Nostradamus goes Quantum

Barbara Jiabao Benedikt[1], Marc Fischlin[1], and Moritz Huppert[1]

[1] Cryptoplexity, Technische Universität Darmstadt, Germany
www.cryptoplexity.de

Abstract In the Nostradamus attack, introduced by Kelsey and Kohno (Eurocrypt 2006), the adversary has to commit to a hash value y of an iterated hash function H such that, when later given a message prefix P, the adversary is able to find a suitable "suffix explanation" S with $\mathsf{H}(P\|S) = y$. Kelsey and Kohno show a herding attack with $2^{2n/3}$ evaluations of the compression function of H (with n bits output and state), locating the attack between preimage attacks and collision search in terms of complexity. Here we investigate the security of Nostradamus attacks for quantum adversaries. We present a quantum herding algorithm for the Nostradamus problem making approximately $\sqrt[3]{n} \cdot 2^{3n/7}$ compression function evaluations, significantly improving over the classical bound. We also prove that quantum herding attacks cannot do better than $2^{3n/7}$ evaluations for random compression functions, showing that our algorithm is (essentially) optimal. We also discuss a slightly less tight bound of roughly $2^{3n/7-s}$ for general Nostradamus attacks against random compression functions, where s is the maximal block length of the adversarially chosen suffix S.