Enabling Post-Quantum Security on Non-Post-Quantum Devices

***Abstract**: The advent of post-quantum computing is impacting organizations across the globe in significant ways. Whether it is a manufacturer trying to integrate and deploy new algorithms or a customer attempting to meet critical milestones in adopting post-quantum security devices, the struggle is rea. There is a path to post-quantum security that does not require replacing all your existing products. In this post, we cover the PROTECT solution, a technology that enables a post-quantum secure boot. Through a novel approach to secure boot, this technology can provide post-quantum security to both existing and future device, thereby preventing unnecessary hardware replacement and significantly reducing costs.*

Comentado [CA1]: This is passive voice; make strong statements like "is impacting organizations" instead.

Regardless of where you might stand in the debate regarding post-quantum computers and when they will hit a "cryptographic inflection point," there is no denying it is impacting our lives. Modern computer systems rely upon cryptographic algorithms to protect user data locally on the system as well as in transit to other systems. The security of user data is rooted in the security of the system access it, and many of those systems rely upon cryptographic algorithms that are not expected to remain secure against future post-quantum computer-based attacks. Of the cryptographic algorithms currently used, asymmetric algorithms are considered the most vulnerable to these future attacks.

Comentado [CA2]: I know your audience is tech types, but an explanation of how this impacts ordinary lives is one I need, even if it's not in the blog post.

The Nation Institute of Standards and Technologies, or NIST, has wrapped up the competition to replace asymmetric cryptographic algorithms[1]. Organizations are working to rapidly adopt these new algorithms mostly through deployment of their own guidelines, such as the Commercial Solutions for Classified (CSfC) by the National Security Agency[2] (NSA), the Migration to Post-Quantum Cryptography document from the Cybersecurity and Infrastructure Security Agency[3] (CISA), and the Transition to Post-Quantum Cryptography Standards by NIST itself[4]. Perhaps the most aggressive timeline for adoption of post-quantum comes from the NSA and the CNSA 2.0 timeline[5].

---

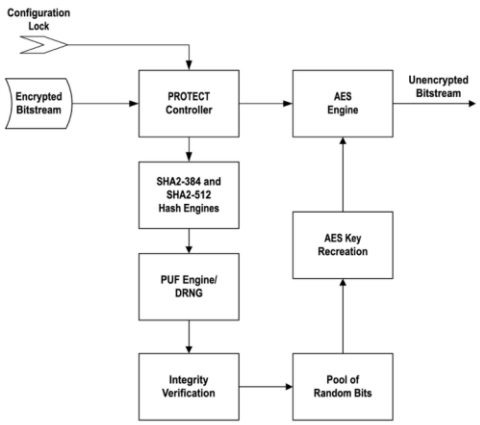
[1] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
[2] https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/capability-packages/CSfC%20Post%20Quantum%20Cryptography%20Guidance%20Addendum%201_0%20Draft%20_5.pdf?ver=wCGPoDQXcJKEWTgbH8xsRA%3D%3D
[3] https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF
[4] https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
[5] https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

To best prepare for the advent of post-quantum computing, NIST has made a significant push to encourage adoption of an approach called *crypto agility*. Crypto agility "describes the capabilities needed to replace and adapt cryptographic algorithms for protocols, applications, software, hardware, and infrastructures without interrupting the flow of a running system to achieve resiliency. "[6] This year, NIST conducted a workshop specifically on this topic with presenters from across Industry and Academia. We were proud to support Intel Corporation in their presentation at this workshop on the Configurable Cryptographic Controller Die, or C3D[7].

One of the core technologies behind the C3D solution is the PROTECT IP, developed in partnership between Dr. Matt Areno from Rickert-Areno Engineering, LLC and Dr. Jim Plusquellic from IC-Safety, LLC. The PROTECT IP is a solution that enables a post-quantum secure boot sequence that does not rely upon traditional asymmetric cryptography. Instead, it implements both authentication and attestation through a patented "key regeneration" using only symmetric and one-way cryptographic functions. As a result, this is a solution that can be implemented on both new and existing devices. Let's dive into some of the details on how PROTECT works.

PROTECT IP

The PROTECT IP works by taking in an existing encrypted bitstream and using that information to regenerate the original key that was used to encrypt it. To do that, a user first generates their symmetric key (assumed to be AES) and encrypts their bitstream (assuming an FPGA, but this could also be firmware or any other loaded logic). Next, within a trusted facility they can provision the system to regenerate that key. Once it regenerates the key, it then decrypts the bitstream and sends it to the fabric engine for programming.



[6] https://csrc.nist.gov/csrc/media/Presentations/2025/nist-pqc-the-road-ahead/images-media/rwcpqc-march2025-moody.pdf
[7] https://csrc.nist.gov/csrc/media/Events/2025/crypto-agility-workshop/documents/presentations/s8-brandon-eames-presentation.pdf

The regeneration process itself starts by computing two separate SHA hashes of the encrypted bitstream. These can be SHA2, SHA3, or any other acceptable one-way function. The important thing is that we use two and they are different block sizes. The reasoning behind this is that while it is conceivably possible for an attacker to create a collision (where two different inputs result in the same output) for one algorithm, it is statistically improbable they could ever do this simultaneously for two separate algorithms. This approach also protects us from certain physical access attacks.

Results from the first SHA2 computation are fed into a physically unclonable function (PUF) solution provided by IC-Safety called SiRF[8]. This value is then combined with known good challenge vectors to create a unique challenge for the PUF, which correspondingly creates a unique response. That response is then combined with the second SHA2 computation and is used as what we refer to as a *pool of random bits (*PORB). The authenticity and integrity of the bitstream is ensured by integrating the SHA2 measurements into both the challenge and response of the PUF. Any modification or alteration of the encrypted bitstream would change the challenge, response, and/or the PORB.

From within the PORB, we can recreate any key the customer wants. Additionally, while the solution utilizes a PUF to recreate a key, it is never used directly as a key itself. This removes any risks or concerns regarding the entropy of the PUF and ensures that the customer is in complete control regarding the characteristics of the key they are using.

Key recreation from the PORB can take many different forms and is highly customizable. A simple approach is to merely create a "key-split", as defined in NIST SP800-152 section 6.7.5[9]. That key split can then be stored in non-volatile memory where, during normal operations, it is combined with the PORB to regenerate or recreate the original key. Additional bits from the PORB would also be used to encrypt the key split should the customer have a higher security requirement. More advanced regeneration mechanisms are also possible and have been implemented by different customers. Regardless of the mechanism used, the resulting key is now provisioned and its regeneration bound to the integrity of the encrypted bitstream, the PROTECT IP itself (covered separately), and target devices through the PUF IP.

The final component of this technology is the *configuration lock mechanism*, or CLM. The CLM is there to prevent an adversary from arbitrarily putting the system back into configuration mode. As with the regeneration logic, there are several different implementations that can be used; likely the simplest would be the usage of traditional

[8] https://www.mdpi.com/2410-387X/6/4/59
[9] https://csrc.nist.gov/pubs/sp/800/152/final

fuses or anti-fuses. A set up could be reconfigurable circuitry, such as with the *Ripper* technology[10]. More advanced, patented solutions[11] also exist and could be used.

Deploying in Your Products

Perhaps the most important aspect of the PROTECT solution is that it is capable of being implemented on existing devices today. Implementations of this technology have already been completed on multiple Microchip FPGAs and are underway for both Xilinx and Altera. PROTECT uses patented mechanism to ensure the integrity of its own implementation, which can also be seamlessly combined with existing secure boot solutions. This means that any customers using existing Xilinx, Altera, or Microchip products that do not currently have a post-quantum secure boot solution can deploy PROTECT within those products and become post-quantum resistant. Additionally, the logic for PROTECT can easily be incorporated into ASIC designs for custom chips or chiplets. The resulting implementation can provide a root of trust based upon post-quantum resistant algorithms expected to be secure for decades to come.

Because the information used to regenerate the key is stored in non-volatile memory (NVM), it can easily be replaced by end customers at any time by an authorized entity. This allows customers to fully provision a part that may be needed by a 3rd party for a short period of time. Once the access is no longer need, the key is removed and/or the encrypted bitstream is changed and their access is effectively revoked without leaving any trace it ever existed. To ensure prior customers are never able to load their firmware again, the CLM can easily incorporate a seed for the SHA2 engines that is changed once the device returns. PROTECT enables and effective *clean-slate* mechanism to ensure post-quantum secure boot without leaving behind any permanent trace.

---

[10] https://scholar.google.com/scholar?q=N.+Dorairaj+D.+Kehlet+A.+Dasgupta%2C+M.M.+Rahman+and+S.+Bhunia.+2022.+RIPPER%3A+Securing+Hardware+IP+through+Fine+Grained+Reduction+of+Boolean+Functions.+Annual+Government+Microcircuit+Applications+Critical+Technology+%28GOMACTech%29.

[11] https://patentimages.storage.googleapis.com/13/cf/89/e00fd887bf0a83/EP4020287B1.pdf