RHQC: post-quantum ratcheted key exchange from coding assumptions

Julien Juaneda*[1,2]

[1]Fédération ENAC ISAE-SUPAERO ONERA – Institut Supérieur de l'Aéronautique et de l'Espace – France

[2]Laboratoire de recherche coopératif dans les télécommunications spatiales et aéronautiques – Institut Supérieur de l'Aéronautique et de l'Espace (ISAE), Thales Alenia Space France, CNES – France

Résumé

Key management has long been a challenge in the design of secure communication systems. In particular, satellite
communication systems exemplify this challenge, given the extensive operational lifespans of satellites and their resource
constraints. Protocols must not only meet demanding performance and reliability requirements but also remain secure
against potential quantum threats that may emerge in the next few decades. To mitigate these risks, there is an urgent
need for cryptographic mechanisms that ensure post-quantum resistance. Along with the need for perfect forward
secrecy (PFS) and post-compromise security (PCS) these requirements lead us to the use of Ratcheted Key Exchange
(RKE) protocols.
The most well known RKE protocol is the Signal protocol widely used by instant messaging applications such
as Signal, Whatsapp or Messenger. Despite its success, it still relies on the Diffie-Hellmann KEM and is therefore
vulnerable to quantum adversaries. However very recently a quantum safe alternative based on Kyber, called Triple
Ratchet has emerged. The present work proposes an alternative by leveraging instead problems based on the Syndrome
Decoding.
Our protocol leverages the Hamming Quasi-Cyclic (HQC) cryptosystem, recently selected by the NIST's PQC
project to become one of the five quantum-resistant cryptographic standards. HQC offers several advantages, including
robust theoretical security proofs, careful control of noise growth and error probabilities in decoding, and minimized
failure rates compared to alternatives. Compared to lattice-based schemes, HQC's simpler structure facilitates the
symmetrization of the cryptographic operations of communicating parties, and its high parameterizability allows for

*Intervenant

flexible adjustments to meet varying security and efficiency requirements. These features make HQC a compelling
choice for building post-quantum RKE protocols, balancing security, efficiency, and practicality.
However, the authors of triple ratchet introduced a new security property for KEMs called ratchet simulatability.
This is a key property to argue PCS for a RKE scheme. As neither HQC.PKE nor HQC.KEM verifies this property, we
propose a new version of HQC that we call HQC.RKEM. This new version of HQC is the main building block of our
RKE protocol. This presentation aims at describing RHQC a practical, efficient, and formally secure post-quantum
RKE protocol tailored to real-world constraints and emerging threats.