NISTIR 8105

Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8105

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8105

Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone
Computer Security Division
Applied and Computational Mathematics Division
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8105

April 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Internal Report 8105
15 pages (April 2016)

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8105

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: NISTIR8105-comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. This Internal Report shares the National Institute of Standards and Technology (NIST)'s current understanding about the status of quantum computing and post-quantum cryptography, and outlines NIST's initial plan to move forward in this space. The report also recognizes the challenge of moving to new cryptographic infrastructures and therefore emphasizes the need for agencies to focus on crypto agility.

Keywords

post-quantum cryptography; public key cryptography; quantum computing; quantum-resistant; quantum-safe.

Table of Contents

List of Appendices

1 Introduction

In the last three decades, public key cryptography has become an indispensable component of our global communication digital infrastructure. These networks support a plethora of applications that are important to our economy, our security, and our way of life, such as mobile phones, internet commerce, social networks, and cloud computing. In such a connected world, the ability of individuals, businesses and governments to communicate securely is of the utmost importance.

Many of our most crucial communication protocols rely principally on three core cryptographic functionalities: public key encryption, digital signatures, and key exchange[1]. Currently, these functionalities are primarily implemented using Diffie-Hellman key exchange, the RSA (Rivest-Shamir-Adleman) cryptosystem, and elliptic curve cryptosystems. The security of these depends on the difficulty of certain number theoretic problems such as Integer Factorization or the Discrete Log Problem over various groups.

In 1994, Peter Shor of Bell Laboratories showed that quantum computers, a new technology leveraging the physical properties of matter and energy to perform calculations, can efficiently solve each of these problems, thereby rendering all public key cryptosystems based on such assumptions impotent [1]. Thus a sufficiently powerful quantum computer will put many forms of modern communication—from key exchange to encryption to digital authentication—in peril.

The discovery that quantum computers could be utilized to solve certain problems faster than classical computers has inspired great interest in quantum computing. Is quantum complexity fundamentally different from classical complexity? When will large-scale quantum computers be built? Is there a way to resist both a quantum and a classical computing adversary? Researchers are working on these questions.

In the twenty years since Shor's discovery, the theory of quantum algorithms has developed significantly. Quantum algorithms achieving exponential speedup have been discovered for several problems relating to physics simulation, number theory, and topology. Nevertheless, the list of problems admitting exponential speedup by quantum computation remains relatively small. In contrast, more modest speedups have been developed for broad classes of problems related to searching, collision finding, and evaluation of Boolean formulae. In particular, Grover's search algorithm proffers a quadratic speedup on unstructured search problems. While such a speedup does not render cryptographic technologies obsolete, it can have the effect of requiring larger key sizes, even in the symmetric key case. See Table 1 for a summary of the impact of large-scale quantum computers on common cryptographic algorithms, such as RSA and the Advanced Encryption Standard (AES). It is not known how far these quantum advantages can be pushed, nor how wide is the gap between feasibility in the classical and quantum models.

[1] NIST standardized digital signature schemes in [FIPS 186-4], as well as public key-based key establishment schemes in [SP800-56A] (using key exchange) and [SP800-56B] (using public key encryption).

The question of when a large-scale quantum computer will be built is complicated and contentious. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some experts even predict that within the next 20 or so years, sufficiently large quantum computers will be built to break essentially all public key schemes currently in use [2]. It has taken almost 20 years to deploy our modern public key cryptography infrastructure. It will take significant effort to ensure a smooth and secure migration from the current widely used cryptosystems to their quantum computing resistant counterparts. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

A large international community has emerged to address the issue of information security in a quantum computing future, in the hope that our public key infrastructure may remain intact by utilizing new quantum-resistant primitives. In the academic world, this new science bears the name "Post-Quantum Cryptography[2]." This is an active area of research, with its own conference series, PQCrypto, which started in 2006. It has received substantial support from national funding agencies, most notably in Europe and Japan, through the European Union (EU) projects PQCrypto and SAFEcrypto, and the CREST Crypto-Math project in Japan.

These efforts have led to advances in fundamental research, paving the way for the deployment of post-quantum cryptosystems in the real world. In the past few years, industry and standards

[2] Post-quantum cryptography should not be conflated with quantum cryptography (or quantum key-distribution), which uses properties of quantum mechanics to create a secure communication channel. This report is only concerned with post-quantum cryptography.

organizations have started their own activities in this field: since 2013, the European Telecommunications Standards Institute (ETSI) has held three “Quantum-Safe Cryptography" workshops, and in 2015 NIST held a workshop on “Cybersecurity in a Post-Quantum World,” which was attended by over 140 people from government, industry, and academia.

NIST has a unique role to play in standardizing post-quantum cryptography, as part of its broader responsibility for the development of standards and guidelines for the protection of non-national-security federal information systems. Many NIST standards, such as the Advanced Encryption Standard (AES), have been developed with broad participation from academia and industry, and have been widely adopted because they are effective solutions, thus helping to protect U.S. information and information systems. NIST standardization of post-quantum cryptography will likely provide similar benefits.

Considering all of these sources, it is clear that the effort to develop quantum-resistant technologies is intensifying. Equally clear is the urgency, implied by these investments, of the need for standardizing new post-quantum public key cryptography. It is critical to engage with the community for NIST cryptographic standards to be endorsed by industry and other standards organizations around the world. This Internal Report shares NIST’s current understanding about the status of quantum computing and post-quantum cryptography, and outlines our initial plan to move forward.

2 An Overview of Quantum-Resistant Cryptography

The most important uses of public key cryptography today are for digital signatures and key establishment. As mentioned in Section 1, the construction of a large-scale quantum computer would render many of these public key cryptosystems insecure. In particular, this includes those based on the difficulty of integer factorization, such as RSA, as well as ones based on the hardness of the discrete log problem. In contrast, the impact on symmetric key systems will not be as drastic (see Table 1). Grover’s algorithm provides a quadratic speed-up for quantum search algorithms in comparison with search algorithms on classical computers. We don’t know that Grover’s algorithm will ever be practically relevant, but if it is, doubling the key size will be sufficient to preserve security. Furthermore, it has been shown that an exponential speed up for search algorithms is impossible, suggesting that symmetric algorithms and hash functions should be usable in a quantum era [3].

Consequently, the search for algorithms believed to be resistant to attacks from both classical and quantum computers has focused on public key algorithms. In this section, we briefly give an overview of the main families for which post-quantum primitives have been proposed. These families include those based on lattices, codes, and multivariate polynomials, as well as a handful of others. For further information, see [4, 5].

Lattice-based cryptography – Cryptosystems based on lattice problems have received renewed interest, for a few reasons. Exciting new applications (such as fully homomorphic encryption, code obfuscation, and attribute-based encryption) have been made possible using lattice-based cryptography. Most lattice-based key establishment algorithms are relatively simple, efficient,

and highly parallelizable. Also, the security of some lattice-based systems are provably secure under a worst-case hardness assumption, rather than on the average case. On the other hand, it has proven difficult to give precise estimates of the security of lattice schemes against even known cryptanalysis techniques.

Code-based cryptography – In 1978, the McEliece cryptosystem was first proposed, and has not been broken since. Since that time, other systems based on error-correcting codes have been proposed. While quite fast, most code-based primitives suffer from having very large key sizes. Newer variants have introduced more structure into the codes in an attempt to reduce the key sizes, however the added structure has also led to successful attacks on some proposals. While there have been some proposals for code-based signatures, code-based cryptography has seen more success with encryption schemes.

Multivariate polynomial cryptography – These schemes are based on the difficulty of solving systems of multivariate polynomials over finite fields. Several multivariate cryptosystems have been proposed over the past few decades, with many having been broken [6]. While there have been some proposals for multivariate encryption schemes, multivariate cryptography has historically been more successful as an approach to signatures.

Hash-based signatures – Hash-based signatures are digital signatures constructed using hash functions. Their security, even against quantum attacks, is well understood. Many of the more efficient hash-based signature schemes have the drawback that the signer must keep a record of the exact number of previously signed messages, and any error in this record will result in insecurity. Another drawback is that they can produce only a limited number of signatures. The number of signatures can be increased, even to the point of being effectively unlimited, but this also increases the signature size.

Other - A variety of systems have been proposed which do not fall into the above families. One such proposal is based on evaluating isogenies on supersingular elliptic curves. While the discrete log problem on elliptic curves can be efficiently solved by Shor's algorithm on a quantum computer, the isogeny problem on supersingular curves has no similar quantum attack known. Like some other proposals, for example those based on the conjugacy search problem and related problems in braid groups, there has not been enough analysis to have much confidence in their security.

It seems improbable that any of the currently known algorithms can serve as a drop-in replacement for what is in use today. One challenge that will likely need to be overcome is that most of the quantum-resistant algorithms have larger key sizes than the algorithms they will replace. This may result in needing to change various Internet protocols, such as the Transport Layer Security (TLS) protocol, or the Internet Key Exchange (IKE). The ways in which this should be done must be carefully considered.

We note that none of the above proposals have been shown to guarantee security against all quantum attacks. A new quantum algorithm may be discovered which breaks some of these schemes. However, this is similar to the state today. Although most public key cryptosystems

come with a security proof, these proofs are based on unproven assumptions. Thus the lack of known attacks is used to justify the security of public key cryptography currently in use. Nonetheless, NIST believes that more research and analysis are needed before any of the above proposed post-quantum algorithms could be recommended for use today. They have not received nearly as much scrutiny from the cryptographic community as the currently deployed algorithms. One exception is hash-based signatures, whose security is well-understood. For certain specific applications, such as digital code signing, hash-based signatures could potentially be standardized in the next few years.

3 Progress in Quantum Computing Hardware

Research into the feasibility of building large-scale quantum computers began in earnest after Peter Shor's 1994 discovery of a polynomial-time quantum algorithm for integer factorization [1]. At the time, it was unclear whether quantum computing would ever be a fundamentally scalable technology. Many leading experts suggested that quantum states were too fragile and subject to the accumulation of error for large-scale quantum computation ever to be realized. This situation changed in the late 1990s with the development of quantum error correcting codes and threshold theorems [7]. These threshold theorems show that if the error rate per logical operation ("quantum gate") in a quantum computer can be brought below a fixed threshold then arbitrarily long quantum computations can be carried out in a reliable and fault-tolerant manner by incorporating error-correction steps throughout the execution of the quantum computation [8].

Over the years, experimentalists have gradually developed improved hardware with ever lower error rates per quantum gate. Simultaneously, theorists have developed new quantum error correction procedures yielding higher fault-tolerance thresholds. Recently, some experiments using ion traps and superconducting circuits have demonstrated universal sets of quantum gates that are nominally below the highest theoretical fault-tolerance thresholds (around 1 %) [9, 10]. This is a significant milestone, which has spurred increased investment from both government and industry. However, it is clear that substantial long-term efforts are needed to move from present-day laboratory demonstrations involving a few qubits up to large-scale quantum computers involving thousands of logical qubits encoded in perhaps hundreds of thousands or millions of physical qubits.

In parallel to the development of general-purpose digital quantum computers, there have been efforts to develop special purpose analog quantum computers, such as quantum annealers (e.g. the D-Wave machine), analog quantum simulators, and boson sampling devices. Some of these devices have been scaled up to far larger numbers of qubits than digital quantum computers have. However, due to their specialized nature, these analog quantum devices are not believed to be of relevance to cryptanalysis.

4 The Path Forward

The need for stronger cryptography is driven by advances in both classical and quantum computing technologies. To maintain security against classical attacks, NIST has already recommended transitions from key sizes and algorithms that provide 80 bits of security, to key sizes and algorithms that provide 112 or 128 bits of security [SP 800-131A]. To provide security against quantum attacks, NIST will have to facilitate a more difficult transition, to new post-quantum cryptosystems.

It is unclear when scalable quantum computers will be available. However, in the past year or so, researchers working on building a quantum computer have estimated that it is likely that a quantum computer capable of breaking 2000-bit RSA in a matter of hours could be built by 2030 for a budget of about a billion dollars [11]. This is a serious long-term threat to the cryptosystems currently standardized by NIST.

It is useful to compare the above predictions with the cost of breaking these cryptosystems using classical computers. Cryptosystems offering 80 bits of security or less, which were phased out in 2011-2013, are at the greatest risk: they can be broken now at a cost ranging from tens of thousands to hundreds of millions of dollars [12, 13, 14, 15]. Cryptosystems offering 112 bits of security are likely to remain secure for some time: they may be breakable for a budget of a billion dollars in 30 to 40 years[3] (using classical computers).

Thus, transitioning from 112 to 128 (or higher) bits of security is perhaps less urgent than transitioning from existing cryptosystems to post-quantum cryptosystems. This post-quantum transition raises many fundamental challenges.

Previous transitions from weaker to stronger cryptography have been based on the bits-of-security paradigm, which measures the security of an algorithm based on the time-complexity of attacking it with a classical computer (e.g. an algorithm is said to have 128 bits of security if the difficulty of attacking it with a classical computer is comparable to the time and resources required to brute-force search for a 128-bit cryptographic key.) NIST Special Publication (SP) 800-57 Part 1 [SP800-57] classifies the algorithms standardized by NIST as of January 2016 into 80, 112, 128, 192 and 256 bits of security. It further recommended that the 80-bit security level is no longer considered sufficiently secure, and the 112-bit security level be phased out by 2031.

Unfortunately, the bits-of-security paradigm does not take into account the security of algorithms against quantum cryptanalysis, so it is inadequate to guide our transition to quantum-resistant cryptography. There is not yet a consensus view on what key lengths will provide acceptable levels of security against quantum attacks. For symmetric key systems, one simple heuristic is to double the key lengths to compensate for the quadratic speedup achieved by Grover's algorithm. But this recommendation may be overly conservative, as quantum computing hardware will likely be more expensive to build than classical hardware. At the same time, this recommendation does not take into account the possibility of more sophisticated quantum attacks

[3] This is based on an extrapolation assuming Moore's law, assuming roughly 90 bits of security is breakable now for one billion dollars and 18 months per bit of security at a given cost.

[16, 17, 18]. Our understanding of quantum cryptanalysis remains rather limited, and more research in this area is urgently needed.

The development of standards for post-quantum cryptography will require significant resources to analyze candidate quantum-resistant schemes, and will require significant public engagement to assure trust in the algorithms NIST chooses to standardize. Interest in the areas of quantum computing and quantum-resistant cryptography has recently increased, due to milestones in the development of quantum computing hardware and the National Security Agency's (NSA) recent changes to its Suite B guidance [19]. This provides an opportunity for engagement with the research community that may not come again before practical quantum computing is truly imminent. Consequently, NIST is beginning to prepare for the transition to quantum-resistant cryptography now.

NIST is taking the following steps to initiate a standardization effort in post-quantum cryptography. NIST plans to specify preliminary evaluation criteria for quantum-resistant public key cryptography standards. The criteria will include security and performance requirements. The draft criteria will be released for public comments in 2016 and hopefully finalized by the end of the year. At that time NIST will begin accepting proposals for quantum-resistant public key encryption, digital signature, and key exchange algorithms. NIST intends to select at least one algorithm providing each of these functionalities for standardization. NIST will establish a submission deadline late in 2017 for algorithms to be considered, allowing the proposals to be subject to 3 to 5 years of public scrutiny before they are standardized.

While this process will have many commonalities with the processes that led to the standardization of AES [20] and SHA3 [21], this is not a competition. NIST sees its role as managing a process of achieving community consensus in a transparent and timely manner. Ideally, several algorithms will emerge as "good choices." NIST may pick one or more of these for standardization in each category. In this respect, NIST's process for standardizing quantum-resistant public key cryptography will be similar to the ongoing block cipher modes development process [22].

When standards for quantum-resistant public key cryptography become available, NIST will reassess the imminence of the threat of quantum computers to existing standards, and may decide to deprecate or withdraw the affected standards thereafter as a result. Agencies should therefore be prepared to transition away from these algorithms as early as 10 years from now. As the replacements for currently standardized public key algorithms are not yet ready, a focus on maintaining crypto agility is imperative. Until new quantum-resistant algorithms are standardized, agencies should continue to use the recommended algorithms currently specified in NIST standards.

Appendix A—References

[FIPS 186-4] Federal Information Processing Standards (FIPS) 186-4, *Digital Signature Standard (DSS)*, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013, 130pp. http://dx.doi.org/10.6028/nist.fips.186-4.

[SP800-56A] NIST Special Publication (SP) 800-56A Revision 2, *Recommendations for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2013, 138pp. http://dx.doi.org/10.6028/nist.sp.800-56ar2.

[SP800-56B] NIST Special Publication (SP) 800-56B Revision 1, *Recommendations for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2014, 131p. http://dx.doi.org/10.6028/nist.sp.800-56br1.

[1] P. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput., 26 (5), 1997, pp. 1484–1509. http://dx.doi.org/10.1137/s0036144598347011.

[2] M. Mosca, *Cybersecurity in an era with quantum computers: will we be ready?* IACR Cryptology ePrint Archive Report 2015/1075, 2015. http://eprint.iacr.org/2015/1075.

[3] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, *Strengths and weaknesses of quantum computing*, SIAM J. Comput., 26 (5), 1997, pp. 1510–1523. http://dx.doi.org/10.1137/s0097539796300933

[4] European Telecommunications Standards Institute White Paper No. 8, *Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges*, June 2015. https://portal.etsi.org/Portals/0/TBpages/QSC/Docs/Quantum_Safe_Whitepaper_1_0_0.pdf [accessed 4/15/2016].

[5] R. Perlner and D. Cooper, *Quantum resistant public key cryptography: a survey*, In Proc. of IDtrust, ACM, 2009, pp. 85-93. http://dx.doi.org/10.1145/1527017.1527028.

[6] V. Dubois, P. Fouque, A. Shamir and J. Stern, *Practical cryptanalysis of SFLASH*, Advances in Cryptology — CRYPTO 2007, Lecture Notes in Comput. Sci. 4622, Springer-Verlag, 2007, pp. 1–12. http://dx.doi.org/10.1007/978-3-540-74143-5_1.

[7] J. Preskill, *Reliable Quantum Computers*, Proc. Roy. Soc. London A, 454, 1998, pp. 385–410. http://dx.doi.org/10.1098/rspa.1998.0167.

[8] D. Lidar, T. Brun, eds., *Quantum Error Correction*, Cambridge University Press, 2013. http://dx.doi.org/10.1017/cbo9781139034807.

[9] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, Y. Chen, B. Chiaro, J. Mutus, C. Neil, *Superconducting quantum circuits at the surface code threshold for fault tolerance*, Nature 508 (7497), 2014, pp. 500–503. http://dx.doi.org/10.1038/nature13171.

[10] T.P. Harty, D.T.C. Allcock, C.J. Balance, L. Guidoni, H.A. Janacek, N.M. Linke, D.N. Stacey, D.M. Lucas, *High-Fidelity Preparation, Gates, Memory, and Readout of a Trapped-Ion Quantum Bit*, Phys. Rev. Lett. 113 (22), 2014. http://dx.doi.org/10.1103/PhysRevLett.113.220501.

[SP 800-131A] NIST Special Publication (SP) 800-131A Revision 1, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2015, 23pp. http://dx.doi.org/10.6028/nist.sp.800-131ar1.

[11] M. Mariantoni, *Building a Superconducting Quantum Computer*, Invited Talk PQCrypto 2014, October 2014 Waterloo, Canada. https://www.youtube.com/watch?v=wWHAs--HA1c [accessed 4/20/2016].

[12] A. Lenstra, E. Tromer, A. Shamir, W. Kortsmit, B. Dodson, J. Hughes, P. Leyland, *Factoring Estimates for a 1024-bit RSA Modulus*, Advances in Cryptology - ASIACRYPT 2003, Lecture Notes in Comput. Sci. 2894, Springer-Verlag, 2003, pp. 55–74. http://dx.doi.org/10.1007/978-3-540-40061-5_4.

[13] M. Stevens, P. Karpman, T Peyrin, *Freestart Collision on Full SHA-1*, IACR Cryptology ePrint Archive 2015/967, 2015. http://eprint.iacr.org/2015/967.

[14] J. Bos, M. Kaihara, T. Kleinjung, A. Lenstra, P. Montgomery, *On the security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography*, IACR Cryptology ePrint Archive 2009/389, 2009. http://eprint.iacr.org/2009/389.

[15] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelin, P. Zimmermann, *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice*, in: Proc. of the 22nd ACM Conference on Computer and Communications Security, Oct. 2015. http://dx.doi.org/10.1145/2810103.2813707.

[SP 800-57] NIST Special Publication (SP) 800-57 Part 1 Revision 4, *Recommendation for Key Management – Part 1: General*, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2016, 160pp. http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4.

[16] P. Campbell, M. Groves, D. Shepherd, *Soliloquy: A Cautionary Tale*, ETSI Workshop on Quantum-Safe Cryptography, 2014. https://docbox.etsi.org/workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf.

[17] M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia, *Quantum Differential and Linear Cryptanalysis*, arXiv preprint ArXiv: 1510.05836, 2015. http://arxiv.org/abs/1510.05836.

[18] H. Kuwakado, M. Morii, *Quantum distinguisher between the 3-round Feistel cipher and the random permutation*, In Proc. of 2010 IEEE International Symposium on Information Theory (ISIT), IEEE, 2010, pp. 2682-2685. http://dx.doi.org/10.1109/isit.2010.5513654.

[19] National Security Agency, *Cryptography Today*, report, August 2015. https://www.nsa.gov/ia/programs/suiteb_cryptography/ [accessed 4/20/2016]. Also at: https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm.

[20] NIST, *AES Competition* [Web page], http://csrc.nist.gov/archive/aes/.

[21] NIST, *SHA-3 Competition* [Web page], http://csrc.nist.gov/groups/ST/hash/sha-3/.

[22] NIST, *Modes Development* [Web page], http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html.