Dear all,

TL;DR: The security proof of HiMQ-3 (Theorem 4) is flawed.

The HiMQ-3 submission document claims that the HiMQ-3 signature scheme is EUF-CMA secure provided that it is hard to find a solution for a system of quadratic equations in the HiMQ-3 family. In other words, the claim is that if the scheme is UF-KOA secure (universal forgery under key-only attack), then the scheme is also EUF-CMA secure.

The proof of this claim is to be found in [1] (Theorem 4.1), where the same claim is made for the ELSA signature scheme. The proof is very similar to the classic proof of [2] for the security of a hash-and-sign signature scheme based on a trapdoor permutation. However, the trapdoor function used by the HiMQ-3 scheme is not a permutation, and this causes the proof to fail.

The proof programs a random oracle by sampling random \( x \), and returning \( P(x) \), where \( P \) is the public key. In the trapdoor permutation setting this is a valid approach, because there is no way to distinguish \( (x,P(x)) \) from \( (P^{-1}(y),y) \), for \( x \) and \( y \) uniformly distributed variables on the domain and codomain of \( P \) respectively. When \( P \) is no longer a permutation (as is the case for HiMQ-3 and ELSA) this might no longer be the case. (In fact, \( P^{-1}(y) \) is not even uniquely defined.) This means that the adversary is no longer guaranteed to function correctly in the simulated environment and that the proof fails.

Kind regards,
Ward
