Applicability of a post-quantum signature in a QKD public channel

[1,2] Roberto Roscino, [2] Kevin Layat, [2] Grégoire Ribordy, [2] Bruno Huttner, and [2] Dario Caselunghe

[1] Department of Mathematics, Università degli studi di Trento

[2] IDQuantique SA, Chemin de la Marbrerie 3, 1227, Geneva, Switzerland

roberto.roscino@idquantique.com
kevin.layat@idquantique.com
gregoire.ribordy@idquantique.com
bruno.huttner@idquantique.com
dario.caselunghe@idquantique.com

1 Introduction and motivations

In a general view we can divide the Quantum Key Distribution (QKD) in two main phases: quantum communication on a quantum channel and post-processing on a public one. In order to avoid the possibility of a Man In The Middle (MITM) attack, one of the most important part of a QKD protocol is the authentication of the public channel, that is the authentication of all the post-processed informations. This is usually done using a symmetric Wegman-Carter authentication (WCA) scheme [1]. The main reason of this choice is related to the unconditional security of the scheme, that takes into account the existence of adversaries with unlimited computational power. However, there is an important drawback that should be considered: in order to start the communication Alice and Bob have to share an initial secret key. Obviously, since the QKD itself is a key agreement scheme, Alice and Bob can authenticate each QKD session using part of the last generated key (that is known by each other). Thus, the pre-shared keys problem concerns only the first QKD authentication. However, each time the communication stops due, for example, to a denial attack, Alice and Bob have to find a way to

share another key in order to re-start the QKD, that is they can't use the same key twice. In practice this is usually done manually, involving expensive procedures in term of time and money. Another way to address the problem is by using an asymmetric scheme just for the first authentication, i.e. by removing the unconditional security requirement in the first authentication steps. Even if this seems a big drawback, there is one important element we want to point out: in many practical instances, the QKD is used to generate short keys that are used with well-studied symmetric encryption such as AES. This means that, in general, we don't use the QKD along with unconditional secure encryption such as the OTP (One Time Pad), due to the necessity of long-keys generation. Thus, in many practical implementation, QKD is already used in a not unconditional secure way.

2 Our proposal

In this work, we study the possibility of an application of a post-quantum signature. The chosen signature is XMSS, which is a hash-based one, and the specific chosen version of the scheme is the new one proposed in [2]. The main strategy is then to use this scheme to authenticate all the post-processing informations needed to obtain a certain amount of secret QKD keys. The latter is determined as the minimal amount of secret keys that we need to start a QKD communication, that is the needed amount of pre-shared keys used to start a WCA. The WCA will then be used for all the authentications different from the first.

In order to study the effective applicability of the strategy above, we have considered a software C implementation of XMSS (based on the Internet draft [4]) and used [3] as the main example/reference for a QKD public channel. Then, we have built two examples of a possible application of the strategy above: in a one-to-one QKD setting and in a multi-link QKD setting. For both of them we have computed the related timings and the space requirements of the scheme, always referring to a software implementation. Finally, we have studied the main differences between the usual WCA and the XMSS signature, also in relation to the two settings above.

3 Our presentation

In our talk we start by presenting a QKD protocol and by explaining the importance of an authentication step in this latter. We also describe the WCA, used in most of the QKD protocols, and the security assumptions and

properties related to it. Then, we focus on the XMSS signature. We explain the main ideas behind the basic scheme, describe the security properties, and make a comparison with the WCA. Finally, we present the two possible applications of the signature in a QKD service channel.

References

[1] M.N.Wegman, J.L.Carter, *New hash functions and their use in authentication and set equality*, J. Comput. Syst. Sci. 22, 265-279, 1981

[2] Andreas Hülsing, Joost Rijneveld, Fang Song. *Mitigating Multi-Target Attacks in Hash-based Signatures*, Pages 387-416 in: Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, Bo-Yin Yang (editors), Public-Key Cryptography PKC 2016, 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I. Lecture Notes in Computer Science 9614. Springer. ISBN 978-3-662-49383-0,2016

[3] Korzh,B. et al. *Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre*, Nature Photon.9, 163-168, 2015

[4] Andreas Hülsing, Denis Butin, Stefan Gazdag, and Aziz Mohaisen. *XMSS: Extended Hash-Based Signatures*. Crypto Forum Research Group Internet-Draft, 2015. https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/