14] Christopher Portmann. Key recycling in authentication. *IEEE Transactions on Information Theory*, 60(7):4383–4396, July 2014. [doi:10.1109/TIT.2014.2317312, arXiv:1202.1229].

[Por17] Christopher Portmann. Quantum authentication with key recycling. In *Advances in Cryptology – EUROCRYPT 2017, Proceedings, Part III*, volume 10212 of *Lecture Notes in Computer Science*, pages 339–368. Springer, 2017. [doi:10.1007/978-3-319-56617-7_12, arXiv:1610.03422].

[SBPC+09] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301–1350, September 2009. [doi:10.1103/RevModPhys.81.1301, arXiv:0802.4155].

[Sha49] Claude Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.