

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>

NIST
**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



★

★

NISTIR 8105

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>

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at <http://csrc.nist.gov/publications>.

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

All comments are subject to release under the Freedom of Information Act (FOIA).

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

1 Introduction1
2 An Overview of Quantum-Resistant Cryptography3
3 Progress in Quantum Computing Hardware.....5
4 The Path Forward6

List of Appendices

Appendix A— References 8

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.

これまでの30年間において、公開鍵を用いる暗号が、グローバルな通信デジタル・インフラストラクチャを構成する不可欠な要素となってきた。それらを用いたネットワークをベースにして、モバイル・フォンや、インターネット・コマース、ソーシャル・ネットワーク、クラウド・コンピューティングなどの多様な応用形態が生み出され、私たちにとって大切な経済／安全／生活様式などがサポートされている。この、接続された世界で重要になるのは、個人／企業／政府が安全にコミュニケーションする能力となる。

Many of our most crucial communication protocols rely principally on three core cryptographic functionalities: public key encryption, digital signatures, and key exchange¹. 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.

重要とされる数多くの通信プロトコルは、公開鍵暗号化、デジタル署名、鍵交換という、3種類のコア暗号機能に依存している。現時点において、それらの機能は、Diffie-Hellman 鍵交換、RSA (Rivest-Shamir-Adleman) 暗号、楕円曲線暗号 (elliptic curve cryptosystems) を用いて実装されている。これらのセキュリティ機能は、Integer FactorizationやDiscrete Log Problemといった、特定の数論的問題の難しさに左右される。

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.

1994年にBell LaboratoriesのPeter Shorが、物質やエネルギーの物理的特性を用いて計算を行う、新しいテクノロジーとしての量子コンピュータを示した。それにより、前述の問題が効果的に解決されると言われるが、この仮定に基づくと、すべての公開鍵暗号システムが無効になる[1]。つまり、十分にパワフルな量子コンピュータは、鍵交換から暗号化／デジタル認証にいたるまでの、各種の最新コミュニケーションを危険にさらすことになる。

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.

古典的なコンピュータと比べて、量子コンピュータは特定の問題をきわめて迅速に解決するという発見により、大きな関心が喚起された。量子コンピュータの複雑さは、古典的なコンピュータ複雑さとは、根本的に異なるのだろうか？大規模な量子コンピュータは、いつになったら構築されるのか？量子コンピューティングと古典的コンピューティングは、敵対するものになるのだろうか？こうした疑問に対して、数多くの研究者たちが取り組んでいる。

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.

Shorの発見から20年が過ぎ、量子アルゴリズムの理論は大きく発展した。指数関数的な高速化を実現していく量子アルゴリズムは、物理シミュレーション／整数論／トポロジーなどに関するいくつかの問題を発見している。

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.

それにもかかわらず、量子コンピュータが指数関数的に高速化されると言われる、解決されるべき問題のリストは広がりを見せていない。その一方では、検索および、不一致の発見、ブール式の評価に関しては、多種多様な問題でのスピードアップが見つけ出されている。特に、Groverの検索アルゴリズムは、構造化されていない検索問題に対して、二次的な高速化を提供する。

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.

このような高速化により、暗号化のテクノロジーが時代遅れになるとは思えないが、たとえば対称キーにも影響が生じ、より大きなキー・サイズが求められるという必要性が生じる。大規模な量子コンピュータが、RSAやAES（Advanced Encryption Standard）などの一般的な暗号アルゴリズムに及ぼす影響の概要については、[Table 1](#)を参照して欲しい。こうした、量子コンピュータの先進性が、どの程度まで押し上げられるかについては、誰にも分かっていない。また、古典モデルと量子モデルが実現できることの違いについても、どれほどのギャップがあるのかが認識されていない。

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.

いつになったら、大規模な量子コンピュータが構築されるのか、という点については議論の余地がある。これまでは、大規模量子コンピュータが物理的に実現できるのかという点が明確ではなかったが、いまでは単なる工学的課題であると、多くの科学者が捉えている。何人かの専門家の予測によると、これからの20年以内に、現時点で使用されている全ての公開鍵スキームを、根本からこじ開けるだけの、十分な規模の量子コンピュータが構築されるという[2]。公開鍵暗号化のための、先進的なインフラストラクチャの導入には、20年近くが費やされてきた。そして、広範囲で使用されている現在の暗号システムを、量子コンピューティングに対抗できるシステムへと、円滑かつ確実に移行していくためには、かなりの努力が必要となる。したがって、量子コンピューティング時代が到来するまでの、正確な時間を予測できてもできなくても、量子コンピューティングに耐え得る情報セキュリティ・システムの準備が必要となる。

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 Cryptography².” 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.

新しい量子耐性プリミティブを用いて、公開鍵の基盤が損なわれないようにし、量子コンピューティング時代の情報セキュリティに対処していくための、大規模な国際的コミュニティが出現した。アカデミックの世界では、この新しい科学に対して、“Post-Quantum Cryptography”という名前が付けられている。それは、2006年に始まったPQCryptoというカンファレンスで活発に研究が進められている分野でもある。また、European Union (EU)のプロジェクトであるPQCryptoやSAFEcryptoや、JapanのプロジェクトであるCREST Crypto-Mathなどを通じて、それらの国々から多大な支援も受けている。

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 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.

こうした一連の試みが、現実の世界におけるポスト量子暗号システムへの道を、切り開いていく基礎研究の進歩につながった。この数年において、産業界と標準化団体は、量子暗号化の分野で独自の活動を開始している。2013年以来、European Telecommunications Standards Institute (ETSI) は、3つのQuantum-Safe Cryptographyワークショップを開催している。また、2015年にNISTは、産学官から140人以上が参加した、Cybersecurity in a Post-Quantum Worldというワークショップを開催している。

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.

NISTのユニークな役割は、セキュリティのためのスタンダードとガイドラインの開発という責任の一環として、連邦政府の情報システムを除いた領域において、ポスト量子暗号の標準化を目指す点である。数多くのNISTスタンダードには、Advanced Encryption Standard (AES) などが含まれ、学界や産業界からの幅広い参加により開発が継続されている。その成果は効果的なソリューションであり、広範囲において活用され、また、米国の情報システムの保護にも役立っている。ポスト量子暗号においても、NISTスタンダードはメリットをもたらすだろう。

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.

様々な情報を考慮すると、量子耐性テクノロジーの開発が、急がれていることが明らかになる。それと同時に、ポスト量子暗号化における公開鍵暗号を、標準化していくための努力も必要になってくる。また、世界の産業界と標準化団体に、NISTの暗号スタンダードを支持してもらうためには、それらのコミュニティと連携することが不可欠となる。今回の内部報告書は、量子コンピューティングと量子暗号の現状について、現時点におけるNISTの理解を共有し、また、初期におけるNISTの計画を概説するものである。

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.

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). 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].

今日における公開鍵暗号の最も重要な用途は、デジタル署名と鍵の確立にある。[Section 1](#)で述べたように、大規模な量子コンピュータが構築されることで、これらの公開鍵暗号システムの大半から、安全性が奪い取られるだろう。とりわけ、RSAなどの整数の因数分解 (integer factorization) の困難さに基づくものと、離散対数 (discrete log problem) の問題の硬度に基づくものが、そこには含まれると指摘しておく。その一方で、対称鍵システムへの影響は劇的ではない ([Table 1](#)参照)。古典的なコンピュータ上の検索アルゴリズムと比較して、Groverのアルゴリズムが量子探索アルゴリズムに提供するものは、二次的 (quadratic) なスピードアップである。現実的な運用において、Groverアルゴリズムが関連するのかが分からないが、もし関連するなら、鍵のサイズを倍にするだけでセキュリティを維持できる。さらに言えば、検索アルゴリズムの指数関数的な高速化は不可能である。したがって、対称アルゴリズムとハッシュ関数が、量子コンピューティングの時代でも利用可能だと示唆される[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

その結果として、古典的なコンピュータと量子コンピュータからの攻撃に対して、耐性があると考えられるアルゴリズムの研究は、公開鍵アルゴリズムに集中していく。このセクションでは、ポスト量子プリミティブとして提案される、主たる項目の概要を簡単に説明していく。それらの項目には、ラティス (lattices)、コード (codes)、多変量多項式 (multivariate polynomials) に基づくものなどが含まれる。詳細については、[4, 5]を参照のこと。

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.

Lattice-based cryptography – いくつかの理由から、ラティスに基づく暗号システムは、新たな関心を集めている。ラティス・ベースの暗号を用いることで、新しい応用形態（完全な同型暗号化、コードの難読化、属性ベースの暗号化など）が可能になった。大部分のラティス・ベースの鍵確立アルゴリズムは、比較的単純であり、高度な並列化を効率よく実現する。また、いくつかのラティス・ベースのシステムの安全性は、平均的なケースと比較して、最悪の硬度を想定した場合でも確かな安全性を提供する。その一方で、既知の解読技術を用いても、ラティス・スキームのセキュリティの、正確な推定値を得ることは困難だと証明されている。

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.

Code-based cryptography – McElieceの暗号システムは、1978年に提案されて以来、解読されていない。また、その時から、誤り訂正符号をベースとする派生システムが提案されている。きわめて高速であるが、大半のコード・ベース・プリミティブは、きわめて長大な鍵サイズを持つことに苦しんでいる。また、最近の派生物は、鍵サイズを縮小するために構造化されたコードを導入しているが、追加された構造を持つコードは、いくつかの攻撃を許している。コード・ベースの署名に関しては、いくつかの議論があるが、多様な暗号化スキームの中で最大の成功を収めている。

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. While there have been some proposals for multivariate encryption schemes, multivariate cryptography has historically

been more successful as an approach to signatures.

Multivariate polynomial cryptography – この種のスキームがベースにするのは、有限体上の多変量多項式を解くことの難しさである。この数十年に渡って、いくつかの多変量暗号システムが提案され、また数多くのもが解読されている[6]。多変量暗号化スキームに対しては、いくつかの提案が存在するが、歴史的にみると証明に対するアプローチとして成功している。

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.

Hash-based signatures – ハッシュ・ベースの署名とは、ハッシュ関数で構築されるデジタル署名のことである。その安全性は、量子攻撃に対しても効果があると認識されている。より効率のよいハッシュ・ベース署名の多くは、以前に署名されたメッセージの正確な値を、署名者が記録しなければならないという欠点を持ち、また、この記録にエラーがあれば安全性も不安定になる。もう1つの欠点として挙げられるのは、限られた数の署名しか生成できない点にある。事実上、署名の数は無制限であるが、署名のサイズも増大していくことになる。

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.

上記の各項目以外にも、多様な仕組みが提案されている。それらの提案の中には、超楕円曲線上のアイソジェニティー（同系性？）評価をベースにするものもある。楕円曲線上の離散対数問題は、Shorの量子コンピュータ・アルゴリズムにより、効率よく解くことができるが、超指数曲線上の同系問題に関しては、それに対する量子攻撃が確認されていない。その他の提案と同様に、共役検索の問題や、編組グループの問題などをベースにしたものもあるが、その安全性に自信を持てるとは理解されていない。

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.

それらの、現時点で認識されているアルゴリズムが、すでに運用されているアルゴリズムに取って代わることはないと思われる。克服すべき1つの課題だと思われるのは、大部分の量子耐性アルゴリズムの鍵サイズが、それにより置き換えられるアルゴリズムよりも、大きな鍵サイズを有する点にある。つまり、TLS (Transport Layer Security) プロトコルや、IKE (Internet Key Exchange) などの、多様なインターネット・プロトコルの変更という必要性が生じるとと思われる。そのための方式については、注意深く考慮する必要がある。

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.

上記の、いずれの提案も、すべての量子攻撃に対する安全性を保証するものではないことを、指摘しておく。新しい量子アルゴリズムが発見され、上記のスキームを破るかもしれないが、それは、いまの伝統的なコンピュータの世界にも言えることである。ほとんどの公開鍵暗号システムには、セキュリティ証明が付いているが、それらの証明は確かなものではないという前提に基づいている。したがって、何らかの攻撃が成功していないという事実が、現時点で使用されている公開鍵暗号のセキュリティを、正当化するために用いられている。

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.

それにもかかわらず NISTは、提案された上記のポスト量子アルゴリズムが、今後は使用されるべきだと推奨する前に、より多くの研究および分析が必要と考えている。それらの量子アルゴリズムは、原時点でデプロイされているアルゴリズムと比べて、暗号化のコミュニティからの厳しい精査を受けていない。1つの例外は、安全性が十分に認識されているハッシュ・ベースの署名である。デジタル・コード署名などの特定の応用分野においては、これからの数年のうちに、ハッシュ・ベース署名が標準化される可能性がある。

=====

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].

ココ！

1994年にPeter Shorが、整数分解のための多項式時間量子アルゴリズムを発見した後に、大規模量子コンピュータ構築の可能性に関する本格的な研究が本始まった[1]。その当時の量子コンピューティングは、その根本からスケーラブルな技術になるかが不透明だった。量子の状態が非常に脆弱であり、これまで実現された大規模な量子計算の誤差の蓄積に直面することを、数多くの有力な専門家たちが示唆していた。しかし、そのような状況は、量子誤り訂正符号と閾値定理の開発により、1990年代後半から変化してきた[7]。この閾値定理とは、量子コンピュータの論理演算（“量子ゲート”）あたりの誤り率が、固定された閾値以下になるなら、実行される量子計算[8]に修正ステップを実施することで、任意の長さを持った量子計算が、誤りなく達成されるというものだ。

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 %). 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.

長い年月をかけて、ハードウェアの改良のための実験が進められ、量子ゲートあたりの誤り率が徐々に低くなってきた。それと同時に、フォールト・トレランス閾値を高くするための、新しい量子誤り訂正手順のための理論も進化してきた。最近なって、イオン・トラップと超伝導回路を用いたいくつかの実験が行われ、名目上の最高の理論的フォールト・トレランス閾値（約1%）を下回る、ユニバーサルな量子ゲートセットが実証された[9, 10]。それが、重要なマイルストーンとなり、政府と産業界からの投資が増えている。しかし、いくつかのQubitsを用いる現在の実験デモから、数千の論理Qubitsを取り込む大規模量子コンピュータに移行し、数十万または数百万の物理Qubitsを符号化していくには、かなりの長期的な努力が必要になることは明白である。

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.

こうした汎用デジタル量子コンピュータの開発と並行して、量子アニール装置（D-Waveマシンなど）や、アナログ量子シミュレータ、ボゾン・サンプリング装置などの、特殊用途のためのアナログ量子コンピュータを開発する努力が進められている。これらのデバイスの中には、デジタル量子コンピュータと比べて、はるかに大きなQubitsへとスケールアップされたものもある。しかし、これらのアナログ量子デバイスは、その特殊な性質のために、解読に用いられるとは考えられていない。

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.

古典的コンピューティング技術と量子コンピューティング技術の進歩により、さらに強固な暗号化が必要とされる。従来からのサーバー攻撃に対するセキュリティ維持のために、すでにNISTが推奨しているのが、80 Bitsセキュリティから 112/128 Bitsセキュリティへ向けた、鍵サイズとアルゴリズム[[SP 800-131A](#)]への移行である。NISTが行うべきことは、これから幕開けするポスト量子暗号システムへ向けた、困難とされる移行の支援であり、また、量子攻撃に対するセキュリティの提供である。

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.

スケーラブルな量子コンピュータが利用可能になる時期は、いまだに不明である。しかし、最近では、2000 BitsのRSAを数時間で解読できる量子コンピュータが、2030年までに約10億ドルの予算で構築できると、量子コンピュータ研究者たちが述べている[[11](#)]。それは、NISTが標準化してきた、現状の暗号システムに対する、深刻かつ長期的な脅威である。

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 years³ (using classical computers).

それらの暗号システムを解読する能力について、量子コンピュータと古典的コンピュー

タを比較することは有益である。最大のリスクに晒されるのは、2011～2013年に段階的に廃止されていく、80 Bitsセキュリティを提供する暗号システムである。具体的に言うと、それらのシステムは、数千ドルから数百万ドルのコストで、ただちに解読される可能性がある [12, 13, 14, 15]。その一方で、112 Bitsセキュリティを提供する暗号システムは、しばらくの間は安全だと考えられる。ただし、30～40年後には、古典的なコンピュータを用いて、10億ドルのコストで解読される可能性がある。

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.

したがって、セキュリティにおける112 Bitsから128 Bits（またはそれ以上）への移行は、既存の暗号システムからポスト量子暗号システムへの移行よりも、緊急性が低いと思われる。そして、このポスト量子への転移は、数多くの基本的な課題を引き起こす。

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.

脆弱な暗号化から強固な暗号化へ向けた、これまでの移行は、古典的コンピュータを用いた攻撃の時間的な問題をベースとして、アルゴリズムの安全性を測定するという、ビット・セキュリティのパラダイムに基づいていた（古典的コンピュータで攻撃することの困難さについては、たとえば128 Bits暗号鍵に対するブルート・フォース攻撃に匹敵する、時間と資源を持つアルゴリズムであれば、128 Bitsのセキュリティを有するとされてきた）。NIST Special Publication (SP) 800-57第1部[SP800-57]は、2016年1月にNISTにより標準化されたアルゴリズムを、80/112/128/192/256 Bitsのセキュリティに分類している。そして推奨するのは、すでに80 Bitsセキュリティ・レベルは十分に安全とは考えられず、また、2031年には112 Bitsセキュリティ・レベルを段階的に廃止することである。

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

残念ながら、現時点におけるセキュリティ・パラダイムは、量子暗号解析に対する

アルゴリズムの安全性を考慮していないため、量子耐性暗号への移行をガイドするだけの準備が整っていない。どれだけの鍵の長さが、量子攻撃に対して許容可能なレベルのセキュリティを提供するかについては、まだコンセンサスが取れていない状況にある。また、対称鍵システムでは、Groverのアルゴリズムが達成する二次的なスピードアップを補償するために、鍵の長さを2倍にするという、簡単な経験則が存在する。しかし、量子コンピューティングのためのハードウェアは、古典的なハードウェアと比べて高価になる可能性があるため、この視点は控えめ過ぎると思われる。同時に、この視点は、より狡猾な量子攻撃の可能性については考慮していない[16, 17, 18]。量子暗号の解読に対する理解は限定されたものであるため、この分野の研究が急務となっている。

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.

ポスト量子暗号のスタンダードを作成するためには、量子耐性候補を分析するための多大なリソースが必要である。また、NISTが標準化するアルゴリズムの信頼性を保証するためには、大規模な公的関与が必須となる。この数年において、量子コンピューティングと量子耐性暗号の分野への関心が高まっている背景には、量子コンピューティング・ハードウェアの開発におけるマイルストーンの達成と、National Security Agency (NSA) のSuite Bガイダンスの変更がある[19]。こうした動きにより、研究者たちのコミュニティとの関わり合いの機会が提供される。この、現実の量子コンピューティングが差し迫る前に訪れる、二度と無いチャンスを活用するために、NISTは量子耐性暗号への移行を準備し始めている。

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.

NISTは、ポスト量子暗号における標準化への取り組みを開始するために、以下に示す手順を踏襲している。NISTは、量子耐性公開鍵暗号のスタンダードに関して、準備のための評価基準を指定する予定である。この評価基準には、セキュリティ要件とパフォーマンス要件が含まれる。

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.

この基準としてのドラフトは、2016年にパブリック・コメントを得るために公開され、2016年年末までに完成する予定である。その時点でNISTは、量子耐性の公開鍵暗号化、デジタル署名、鍵交換アルゴリズムに関して、提案の受け入れを開始する予定である。NISTは、標準化のための方法論として、それぞれの策定されたカテゴリにおいて、少なくとも1つのアルゴリズムを選択する予定である。NISTは、2017年後半の提出期限を検討している。それにより、提案が標準化されるまでに、3年～5年の公的審査を受けることを可能にする。

While this process will have many commonalities with the processes that led to the standardization of AES [20] and SHA3, 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].

このプロセスは、AES [20] や SHA3 [21]が標準に至ったプロセスと、数多くの共通点を持つが、そこには競合はあり得ない。NISTは、透明性を確保したタイムリーな方法で、コミュニティとのコンセンサスを達成するためのプロセスを、管理する役割を果たすと考える。理想的には、いくつかのアルゴリズムが、適切な選択肢として浮上することである。NISTは、各カテゴリの標準化のために、複数のアルゴリズムを選ぶかもしれない。この点において、量子耐性公開鍵暗号を標準化するNISTのプロセスは、いま進行しているブロック暗号モード開発プロセス[22]と同様である。

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.

量子耐性公開鍵暗号のスタンダードが利用可能になるとき、量子コンピュータの脅威が、既存の基準に差し迫っているかどうかを、NISTは再評価するだろう。その結果として、影響を受ける基準については見直しを行い、撤回する可能性がある。したがって、政府機関は今から10年後に、それらのアルゴリズムからの移行を準備すべきである。現時点では、標準化されている公開鍵アルゴリズムの代替が準備されていないため、暗号に関するアジリティを維持することに重点が置かれている。新しい量子耐性アルゴリズムが標準化されるまで、現時点でNISTが指定している推奨アルゴリズムを、政府機関は継続して使用すべきである。

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.

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_CRYPTOS07_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.