To the P1363 Working Group

From Hugo Krawczyk

This is a short note on HMQV in preparation for the upcoming meeting where inclusion of the protocol in the P1363 is to be discussed. Given that 2 years already passed since I presented this work to the group (and one year since I provided a detailed P1363 spec of the protocol), it seems that a short "executive summary" on this work would be beneficial. (For full details see my specification of HMQV for P1363 as well as the crypto paper that includes the analysis work.)

I am proposing HMQV for inclusion in P1363 as a key agreement mechanism, in addition to the already existing key agreement protocols. HMQV is a variant of the MQV key agreement protocol that preserves (or even improves!) the outstanding performance of the original MQV protocol while offering a wide array of well-defined security properties all backed by formal analysis and cryptographic proofs (in the random oracle model). Thanks to its detailed analysis, HMQV provides provable security while dispensing with several of the safeguards required in MQV. This results in a more robust and more secure protocol that minimizes its reliance on external mechanisms (such as the performance of special tests by the CA) and on system/infrastructure assumptions, and even increases protocol efficiency.

I would like to believe that rigorous modern analysis is becoming a requirement, whenever possible, for the adoption of cryptographic techniques into standards and into practice, certainly in the case of a careful set of standards such as P1363. Hence, I assume that the fact that HMQV is backed by a rigorous analysis will be seen by the group as a substantial improvement over MQV where such formal analysis is lacking. So instead of repeating the importance of theoretically well-founded cryptography, let me mention in short some of the central *practical* advantages of HMQV over MQV (advantages that are a direct product of the improved understanding of these protocols obtained via the analysis work!)

- HMQV does not depend on a CA (or other parties) performing "proofs of possession" of private keys at the time of public key registration or verification;
- HMQV never requires the testing for prime order of long-term public keys and requires the testing of ephemeral public keys only in specific attack scenarios;
- HMQV provides entity- and key- authentication as a built-in mechanism without depending on the parameters to the key derivation function or other external mechanisms. In particular, the basic two-message HMQV protocol already provides full authentication, including provable resistance to UKS and KCI attacks[1].

[1] Failure to UKS attacks is a serious authentication concern (especially in the setting of "known-key attacks") where two honest parties compute the same session key but have inconsistent views of who the

The relaxation of the testing requirements on the private and public keys, as mentioned above, greatly simplifies the deployment and practice of the protocol and makes it more secure in many practical scenarios such as in the common real-life cases in which proofs of possession (PoP) are *not* performed by the certification entity. We note that PoPs are notoriously hard to be done correctly (and securely) especially in cases like MQV/HMQV where the secret key is not a signature key and hence the key does lend itself to a well-defined "self-proving" mechanism. For another illustrative example, consider the plaussible scwnario in which parties possess certificates for signature keys but not for (long-term) HMQV keys. In this case, parties can sign their own HMQV public key (using their certified signature keys) and peers can verify (and cache) the signatures. This is fine with HMQV which does not require any tests by the CA on the peer's public key but it will not work with MQV (where one cannot trust that the peer chose a correct public key, even if it self-certified the key). In such a scenario, MQV can only work if one moves the CA tests to the real-time protocol; however, not only would this jeopardize the protocol efficiency but it is not even clear how a "proof of possession", as required by MQV, would be perfomed in such a case.

Moreover, in many practical scenarios HMQV fully dispenses with prime order tests and co-factor exponentiation of ephemeral keys, thus further improving on MQV performance (the exact cost of these tests depends on the underlying group). Specifically, it is proven that, in a model where the attacker has no access to ephemeral exponents, HMQV is secure without these tests. Such settings are common (and even mandatory) in many applications; for example, in a DSA signature scheme ephemeral and long-term secrets must be equally protected since the exposure of a single ephemeral secret value compromises the whole private signing key. In a setting where ephemeral exponents are significantly more vulnerable than long-term secrets, HMQV requires co-factor exponentiation or a *single* prime-order test. Even in this case HMQV requires NO separate test on the long-term public key (except for a trivial non-zero test).

I hope that this short note is useful to the group. Do not hesitate to contact me if additional information is needed.

Thanks for your consideration.

Hugo

peer to the exchange is. Resistance to KCI attacks means that even if the attacker learns the long-term private key of Alice, he still cannot impersonate other parties to Alice. Resistance to both UKS and KCI attacks are listed as explicit goals of MQV but only partially achieved by the original protocol.