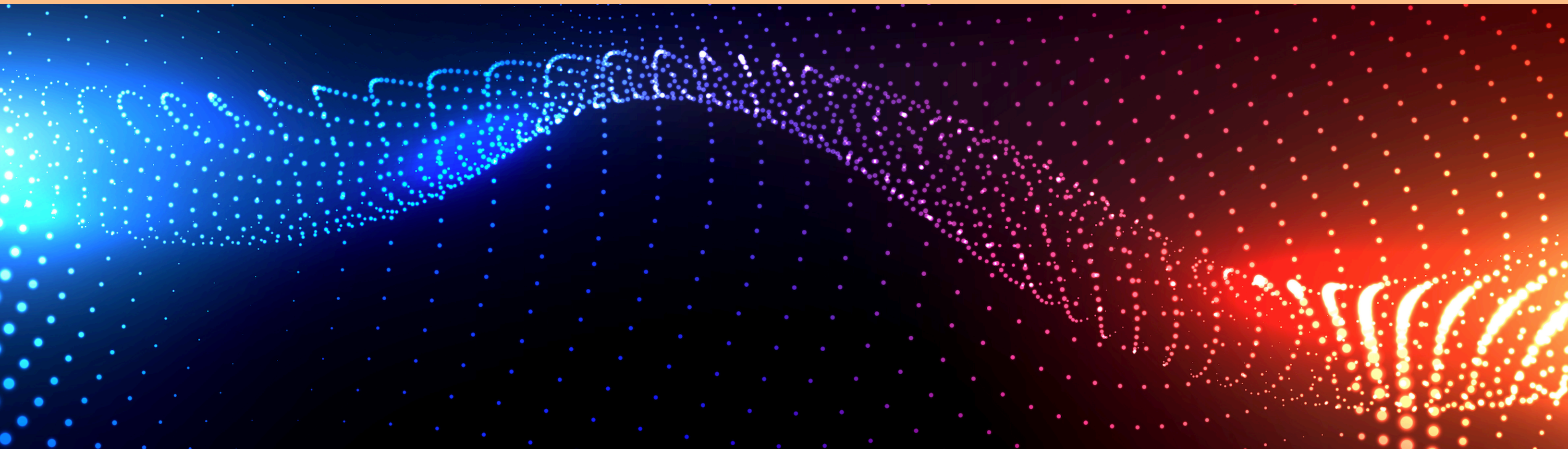


Intrinsic ID PUFs: An Antidote to Post-Quantum Uncertainty

Why should I (not) be concerned about using post-quantum cryptography?

You've probably been hearing a lot lately about the quantum-computing threat to cryptography. If so, you probably also have a lot of questions about what this "quantum threat" is and how it will impact your cryptographic solutions. Let's take a look at some of the most common questions about quantum computing and its impact on cryptography

What is a quantum computer?

A quantum computer is not a very fast general-purpose supercomputer, nor can it magically operate in a massively parallel manner. Instead, it efficiently executes unique quantum algorithms. These algorithms can in theory perform certain very specific computations much more efficiently than any traditional computer could.

However, the development of a meaningful quantum computer, i.e., one that can in practice outperform a modern traditional computer, is exceptionally difficult. Quantum computing technology has been in development since the 1980s, with gradually improving operational quantum computers since the 2010s. However, even extrapolating the current state of the art into the future, and assuming an exponential improvement equivalent to Moore's law for traditional computers, experts estimate that it will still take at least 15 to 20 years for a meaningful quantum computer to become a reality.[1,2]

What is the quantum threat to cryptography ?

In the 1990s, it was discovered that some quantum algorithms can impact the security of certain traditional cryptographic techniques. Two quantum algorithms have raised concern:

[1] "Report on Post-Quantum Cryptography", NIST Information Technology Laboratory, NISTIR 8105, April 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[2] "2021 Quantum Threat Timeline Report", Global Risk Institute (GRI), M. Mosca and M. Piani, January, 2022, https://globalriskinstitute.org/mp-files/quantum-threat-timeline-report-2021-full-report.pdf

The impact of quantum computers on current-day public-key cryptography is problematic and needs to be fixed.

1. **Shor's algorithm**, invented in 1994 by Peter Shor, is an efficient quantum algorithm for factoring large integers, and for solving a few related number-theoretical problems. Currently, there are no known efficient-factoring algorithms for traditional computers, a fact that provides the basis of security for several classic public-key cryptographic techniques.
2. **Grover's algorithm**, invented in 1996 by Lov Grover, is a quantum algorithm that can search for the inverse of a generic function quadratically faster than a traditional computer can. In cryptographic terms, searching for inverses is equivalent to a brute-force attack (e.g., on an unknown secret key value). The difficulty of such attacks forms the basis of security for most symmetric cryptography primitives.

These quantum algorithms, if they can be executed on a meaningful quantum computer, will impact the security of current cryptographic techniques.

What is the impact on my public-key cryptography solutions?

By far the most important and most widely used public-key primitives today are based on RSA, discrete-logarithm, or elliptic curve cryptography. When meaningful quantum computers become operational, all of these can be efficiently solved by Shor's algorithm. This will make virtually all public-key cryptography in current use insecure.

For the affected public-key encryption and key exchange primitives, this threat is already real today. An attacker capturing and storing encrypted messages exchanged now (or in the past), could decrypt them in the future when meaningful quantum computers are operational. So, highly sensitive and/or long-term secrets communicated up to today are already at risk.

If you use the affected signing primitives in short-term commitments of less than 15 years, the problem is less urgent. However, if meaningful quantum computers become available, the value of any signature will be voided from that point. So, you shouldn't use the affected primitives for signing long-term commitments that still need to be verifiable in 15-20 years or more.

Over the last decade, the cryptographic community has designed new public-key primitives that are based on mathematical problems that cannot be solved by Shor's algorithm (or any other known efficient algorithm, quantum or otherwise). These algorithms are generally referred to as post-quantum cryptography. NIST recently announced a selection of these algorithms for standardization[3].

What is the impact on my symmetric cryptography solutions?

The security level of a well-designed symmetric key primitive is equivalent to the effort needed for brute-forcing the secret key. On a traditional computer, the effort of brute-forcing a secret key is directly exponential in the key's length. When a meaningful quantum computer can be used, Grover's algorithm can speed up the brute-force attack quadratically. The needed effort remains exponential, though only in half of the key's length. So, Grover's algorithm could be said to reduce the security of any given-length algorithm by 50%.

[3] "PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates", NIST Information Technology Laboratory, July 5, 2022, https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

The practical impact of quantum computers on symmetric cryptography is, for the moment, very limited.

However, there are some important things to keep in mind:

- Grover's algorithm is an optimal brute-force strategy (quantum or otherwise),[4] so the quadratic speed-up is the worst-case security impact.
- There are strong indications that it is not possible to meaningfully parallelize the execution of Grover's algorithm.[2,5,6,7] In a traditional brute-force attack, doubling the number of computers used will cut the computation time in half. Such a scaling is not possible for Grover's algorithm on a quantum computer, which makes its use in a brute-force attack very impractical.
- Before Grover's algorithm can be used to perform real-world brute-force attacks on 128-bit keys, the performance of quantum computers must improve tremendously. Very modern traditional supercomputers can barely perform computations with a complexity exponential in 128/2=64 bits in a practically feasible time (several months). Based on their current state and rate of progress, it will be much, much more than 20 years before quantum computers could be at that same level.[6]

The practical impact of quantum computers on symmetric cryptography is, for the moment, very limited. Worst-case, the security strength of currently used primitives is reduced by 50% (of their key length), but due to the limitations of Grover's algorithm, that is an overly pessimistic assumption for the near future. Doubling the length of symmetric keys to withstand quantum brute-force attacks is a very broad blanket measure that will certainly solve the problem, but is too conservative. Today, there are no mandated recommendations for quantum-hardening symmetric-key cryptography, and 128-bit security strength primitives like AES-128 or SHA-256 are considered safe to use now and in the foreseeable future.

Is there an impact on information-theoretical security?

Information-theoretically secure methods (also called unconditional or perfect security) are algorithmic techniques for which security claims are mathematically proven. Some important information-theoretically secure constructions and primitives include the Vernam cipher, Shamir's secret sharing, Quantum key distribution[8] (not to be confused with post-quantum cryptography), entropy sources and physical unclonable functions (PUFs), and fuzzy commitment schemes[9].

[4] "Grover's quantum searching algorithm is optimal", C. Zalka, Phys. Rev. A 60, 2746, October 1, 1999, https://journals.aps.org/pra/abstract/10.1103/PhysRevA.60.2746

[5] "Reassessing Grover's Algorithm", S. Fluhrer, IACR ePrint 2017/811, https://eprint.iacr.org/2017/811.pdf

[6] "NIST's pleasant post-quantum surprise", Bas Westerbaan, CloudFlare, July 8, 2022, https://blog.cloudflare.com/nist-post-quantum-surprise/

[7] "Post-Quantum Cryptography - FAQs: To protect against the threat of quantum computers, should we double the key length for AES now? (added 11/18/18)", NIST Information Technology Laboratory, https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs

[8] "Quantum cryptography: Public key distribution and coin tossing", C. H. Bennett and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, December, 1984, https://arxiv.org/abs/2003.06557

[9] "A fuzzy commitment scheme", A. Juels and M. Wattenberg, Proceedings of the 6th ACM conference on Computer and Communications Security, November, 1999, https://dl.acm.org/doi/pdf/10.1145/319709.319714

Information-theoretically secure constructions are not impacted at all by the quantum threat.

Because an information-theoretical proof demonstrates that an adversary does not have sufficient information to break the security claim, regardless of its computing power – quantum or otherwise – information-theoretically secure constructions are not impacted by the quantum threat.

Intrinsic ID PUFs: An antidote for post-quantum security uncertainty

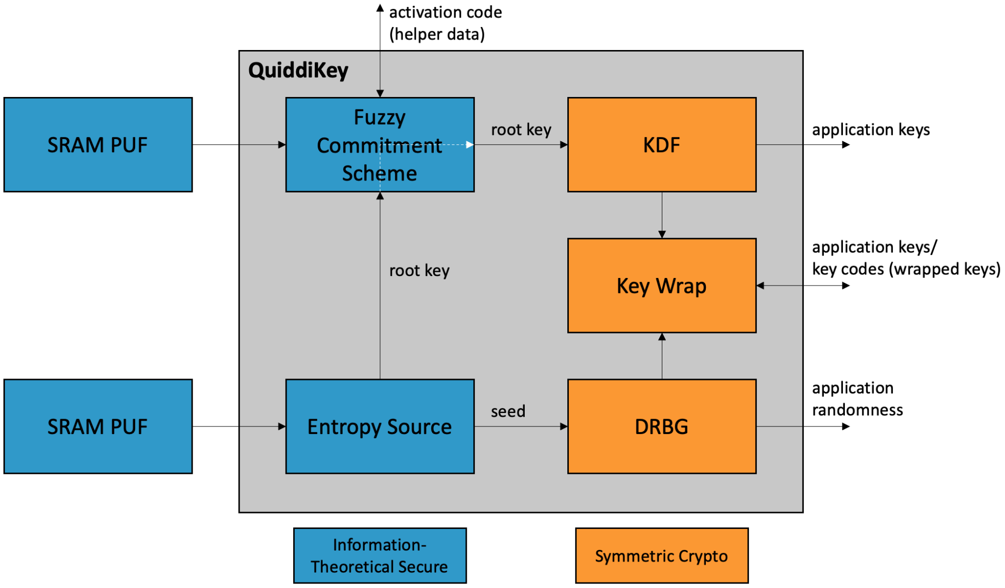
Intrinsic ID SRAM PUFs

The core technology underpinning all Intrinsic ID products is an SRAM PUF. Like other PUFs, an SRAM PUF generates device-unique responses that stem from unpredictable variations originating in the production process of silicon chips. The operation of an SRAM PUF is based on a conventional SRAM circuit readily available in virtually all digital chips.

Based on years of continuous measurements and analysis, Intrinsic ID has developed stochastic models that describe the behavior of its SRAM PUFs very accurately[10]. Using these models, we can determine tight bounds on the unpredictability of SRAM PUFs. These unpredictability bounds are expressed in terms of entropy, and are fundamental in nature, and cannot be overcome by any amount of computation, quantum or otherwise.

Intrinsic ID Quiddikey

QuiddiKey is a hardware security solution based on SRAM PUF technology. The central component of QuiddiKey is a *fuzzy commitment scheme*[9] that protects a root key with an SRAM PUF response and produces public helper data. It is information-theoretically proven that the helper data discloses zero information on the root key, so the fact that the helper data is public has no impact on the root key's security.



[10] "An Accurate Probabilistic Reliability Model for Silicon PUFs", R. Maes, Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, 2013, https://www.iacr.org/archive/ches2013/80860176/80860176.pdf

This no-leakage proof – kept intact over years of field deployment on hundreds of millions of devices – relies on the PUF employed by the system to be an entropy source, as expressed by its stochastic model. QuiddiKey uses its entropy source to initialize its root key for the very first time, which is subsequently protected by the fuzzy commitment scheme.

In addition to the fuzzy commitment scheme and the entropy source, QuiddiKey also implements cryptographic operations based on certified standard-compliant constructions making use of standard symmetric crypto primitives, particularly AES and SHA-256.[11] These operations include:

- a key derivation function (KDF) that uses the root key protected by the fuzzy commitment scheme as a key derivation key.
- a deterministic random bit generator (DRBG) that is initially seeded by a high-entropy seed coming from the entropy source.
- key wrapping functionality, essentially a form of authenticated encryption, for the protection of externally provided application keys using a key-wrapping key derived from the root key protected by the fuzzy commitment scheme.

Intrinsic ID: proven security for a post-quantum world

The security architecture of QuiddiKey is based on information-theoretically secure components for the generation and protection of a root key, and on established symmetric cryptography for other cryptographic functions. Information-theoretically secure constructions are impervious to quantum attacks. The impact of the quantum threat on symmetric cryptography is very limited and does not require any remediation now or in the foreseeable future. Importantly, QuiddiKey does not deploy any quantum-vulnerable public-key cryptographic primitives.

All variants of QuiddiKey are quantum-secure and in accordance with recommended post-quantum guidelines. The use of the 256-bit security strength variant of QuiddiKey will offer strong quantum-resistance, even in a distant future, but also the 128-bit variant is considered perfectly safe to use now and in the foreseeable time to come.

[11] NIST Information Technology Laboratory, Cryptographic Algorithm Validation Program CAVP, validation #A2516, https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=35127