

Эволюция криптографии.

Материалы международной конференции Information Systems Security Association (ISSA)

25.04.2017

<https://www.issa.org/?page=April2017>



Добро пожаловать на международную конференцию ISSA. Эта конференция посвящена эволюции криптографии <реклама о 15% скидке за присоединение к ISSA>. По окончании конференции мы пришлем Вам материалы и вопросы. Вы сможете ответить на вопросы и в случае успешных ответов получить CPE Credits. Позвольте представить вам модераторов

Internet of Things



Today's Moderator:

Jason Sabin

Chief Security Officer, DigiCert, Inc.



*To ask a question:
Type in your question in the
Questions area of your screen.
#ISSAWebConf*

Джейсон Сейбин, главный офицер безопасности (Chief Security Officer), Джейсон Сейбин работает в этой должности в DigiCert с 2012 года, занимается защитой сети и систем DigiCert и комплаенс. Он первым построил в компании команду пентестеров, регулярно вносит вклад информирование о безопасности в СМИ и имеет более 16 патентов. Джейсон пришел к нам как гость и начинает конференцию.

Джейсон

Приветствую всех пришедших 17 апреля 2017 года на конференцию ISSA "Эволюция криптографии".

Криптография - это судьба для защиты людей и компаний от массового разрушения данных во времена меняющейся реальности. По мере того как пароли умирают, вы будете иметь неожиданные сюрпризы. Криптографическая защита имеет свои основы, правила защиты данных и контроля доступа, с которыми все вы будете сталкиваться и которые мы обсудим в следующем раунде этого обсуждения. Есть много направлений – защита от угроз и уязвимостей, новые угрозы, новые стандарты FIPS (FIPS – Federal Information Processing Standards, Федеральные Стандарты Обработки Информации США), и требует сильного менеджмента, регулярных тренировок. Криптография принимает на себя удар, нужно быть готовым к криминальным временам.

Сегодня у нас три спикера



The slide features a light blue background with a white header bar. The header bar contains the text "Speaker Introduction" in a large, bold, black font on the left and the ISSA logo on the right. The ISSA logo consists of a globe icon followed by the text "ISSA" in a bold, blue font, with "Information Systems Security Association International" in a smaller font below it. Below the header bar, the text "Today's Speakers" is displayed in a large, black font. Underneath, three speakers are listed, each with their name in bold and their title in a regular black font. A mouse cursor is visible in the bottom left corner of the slide.

Speaker Introduction

ISSA
Information Systems Security Association
International

Today's Speakers

Mark Minnoch
Technical Account Manager at SafeLogic

Michele Mosca
Co-founder and deputy director of the Institute for Quantum Computing at the University of Waterloo

William Whyte
Chief Technology Officer, OnBoard Security, Inc.

Они являются экспертами в квантум компьютинг. Марк Миннок – эксперт, работающий в СейфЛоджик. Доктор Майкл Моска – сооснователь и заместитель директора в институте Квантум компьютинг в Университете Ватерлоо. И доктор Вилиам Вайт – главный офицер безопасности в компании Онборд Секьюрити Инк. Первую презентацию представляет Марк Миннок

Speaker Introduction



Mark Minnoch

- Technical Account Manager at SafeLogic
- Has helped technology vendors complete hundreds of successful FIPS 140-2 validations
- Previous roles as FIPS Security Engineer, FIPS Laboratory Director, and Account Manager at the largest FIPS 140-2 testing lab in the world
- Collector of pinball machines



Информация о Марке на этом слайде. Он экаунт менеджер в СейфЛоджик. Успешно внедрил проверку FIPS 140-2. Исследовал энтропию в реальном времени на машинах для пинболла.



FIPS 140-2 Out of Date?

Mark J. Minnoch, CISSP CISA
SafeLogic Inc.

Марк, передаю тебе слово.

Марк. Спасибо. Было упомянуто, что могут встречаться рассогласования в нашей программе. Прямо сейчас мы остановимся на FIPS 140-2.

FIPS 140-2 Fun Facts



- FIPS = Federal Information Processing Standards
- FIPS 140-2 Publication released May 25, 2001
- The Cryptographic Module Validation Program (CMVP) is a joint effort between NIST and CSE
- CMVP validates cryptographic modules to FIPS 140-2 requirements
- **FIPS 140-2 is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information**

Bottom Line: If crypto is used to protect sensitive info, then it needs to be FIPS 140-2 validated

FIPS 140-2 применим ко всем федеральным агентствам, которые используют криптографические системы безопасности для защиты конфиденциальной информации. Это компромисс между NIST в США и CSE в Канаде, и программами многокритериальной криптографии (other multivaldation cryptography program), используемым в других странах. Сертификат соответствия FIPS 140-2 нужен вам, если вы продаете криптографические программы. Есть направления бизнеса и компании, например финансовые организации, которые могут иметь свои специфические стандарты, но они должны быть не слабее FIPS 140-2.

FIPS 140-2 Out of Date?




YES!

- “Sweet Sixteen” next month
- FIPS 140-3 (or -4) has no published schedule
- ISO 19790:2012 (proposed replacement) turning 5
- Long lead time for NIST to approve algorithms
- FIPS 140-2 validation ≠ Security

В ближайшие месяцы мы можем ожидать утверждения “Sweet Sixteen” с последующим переходом к новой версии FIPS. К сожалению NIST нужно много времени для улучшения алгоритмов. Что нам нужно делать в преддверии квантовой эры? К сожалению, соблюдение FIPS140-2 не гарантирует безопасность. Значит ли это, что он устарел? Нет.

FIPS 140-2 Out of Date?



NO!

- Record year in 2016 for FIPS 140-2 Certs.
- 34% were software modules
- CMVP reviewing reports quickly
- ROI

Bottom Line: FIPS validations provide value to Vendors (sales) and End Customers (audits)

Нужно обновить сертификаты, используемые в FIPS 140-2. Нужно сосредоточиться на аппаратных модулях, обеспечивающих логику криптографии. Это очень важный вопрос (It is very high centric question). Проверки показывают, что около 34% программных модулей не обновлялись и могут устареть. И даже если сам стандарт является стабильным, мы должны быть готовы принять новые технологии. Необходимо проверить криптографические модули проверки программа (CMVP, - <https://support.microsoft.com/ru-ru/help/811833/-system-cryptography-use-fips-compliant-algorithms-for-encryption,-hashing,-and-signing-security-setting-effects-in-windows-xp-and-in-later-versions-of-windows>). CMVP позволяет докладывать о состоянии криптозащиты. Об обновлении CMVP поставщики могут забывать, и это ослабляет криптографическую защиту. Проверка FIPS обеспечивает ценность и для поставщиков, и для конечных клиентов. Вендоры должны понимать риски, которые влечет для них отсутствие сертификатов FIPS при проверке федеральных агентов. Покупатели могут сами проводить проверку (аудит) приобретаемой продукции. Помощь покупателям может быть очень полезной при обеспечении защиты.



Этот слайд показывает сертификацию по уровню безопасности на протяжении нескольких последних лет. В 2016 году количество сертификатов было максимальным. Это отражает возросшие требования к криптографической защите. Количество сертификатов достигло четвертого уровня. Это демонстрирует возрастающий тренд в криптографических потребностях.

Мне нравится классификация криптологии как инструмента, а не фурнитуры (мебели). Насколько значима для меня фурнитура (мебель) без инструментов? Если есть хорошие инструменты, вы сможете сделать много хорошей фурнитуры (мебели), поэтому инструменты важнее.

What Crypto Takes the Heat?

- Crypto is the tool, not the furniture
- Are only NIST Approved algorithms "good tools"?
- Know your target
- Develop a post quantum strategy

Bottom Line: Different "tools" are required for a post quantum world

Запомните этот слайд для ответа на вопрос, нужно ли вам соответствие NIST. Работает принцип – знай своего клиента.

Post Quantum FIPS Options

- Follow the herd; do nothing
- Wait for NIST to approve algorithms
- Ask your Product Managers about their roadmap plans
- Ask your Technology Vendors about their roadmap plans
- Implement or seek a "Hybrid Approach"
 - Post quantum crypto **and** NIST approved crypto
 - Belt and suspenders

Bottom Line: FIPS 140-2 and post quantum crypto can coexist today

Вопрос – где место FIPS в пост-квантовом мире ? FIPS ничему не противоречит и может существовать в пост-квантовом мире. Ваша позиция зависит от того, вы продавец или покупатель.



Это моя контактная информация. Я доступен для комментариев по криптографии



Вопрос. Эй, Марк, ... <вопрос от поставщика про американский compliance> и затем тема о соответствии FIPS криптовалюты dash. Ответ – нужно останавливаться на нюансах криптовалют и придерживаться регламентов FIPS.

Speaker Introduction



Dr. Michele Mosca

- Co-founder and deputy director of the Institute for Quantum Computing at the University of Waterloo.
- Founding member of the Perimeter Institute for Theoretical Physics
- Co-founded evolution Q Inc.
- Widely published author in top journals and textbooks



Следующий докладчик – доктор Майкл Моска. Доктор Майкл - сооснователь Q-inc, много работал над квантовым компьютером и опубликовал несколько книг. Он занимался квантовыми компьютерами и квантовыми вычислениями, широко известен в академических кругах и в промышленности в связи с квантовыми компьютерами. Он сооснователь института по квантовым компьютерам и профессор теоретической физики. Занимается quantum-vulnerable systems. Он нам расскажет о квантовых вычислениях и криптографических утилитах, которые существуют в квантовых технологиях. Слово Майклу

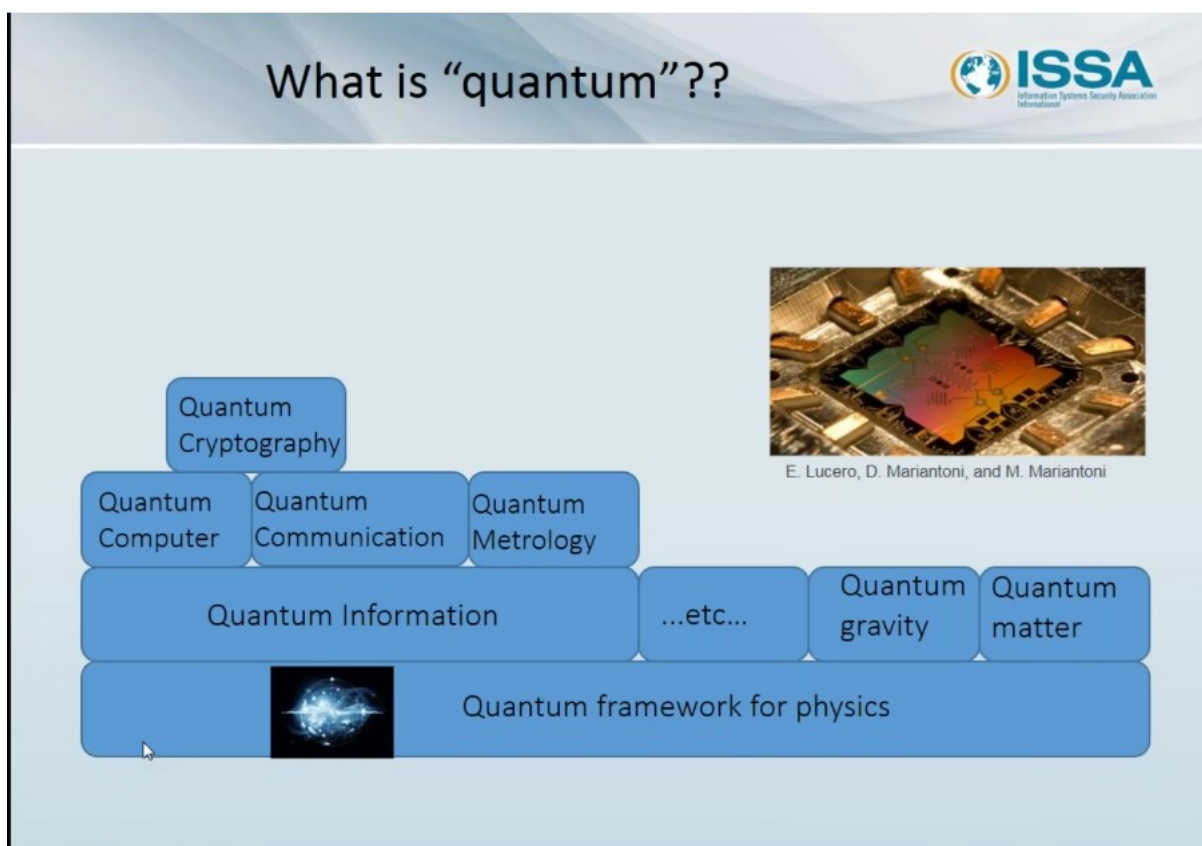


Preparing for the quantum era

Michele Mosca
evolutionQ Inc.

*Institute for Quantum Computing, University of Waterloo
Perimeter Institute for Theoretical Physics*

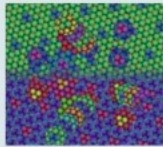
Большое спасибо за возможность выступить по такой интересной для меня теме. Остановимся на слайде, с помощью которого я попробую объяснить, что такое квантум.



Многие люди обсуждают эту тему, понимая под квантумом совершенно разные вещи. По сути квантум – это всего лишь математическая основа. Это несколько страниц математических правил и формул, объясняющих суть физических явлений. Квантовая физика и квантовая механика объясняют природу квантовых структур. За несколько много лет было много исследований квантовой информации, предмета квантовой информатики. Большую роль играют квантовые контакты и использование квантовых битов. Они важны квантовой метрологии и квантовых измерений. Эти исследования изучают структуру квантовых измерений и квантовую криптографию в широком смысле слова. В широком смысле это криптография на контактах квантовых устройств. Существует также квантовая криптография в узком смысле слова.

Новая парадигма в физике вызывает новые парадигмы в близких областях. Разработка новых материалов, оптимизация производственных процессов, безопасная связь и другие разнообразные примеры. Люди могут использовать квантовые технологии в разных областях. Например, для определения опасных материалов, и других вещей. Существует много применений квантовых технологий.

New paradigm brings new possibilities



Designing new materials, drugs, etc.



Optimizing



Sensing and measuring



Secure communication



What else???

Итак, квантовая криптография. Квантовая генерация случайных чисел. Это гонки наперегонки, но нужно быть устойчивым к завтрашним технологиям. Например, ситуация с платежными процессами.

Quantum Cryptography



- Quantum Random Number Generation (QRNG)
- Quantum Key Establishment (QKD)
- Other...



www.quintessencelabs.com



whitewoodsecurity.com



Courtesy of Qiang Zhang, USTC

Beijing-Shanghai QKD Backbone



swissquantum.idquantique.com/?-Network

SwissQuantum Network



<http://www.uqcc.org/QKDnetwork/>

Tokyo QKD Network



<http://www.battelle.org/our-work/national-security/cyber-innovations/quantum-key-distribution>

Battelle QKD Network
Columbus, Ohio, USA



<http://www.idquantique.com/photocounting/clavis3-qkd-platform/>



<http://www.quantum-comm.com/index.php/Cate/index/pid/1>



<http://www.qasky.com/Product.aspx?id=94>

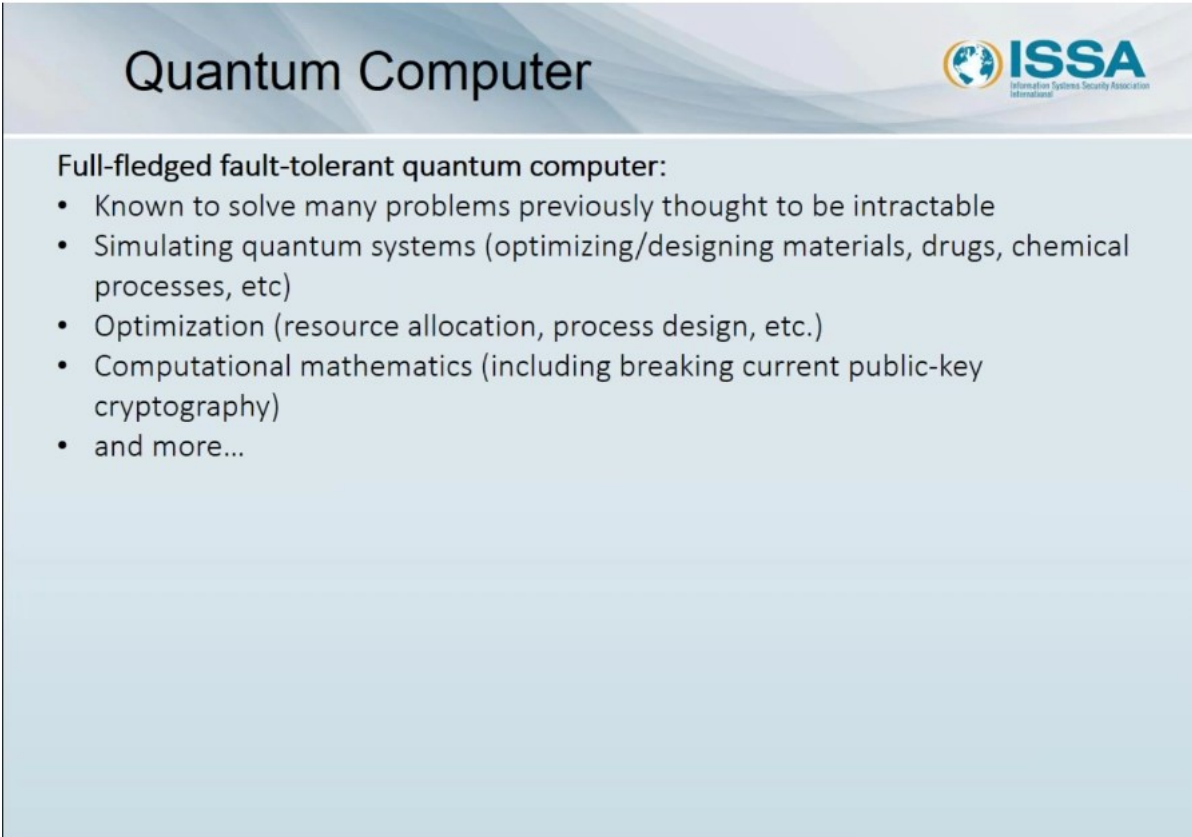
Нужна высокая ответственность в применении квантовых технологий. Этот слайд оказывает применения следующего поколения вычислений. Я расскажу о нескольких примерах. Квантовые технологии. Какие устройства получают пользу от квантовых технологий? Это зависит от паранойи, насколько вы готовы доверять технике.

Quantum key distribution (QKD)


Распределение квантовых ключей.

Работает в стандартных алгоритмах при использовании квантовых алгоритмов для распределения ключей. В качестве транспорта можно использовать RSA. Когда ключ, сгенерированный квантовым компьютером, установлен, для коммуникаций можно использовать симметричный протокол. Такой механизм по сути реализует симметричный алгоритм при соединении точка-точка.

Ниже представлен слайд о квантум-крипто. По функционалу вы можете писать программу и одновременно выполнять ее на квантовом компьютере.



Quantum Computer



Full-fledged fault-tolerant quantum computer:

- Known to solve many problems previously thought to be intractable
- Simulating quantum systems (optimizing/designing materials, drugs, chemical processes, etc)
- Optimization (resource allocation, process design, etc.)
- Computational mathematics (including breaking current public-key cryptography)
- and more...

При этом результаты выполнения такого кода надежны, им можно доверять. Тем не менее существуют другие проблемы, которые пока нельзя решить. Например, моделировать одновременно другой квантовый компьютер. Это может быть полезным в разработке материалов следующего поколения, производстве лекарств, оптимизации химических процессов и т.п.

Более общая оптимизация – квантовая система может ускорять вычисления, но экспоненциальному ускорению могут мешать проблемы, не связанные с квантовым распределением. Например, существенное повышение скорости k_{si} -квадратичного ускорения (substantial k_{si} -quadratic speed-up). На это влияют вопросы вычислительной математики.

Quantum Computer



Full-fledged fault-tolerant quantum computer:

- Known to solve many problems previously thought to be intractable
- Simulating quantum systems (optimizing/designing materials, drugs, chemical processes, etc)
- Optimization (resource allocation, process design, etc.)
- Computational mathematics (including breaking current public-key cryptography)
- and more...

Non-fault-tolerant quantum devices:

- Not a known threat to cryptography
- Can they capture *some* of the power of quantum computation (and bypass some/all the cost of fault-tolerance)?
- Can they simulate themselves or similar systems faster/cheaper than conventional computers?
- Can they solve *useful* problems better than conventional devices?

Вопросы совместимости у квантовой криптографии возникают при использовании криптографии с открытым ключом. Но не стоит паниковать, это наименее критичные проблемы на сегодняшний день. Люди довольны, если удастся при работе с квантовым компьютером использовать хотя бы часть возможностей, о которых я упомянул. Люди могут добиться своих результатов из-за экономических эффектов, отказоустойчивость дорого стоит. Добиться ее потребует времени. Поэтому возможно развитие пойдет более дешевым путем. Добыть часть экономического усиления мощности на существующих устройствах, таких как DWave. Google тоже работает над этой проблемой. Будем надеяться, что удастся решить проблему отказоустойчивости. Сейчас идут активные работы над такими задачами.

How secure will our current crypto algorithms be?

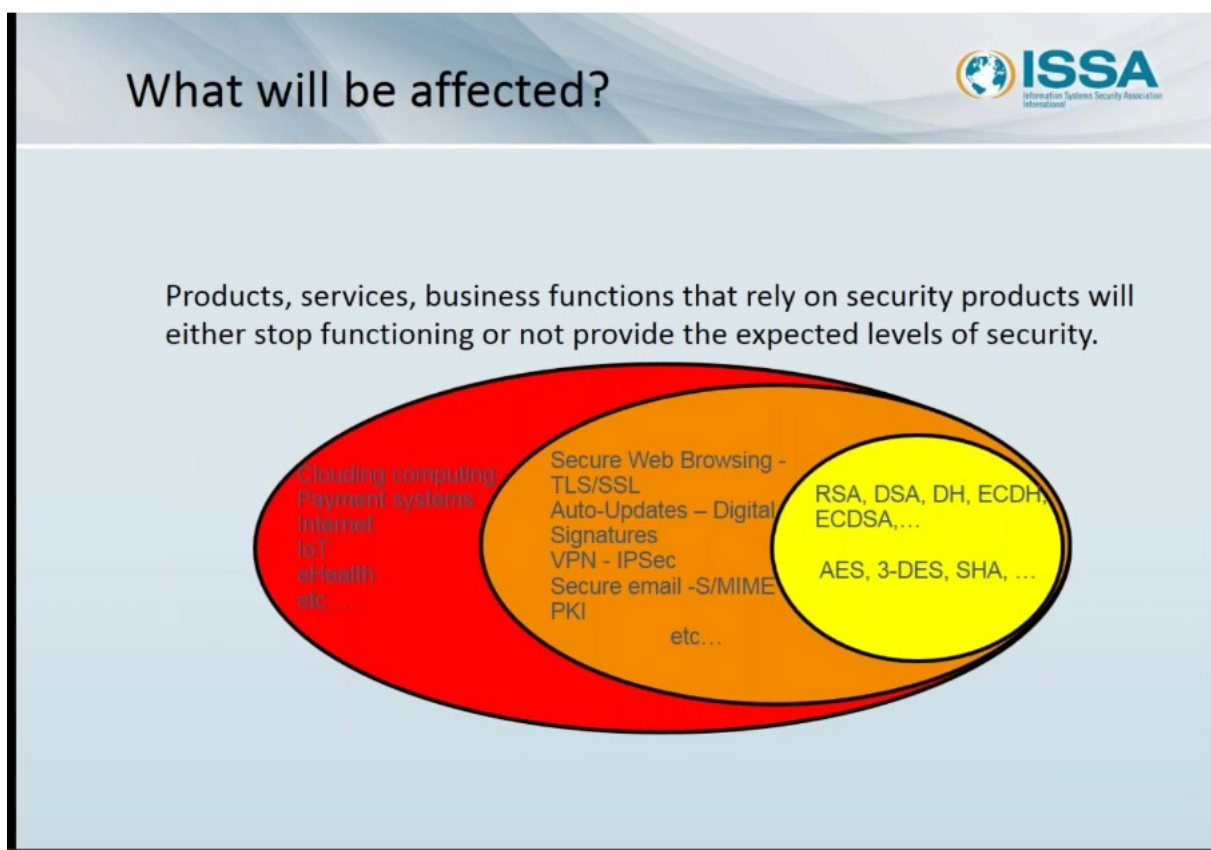


Algorithm	Key Length	Security level (Conventional Computer)	Security level (Quantum Computer)
RSA-1024	1024 bits	80 bits	~0 bits
RSA-2048	2048 bits	112 bits	~0 bits
ECC-256	256 bits	128 bits	~0 bits
ECC-384	384 bits	192 bits	~0 bits
AES-128	128 bits	128 bits	~64 bits
AES-256	256 bits	256 bits	~128 bits

Итак, насколько действительно эффективны квантовые компьютеры? Что мы видим, если сравниваем криптографию? Насколько квантовый компьютер ускоряет вычисления?

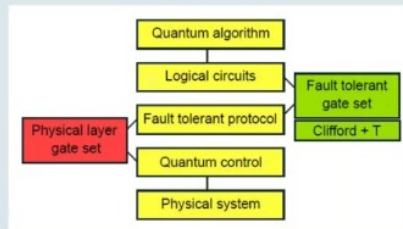
Для симметричных ключей RSA и ECC ускорение значительное. Время расшифрования на квантовом компьютере сравнимо с временем зашифрования. Длина ключа не является критическим параметром для выбора решения. Для симметричной криптографии с длинными ключами ускорение квантового компьютера может быть существенным. Для асимметричной криптографии (AES) ускорение гораздо меньше.

Что означает на практике существенное превосходство квантовых алгоритмов над симметричными алгоритмами шифрования? Продукты, сервисы и бизнес-функции, использующие продукты безопасности, либо перестанут работать, либо не будут обеспечивать ожидаемый уровень защиты



Насколько велика потребность в квантовых компьютерах? Можно упростить вопрос, разбив его на два – сколько квантового аппаратного обеспечения необходимо? Сколько квантового программного обеспечения необходимо? Задача неоднозначна, ответ зависит от того, какие именно слои мы хотим усилить. Мы хотим ускорить физическую систему, что означает снижение шума, ускорить вычисления, можно рассматривать ускорение по уровням. Мы отличаем физический уровень от логического уровня. Скорость обработки изменяется от нескольких месяцев до нескольких часов. Результат зависит от того, сколько мы задействуем квантовых ресурсов.

How large of a quantum computer is needed?



Institute for Quantum Computing • Events • 2015 • June •

Quantum Programming and Circuits Workshop

Monday, June 8, 2015 (all day) to Thursday, June 11, 2015 (all day)

The workshop aims at bringing together researchers from quantum computing and classical programming languages. Open questions that we anticipate this group to tackle include new methods for circuit synthesis and optimization, compiler optimizations and rewriting, embedded languages versus non-embedded languages, implementations of type systems and error reporting for quantum languages, techniques for verifying the correctness of quantum programs, and new techniques for compiling efficient circuits and protocols for fault-tolerant questions and their 2D layout.

<https://qsoft.iqc.uwaterloo.ca/>
(Quantum Compiler tools, Quantum Computer Simulator – Quantum++ , etc.)

На каком уровне ускорение существенно? На приведенной диаграмме этот уровень обозначен стрелкой вблизи желтой полосы и основан на физике. Этот уровень не означает ускорение кубитов. Мы создаем интегрированную систему, которая является по принципу построения масштабируемой. Ускорение на уровне логической памяти является более надежным, чем на уровне физической памяти. И результат зависит от качества кубит.

REVIEW SCIENCE VOL 339 8 MARCH 2013

Superconducting Circuits for Quantum Information: An Outlook

M. H. Devoret^{1,2} and R. J. Schoelkopf^{1*}

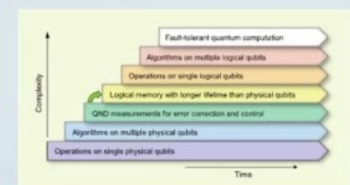


Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they are also at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously obtained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit component.

Science Advances

Home News Journals Topics Careers

RESEARCH ARTICLE QUANTUM COMPUTING

Blueprint for a microwave trapped ion quantum computer

SHARE

Spencer Lakebold¹, Sebastian Wüster¹, Austin G. Fowler¹, Klaus Mollenh¹, Simon J. Devitt¹, Christof Wunderlich² and Wolfgang K. Hensinger^{1*}

* Author affiliations
* Corresponding author: Email: w.k.hensinger@hawaii.edu

Science Advances 05 Feb 2017
DOI: 10.1126/sciadv.1200249

Vacuum chamber with >1.2 million q-junctions each

What is 'z'?



Mosca:

[Oxford] 1996: "20 qubits in 20 years"

[NIST April 2015, ISACA September 2015]:

"1/7 chance of breaking RSA-2048 by 2026, 1/2 chance by 2031"

Microsoft Research [October 2015]: *Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer within a decade. ...Use of a quantum computer enables much larger and more accurate simulations than with any known classical algorithm, and will allow many open questions in quantum materials to be resolved once a small quantum computer with around one hundred logical qubits becomes available.*

Z (читается Зи) – это время срыва (collapse time), которое нужно компьютеру для взлома RSA или ECC алгоритмов. Сейчас 20 лет означает по существу ноль. 20 лет эквивалентно 20 кубитам. С вероятностью 1/7 RSA-2048 будет взломан к 2026 году.

Quantum-safe cryptographic tool-chest

conventional quantum-safe cryptography

a.k.a. Quantum Resistant Algorithms (QRA) or Post-Quantum Cryptography

- Deployable without quantum technologies
- Believed/hoped to be secure against quantum computer attacks of the future

+ quantum cryptography

- Requires some quantum technologies (less than a large-scale quantum computer)
- Typically no computational assumptions and thus known to be cryptographically secure against quantum attacks

Both sets of cryptographic tools can work very well together in quantum-safe cryptographic ecosystem

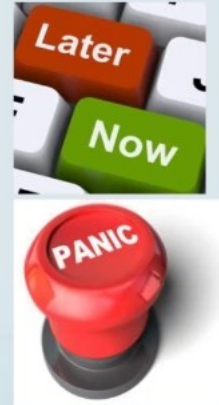
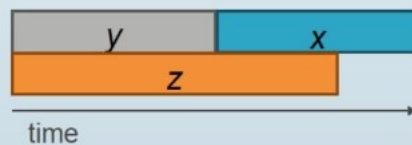
Мы можем выбрать вариант совместного использования классической и квантовой криптографии. Квантовая криптография как новая технология несет риск новых, пока неизвестных возможностей для криптоанализа. Использование только одного метода хуже, чем использование одновременно нескольких методов шифрования.

Do we need to worry *now*?

Depends on:

- X = *security shelf-life*
- Y = *migration time*
- Z = *collapse time*

“Theorem”: If $X + Y > Z$, then worry.



Пора ли нам уже сейчас начинать беспокоиться? Это зависит от нескольких параметров. Кому-то может и пора, но далеко не всем. Коммерческим компаниям можно пока не беспокоиться. По сути это зависит от требований регулятора к криптостойкости. Понятно, что полный ноль – это ноль минут. Но во многих случаях существуют нормативные требования, определенные соглашениями с потребителем о предоставлении определенного уровня безопасности. Уровень z может свидетельствовать о предоставлении потребителю определенного уровня безопасности. Критерии беспокойства проиллюстрированы на следующем слайде

Bottom line



Fact: If $X+Y>Z$, then you will not be able to provide the required X years of security.

Fact: If $Y>Z$ then cyber systems will collapse in Z years with no quick fix.

Prediction: In the next 6-24 months, organizations will be differentiated by whether or not they have a well-articulated quantum risk management plan.

Пороговые значения – как обеспечить необходимые период безопасности?

Quantum Risk Assessment



Phase 1- Identify and document assets, and their current cryptographic protection.

Phase 2- Research the state of emerging quantum technologies, and the timelines for availability of quantum computers.

Phase 3- Identify and document threat actors, and estimate their time to access quantum technology “z”.

Phase 4- Identify the lifetime of your assets “x”, and the time required to migrate the organizations technical infrastructure to a quantum-safe state “y”.

Phase 5- Determine quantum risk by calculating whether business assets will become vulnerable before the organization can move to protect them. ($x + y > z ?$)

Phase 6- Identify and prioritize the activities required to maintain awareness, and to migrate the organization’s technology to a quantum-safe state.

<http://www.evolutionq.com/methodology-for-qra.html>

Первый шаг начинается с идентификации активов и необходимости их криптографической защиты. Что это означает для меня, для моей организации, для моих клиентов? Может это не представляет проблемы для вас.

- Допустим, на первом шаге выяснилось, что настало время для квантовой защиты.
- Тогда второй шаг. Исследовать состояние возникающих квантовых технологий и сроки доступности квантовых компьютеров.
- На третьем шаге мы для каждого актива оцениваем время z достижения необходимости использовать квантовые технологии для защиты этого актива. Нужно определить активы и оценить время жизни каждого. Определите и задокументируйте участников угрозы и оцените их время доступа к квантовой технологии «z». При этом нужно учесть криптографический запас (cryptographic margin), который может оказаться большим. Составить информацию в разрезе клиентов: имя клиента (пользователя) – достаточное время необходимой криптографической защиты – подписка клиента на обновления продукта. Потребовать с поставщиков имена их аудиторов, проверяющих сертификаты на криптопродукты.
- Поставщики должны предоставить сертификат своих заменителей

Testing new tools



openquantumsafe.org



OUR TEAM

Project leaders
Michele Mosca (University of Waterloo)
Douglas Stebila (McMaster University)

Contributors
List of contributors to liboqs on GitHub

Acknowledgements
liboqs incorporates and adapts a variety of open source cryptographic software, including:

- BCNIST: Ring-LWE key exchange code by Bos, Costello, Naehrig, and Stebila
- NewHope: Ring-LWE key exchange code by Alkim, Ducos, Poppelmann, and Schwabe
- MSR NewHope: Ring-LWE key exchange code by Longa and Naehrig, source code contributed by Christian Paquin
- Frodo: LWE key exchange code by Bos, Costello, Ducos, Mironov, Naehrig, Micalebiani, Raghurathan, and Stebila
- SIDH key exchange code by Costello, Longa, and Naehrig, source code contributed by Christian Paquin
- McEliece: Niederreiter (McEliece) Goppa-code key exchange code by Bernstein, Chou, and Schwabe
- CHACHA20 code by Daniel J. Bernstein
- AES code by Chris Huibert
- SHA3 code from Superscop

liboqs provides wrappers to the following external libraries for some algorithms:

- NTRUEncrypt

Отступление – ресурсы, перечисленные на слайде

Сайт <http://www.evolutionq.com/methodology-for-qra.html>

В статье “Методология оценки квантового риска” рассматриваются детали оценки квантового риска и обстоятельства, которые могут возникнуть на каждом шагу оценки.

A Methodology for Quantum Risk Assessment

Author: Dr. Michele Mosca & John Mulholland

GRI GLOBAL RISK INSTITUTE

Потребности пользователей и ресурсы поставщиков, возможности науки и все, что уже накоплено и может использоваться, позволяет лучше понять процесс и методологию оценки.

Тестирование новых инструментов

Полезны ресурсы по обмену ключами при обучении с ошибками (Ring-LWE key exchange code, RLWE-KEX, Ring Learning with Errors Key Exchange, https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BC%D0%B5%D0%BD_%D0%BA%D0%BB%D1%8E%D1%87%D0%B0%D0%BC%D0%B8_%D0%BF%D1%80%D0%B8_%D0%BE%D0%B1%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B8_%D1%81_%D0%BE%D1%88%D0%B8%D

[0%B1%D0%BA%D0%B0%D0%BC%D0%B8#cite_note-.D0.92.D0.B0.D0.BB.D0.B8.D0.B5.D0.B2.E2.80.942000.E2.80.94.E2.80.94-1](#)).

RLWE-КЕХ - один из алгоритмов с открытым ключом, который предназначен для защиты от противника, обладающего квантовым компьютером.

Еще в 2014 году проходила информация о том, что Агентство национальной безопасности (АНБ) США пытается создать собственный квантовый компьютер, который смог бы взломать практически любую систему шифрования. Информация происходит из документов, обнародованных бывшим сотрудником ведомства Эдвардом Сноуденом (моя ссылка <https://lenta.ru/news/2014/01/03/quantum/>). Проект является частью исследовательской программы «Внедрение в сложные цели», на осуществление которой выделено 79,7 миллиона долларов. Большая часть работ проводится в Лаборатории физических наук в Колледж-Парке в штате Мэриленд.

Интересны также ресурсы на github:

- Кольцевое обучение с ошибками (RLWE) - это вычислительная проблема, которая служит основой новых криптографических алгоритмов, предназначенных для защиты от криптоанализа на квантовых компьютерах, а также для обеспечения основы для гомоморфного шифрования. RLWE более правильно называть Learning with Errors over Rings и просто задача большего обучения с ошибками (LWE), специализирующаяся на полиномиальных кольцах над конечными полями. Из-за предполагаемой трудности решения проблемы RLWE даже на квантовом компьютере криптография на основе RLWE может стать основой для криптографии с открытым ключом в будущем, так же, как проблема целочисленной факторизации и дискретного логарифма послужила основой для криптографии с открытым ключом. Важной особенностью базирования криптографии в кольцевом обучении с проблемой ошибок является тот факт, что решение проблемы RLWE может быть сведено к NP-Hard Shortest Vector Problem (SVP) в решетке. GitHub - vscrypto/ringlwe_power: A Practical Ring-LWE Key Exchange и GitHub - dstebila/rlwekex: DEPRECATED <https://github.com/dstebila/rlwekex>
- Ресурсы по суперсингулярному изогенному обмену ключами Диффи-Хеллмана (SIDH) <https://www.microsoft.com/en-us/research/project/sidh-library/> , <https://github.com/Microsoft/PQCrypto-SIDH> , <https://github.com/dconnolly/msr-sidh>
- gorra-code key exchange code <https://www.win.tue.nl/~tchou/mcbits/>
- <https://github.com/lwe-frodo/lwe-frodo> Постквантовый обмен ключами от обучения с ошибками - из статьи "Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE", published in ACM CCS 2016, <https://eprint.iacr.org/2016/659>
- NTRUEncrypt: самый быстрый асимметричный шифр <https://habrahabr.ru/post/118458/> Американский комитет Accredited Standards Committee X9 в апреле 2011 года утвердил использование самого быстрого алгоритма асимметричного шифрования NTRU (NTRUEncrypt). Удивительно, но широкая публика раньше ничего не слышала о таком алгоритме, а вот он уже становится технологическим стандартом для финансовых транзакций, причём демонстрирует быстроедействие на четыре порядка быстрее RSA за счёт хорошей параллелизации.

Например, графический процессор GTX280 может осуществлять до 200 000 операций в секунду шифрования 256-битным ключом NTRU. Это уже сравнимо скорее с симметричными ключами, например, это всего в 20x медленнее AES.

Утверждённый стандарт X9.98 описывает использование алгоритма NTRU в финансовых приложениях. Здесь он будет конкурировать с RSA и криптосистемами на

эллиптических кривых (ECC). По крайней мере, так думает Эд Адамс, исполнительный директор компании Security Innovation, владелец прав и патентов на алгоритм NTRU.

NTRU был изобретён ещё в середине 90-х. В отличие от RSA, не получил широкого распространения, потому что с самого начала нужно было повысить стойкость и производительность этого шифра. Сейчас все недостатки исправлены и на практике NTRU уже считается намного быстрее, чем RSA. Данный факт подтверждают даже сами специалисты RSA Labs, а также независимые исследования.

Одно из таких сравнительных исследований провели криптологи из Лёвенского католического университета (Бельгия). Они выяснили, что при тестировании с максимальными настройками безопасности NTRU на четыре порядка быстрее RSA и на три порядка быстрее ECC (PDF).

Система RSA бы разработана в 70-е годы, она считается более зрелой криптографической технологией и применяется во многих приложениях, а её надёжность не вызывает сомнений, тогда как NTRU ещё нуждается в пристальном изучении. Так что вряд ли переход на новые стандарты будет быстрым. Однако Адамс уверен, что его детище в будущем может оказаться надёжнее RSA: он объясняет, что NTRU основан на решётчатой конструкции, которая потенциально лучше противостоит компьютерным атакам так называемого «квантового типа», то есть атакам с использованием квантовых компьютеров.

На github представлены следующие проекты NTRU

- Main `libntruencrypt` repository
<https://github.com/NTRUOpenSourceProject/NTRUEncrypt>
- C Implementation of NTRUEncrypt <https://github.com/tbuktu/libntru>
- Java implementation of NTRUEncrypt and NTRUSign `tbuktu/ntru`
<https://github.com/tbuktu/ntru>
- NTRUOpenSourceProject/NTRUEncrypt-java
<https://github.com/NTRUOpenSourceProject/NTRUEncrypt-java>
- zhenfeizhang/NTRUEncrypt <https://github.com/zhenfeizhang/NTRUEncrypt>
- NTRUOpenSourceProject
<https://github.com/NTRUOpenSourceProject/NTRUEncrypt-ebats>
- Simple example made in NetBeans using the NTRUEncrypt SDK
<https://github.com/cptwin/NTRUEncryptExample>
- NTRUEncrypt library interface for Rust <https://github.com/FractalGlobal/ntru-rs>
- A java implementation of NTRUEncrypt cryptosystem. Updated on 22 Mar
<https://github.com/zhenfeizhang/NTRUEncrypt-Java>
- src/ subtree extracted from NTRUEncrypt. Updated on 9 Apr 2014
<https://github.com/jschanck-si/NTRUEncrypt-core>
- Parameter Generation for NTRUEncrypt. Updated 3 days ago.
<https://github.com/NTRUOpenSourceProject/ntru-params>

(моя ссылка https://en.wikipedia.org/wiki/Quantum_key_distribution) – это использование квантовой криптографии для безопасных коммуникаций. При которых стороны могут разговаривать, не опасаясь перехвата разговора через воспроизведение ключей. Конечно можно использовать и RSA, и протокол Диффи-Хеллмана. Если произошел обмен ключами, то можно использовать эти ключи для протоколов, использующих симметричное шифрование.

Замечания переводчика.

Здесь <https://cryptoworld.su/%D1%83%D1%80%D0%BE%D0%BA%D0%B8-%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8-%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BA%D0%BB/> рассмотрены атаки по шифротексту

Случайная последовательность поможет защитить и от атаки по шифротексту. Суть такой атаки заключается в том, что злоумышленник перехватывает необходимое количество шифротекстов и анализирует их с целью подобрать секретный ключ. Пример — атака на шифр Вернама в предыдущей статье цикла.

Если ты уверен, что твой ключ абсолютно случаен и подобная ситуация тебе нипочем не страшна, рекомендую проверить его на соответствие требованиям стандарта NIST. Если ключ не случайный, опытный криптоаналитик сможет распознать алгоритм шифрования и, возможно, даже получить ключ. А уж если ему в руки попадут еще и открытые тексты — пиши пропало.

В современных системах, чтобы сгенерировать случайную последовательность для ключа, применяют различные подходы. Стандартные UNIX утилиты `random` и `urandom` хэшируют данные, снимаемые со счетчика тактов процессора во время аппаратных прерываний. Microsoft Crypto API берет хэш от внутреннего состояния компьютера — текущего времени, размера жесткого диска, размера свободной памяти, номера процесса и так далее. В ход также идут всевозможные случайные данные. Например, в процессе оцифровки звукового сигнала на линейный вход звуковой карты приходит аналоговый электрический сигнал, который содержит шум, состоящий из:

радиопомех и наводок от соседних устройств и радиозэфира;

помех электропитания;

теплого шума случайного движения электронов в компонентах электрической схемы.

Используется и квантовый шум, который носит истинно случайный характер. Квантовый шум «проникает» в цифровую часть звуковой карты, где его можно сразу и использовать. Также нередко прибегают к помощи пользователя, требуя набирать случайные символы на клавиатуре, двигать мышкой, пока идет генерация сигнала, или произносить определенные слова.

Теперь немного о времени жизни ключа. Для нас этот показатель очень важен — ведь чем дольше ключ находится в обращении, тем легче злоумышленнику его получить и тем большую ценность этот ключ для него представляет. С самого момента генерации секретного ключа нужно задуматься, как часто его нужно менять. Кроме того, важный момент — уничтожение секретного ключа. Если речь идет о сессионном ключе, его стоит безвозвратно уничтожить сразу по окончании сеанса связи. Если речь о долговременном — пусть живет указанный срок, но, опять же, ни секундой дольше.

Сессионные ключи, несмотря на их недолгий срок службы, играют важную роль. Они используются повсеместно, начиная от защищенной TLS сессии и заканчивая прикладными программами (например, мессенджерами). Также сессионные ключи применяются при входе в личный кабинет интернет-банка и иных подобных сервисах, где речь идет об особо важных данных и ключи важно менять как можно чаще.)

Продолжение.

Мы с международными коллегами обсуждали вопрос дальнейших действий в связи с квантовыми компьютерами и решили решать эти проблемы совместно. Мы реализовали некоторые платформы с открытым исходным кодом (we realized some open source platforms). На слайде приведен список реализаций. Вы можете протестировать эти реализации. Они могут быть очень полезными для отдельных задач при реализации криптографических методов в практических отраслях, например в финансах. Криптографические примитивы дают тонкий слой для тестов для проникновения (pentest applications). Мы реализовали часть алгоритмов в коде программ. Это важно для дальнейшего планирования

Security is a choice

ISSA
Information Systems Security Association
Membership

REGULATIONS
COMPLIANCE

RISK
TRANS

Priorities
1.
2.
3.

Proactive
Reactive

Release
Testing
Development
Analysis
Planning
Requirements

Problematic choices:

- “Do nothing: my vendors will take care of this for me”
- “Do nothing until NIST standardization is done”
- “Get it over with”

48:09 1:58:10

Узкие места, которые у нас возникают – очень важные технические и математические вызовы, сопровождающиеся в том числе политическими вопросами. Самые трудные проблемы – не технические вызовы, это бизнес, затрагивающий вопросы политики на высоком уровне (high level policy decisions) и аутсорсинга, принятие дорожной карты проекта и согласование на верхнем уровне политических решений. Мы рекомендуем интеграцию со стандартом NIST и применение обычных практик риск менеджмента. Есть несколько вариантов, которые вы можете выбрать (there are some choices you can make), такой выбор может быть проблематичным. Он также может зависеть от поставщика решения. Нужно будет провести дружелюбные переговоры с поставщиками решений. Вы защищаете активы, и обеспечение целостности может потребовать больше времени. Если ваш поставщик испытывает трудности с продажей самых современных устройств, проведите с ним переговоры об актуальности спецификаций. Возможно лучше ничего не делать до тех пор, пока безопасность не стандартизирована, это криптография. В то же время вы можете реализовать нужную вам криптографию сами. Это требующий очень высокой квалификации бизнес. Крупные компании могут идти этим путем, но средние и малые предприятия могут затруднять читать научные статьи и внедрять их. Следуйте процессам, утвержденным NIST. Не делать ничего очень рискованно. Определите свои потребности. И следуйте стандартам NIST, который выпускает стандарты не только для SWIFT, но и для других протоколов. Только сильная криптография обеспечит защиту. Определите, какие продукты вы используете. Возможно Вам нужны более сильные и гибкие (more agile) криптографические реализации. Вам нужно умение реагировать на неожиданные угрозы и быстро их устранять (you need ability to respond unexpected threats and fix it quickly). Проверьте ваше унаследованное программное обеспечение, аппаратное обеспечение. К сожалению это может потребовать много времени. Но я думаю, что промедление – неправильный подход. Думаю правильный срок выполнения таких действий –

следующие пару лет. И я поддерживаю проверенный подход. Люди любят использовать ECC или RSA. Для обычных компьютеров ECC защищает от классических атак. Пока в течение ближайших лет люди будут изучать квантовые компьютеры они могут осознать, что гибридная архитектура обеспечивает лучшую производительность. Использование гибридной архитектуры может намного повысить продуктивность.



Хочу подчеркнуть, что мы действительно имеем историческую возможность. Поскольку у нас уже есть квантовые компьютеры, мы осознаем, что основа кибербезопасности будет нарушена, но не сегодня, а в течение нескольких десятилетий, примерно к 2040-му году. Хуже всего то, что он разрушает основы классической криптографии (дословно *retired cryptography*). Доверие будет нарушено (*trust will be broken*). Как только мы будем иметь готовые квантовые компьютеры, сам квантум окажется угрозой. Это вынуждает нас пересматривать основы криптографической инфраструктуры (дословно *that is why retired cryptography built off*, Именно поэтому построенная криптография в отставке) - все взломы, которые мы видим сейчас, человеческие ошибки и так далее..(*All the hacks we see now, human mistakes and so on*). Мы имеем хрупкую криптографическую инфраструктуру. Основание криптографии нарушено (*the crypto foundation has been broken*) Нам нужен более безопасный криптографический фундамент (*We need more secure cryptographic foundation*). Нам и европейцам нужна более сильная криптография. Возникли умные контракты (*smart contracts*). Квантум вынуждает нас перестраивать основы. Это шанс построить более сильную криптографию, обеспечивающую БОльшую безопасность в кибермире

The choice is ours



Embrace quantum technologies that will help humanity *and* live in a safer cyber-enhanced world?



Yes

No

Мы хотим охватить замечательные вещи криптотехнологий и создать более безопасный мир.



Thank you!!

Comments, questions and feedback are very welcome.

michele.mosca@uwaterloo.ca

michele.mosca@evolutionQ.com

QUESTIONS?


Каковы наши планы? Будем развивать новые квантовые технологии (emerging quantum technologies). Спасибо за внимание , задавайте вопросы.

Вопрос: Какие ваши личные планы?

Ответ – я планирую заниматься анализом рисков. Это огромный объем, я планирую провести несколько вебинаров. Нужно инвентаризировать свои активы и провести опрос среди клиентов на предмет устойчивости к квантому (quantum-resistance). При проведении криптоанализа имеющейся системы может выясниться, что утерянные ключи можно восстановить, VPN можно расшифровать. Нужно обязательно поменять все криптоключи. Наверняка найдутся непредвиденные уязвимости. Нужно пересмотреть основы операционной логики там, где вы используете симметричную криптографию. Может понадобится обновление алгоритмов, внедрение более сильного криптографического программного и аппаратного обеспечения.


Ведущий – спасибо, Майкл. Мы представляем финальную презентацию нашей конференции

Speaker Introduction



Dr. William Whyte

- Chief Technology Officer at OnBoard Security, Inc.
- Previously served as Chief Scientist at Security Innovation and CTO for NTRU Cryptosystems and Senior Cryptographer with Baltimore Technologies in Dublin, Ireland
- Currently the chair of the IEEE 1363 Working Group for new standards in public key cryptography



Доктор Вильям Вайт работает главным технологическим менеджером, занимается инновационной деятельностью в области безопасности и проводит криптографические исследования. Он работает СТО для NTRU Cryptosystems и главным криптографом для Балтимор Текнолоджис в Дублине. Он также возглавляет рабочую группу IEEE 1363, занимающуюся новыми стандартами в криптографии с открытым ключом. Он имеет окторскую степень Оксфордского университета по статистической механике и нейросетям. Добро пожаловать, Вильям.

Спасибо большое, рад выступать в вашей аудитории.

Evolution to post-quantum cryptography

William Whyte, Onboard Security

2017-04-25

Мое выступление продолжит вопросы, рассматриваемые в предыдущем выступлении. Включая вопросы математики, криптографии, квантовых вычислений и фазовых переходов.


Comparing Post-Quantum Asymmetric Crypto Algorithms

- Additional data needed for post-quantum crypto algorithms
 - NTRU needs 600 additional bytes.
 - R-LWE needs 1100 bytes.
 - McEliece needs 1 Mbyte.
- NTRU: Lattice-based encryption algorithm, invented in 1996, standardized since 2008
- R-LWE is a new algorithm that has been around in various forms since 2005
 - Lattice-based cryptographic algorithm like NTRU
 - Attractive provable security properties but pays the price in lower performance and larger keys.
- McEliece is based on coding theory and has been around since 1978
 - Enormous key and very large minimum ciphertext size make it impractical for most applications.
 - Has been available for scrutiny for quite a while but it is not clear it has received quality scrutiny

Люди на практике часто используют криптографию с открытым ключом, это общепринято, всех устраивает и решает стандартные задачи. Эта презентация является во многом образовательной. На этом слайде представлены алгоритмы, которые могут компенсировать недостатки классической криптографии. Отмечу алгоритмы шифрования на основе решетки

(Lattice-based encryption algorithms https://en.wikipedia.org/wiki/Lattice-based_cryptography). Если мы сравним существующие алгоритмы, в большинстве своем использующие эллиптические кривые, то увидим, что они востребованы и используются в электронных подписях документов. С 2009 года мы наблюдали успешные атаки по взлому RSA. <лирика по поводу ненастоящего белого шума>. В криптографии многое основано на нормальном распределении случайных величин, где шум – очень маленькие случайные числа.

NTRU:




- $g/f = 71 \pmod{124}$
- g and f are both “small”
- Find g and f .

- Easy in one dimension
- But we can define “division” of multi-dimensional objects
 - ❑ Work in a “polynomial ring”
- As dimension goes into the hundreds, this problem becomes very hard to solve

Продемонстрирую, как это работает, на примере с маленькими числами. Рассмотрим пример на слайде, где у нас два маленьких числа, одно из которых делим на другое. Если я беру маленькие числа, задача решается легко. Но при возрастании чисел и введению многомерности задача становится нерешаемой, обработка сигнала превращается в кольцо. Когда размерность превышает сотню, задача становится нерешаемой.


NTRUEncrypt – Performance



Algorithm	Key Generation	Encryption	Decryption
NTRU (439)	2588	128	204
rsa3072	1313224	9280	18382
curve25519	230	219	219
ecfp256q	92	301	301
nistp256	485	1672	1672

- Security level = 128
- Benchmarked on SUPERCOP: <http://bench.cr.yp.to/supercop.html>
- Units: k cycles. 1 second = 2.7×10^9 cycles with a 2.7 GHz CPU
- Specs: <https://github.com/NTRUOpenSourceProject/ntru-crypto/blob/master/doc/EESS1-v3.1.pdf>
- Security arguments and how to derive the parameters: <https://eprint.iacr.org/2015/708>


Этот слайд показывает преимущество эллиптических кривых с точки зрения криптостойкости алгоритма (Примечание переводчика – исходники supercop на github <https://github.com/floodyberry/supercop>)



Comparing Post-Quantum Signature Algorithms

- pqNTRUsign-563 (128 bit strength)
 - ❑ 1056 bytes key and signature sizes.
 - ❑ Implementation exists. Ready for standardization.
- BLISS signature – a scheme instantiated over NTRU lattices
 - ❑ 630 bytes key and signature sizes.
 - ❑ Did not provide parameters for quantum security
 - ❑ Implementation from academia. Unclear about standardization process.
- XMSS – a stateful hash based signature scheme
 - ❑ Large signature size, 8400 bytes.
 - ❑ Undergoing standardization process.
- SPHINCS – a stateless hash based signature scheme
 - ❑ Large key size, 1000 bytes, and even large signature size, 41,000 bytes.

Здесь вы можете сравнить разные алгоритмы подписи и выбрать для себя победителя. Обратите внимание на замену 128-битного алгоритма подписи на алгоритм с большим размером ключа. Все алгоритмы подписи основаны на хэш-функциях. Выбраны минимальные возможные размерности из предположений безопасности. Эти алгоритмы более безопасны, чем используемые сейчас. Самая нижняя строка на слайде относится к алгоритму с ключом самого большого размера



Getting there from here

Рассмотрим возможные варианты квантово-безопасных наборов шифров

Possible solutions



- 1. Define a quantum-safe ciphersuite
 - ❑ Solves the problem!
 - ❑ but...
 - ✓ No community consensus on a quantum-safe encryption algorithm
 - ✓ Not clear there's appetite to roll out a whole new set of algorithms given that the ECC discussion is still going on
 - ✓ No good quantum-safe signatures
- 2. "Quantum-safe" existing ciphersuites

Специально-компактный SSL/TLS. Берем существующую технологию и компенсируем ее недостатки, смешивая две системы.

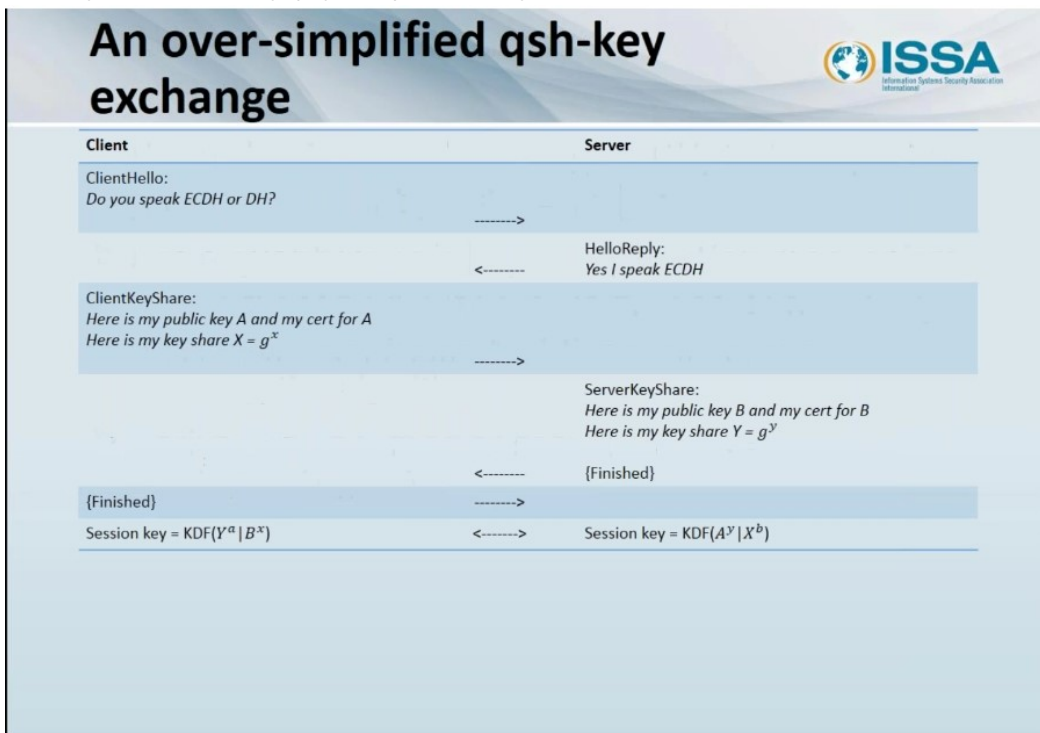
QSH = Classic handshake + QS-KEM



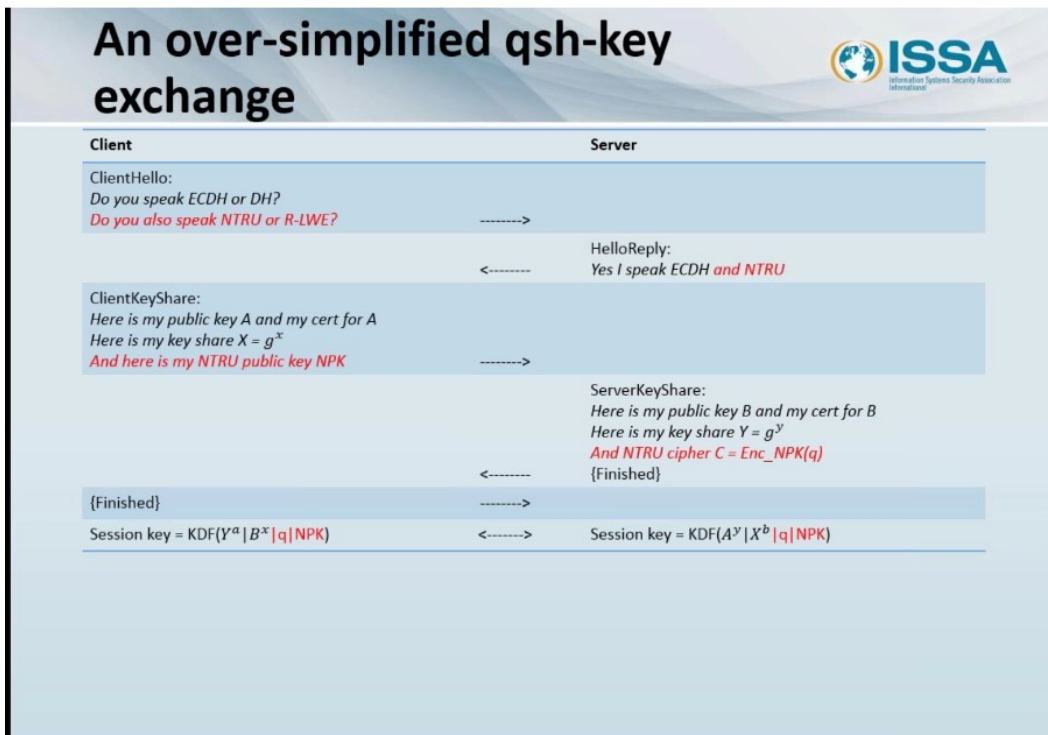
- Use a classic handshake (e.g. ECDH) to transport a premaster secret $pms1 := Y^a | B^x$
- Use a quantum-safe key encapsulation mechanism to transport another premaster secret $pms2 := q$
 - ❑ Plug-and-play for most existing quantum-safe encryption algorithms
- Derive the final master secret as $ms := KDF(pms1 | pms2)$

В этом случае мы смешиваем классический handshake и квантовую криптографию <https://www.ietf.org/proceedings/interim-2015-tls-03/slides/slides-interim-2015-tls-3-2.pdf>
Выводим private key из длинного и короткого ключей. (Примечание. Детали здесь <https://www.potaroo.net/ietf/all-ids/draft-whyte-select-pkc-qsh-02.txt>)

Преимущество – plug-and-play генерация секретных ключей для общих операций. При расшифровывании придется иметь дело со смешанным ключом и дополнительной безопасностью. Сейчас мы все чаще имеем дело с необходимостью расшифровать записанный зашифрованный трафик. Достаточно, если такая возможность будет при остановке в определенных точках. И нам нужно защититься от перехвата зашифрованного трафика. Причем важно защитить аутентификацию и обеспечить защиту от перехвата трафика, и в такой ситуации вам никто не даст спасательный жилет. Нужно обеспечить защиту по слоистому (layered) принципу.



На этом слайде показана типичная процедура обмена ключами и генерации сессионного ключа.



Здесь мы расширяем существующие операции, добавляя дополнительные поля. Мы не обмениваемся существующими ключами.

QSH is secure



- At least does no harm
- pms1 is (classically) authenticated
- pms2 is quantum-safe
- $ms := \text{KDF}(pms1 | pms2)$ is both authenticated and quantum-safe

- Defeat harvest-then-decrypt attack with low cost
- Inherit classical authentication
- Lack of quantum-safe authentication
 - ❑ Authenticity can wait, privacy can't...

Комментарий переводчика: harvest-then-decrypt часто упоминается в связи с функционированием сети TOR, например <https://lists.torproject.org/pipermail/tor-dev/2016-February/010379.html>

Даже если криптография вас не беспокоит сейчас, она вам понадобится в будущем.

QSH incurs minimum cost



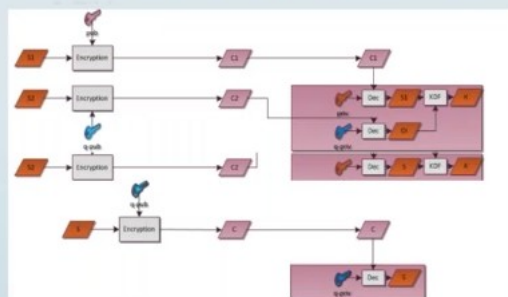
- Extra work: a public key generation, an encryption and a decryption
- More load on clients, less on servers
- Packet size increase is significant for all known quantum-safe algorithms though

При этом защита не потребует от вас больших затрат. Можно минимизировать объем вычислений.

Quantum-safe devices running in FIPS Approved mode



- NIST has stated that hybrid mode is Approvable
- OtherInfo can be obtained using non-Approved security mechanisms; FIPS-approved devices, running in FIPS Approved Mode, can carry out QSH
- Five years (?): NIST approves quantum-safe algorithms: FIPS-approved devices can be in FIPS mode while only running quantum-safe algorithms



Можно ожидать, что в течение ближайших пяти лет NIST одобрит защищенный от квантовых компьютеров алгоритм и устройства. Фактически нужно не только утвердить алгоритмы, но и согласовать полную документацию, подтверждающую, что одобренные устройства работают именно в одобренной моде, а также поддерживать изменения в документации.

QSH summary

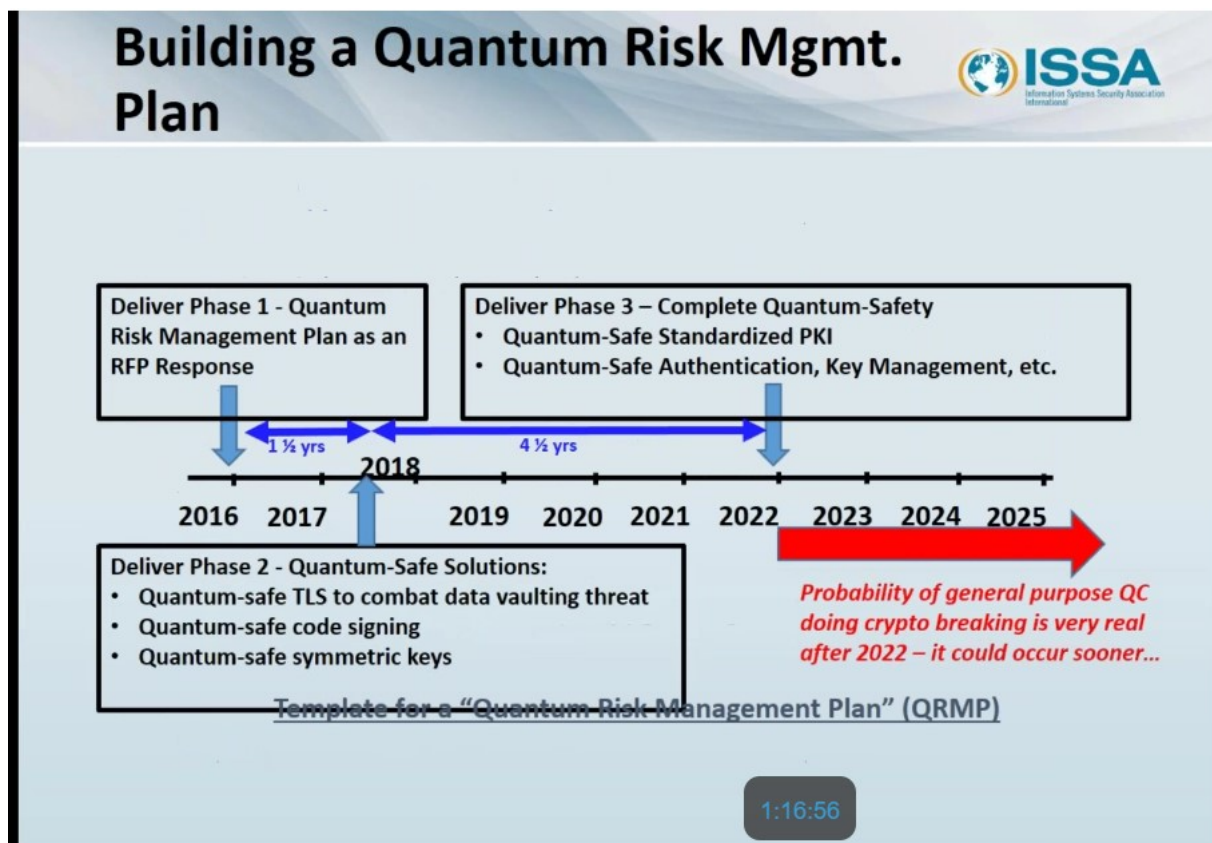


- QSH for TLS1.2 and TLS1.3
 - ❑ <http://www.ietf.org/id/draft-whyte-qsh-tls13-04.txt>
- Selecting QS crypto for QSH
 - ❑ <http://www.ietf.org/id/draft-whyte-select-pkc-qsh-00.txt>
- Working code with WolfSSL
 - ❑ <https://github.com/wolfSSL/wolfssl>
- qstor code:
 - ❑ Requires a patch to fix cell size issue
 - ❑ <https://github.com/NTRUOpenSourceProject/ntru-tor>
- Security proof:
 - ❑ <https://eprint.iacr.org/2015/287.pdf>

Примечания переводчика. Вместо ссылки

<http://www.ietf.org/id/draft-whyte-select-pkc-qsh-00.txt> - ссылка <https://tools.ietf.org/id/draft-whyte-select-pkc-qsh-00.txt>

Здесь вы можете найти спецификации, включая две спецификации TLS - версии 1.2 и 1.3 версии SSL. Криптографы работают с SSL и с TOR. Присутствуют объяснения и таблицы для линкера.



Сейчас действительно хорошее время для организации разработки планов по квантовому риск менеджменту. И сейчас самое время собрать и разработать планы по развитию и эволюции ваших информационных систем. Сейчас действительно хороший шанс использовать квантовую криптографию для разработки и улучшения ваших систем. Квантум – серьезная угроза безопасности, нужно разработать соответствующий ответ на эту угрозу. К 2022 году пора приступать к поставке разработанных систем. И поэтому мы ищем кибер-решения для реализации существующих планов по крипто. И, не забывая о комплаенсе, спросите ваших поставщиков об их планах. Это нужно для понимания, насколько вы можете рассчитывать на их криптографические решения. С появлением и использованием реальных квантовых компьютеров переход на них может быть резким и разрушительным.



Большое спасибо за ваше внимание.

Ведущий – спасибо Вильям за Ваш рассказ. Для меня Ваш рассказ, особенно QSH, был очень-очень интересным. Я бы задал Вам первый вопрос. Есть перспективы у соединения квантовой криптографии и TLS? Вильям: Да, это хороший вопрос. Нужно смотреть определения и алгоритмы для крипто и TLS. У TLS есть две версии, смотрим TLS 1.3. Сейчас потребители должны проверять, пен-тестить (pentest=penetration test, тест на проникновение) и требовать от поставщиков поставки в их решениях именно версии TLS 1.3. Это может компенсировать риски квантума, именно TLS 1.3 решения. Есть ли тесты, например Microsoft, о деталях TLS 1.3?

Комментарии переводчика.

У Microsoft по состоянию на апрель 2017 имеем TLS 1.2.

<https://blogs.msdn.microsoft.com/kaushal/2011/10/02/support-for-ssl-tls-protocols-on-windows/>

<https://support.microsoft.com/ru-ru/help/3140245/update-to-enable-tls-1.1-and-tls-1.2-as-a-default-secure-protocols-in-winhttp-in-windows>

<https://support.microsoft.com/ru-ru/help/3135244/tls-1.2-support-for-microsoft-sql-server>

<https://support.microsoft.com/en-ae/help/3135244/tls-1.2-support-for-microsoft-sql-server>

У других поставщиков в 2014 году наблюдался апгрейд на TLS 1.2, например

<https://www.entrust.com/moving-tls-1-2/>

Заметьте, TLS – продукт с открытым исходным кодом.

Open Discussion & Q&A



- **Jason Sabin - Moderator**
- **Mark Minnoch**
- **Michele Mosca**
- **William Whyte**

To ask a question:

Type in your question in the **Questions** area of your screen.

You may need to click on the double arrows to open this function.

#ISSAWebConf

Модератор. Я могу поблагодарить докладчиков, они представили сегодня очень продуманную информацию. Переключитесь и задайте интересные вопросы, которые у вас есть. И я призываю вас поднять голову и задавать вопросы в вашей профессиональной среде.

Марк, что Вы можете сказать о криптоалгоритмах? Вы реально только разрабатываете криптоалгоритмы? Нужно ли при внедрении выполнять их валидацию?

Марк. Спасибо за хороший вопрос. Позвольте переформулировать его более простым языком. Следует ли разрабатывать взламываемые алгоритмы? (смех). Правила таковы, что при вводе системы в эксплуатацию нужно провести проверку: тесты на проникновение (pentesting), обеспечив хороший уровень изоляции и проверив трудность взлома получившейся системы. Нужно проверить все имеющиеся сертификаты для аппаратных устройств. Проверить, что аппаратные устройства (приборы) получают другую проверку и имеют необходимые сертификаты. Технологии меняются и требуют изменения программ. Изменяется требуемая длина ключевой информации. Программные компоненты могут требовать изменений, отличающихся от изменений аппаратной части. Например, продукт, в который встроена определенная криптографическая библиотека, может требовать изменения для приборов, использующих эту библиотеку. Поставщики продают решения. Нужно соответствие криптографии, поставляющейся с их решениями, проверять отдельно, а криптографию проверять отдельно с учетом требуемой специфики (peculiar apart).

Модератор: Окей, отлично, спасибо (1:45:23). Это большое разъяснение. Майкл, вопрос к Вам: если в криптографии найдена ошибка, backdoor или ошибка другого типа, то нужно ли о ней докладывать и, если нужно, то куда?

Марк. Зависит от ошибки. Это недостаток (flaw) или криптографическая коллизия? (*collision*. Комментарий переводчика: от криптографии требуется Collision resistance https://en.wikipedia.org/wiki/Collision_resistance)

Модератор. В NIST наблюдали и описывали разные случаи flaw. Мой вопрос относится к хорошо построенным приложениям, имеющим backdoors (мой комментарий: Backdoor — это программа (или ее фрагмент), которая может быть внедрена на компьютер пользователя, предоставляя злоумышленнику возможность удаленного управления компьютером.

Пояснение

Программы Backdoor специально разрабатываются для получения несанкционированного (и незаметного) доступа к ресурсам компьютера.

Такие программы как бы создают для злоумышленника «черный вход» в систему, поэтому они и называются программами Backdoor (что в переводе с английского означает «черный ход» или «потайная дверь»). <https://www.dialognauka.ru/support/glossary/4604/>)

Марк. Нам нужно знать о генераторах случайных величин. В них тоже может содержаться backdoor. Криптографическое сообщество должно помнить об основах применяемых алгоритмов, например об алгоритмах, построенных на эллиптических кривых, и о процессах установления ключей. О хранении публичных ключей и электронных подписях. Внимательно изучите процессы хранения открытых ключей и риски, вовлеченные в процесс хранения открытых ключей, соблюдаются ли фундаментальные примитивы. Действительно ли риски низкие или backdoors могут быть внедрены в связи с открытыми ключами.

Модератор. Окей, отлично, отлично.

Марк. Я думаю вовлеченные в это люди могут проверять свои конфигурации CFG (комментарии переводчика- конфигурационные файлы, криптоключи идут с расширением .cfg) (1:43:13)

Модератор. Вильям, вопрос для Вас. Как Вы можете оценить изменения в криптографии для экономических областей? Каково влияние на разработки в криптографии разработок в квантовых технологиях?

Вильям. Интересный вопрос, спасибо. Работы по криптографии, в том числе по разработке собственных криптографических алгоритмов, ведутся во всех индустриях. В том числе в финансовой, где квантовые компьютеры могут многое изменить. Действительно для банков изменения в криптографии могут перевернуть весь бизнес. Банки основываются на отчетности, но в эту отчетность изменения криптографии могут не попадать. Как и в комплаенс. Предполагаю, что изменения в практиках и законах могут занять лет пять. И вычислительные усилия потребуют еще лет пять. Развитие компьютерных алгоритмов не останавливается, в том числе алгоритмов анализа трафика. Бизнес занимается этой темой, включая собственные внедрения криптографических алгоритмов. И я отвечаю на Ваш вопрос, с моей точки зрения внимание нужно обратить также и на секретные ключи и на управление ключевыми парами. DWave уже показал quantum random numbers

Я хочу спросить - могут ли квантовые компьютеры и квантовая связь быть дешевле по вашему опыту? Разработка квантовых алгоритмов не останавливается. Но нужно ли вкладываться в разработку квантовых алгоритмов? По мере того как вычислительные мощности растут, будут ли

востребованы квантовые алгоритмы? Сейчас с помощью имеющихся квантовых алгоритмов мы можем взломать любую цифровую подпись. Ничто не гарантирует, что, проснувшись завтра утром, мы не обнаружим, что все уже взломано. Сейчас с помощью квантовых алгоритмов мы можем обрабатывать любой трафик.

(Примечание переводчика – NIST уже открыл проект по обеспечению защиты от взлома квантовыми компьютерами <https://www.cnet.com/news/quantum-computer-encryption-hacking-us-government-protect/> “ US government: Help us protect computers from quantum hacking

The same government seeking to future-proof its secrets and our own digital privacy also wants to make sure it can bypass encryption.”) Одновременно идет дискуссия о том, стоит ли ослаблять стандарты NIST. Нужно подготовиться к внедрению защиты, которую мы готовим на различных уровнях защиты. И одна из первых линий защиты будет посвящена квантовым компьютерам. Такие компьютеры могут появиться быстрее, чем мы ожидаем. И мы должны быть уверены в своей защите от всех видов риска.

Модератор.

Большое спасибо. Очень полезно. Вы подчеркнули важность определения уровня приемлемого риска, разработки стратегии управления рисками, и многие компании уже занимаются этим. С моей точки зрения важна разработка параметров риска. Некоторые из видов риска будут блокированы самими участниками финансового рынка. Мы рассмотрели сегодня много важных вопросов. Итак, Марк, Майкл и Вильям, подведите итог.

Марк – нужно понимать важность криптоалгоритмов и для поставщиков технологических продуктов, и внедренцев этих продуктов, и для продакт менеджеров для обеспечения уверенности в готовности к будущим изменениям. Таким образом, квантово-безопасная криптография (quantum-safe cryptography) это наше ближайшее будущее.

Модератор. Спасибо, Марк. Майкл?

Майкл. Я хочу подчеркнуть важность изучения и планирования сейчас. Несмотря на дороговизну технологии, нужно начинать диалог, начинать планирование и оценки (assessments). Нужно понимать важность математической постановки и процессов, начиная изучение этих процессов сейчас, в течение ближайшего десятилетия.

Модератор.

Большое спасибо. Мы видим, что обсуждаемые нами принципы очень важны для систем промышленного контроля и для систем классического типа, реализующих взаимодействие клиент-сервер. Также они важны для IoT устройств.

Майкл. Да, каждый день мы видим все больше поставщиков технологических решений при управлении реквизитами доступа на уровне предприятий. Для людей, использующих Интернет вещей, нужны криптографические алгоритмы. Я вижу большую возможность для расширения областей, в которых используются криптографические алгоритмы. Все больше криптографических модулей встраиваются в устройства. Технологический прогресс дает возможность выбирать для криптографии аппаратное или программное исполнение.

Модератор. Спасибо. Здесь Вы очень понятно пояснили. Майкл, вопрос для Вас – существует ли у поставщиков условный флаг, скажем backdoor для квантовых алгоритмов? Квантовые вычисления могут быть хорошо построены с использованием бэкдоров.

Майкл – генераторы случайных чисел – хороший пример. Экспортеры знакомы с ограничениями на криптографический функционал. Например, в алгоритмах эллиптических кривых используются определенные практики. Обмен ключами и генерация сессионного ключа для электронной подписи – это пре-фундаментальный примитив, который должен быть тщательно изучен. Действительно, backdoor, встроенный на этом примитивном уровне, в алгоритмах, например, электронной подписи думаю не несет больших рисков. Сейчас многие занимаются пост-квантовыми примитивами.

Модератор. Вильям, вопрос для Вас. Как количественно оценить в деньгах риски квантовых технологий?

Вильям. Спасибо за хороший вопрос. Квантум - новая технология, думаю банки оценят ее риски для бизнеса. Предполагаю, переход на эту технологию может занять лет пять. Нужно следить за развитием квантовых алгоритмов, но развитие классической криптографии тоже не останавливается. И мы должны быть готовы к тому, что однажды проснувшись, мы обнаружим новый тип инцидентов.

Модератор Спасибо. Мы обсудили уровни риска квантовой криптографии и меры, которыми мы можем его компенсировать. Марк, Майкл и Вильям. Прошу каждого из вас подвести итог нашему обсуждению квантовых алгоритмов.

Марк. Я думаю, что какое-то время могут существовать проверенные классические алгоритмы, но технологическим поставщикам и продакт менеджерам нужно прорабатывать способы разработки квантум-безопасных алгоритмов и поставки клиентам квантум-безопасных устройств и решений.

Модератор. Спасибо, Марк. Макл?

Майкл. Хочу подчеркнуть важность изучения и планирования сейчас деятельности на ближайшие годы. Несмотря на высокие расходы на такую операционную деятельность, необходимо заложить в бюджеты соответствующие суммы уже сейчас. Это технологии, обеспечивающие завтрашнюю безопасность. Промедление не приемлемо в противостоянии с русскими. Backdoors должны быть выполнены на очень высоком уровне. И нам необходимо централизовать криптоменеджмент и криптоанализ с учетом квантовых технологий. Процессы NIST уже стартовали, и многие люди ищут способы сопротивления (преодоления рисков?) новых технологий – квантум-эффектов. Нам нужно централизовать наши усилия. Успешное преодоление угроз квантовой криптографии будет важным много-много лет, пора строить составляющие компоненты.

Модератор. Спасибо. Вильям?

Вильям. Я думаю самое время спросить поставщиков об их планах в связи с квантовой криптографией, как они планируют страховаться против воздействия новых технологий.

Модератор. Благодарю каждого из вас – Марк, Майкл и Вильям – за участие и за предоставленную информацию. На слайде ниже – ссылки, по которым все участники могут получить запись web-конференции

Web Conference Survey



A recording of the conference and a link to the survey to get CPE credit for attending the April ISSA International Web Conference will soon be available at: <https://www.issa.org/page/April2017> and check out previous web conferences at <https://www.issa.org/?OnDemandWebConf>

If you or your company are interested in becoming a sponsor for the monthly ISSA International Web Conferences, please visit: <https://www.issa.org/?page=BecomeASponsor>

01:27

Приглашаю участников конференции присоединиться к ISSA с 15% скидкой

Join ISSA



Webinar attendees can join ISSA at a 15% discount by using the code **WEBCON42** during the checkout process

The discount is available for all memberships except Students, and can also be used to renew your membership