National Security Agency | Frequently Asked Questions

Quantum Computing and Post-Quantum Cryptography

General Information

Q: What is a quantum computer, and how is it different from the computers we use today?
A: Quantum computers can, in principle, perform certain mathematical algorithms exponentially faster than a classical computer. In place of ordinary bits used by today's computers, quantum computers use "qubits" that behave and interact according to the laws of quantum mechanics. This quantum physics-based behavior would enable a sufficiently large-scale quantum computer to perform specific mathematical calculations that would be infeasible for any conventional computer.

Q: What is a "Cryptographically Relevant Quantum Computer" (CRQC)?
A: Small, laboratory-scale examples of quantum computers have been built. Some larger systems have also been proposed that can address some types of computation, but which may not be suitable for analyzing cryptographic algorithms. CRQC is used to specifically describe quantum computers that are capable of actually attacking real world cryptographic systems that would be infeasible to attack with a normal computer.

Q: What is the threat if a CRQC were developed?
A: If realizable, a CRQC would be capable of undermining the widely deployed public key algorithms used for asymmetric key exchanges and digital signatures. National Security Systems (NSS) — systems that carry classified or otherwise sensitive military or intelligence information — use public key cryptography as a critical component to protect the confidentiality, integrity, and authenticity of national security information. Without effective mitigation, the impact of adversarial use of a quantum computer could be devastating to NSS and our nation, especially in cases where such information needs to be protected for many decades.

Q: Can I mitigate the quantum threat by using a pre-shared key?
A: Many commercial protocols allow a pre-shared key option that may mitigate the quantum threat, and some allow the combination of pre-shared and asymmetric keys in the same negotiation. However, this issue can be complex. Customers who wish to explore this option should contact NSA or follow guidance provided by the Commercial Solutions for Classified (CSfC) program.

Q: What is "quantum-resistant" or "post-quantum" cryptography?
A: Quantum-resistant, quantum-safe, and post-quantum cryptography are all terms used to describe cryptographic algorithms that run on standard encryption/decryption devices and are widely recognized by experts to be resistant to cryptanalytic attacks from both classical and quantum computers. Although cryptanalysis using classical computing has been a subject of intense interest for many decades, the art and science of cryptanalysis that involves a (potential) quantum computer is still relatively new. Algorithms believed to be safe against an adversary that might one day have a CRQC are referred to by some using the term "quantum-resistant" or "quantum-safe." It is generally expected that any "quantum-resistant" or "quantum-safe" standard will be secure against all envisioned and understood quantum computing capabilities. "Post-quantum" is a neutral term often used to simply convey that these algorithms are designed with the quantum threat in mind. Note that post-quantum does not mean that these algorithms are only for use after a CRQC is built.

Q: Will quantum computers affect non-public key (i.e., symmetric) algorithms?
A: It is generally accepted by experts in this field that quantum computing techniques are much less effective in attacking symmetric algorithms than against widely used public key algorithms. While public key cryptography requires changes in the fundamental design, symmetric algorithms are believed to be secure, provided a sufficiently large key size is used. The symmetric key algorithms of the Commercial National Security Algorithm (CNSA) Suite were selected to be secure for NSS usage even if a CRQC is developed.

Q: Is NSA worried about the threat posed by a potential quantum computer because a CRQC exists?
A: NSA does not know when or even if a quantum computer of sufficient size and power to exploit public key cryptography (a CRQC) will exist.

Q: Why does NSA care about quantum computing today? Isn't quantum computing a long way off?
A: The cryptographic systems that NSA produces, certifies, and supports often have very long lifecycles. NSA has to produce requirements today for systems that will be used for many decades in the future, and data protected by these systems will still require cryptographic protection for decades after these solutions are replaced. There is growing research in the area of quantum computing, and global interest in its pursuit have provoked NSA to ensure the enduring protection of NSS by encouraging the development of post-quantum cryptographic standards and planning for an eventual transition.

Q: What are the timeframes in NSS for deployment of new algorithms, use of equipment, and national security information intelligence value?
A: New cryptography can take 20 years or more to be fully deployed to all National Security Systems. NSS equipment is often used for decades after deployment. National security information intelligence value varies depending on classification, sensitivity, and subject, but it can require protection for many decades.

Q: How do I transition to a quantum-resistant system?
A: The CNSA Suite represents the interim strategy as the commercial space transitions to quantum-resistant public key. Following CNSA guidance and future NSA cryptographic suite announcements will provide the quickest path to securely mitigate the quantum threat against NSS. While anticipatory work to plan and prepare for the transition is underway, acquisitions should await NSA authorization.

Q: What is quantum key distribution (QKD) and quantum cryptography?
A: The field of quantum cryptography involves specialized hardware that makes use of the physics of quantum mechanics (as opposed to the use of mathematics in algorithmic cryptography) to protect secrets. The most common example today uses quantum physics to distribute keys for use in a traditional symmetric algorithm, and is thus known as quantum key distribution. This technology exists today and is distinct from the quantum computing technology that might one day be used to attack mathematically based cryptographic algorithms. The sole function of QKD is to distribute keys between users and hence it is only one part of a cryptographic system.

Q: Are QKD systems unconditionally secure?
A: No. While there are security proofs for theoretical QKD protocols, there are no security proofs for actual QKD hardware/software implementations. There is no standard methodology to test QKD hardware, and there are no established interoperability, implementation, or certification standards to which these devices may be built. This causes the actual security of particular systems to be difficult to quantify, leading in some cases to vulnerabilities.

Q: Should I use a QKD system to protect my NSS from a quantum computer?
A: No. The technology involved is of significant scientific interest, but it only addresses some security threats and it requires significant engineering modifications to NSS communications systems. NSA does not consider QKD a practical security solution for protecting national security information. NSS owners should not be using or researching QKD at this time without direct consultation with NSA. For specific questions, NSS owners can contact NSA.

Q: What is a quantum random number generator (quantum RNG)?
A: Quantum RNGs are hardware random number generators that use specific quantum effects to generate nondeterministic randomness. They are a commercial technology available today that is distinct from the use of quantum computing to attack cryptographic algorithms. There are a variety of non-quantum RNGs available that have been appropriately validated or certified as acceptable for use in NSS or other government applications. They will remain secure even if a CRQC is built. The decision on what RNG is appropriate to use in a specific scenario depends on many factors, and any RNG should be acceptable if properly certified/approved and implemented within the constraints of that approval.

Commercial National Security Algorithm Suite

Q: What is the CNSA Suite?
A: The CNSA Suite is the suite of algorithms identified in the Committee on National Security Systems Policy 15 (CNSSP-15) for protecting NSS, including classified information. The CNSA Suite includes:

Algorithm	Usage
RSA 3072-bit or larger	Key Establishment, Digital Signature
Diffie-Hellman (DH) 3072-bit or larger	Key Establishment
ECDH with NIST P-384	Key Establishment
ECDSA with NIST P-384	Digital Signature
SHA-384	Integrity Protection
AES-256	Confidentiality

Q: What is CNSSP-15?
A: CNSSP-15 specifies commercial cryptographic algorithms for use in protecting NSS, in conjunction with other CNSS and NSA documented processes. It was originally the policy document that specified “NSA Suite B” and now it describes the Commercial National Security Algorithm Suite. Further details about CNSS can be found at cnss.gov.

Q: How does the current CNSSP-15 differ from the previous version?
A: The October 2016 update to CNSSP-15 made three significant changes:

- It replaced the previous requirement to transition systems to Suite B standards, instead specifying a larger selection of algorithms (the CNSA Suite) in order to allow extended use of existing solutions while post-quantum standards are being developed.
- It consolidated the two security levels of Suite B into a single set of requirements for use at all levels.
- The previous CNSS policy was directed explicitly at classified information, but the updated policy applies to all NSS — classified and unclassified. For guidance on determining if a system is an NSS see NIST SP 800-59.

Q: How did NSA determine the sizes of RSA and Diffie-Hellman to use?
A: In CNSS Advisory Memorandum 02-15, NSA changed the status of these algorithms from “legacy” to “supported” in order to allow their extended use until quantum-resistant cryptography is available, which continued in CNSSP-15. The selection of a 3072-bit key size for RSA and Diffie-Hellman was made after considering the expected longevity of the NSS that would need to use these algorithms and the practical technology constraints of some of those systems. Larger sizes for RSA and Diffie-Hellman are acceptable, as specified in the guidance. If needed, NSA can provide additional guidance to vendors and NSS developers, operators and users on the appropriate key sizes for their specific application.

Q: How does CNSSP-15 relate to CNSSI-1253, NIST SP 800-53, and the RMF process?
A: CNSS Instruction 1253 (CNSSI-1253) mandates the use of the Risk Management Framework (RMF) as documented in National Institute of Standards and Technologies (NIST) Special Publications (SP) 800-39 and 800-53 in the management of National Security Information Systems. SP 800-53 includes security controls that relate to cryptography. For NSS, the "NSA Approved" selection is required. Unless otherwise stated by NSA,

the "NSA Approved" cryptography selection should be understood to include the CNSA algorithm requirements as well as all other relevant guidance from NSA on product validation and operation.

Q: Aren't the public key algorithms in the CNSA Suite all vulnerable to quantum attacks?
A: The public key algorithms (RSA, Diffie-Hellman, ECDH, and ECDSA) are all potentially vulnerable to attack by a CRQC. The intent of the interim strategy is to allow more flexibility for customers and vendors in the near term to save on costs while robust quantum-resistant standards are being developed and thoroughly evaluated by the cryptographic community.

Q: What about the symmetric algorithms in the CNSA Suite?
A: The CNSA Suite mandates symmetric algorithms with sufficient strength to resist anticipated quantum computing threats. The intent is to only update the public key components of the suite with quantum-resistant components.

Q: What about Suite B?
A: The term "Suite B" had become associated with a specific, fixed set of algorithms rather than with the use of selected public algorithms to protect classified information. To avoid confusion, the term "Suite B" is no longer being used.

Q: What about the Suite B Requests for Comments published by the Internet Engineering Task Force (IETF)?
A: The Suite B RFCs are no longer appropriate for use, and have been classified as Historic in RFC 8423. New guidance describing how to implement CNSA Suite algorithms in common IETF protocols is becoming available as informational RFCs and in NSA releases. This should be applied throughout the NSS space. Note that the protocol specific guidance may include only some CNSA Suite algorithms, may mandate specific modes and options, and/or may allow inclusion of non-CNSA Suite algorithms as appropriate. These exceptions are based on the specific technical details and/or market availability of the technologies involved and are allowed by CNSSP-15, but may change as CNSA support becomes available.

Q: How should the broader government community understand CNSSP-15 requirements?
A: NSA establishes requirements for NSS. Often these systems store and/or communicate information that requires protection for long periods against targeted efforts by sophisticated and well-resourced adversaries in potential wartime settings. General government users may or may not have such stringent requirements. NIST has the responsibility for establishing cryptographic standards for other government systems. NSA expects to continue maintaining a high security standard for commercial products used in these applications that will be selected from the general NIST cryptographic standards. If there is uncertainty about whether a specific system is subject to the NSS requirements, NIST and NSA are available to assist in addressing the question. See also NIST SP 800-59.

Q: Given the range of algorithm options and sizes to choose from, which is best?
A: The October 2016 version of CNSSP-15 alerts the developers and operators of NSS of the need to transition to quantum-resistant algorithms in the future and permits greater flexibility in algorithm choice than was allowed under previous guidance. This flexibility is intended to minimize the risk of making existing systems upgrade their equipment to meet a temporary standard, only to then require them again to upgrade to use post-quantum solutions. Within this framework, developers, operators and users may choose the most cost effective path to comply with the policy while planning their migration path to future post-quantum asymmetric cryptography. NSS developers, operators or users who need additional guidance should contact NSA.

Q: Which specific algorithm parameters should NSS use?
A: NSS users should select well-established and validated parameter sets specified in NIST-endorsed standards that comply with the minimum required sizes. For many of the most common protocols, NSA is producing specific guidance on selections that are acceptable. For IETF protocols, specific RFCs have been or will be published and made available. For other applications, some specific examples that are acceptable include:

- Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve DSA (ECDSA) must use the NIST P-384 parameters.
- RSA should use moduli that have a minimum size of 3072 bits (other than the noted PKI exception), and keys should be generated in accordance with all relevant NIST standards and guidance.
- Diffie-Hellman should use a prime modulus of at least 3072 bits as specified in established standards. Typical examples would include IETF RFC 3526 (Groups 15-18) or RFC 7919 (groups ffdhe3072 and larger).

Q: I have already provisioned RSA 4096 certificates on a number of devices used in NSS. Should I move to RSA 3072 certificates?
A: Not necessarily. RSA with 4096 modulus size exceeds the 3072 minimum modulus size and is acceptable for use. Because of the nature of RSA, interoperability questions do not have as clear an answer as with elliptic curve systems. If an NSS customer has a question, they should contact NSA.

Q: For RSA and Diffie-Hellman based solutions, the CNSA Suite includes only a minimum size. Can I use the NIST P-521 curve for ECDH or ECDSA on NSS?
A: Cryptographic libraries implementing RSA and DH have long supported multiple key sizes, and there is a diverse range of sizes already in use. To save costs, the existing use of larger key sizes is allowed to continue in CNSA. For elliptic curve cryptography, specific parameters must be programmed, and P-384 was the common parameter set established in Suite B when this technology was first deployed. To enhance system interoperability, NSA retained the requirement to use only NIST P-384 in the CNSA definition. NSS operators who wish to use an algorithm outside of the officially specified CNSA Suite should always consult with NSA. However, if interoperability is not a concern, P-521 would likely be considered acceptable.

Q: What about new elliptic curves and associated algorithms?
A: Given the transition time required for most government programs to integrate new cryptography; the large established base of existing solutions; the desire to preserve interoperability with existing systems; and the expected standardization of post-quantum algorithms, NSA does not anticipate including additional algorithms or parameter selections in the CNSA Suite.

Q: What does the CNSSP-15 mean when it says SHA-256 and 2048-bit RSA are allowed for PKI systems used for Community of Interest separation?
A: Within the government, there exist large-scale PKI deployments (such as the DoD PKI) that are based on 2048-bit RSA. These systems are often used to provide additional access control functions within an already-secured system or for official communications on unclassified networks. Given the time and expense required to change these systems and the specific environments in which they operate, CNSS Policy 15 allows a blanket exception for these existing implementations until a post-quantum transition can be implemented.

Q: Are there other cases where SHA-256, 2048-bit RSA, or other NIST algorithms will be allowed?
A: As part of Suite B, devices were often required to support P-384 and SHA-384 as an option. Some systems, especially those based on specialized hardware, may not be easily modified to comply with CNSA standards. Guidance regarding acceptable alternatives may be provided as part of Capabilities Packages released by the CSfC program or via other NSA publications. If a selection is documented as acceptable in a CSfC Capabilities Package, it can be generally understood to be NSA-approved for use in the same role within the broader NSS at the unclassified level as well until that Capability Package expires. Other specific use cases may also warrant exceptions. When specific questions arise and there is no other published guidance, NSA should be consulted.

Q: Can we use alternative NIST standardized hash functions?
A: SHA-384 support was included in previous versions of CNSSP-15 and it is judged to provide sufficient security for NSS. For interoperability purposes, the selection of a single hash function has been maintained in the CNSA Suite. NSA does not anticipate revisiting this decision until the post-quantum algorithm transition. There are some applications where truncated hash values are used appropriately or other hash functions may be a better choice. In specific scenarios where different length hash outputs are needed and/or SHA-384 is not generally supported, protocol-specific guidance may be issued or customers may consult with NSA for clarification.

Q: What are “stateful” hash-based signatures?
A: There are now public standards for “stateful” hash-based signatures, which require an internal “state” to be updated with each use to maintain security. Their mathematical security is widely accepted. However, they have some properties that make them unsuitable for general use. These algorithms may be appropriate for use in specific scenarios such as firmware signing. NIST SP 800-208 standardizes and provides guidance for the use of these signatures.

Q: Can I use stateful hash-based signatures?
A: NSA recommends the use of SP 800-208 hash-based signatures, when implemented on properly validated cryptographic modules, to protect NSS in the specialized scenarios outlined in the standard; e.g., for firmware signing. Our preferred parameter set is Section 4.2, LMS with SHA-256/192.

Q: I have long data life concerns and want to adopt CSfC solutions. How can I ensure my communications and data remain secure against an adversary with a quantum computer?
A: Some CSfC solutions may be implemented using symmetric, pre-shared keys that protect against the long-term quantum computing threat. NSA considers the use of pre-shared symmetric keys in a standards-compliant fashion to be a better near-term post-quantum solution than implementation of experimental post-quantum asymmetric algorithms that may or may not be proven secure and which will not be compatible with NIST standards. For more info, contact the CSfC program office.

Q: The data I have on my particular NSS only requires protection for a short time. Do I really need to comply with the increased algorithm strengths of CNSSP-15?
A: NSA mandates transitioning algorithms for NSS in order to conform to a common standard and to ensure interoperability. NSS developers and operators should transition to comply or consult with NSA about the issues involved in their specific scenario.

Q: When will CNSA be updated to quantum-resistant algorithms?
A: The intention is to update CNSA to remove quantum-vulnerable algorithms and replace them with a subset of the quantum-resistant algorithms selected by NIST at the end of the third round of the NIST post-quantum effort – NIST determines the timeline for each round. See the Future Cryptography section of this FAQ for more information.

Commercial Solutions for Classified (CSfC) and National Information Assurance Partnership (NIAP)

Q: Can I use any CNSA capable product(s) in my NSS without going through NIAP/CSfC?
A: No. CNSSP-11 states, "All Commercial-off-the-Shelf (COTS) Information Assurance (IA) and IA-enabled Information Technology (IT) products acquired for use to protect information on National Security Systems shall comply with the requirements of the NIAP program in accordance with NSA-approved processes and, where applicable, the requirements of the Federal Information Processing Standards (FIPS) Cryptographic validation program(s)." Furthermore, CNSSP-7 states that a CSfC solution that has been approved by the appropriate Authorizing Official and registered with NSA's CSfC Program Management Office as being compliant with an NSA-provided Capability Package may be used to protect NSS.

Q: I have a product/solution built for NSS to meet NIAP Protection Profiles and/or a CSfC Capability Package. How does this affect me?
A: NIAP Protection Profiles and CSfC Capability Packages are regularly updated to align with CNSSP-15. Note that the Protection Profile process is driven by the technology available on the commercial market and is intended to accommodate a wide selection of use cases beyond CSfC. Therefore, the NIAP Protection Profiles may include a broad set of algorithms which are not found in CNSA or CSfC. The CSfC Capability Packages have been updated to align with the CNSA Suite requirements and describe how to use layering of commercial encryption in specific configurations to protect classified information.

NSA may, on a case-by-case basis, approve alternative algorithm choices as part of the CSfC process, primarily when the marketplace does not yet provide sufficient CNSA-compliant products. This approval can be assumed to imply that NSA also approves of the same cryptography in NSS operating at the unclassified level using the same technology. Independent of the CSfC process, NSA issues other guidance specific to products or technologies used in NSS. This guidance may also include non-CNSA selections. However, it should be understood that the Capability Package or other NSA guidance that indicates approval for non-CNSA selections might change if and when market support for CNSA Suite selections exists.

Future Algorithms and Cryptography

Q: Where will the quantum-resistant public key algorithms used in CNSA come from?
A: NIST is in the process of standardizing quantum-resistant public key in their Post-Quantum Standardization Effort, which started in 2016. This multi-year effort is analyzing a large variety of confidentiality and authentication algorithms for inclusion in future standards. NSA expects to add lattice-based algorithms from the NIST process to CNSA at the end of Round 3 – this timeline is determined by NIST.

Q: Is there a quantum-resistant public key algorithm that commercial vendors should adopt today?
A: There is not a quantum-resistant public key algorithm that commercial vendors should adopt with the exception of stateful hash signatures for firmware. While a number of interesting quantum-resistant public key algorithms are being considered by NIST, there are no approved, generally usable standards at this time. NSA is waiting for the NIST process to be completed and for standards to be published. When the NIST process selects algorithms for standardization that are suitable for NSS use, NSA will establish a roadmap and timeline for the transition of NSS. Vendors and purchasers should anticipate an eventual need to migrate to NIST post-quantum cryptographic standards and they should be developing/purchasing products that allow for a secure and low-complexity upgrade to new algorithms. Once NIST post-quantum cryptographic standards are published and certification procedures for those algorithms are established, CNSSP-15 will be updated with a timeline for required use of the post-quantum algorithms and disuse of the quantum-vulnerable portion of the current CNSA Suite of algorithms. The nature of this timeline will depend upon the standards selected and the ability of the market to provide supporting products. NSS customers are reminded that NSA does **not** recommend and policy does not allow implementing or using unapproved, non-standard or experimental cryptographic algorithms. The field of quantum-resistant cryptography is no exception.

Q: What can developers and programs do to prepare for a future quantum-resistant algorithm suite?
A: The AES-256 and SHA-384 algorithms in CNSA are considered safe against attack by a large quantum computer. Developers can deploy these algorithms. NSA does not recommend adding non-standardized algorithms into deployed, certified systems and products. NSA has stated that it expects to select a lattice-based algorithm from the NIST finalists. Developers should begin to experiment with these choices and provide feedback to the NIST process about any issues discovered. Programs should anticipate that after NIST provides the needed standards there would be rapid movement toward requiring support of a quantum-resistant standard in new acquisitions. Further, it will be expected that software-upgradable devices will also add support promptly as part of the normal update process. While the exact transition timeline cannot be determined at this stage, it would be prudent for programs to incorporate requirements to experiment with these candidate algorithms and ensure the ability to promptly upgrade when the time comes.

Q: When will quantum-resistant cryptography standards be available?
A: This question is best addressed by NIST. Learn more about NIST's standardization efforts.

Q: When will NSA select a NIST-approved algorithm?
A: NIST has indicated that it will likely standardize multiple post-quantum algorithms at multiple security levels from their Round 3 finalists, to include a lattice-based algorithm for confidentiality and a lattice-based signature. To enable interoperability within NSS, NSA anticipates using these lattice-based standards, likely at one of the higher security levels. The precise choice will be announced after NIST makes its selections. There is usually a significant period of time between a NIST selection announcement and publication of the final standard. NSA may announce its choice(s) before the final NIST standard is published in order to help the NSS community plan for implementation. Official deployment will not begin until the final standard is published; certification and validation processes are in place; and a robust plan for post-quantum cryptography acquisition, transition and interoperability is established. It is likely that commercial vendors will be offering some support before the process is complete. NSA has full confidence in the NIST Post-Quantum Cryptography Standardization process.

Q: Where can I get further information?
A: For Commercial Solutions for Classified (CSfC) program specific questions; customers should contact the CSfC Management Office at CSfC@nsa.gov.
Other specific questions from National Security Systems (NSS) users may be addressed via email to NSACryptoToday@nsa.gov or through normal business channels.

Note: Please coordinate any engagement on this matter with the Cybersecurity Directorate leads via cybersecurity@nsa.gov. Please defer any media inquiries to MediaRelations@nsa.gov.