Challenges in quantum cryptography
Вызовы в квантовой криптографии

From theory to practice –
От теории к практике

Основные достижения теории и эксперимента в области практической квантовой криптографии

- квантовая генерация случайных чисел,
- квантовая выработка и передача ключей,
- квантовое шифрование,
- детерминированная квантовая связь,
- квантовая аутентификация,
- квантовое хэширование,
- квантовая цифровая подпись,
- квантовые протоколы бросания монеты, передачи бита на хранение, квантовые игры,
- квантовая память (в том числе ассоциативная) и защищенные хранилища данных,
- квантовый «взлом» криптосистем, алгоритмы для квантовых компьютеров,
- …?

Quantum cryptography for the security communications 1

Services of the QKD for the links and the networks.

Services of the encryption for the links and the networks.

Services of the control systems.

Quantum cryptography for the security communications 2

Services of the QKD, the encryption and the control systems for the links and the networks by:

- fiber optics communications,
- atmospheric optics communications,
- space (orbital) inter-satellite communications,
- interfaces for separate quantum computers.

Quantum cryptography for the financial and insurance sectors

- генерация случайных чисел (ДСЧ) для банковских карт, полисов страхования, документов строгой отчетности;
- защита финансовых транзакций и обработки информации в страховых случаях с помощью квантовой подписи и хэширования;
- защита взаимодействия с платежными, транспортными и банковскими терминалами (АТМ);
- …

Quantum cryptography for the Digital Economics 1

Сервисы безопасности для Security services for :

-«умного города» (“The Smart City”),

-«умного дома» (“the smart house”),

-«умного офиса» (“the smart office”);

Quantum cryptography for the Digital Economics 2

Сервисы безопасности для:

(Security services for):

-«электронной торговли» (“The e-commerce”),

-«промышленного интернета» (“The industrial internet”),

-«интернета вещей» (“the internet of things”);

Quantum cryptography for the Digital Economics 3

Сервисы безопасности для:

(Security services for):

-«умного транспорта», включая беспилотные транспортные средства, дроны и роботы (“The Smart transport”),

- охранных систем объектов и автомобилей,

- систем «свой – чужой»,

- …

Quantum cryptography for the social services in the future

- Квантовые идентификаторы для ГИС ЕСИА, аптек, поликлиник, больниц.
- Квантовый нотариат.
- Интегрированные квантовые ключи доступа на объекты (в системы) и получения социальных услуг, в т.ч. здравоохранения и образования).
- Сервисы (ключи, услуги) для доступа к персональной геномной информации.

Проблемы, требующие решения для развития и практического внедрения квантовых криптографических систем

- формирование моделей угроз и нарушителя для ККС с учетом их технической реализации и сфер применения;
- доказательства криптографической стойкости и специальных свойств с учетом применений в составе (интеграции) СВТ, комплексов шифровальных средств, телекоммуникационного оборудования, приложений и т.д.;
- создание модели угроз, нарушителя, криптосхем, протоколов, обоснование стойкости для квантовых повторителей (репитеров), маршрутизаторов и других подобных преобразователей для ККС;
- развитие и обоснование математических моделей и доказательства свойств криптографических примитивов, протоколов и алгоритмов, использующих многокубитные квантовые состояния (прежде всего, несепарабельные);
- развитие методов криптосинтеза, криптоанализа (в т.ч. анализ протоколов, и методов «информационного доступа» для ККС.

Факторы ускорения внедрения Quantum cryptography

Дорожные карты квантовых технологий (РГ ЕС, ФПИ и НТИ), интеграция усилий в рамках программно-целевого подхода.

Повышение качества и обоснование доказательств. Проведение тематических исследований создаваемых ККС.

Выполнение требований регуляторов, деятельность в рамках системы лицензирования и сертификации СКЗИ,

Миниатюризация и снижение энергопотребления. Достижение импортонезависимости.

Интеграция с услугами и инфраструктурой.

Распространение лучших практик и стандартизация. Участие ТК 26.

Реклама и маркетинг, проведение конференций и участие в выставках.

Выход на зарубежные рынки.

Подготовка кадров с криптографическим образованием. Специализация в рамках образовательного стандарта.

Вопросы для дискуссии

1. Имеются ли научно-технические достижения в РФ по созданию систем на основе квантовой криптографии, достаточные для обеспечения нужд отраслей экономики, кредитно-финансовой сферы и органов государственного управления?
2. Что на уровне решения математических и других научно-технических задач необходимо решить для внедрения ККС?
3. Достаточны ли действующие в РФ нормативные и методические документы для разработки и применения ККС? Что из опыта работы международных (зарубежных) организаций может быть использовано в РФ в области нормативного обеспечения квантовой криптографии?
4. Существуют ли документы регламентирующих государственных институтов в других странах (например, НИСТ США), относящиеся к области квантовой криптографии, и каковы они?
5. Какова возможная роль Технического комитета по стандартизации «Криптографическая защита информации» (ТК26) в интересах разработки и применения ККС? Можно ли выделить перспективные направления работ для совмещения ККС и существующих классических протокольных решений (TLS, IKEv2/IPSec), в т.ч. разрабатываемых в ТК26?
6. Существуют ли новые математические задачи, возникающие в связи с появлением квантовых технологий обработки информации, и каковы они?

Вопрос №1 для дискуссии

Имеются ли научно-технические достижения в РФ по созданию систем на основе квантовой криптографии, достаточные для обеспечения нужд отраслей экономики, кредитно-финансовой сферы и органов государственного управления?

- работы РКЦ, Сколково
- работы Казанского КЦ, ИТМО, …
- работы ФПИ
- работы …

Вопрос №1 для дискуссии

Перечень критериев для оценки готовности квантовой криптографии к практическому внедрению:

а) адекватный критерий криптографического качества ключей, вырабатываемых системами КРК;

б) перечень актуальных атак на квантовые криптографические протоколы и их техническую реализацию, а также сценариев их применения (комбинирования);

в) полноценный и гибкий инструментарий для построения криптосхем (математических моделей) квантовых криптографических протоколов и технических реализаций систем КРК;

г) компоненты квантовых каналов, допускающие достаточно полное и экспериментально верифицируемое описание физических свойств, критичных для заданных протоколов КРК;

д) доказуемо стойкие *при их технической реализации на современной компонентной базе* протоколы КРК;

е) наличие заинтересованных потребителей квантовой криптографии и моделей угроз безопасности КРК, адаптированных к потребностям данных потребителей;

ж) методы и средства верификации правильности аппаратно-программной реализации квантовых протоколов, а также практической защищённости конечного изделия от атак на техническую реализацию;

з) апробированные в плане практической безопасности программно-аппаратные решения по интеграции систем КРК в глобальную сетевую инфраструктуру (защищенность систем КРК от сетевых атак, вирусов и т.п.);

и) апробированные в плане практической безопасности решения по интеграции систем КРК с программными и аппаратно-программными СКЗИ;

к) наличие полноценных технических стандартов и требований к системам КРК;

л) наличие эффективной системы экспертной оценки практической безопасности систем КРК, а также СКЗИ с интегрированной подсистемой КРК;

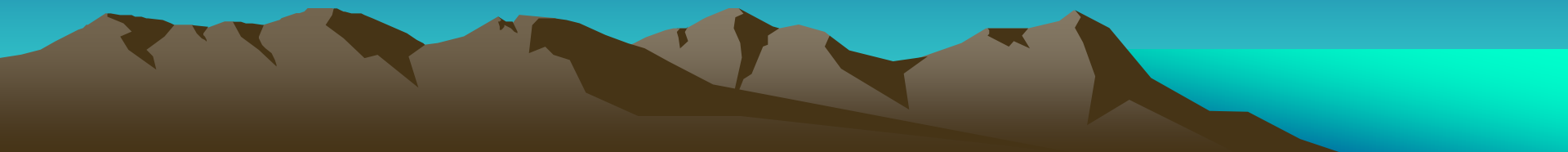
м) наличие полнофункциональных технических реализаций систем КРК и СКЗИ с интегрированной подсистемой КРК, готовых к проведению тематических исследований;

н) наличие экономически эффективных, удовлетворяющих требованиям потребителей и аттестованных по требованиям к безопасности информации опытных образцов СКЗИ с интегрированной подсистемой КРК.

Вопрос №2 для дискуссии

Что на уровне решения математических и других научно-технических задач необходимо решить для внедрения ККС?

- Решение задач, связанных с доказательством стойкости протоколов для ККС
- Решение задач, связанных с гарантированной детерминированной квантовой передачей информации
- Решение задач синтеза стойких ККС
- Решение задач сетевой безопасности для применений ККС



Вопрос №3 для дискуссии

Достаточны ли действующие в РФ нормативные и методические документы для разработки и применения ККС? Что из опыта работы международных (зарубежных) организаций может быть использовано в РФ в области нормативного обеспечения квантовой криптографии?

- Постановление Правительства РФ от 16.04.2012 г. № 313.
- Положение ПКЗ-2005.
- Требования к СКЗИ.
- Стандарты ETSI.
- …

Вопрос №4 для дискуссии

Существуют ли документы регламентирующих государственных институтов в других странах (например, НИСТ США), относящиеся к области квантовой криптографии, и каковы они?

QC in documents of NIST and HS

Cyber Security Division

Transition to Practice Technology Guide 2017

Homeland Security
Science and Technology

2014 Technologies Summary

For additional information about any of the following technologies contact the TTP program at **ST.TTP@hq.dhs.gov**

CodeDNA

Johns Hopkins Applied Physics Laboratory: CodeDNA is a scalable, shareable technology that facilitates community-based defense against malware attacks. It supports crowd-sourcing of information by providing a robust malware identifier (fingerprint) that is deterministic and repeatable for correlating reports, analyses, and other information about attackers, yet cannot be used to re-create the original malware.

For more information, contact
Shaku Harshavardhana, ***Shaku.Harshavardhana@jhuapl.edu***
and Kathleen McGill, ***Kathleen.McGill@jhuapl.edu***

LOCKMA

Massachusetts Institute of Technology–Lincoln Laboratory: Lincoln Open Cryptographic Key Management Architecture (LOCKMA) is a software component that simplifies the task of adding cryptographic protections and underlying key management to software applications and embedded devices such as mobile devices, unmanned vehicles and sensors as well as larger systems. LOCKMA is licensed to several companies for use in government solutions.

For more information,
contact Roger Khazan, ***rkh@ll.mit.edu***

Quantum Security

Los Alamos National Laboratory: Quantum Security is comprised of two technologies: *Velocirandor,* a small, low-cost, deployable solution for the generation of secret random numbers (keys) at high rates, and *Quantum Secured Communications,* which leverages Quantum Key Distribution to replace all of the key management services provided by a public key infrastructure. Velocirandor and Quantum Secured Communications are licensed and available commercially from Whitewood Encryptions Systems.

For more information,
contact Raymond Newell, ***raymond@lanl.gov***

Digital Ants

Pacific Northwest National Laboratory: Digital Ants is a nature-inspired resilient cybersecurity technology designed to protect large enterprise networks and next-generation critical infrastructures. Digital Ants is lightweight and uses automatic learning to reduce the human cost of configuration and supervision. Digital Ants uses minimal network and computational resources.

For more information,
contact David McKinnon, ***david.mckinnon@pnnl.gov***

CryptAC

Massachusetts Institute of Technology–Lincoln Laboratory: CryptAC provides cryptographic access control to enable secure storage of data in public clouds. It presents a seamless view of fine-grained access control and data organization to return control of data security to data owners and separate data security from storage management to enable interoperability with multiple cloud service providers.

For more information,
contact Gene Itkis, ***itkis@ll.mit.edu***

PACRAT

Pacific Northwest National Laboratory: The Physical and Cyber Risk Analysis Tool (PACRAT), a vulnerability and risk analysis software package, blends the methodology and assessment process used in physical and cybersecurity domains to provide a comprehensive assessment of the security strategy. PACRAT has been licensed to Rhino Corp adding capability to its existing products.

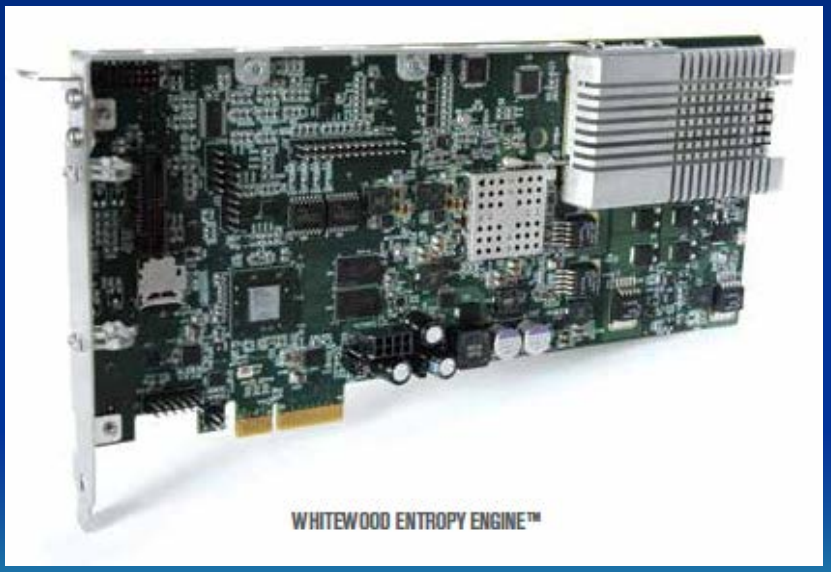
For more information,
contact Doug MacDonald, ***douglas.macdonald@pnnl.gov***

QC in documents of NIST and HS

Quantum Security

Los Alamos National Laboratory: Quantum Security is comprised of two technologies: *Velocirandor*, a small, low-cost, deployable solution for the generation of secret random numbers (keys) at high rates, and *Quantum Secured Communications*, which leverages Quantum Key Distribution to replace all of the key management services provided by a public key infrastructure. Velocirandor and Quantum Secured Communications are licensed and available commercially from Whitewood Encryptions Systems.

For more information,
contact Raymond Newell, ***raymond@lanl.gov***



Вопрос №5 для дискуссии

Какова возможная роль Технического комитета по стандартизации «Криптографическая защита информации» (ТК026) в интересах разработки и применения ККС? Можно ли выделить перспективные направления работ для совмещения ККС и существующих классических протокольных решений (TLS, IKEv2/IPSec), в т.ч. разрабатываемых в ТК026?

- Рекомендации по стандартизации ТК026 «Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации (2016). www.tc26.ru/standard/draft/Принципы_14.11.2016.pdf
- Состояние работ в рамках экспертного совета по криптографии в IETF.
- Рекомендации ТК026, требующие развития. Направления движения.

Вопрос №6 для дискуссии

Существуют ли новые математические задачи, возникающие в связи с появлением квантовых технологий обработки информации, и каковы они?

- Синтез квантовых протоколов и криптографических примитивов (квантовый хэш, квантовая подпись, детерминированная квантовая передача, и т.п.), в том числе с использованием несепарабельных многокубитовых квантовых состояний.
- Оценка криптографических качеств криптографических алгоритмов и протоколов с учетом развития квантовых вычислений и компьютеров.