# Post-Quantum Cryptography Standardization
# Historical FAQs

**Q: What is the rationale to convert time and space complexity of known attacks into a single number for quantum and classical security?**

A: NIST's definition of s bits of quantum security is "as hard to break as a block cipher with a 2s bit key, assuming a relatively efficient and scalable quantum computing architecture is available." According to the analysis of Zalka[1] the best generic quantum attack on a 2s-bit block cipher requires a quantum circuit with depth*(squareroot (space)) proportional 2^s. This would suggest that quantum security should be defined as the minimum possible value of log(depth*(squareroot (space))) plus a constant (to put the quantum security of AES 128 at precisely 64 bits of quantum security,) accross all quantum and classical algorithms. This formula should only be taken as a rough guess, though, as there are additional factors to consider: Extremely serial and extremely parallel attacks are likely to be of limited practical relevance, even if the above formula rates them as most efficient. Likewise, even under the assumption that a relatively scalable and efficient quantum computing architecture is available, it is still likely that purely classical algorithms will be easier to implement than the formula suggests, and quantum algorithms that, unlike parallel versions of Grover's algorithms, cannot be divided into small, unentangled, subcircuits, will be harder to implement than the formula suggests. NIST plans to take these practical considerations into account when making its evaluations.

Similarly, NIST's definition of s bits of classical security is "as hard to break as a block cipher with an s bit key, assuming quantum computers are not available." This suggests that classical security should be estimated as the minimum value of log(depth*space) plus a constant, over all classical attack algorithms.

**Q: Why are hash functions assigned fewer bits of quantum security than classical security?**

**A**: Bernstein[2] is widely cited as demonstrating that the most efficient quantum algorithm for finding hash collisions is the classical algorithm given by Van Oorschot and Wiener[3]. NIST believes this analysis is correct. Nonetheless, NIST's security goal, that schemes claiming s bits of quantum security be at least as secure against cryptanalysis as a 2s bit block cipher leads to differing definitions for quantum and classical security. In particular, quantum search for a 2s bit key does not parallelize well. It is NIST's judgement that, since cryptanalysis in the real world tends to be most successful when it can take advantage of highly parallel implementations for attacks, finding collisions in a 2s bit hash function must be considered easier than searching for the key of a 2s-bit block cipher, even in a world with ubiquitous

---

[1] Christof Zalka, Grover's quantum searching algorithm is optimal, Physical Review A, 60:2746-2751, 1999 http://arxiv.org/abs/quant-ph/9711070

[2] Daniel J. Bernstein, Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? https://cr.yp.to/hash/collisioncost-20090517.pdf

[3] Paul C. van Oorschot, Michael Wiener, Parallel collision search with cryptanalytic applications, Journal of Cryptology 12 (1999) http://people.scs.carleton.ca/~paulv/papers/JoC97.pdf

quantum computing. NIST therefore assigns fewer than s bits of quantum security against collision to 2s bit hash functions.