Уязвимости блокчейн и других новых технологий

Григорий Маршалко

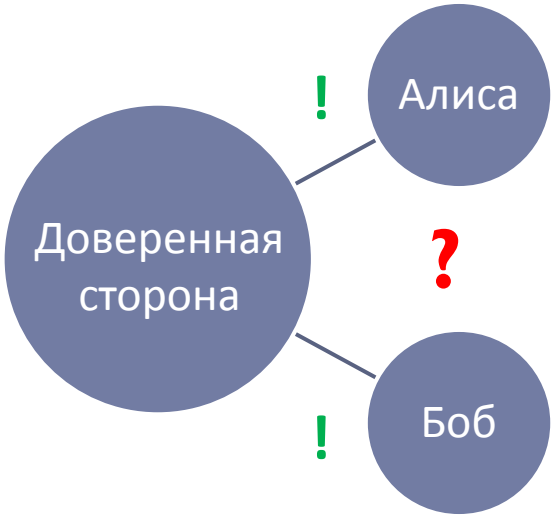
Текущие тренды

Классический блокчейн: замена доверенной стороны

Блокчейн

- Реестр, фиксирующий каждое состояние системы
- Криптография: вычислительно сложно внести изменение в созданную ранее запись
- Проверка: множество идентичных копий реестра
- Ано(псевдо)нимность: защита от утечек персданных

Классика

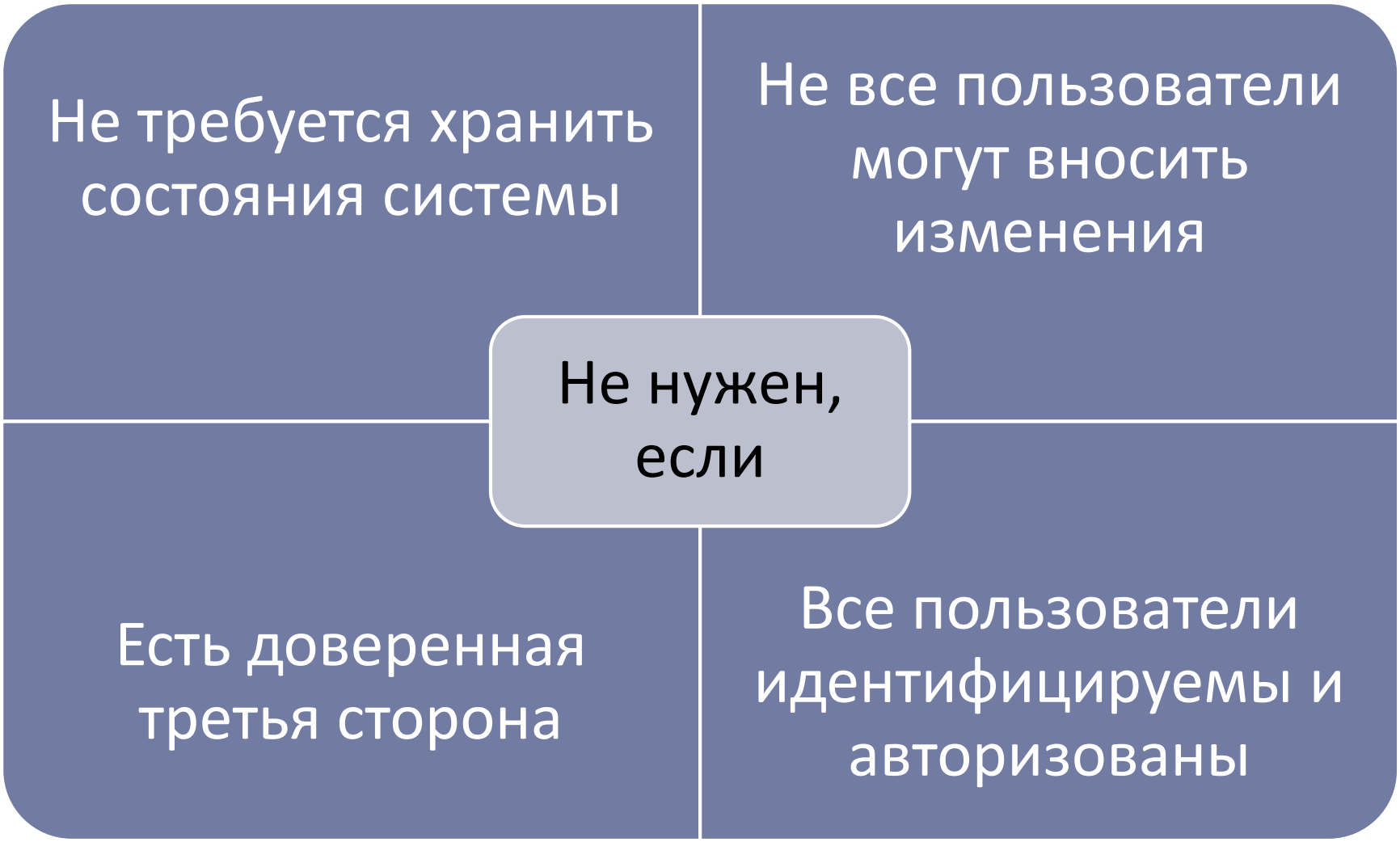


Блокчейн: цифровой и реальный мир

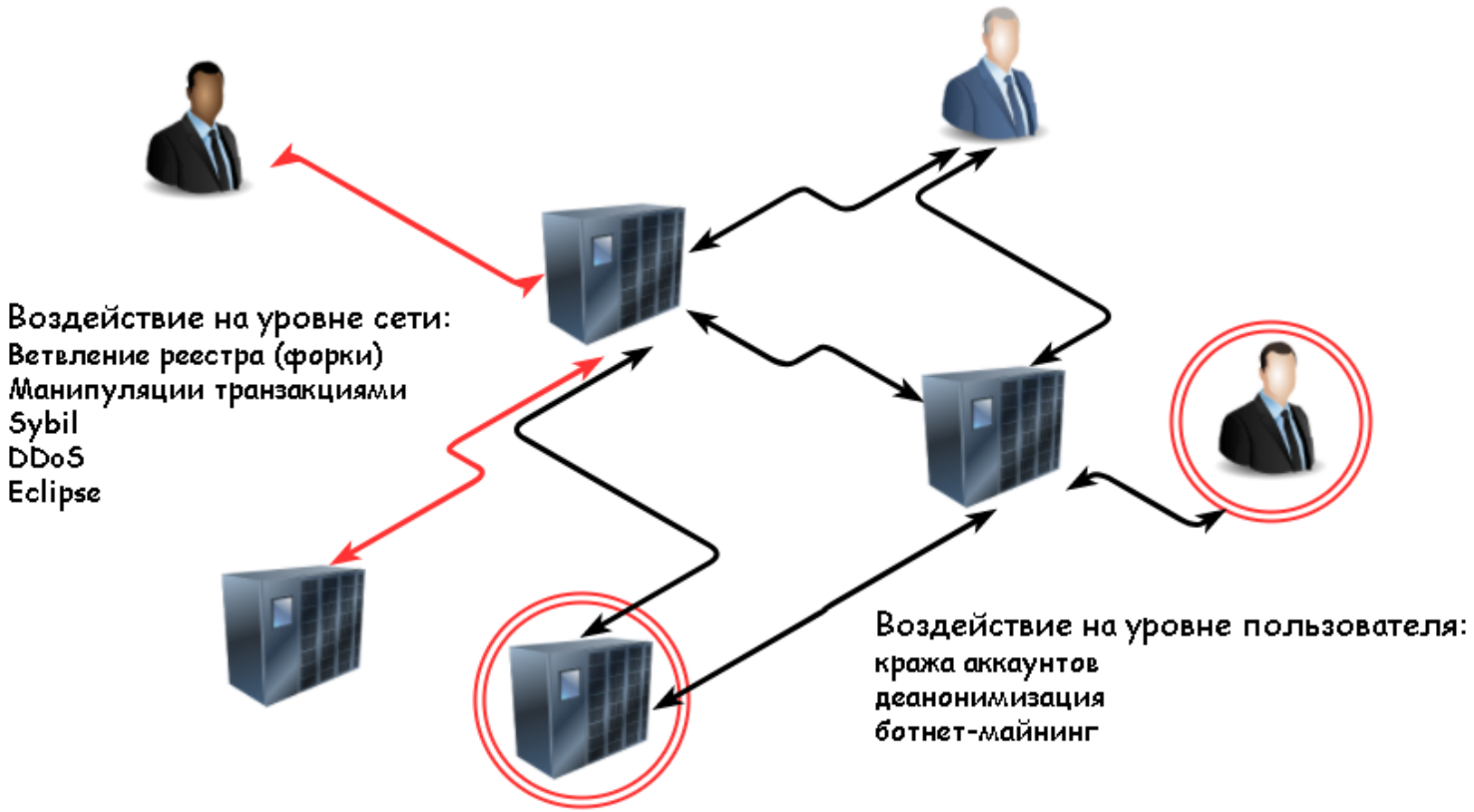
Классический блокчейн создан исключительно для цифровой среды (криптовалюты – работающий пример)

Как его соотнести с окружающей нас средой? (регистрация прав, контроль за перемещением товаров) – ответа пока нет

А нужен ли вам блокчейн?



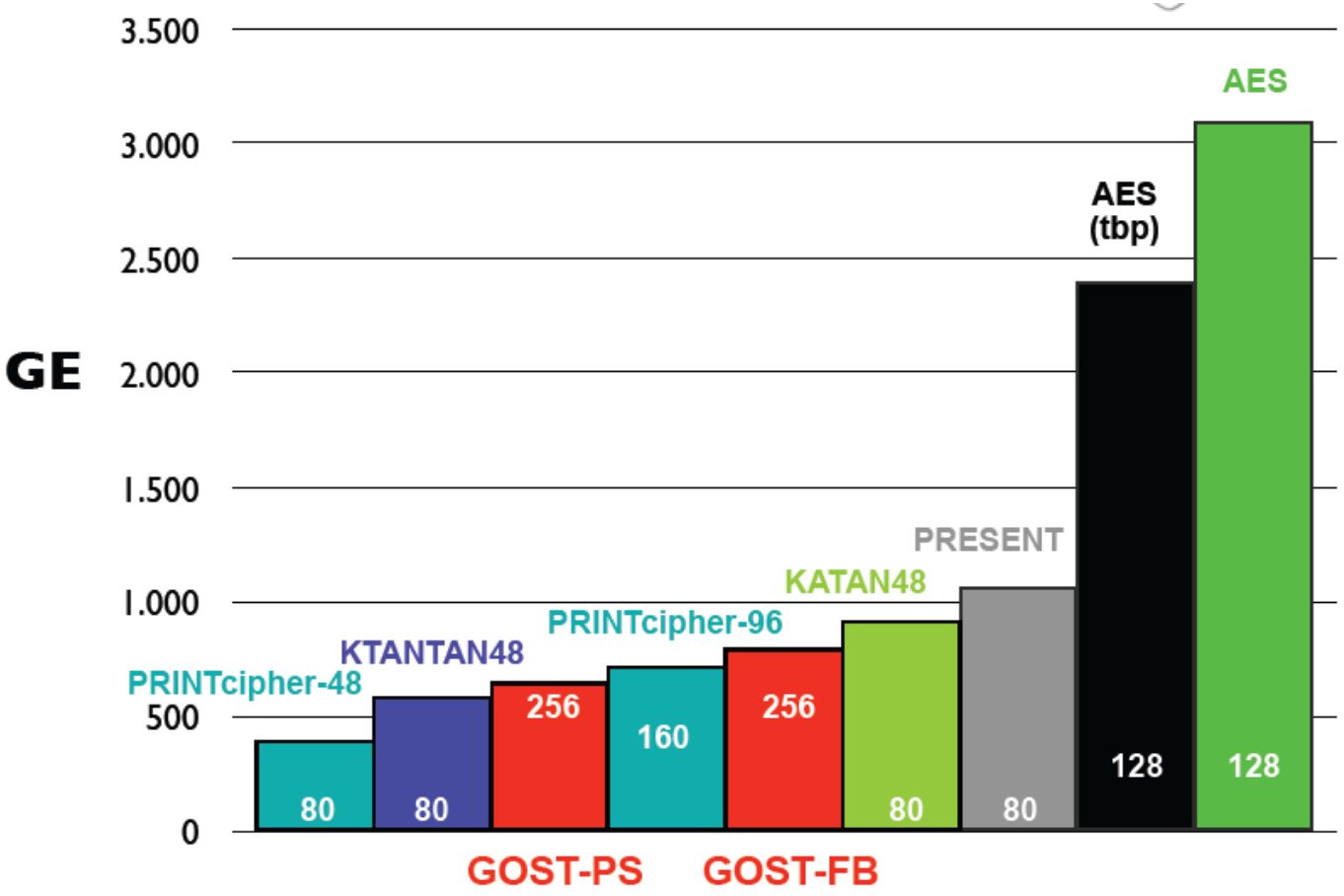
Уязвимости блокчейна



Интернет вещей: проблемы применения классических подходов ИБ

Интернет вещей: российская низкоресурсная криптография

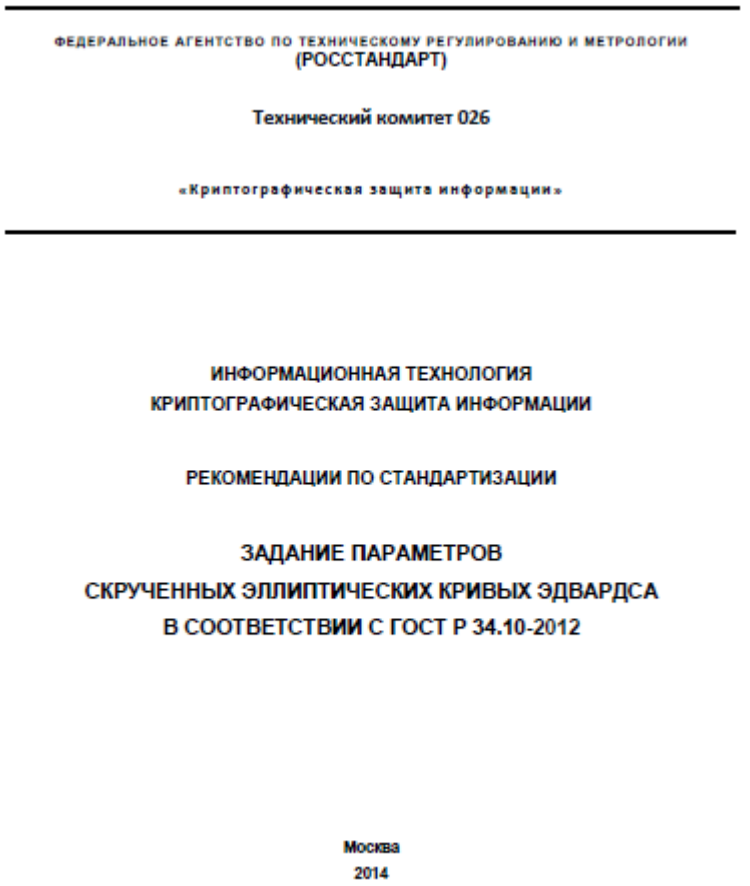
Российский блочный шифр «Магма» ГОСТ Р 34.12-1015
-- один из мировых лидеров среди низкоресурсных алгоритмов



Интернет вещей: российская низкоресурсная криптография

- Задание параметров скрученных эллиптических кривых в форме Эдвардса с ГОСТ Р 34.10-2012

Асимметричная криптография



ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(РОССТАНДАРТ)

Технический комитет 026

«Криптографическая защита информации»

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

ЗАДАНИЕ ПАРАМЕТРОВ
СКРУЧЕННЫХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ ЭДВАРДСА
В СООТВЕТСТВИИ С ГОСТ Р 34.10-2012

Москва
2014

Интернет вещей: российская низкоресурсная криптография

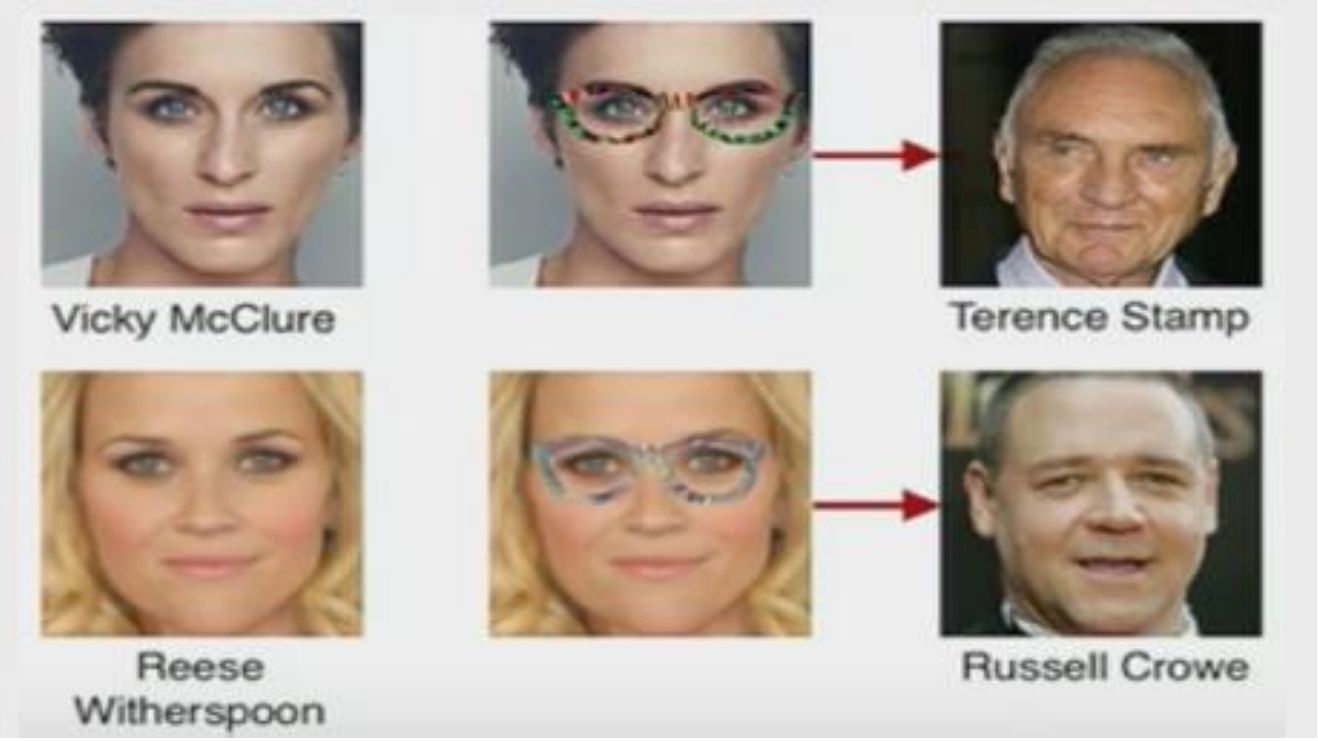
Самая большая проблема: «тяжелые» классические протоколы SSL/TLS/IpSec

Рабочая группа Технического комитета по стандартизации ТК 26 по разработке «легкого» и безопасного протокола для Интернета вещей

Криптографические механизмы для M2M и индустриальных систем

Биометрия: сложные системы с большим числом угроз

Биометрия:развитие методов распознавания позволяет создавать новые методы атак



Квантовая криптография: теория

- Только в 2016 г. удалось соотнести уровни безопасности в квантовой и классической криптографии

О сложности перебора ключей в квантовой криптографии

С. Н. Молотков[1)]

Академия криптографии РФ, 121552 Москва, Россия

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Факультет вычислительной математики и кибернетики МГУ им. Ломоносова, 119991 Москва, Россия

Поступила в редакцию 2 ноября 2015 г.

После переработки 18 января 2016 г.

Доказательства секретности ключей в квантовой криптографии используют в качестве критерия секретности следовое расстояние. В ряде работ высказывались сомнения в том, что данный критерий может быть сведен к критериям, которые используются в классической криптографии. В работе дается ответ на следующий вопрос. Пусть в результате работы системы квантовой криптографии получен ε-секретный ключ, который будет использоваться неоднократно в классических алгоритмах шифрования и про который гарантируется, что $\frac{1}{2}||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon$. Насколько ε-секретный ключ уменьшит число шагов (трудоемкость) перебора по сравнению с использованием идеальных ключей? Показана прямая связь между сложностью полного перебора ключей, который является одним из основных критериев сек-

Criteria of key security

I. M. Arbekov

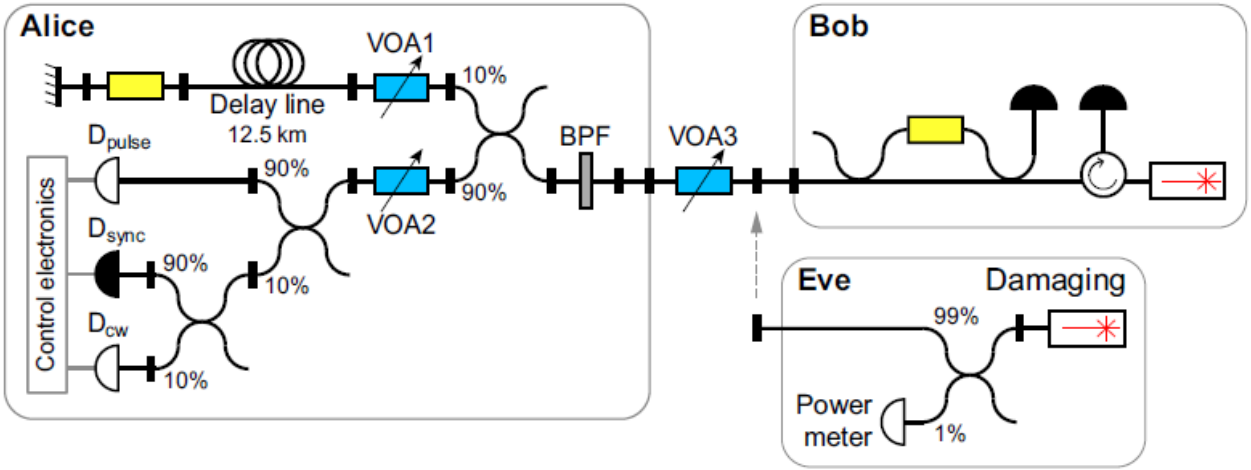
InfoTeCS, OJSC, Moscow

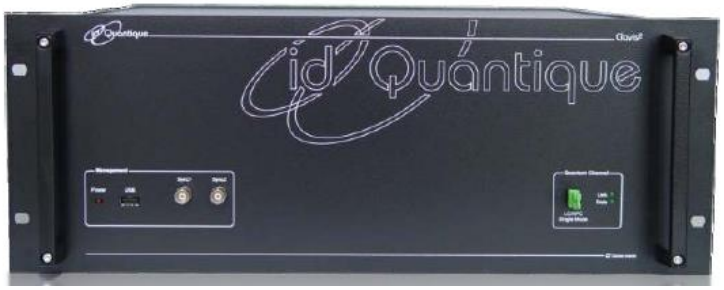
Abstract. We formalize the notion of practical security of the encryption scheme introduced by C.Shannon as “the average amount of work to determine the key. . . ” and define the corresponding practical security of key criterion. A comparison of the proposed criterion with the entropy criterion and the total variance criterion used in the quantum cryptography is given.

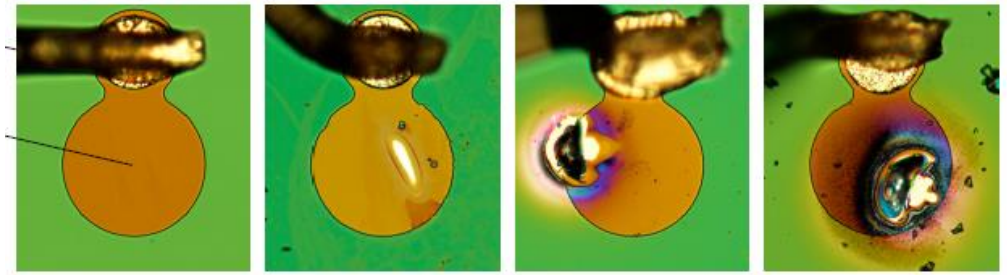
Keywords: models of key generation, key security, brute force attack optimization

Квантовая криптография: практика

- Большинство квантовых криптографических систем крайне уязвимы к атакам в силу несовершенства элементной базы.







Квантовая криптография: сертификация

Временные требования к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну (утверждены в июле 2017 г.)

Вместо эпилога

Эффективная цифровизация возможна при наличии твердого базиса информационной безопасности

Вопросы информационной безопасности необходимо рассматривать уже на этапе проектирования

В цифровом мире недооценка угроз информационной безопасности может разрушить даже самый привлекательный проект

Необходимость внедрения новых технологий, в том числе ИБ, должна оцениваться исходя из экономической целесообразности