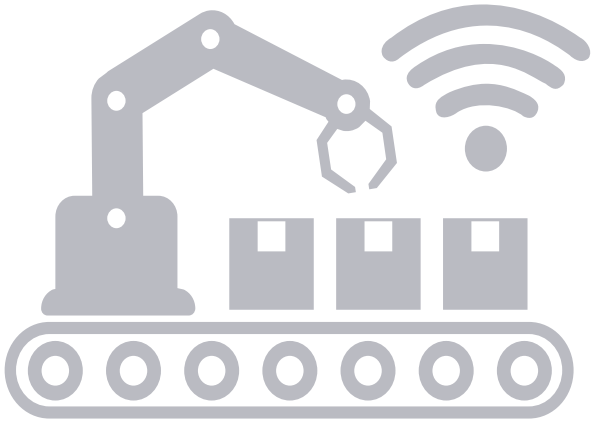
ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Лаборатория Кибербезопасности



ГРУППОВАЯ АУТЕНТИФИКАЦИЯ НА РЕШЕТКАХ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ

Ярмак А.В., Рехвиашвили И.Ш., Александрова Е.Б.

Москва
2020

Кибербезопасность и промышленный Интернет Вещей (IIoT)

- **ТРАНСПОРТ**
- **ЭНЕРГЕТИКА**
- **ПРОИЗВОДСТВО**
- **ЗДРАВООХРАНЕНИЕ**

Факторы, ограничивающие внедрение технологий IIoT*

46 %
ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

35 %
ОТСУТСТВИЕ ЕДИНЫХ СТАНДАРТОВ

*согласно исследованию Morgan Stanley-Automation World Industrial Automation Survey, AlphaWise

СПЕЦИФИКА ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ В КРУПНОМАСШТАБНЫХ ПРОМЫШЛЕННЫХ СИСТЕМАХ

- большое число узлов системы
- распределенность узлов
- разнородность вычислительных возможностей и ролей устройств
- избыточность устройств и динамическая топология сети

Типы устройств в промышленном Интернете Вещей

Анализ данных и управление

Хранение данных (облако)

Сбор данных

Типы устройств с ограниченной вычислительной мощностью в IIoT

Датчики, актуаторы

FPGA 4-, 8-, 16-bit, User Flash Memory 100-2000 Кб

Контроллеры

Arduino Industrial 101: Atheros AR9331 400 МГц, 16 Мб flash, 64 Мб ОЗУ
WISE-5231 от ICP DAS: Cortex-A8 CPU до 1 ГГц, до 4 Гб

Шлюзы

Intel Atom dual core 1.33 ГГц, 2Гб
16-разрядное RISC CPU (до 25 МГц), STM32F407ZE 168 МГц

Одноплатные компьютеры

Raspberry Pi 3: ARM Cortex A53 1.2 ГГц, 1 Гб
DragonBoard 820c: 64-bit Kryo quad-core CPU до 2.15 ГГц, 3Гб ОЗУ, 32 Гб Flash

Протоколы M2M-взаимодействия в IIoT

OPC UA

Механизмы защиты:
профили защиты, TLS/SSL

DDS The Proven Data Connectivity Standard for the IoT

Механизмы защиты:
Контроль доступа, DTLS

MQTT.ORG

Механизмы защиты:
TLS/SSL

CoAP

Механизмы защиты:
DTLS, IPSec

AMQP Advanced Message Queuing Protocol

Механизмы защиты:
TLS/SSL

Возможность внедрения новых алгоритмов	OPC-UA	MQTT	AMQP	DDS	CoAP
На транспортном уровне	+	+	+	+	+
На прикладном уровне		+	+	+	+
В виде плагина				+	
Сложность внедрения	высокая	средняя	средняя	низкая	средняя

Групповая аутентификация в IIoT. Пути решения

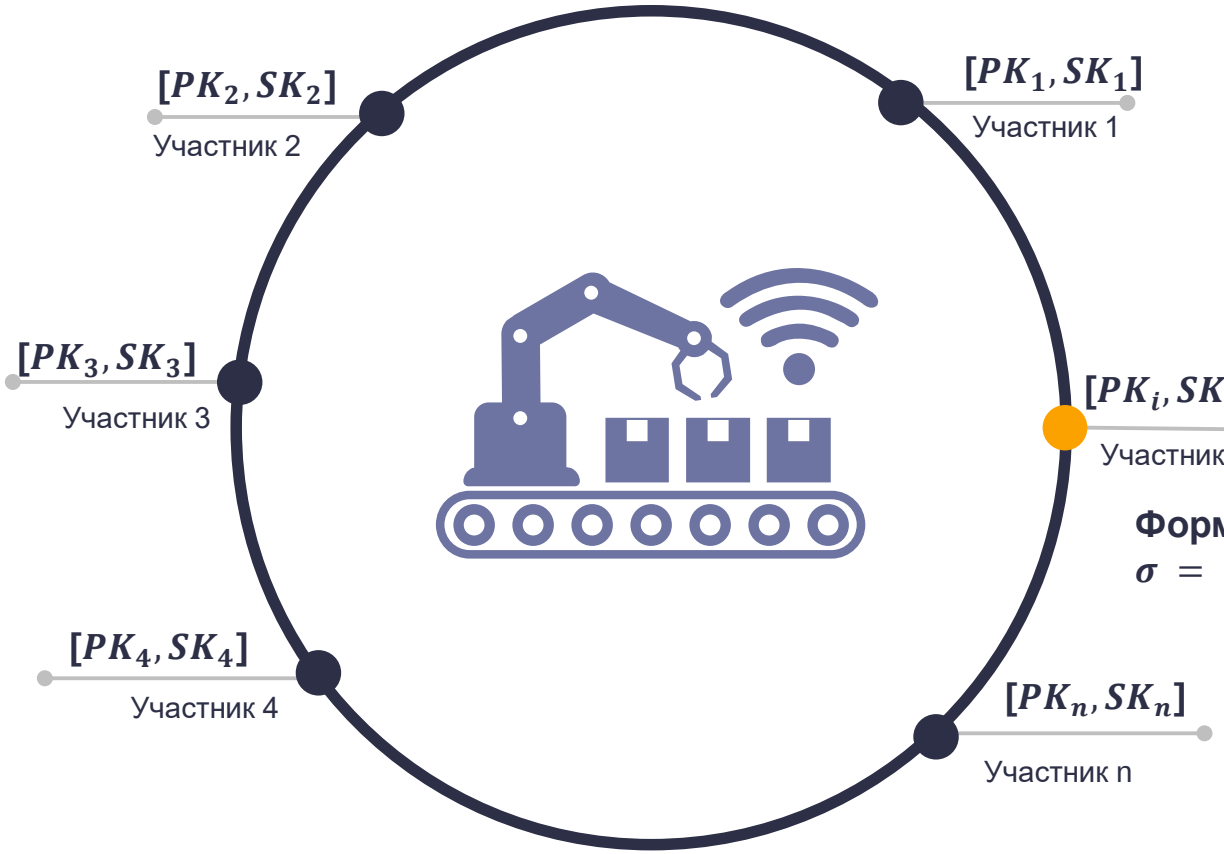
КРИТЕРИИ

- по ролям
- согласно технологическому подпроцессу
- по местоположению
- по вычислительной мощности и т.п.

Особенности подписи	**Групповая подпись**	**Кольцевая подпись**	**Пороговая подпись**	**Коллективная подпись**
Количество подписывающих	Один участник	Один участник	t участников, где t – пороговое значение	Все участники группы
Доверенная сторона	Требуется (выпускающий менеджер, раскрывающий менеджер)	Не требуется	Требуется при разделении секрета, совмещении частичных подписей	Не требуется
Возможность установления личности подписывающих	Только при участии раскрывающего менеджера	Нет	Нет	Да

Кольцевая подпись

Кольцевая подпись – механизм групповой аутентификации, обеспечивающий полную анонимность узлов в рамках группы



Формирование подписи

$\sigma = Ring\_sign_{SKi}(m, PK1, PK2, \dots, PKn)$

m, σ

Проверка подписи

$Ring\_verify(m, \sigma)$

Проверяющий

$PK1,$
$PK2,$
$\dots$
PKn

Сертификат кольца

Решетки как математический аппарат для построения схем аутентификации

ЭФФЕКТИВНОСТЬ НА УСТРОЙСТВАХ С ОГРАНИЧЕННОЙ МОЩНОСТЬЮ

Известны реализации решеточных подписей для малоресурсных устройств

Схема	Устройство	CPU	MHz	Циклы	Время, мс	Память (KB)
***BLISS-128**	ATxmega128	8-bit	32	Подпись 10,156,247 Проверка 2,760,244	317.4 86.3	18.4
****Falcon-512**	ARM Cortex-M4F	32-bit	24	Подпись 80,503,242 Проверка 530,900	479 3.2	64

*Xu R. et al. Lighting the way to a smart world: Lattice-based cryptography for internet of things

**Oder T. et al. Towards practical microcontroller implementation of the signature scheme Falcon

КВАНТОВЫЙ КОМПЬЮТЕР

Необходимость поиска новых математических задач, устойчивых к атакам на квантовом компьютере

НЕБОЛЬШАЯ ДЛИНА ПАРАМЕТРОВ ПО СРАВНЕНИЮ С ДРУГИМИ ПОСТКВАНТОВЫМИ КРИПТОСИСТЕМАМИ

Среди подписей-кандидатов конкурса NIST решеточные схемы имеют наименьшую длину параметров

Схема	Длина закрытого ключа, байт	Длина открытого ключа, байт	Длина подписи
Falcon	1852	897	617
qTESLA	1216	1504	1376

СХЕМА КОЛЬЦЕВОЙ ПОДПИСИ НА РЕШЕТКАХ

В основе схемы, представленной в работе Wang S. «Lattice-based ring signature scheme under the random oracle model», лежит вычислительно трудная задача поиска вектора по норме: для заданной матрицы $A \in \boldsymbol{Z}_q^{n\times m}$ найти вектор $\boldsymbol{v} \in \boldsymbol{Z}^m \backslash \{0\}$ такой, что $A\boldsymbol{v} = \boldsymbol{0}$ и $\|\boldsymbol{v}\| \leq \beta$ для некоторого заданного β.

Алгоритм генерации ключей $\boldsymbol{Ring\_gen}$: генерирует пару (pk_i, sk_i). Использует процедуры $TrapGen$ и $SamplePr$ для генерации матриц $\boldsymbol{A}_i \in \boldsymbol{Z}_q^{n\times m}$ (ключ проверки) и $\boldsymbol{S}_i \in \boldsymbol{Z}_q^{m\times k}$(ключ подписи), а также матрицы $\boldsymbol{T} = \boldsymbol{A}_i\boldsymbol{S}_i$.

Проблемы в существующих схемах кольцевой подписи

ДИНАМИЧЕСКОЕ КОЛЬЦО

При формировании подписи каждый узел должен иметь список актуальных открытых ключей других участников

СТАТИЧЕСКОЕ КОЛЬЦО

Необходимо обеспечить отзыв права подписи без перегенерации ключей остальных узлов

Сравнение механизмов отзыва

Механизм отзыва	Влияние на размер		Влияние на время		Обновления	
	ключей	подписи	формирования подписи	проверки подписи	для автора подписи	для проверяющего
с перевыпуском ключей	–	–	–	–	O(n)	O(1)
с черным списком	–	O(n)	O(n)	O(n)	O(n)	O(n)
локальный для проверяющего	–	–	–	O(n)	–	O(n)
со связыванием	O(1)	O(1)	O(1)	–	–	–

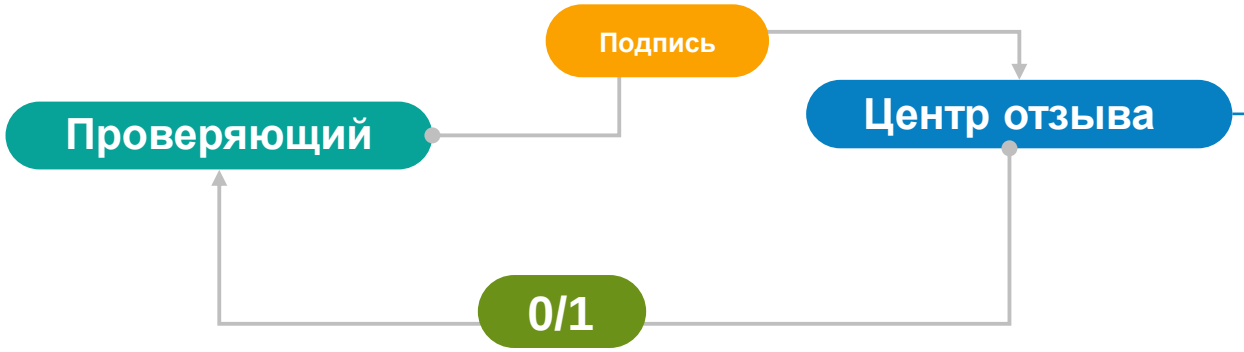
n – число участников кольца

Кольцевые подписи с контролируемой связываемостью

В схему кольцевой подписи вводится менеджер связывания, обладающий возможностью определить, были ли две подписи сформированы одним и тем же пользователем, без возможности идентифицировать этого пользователя

Применение свойства связывания для отзыва права подписи

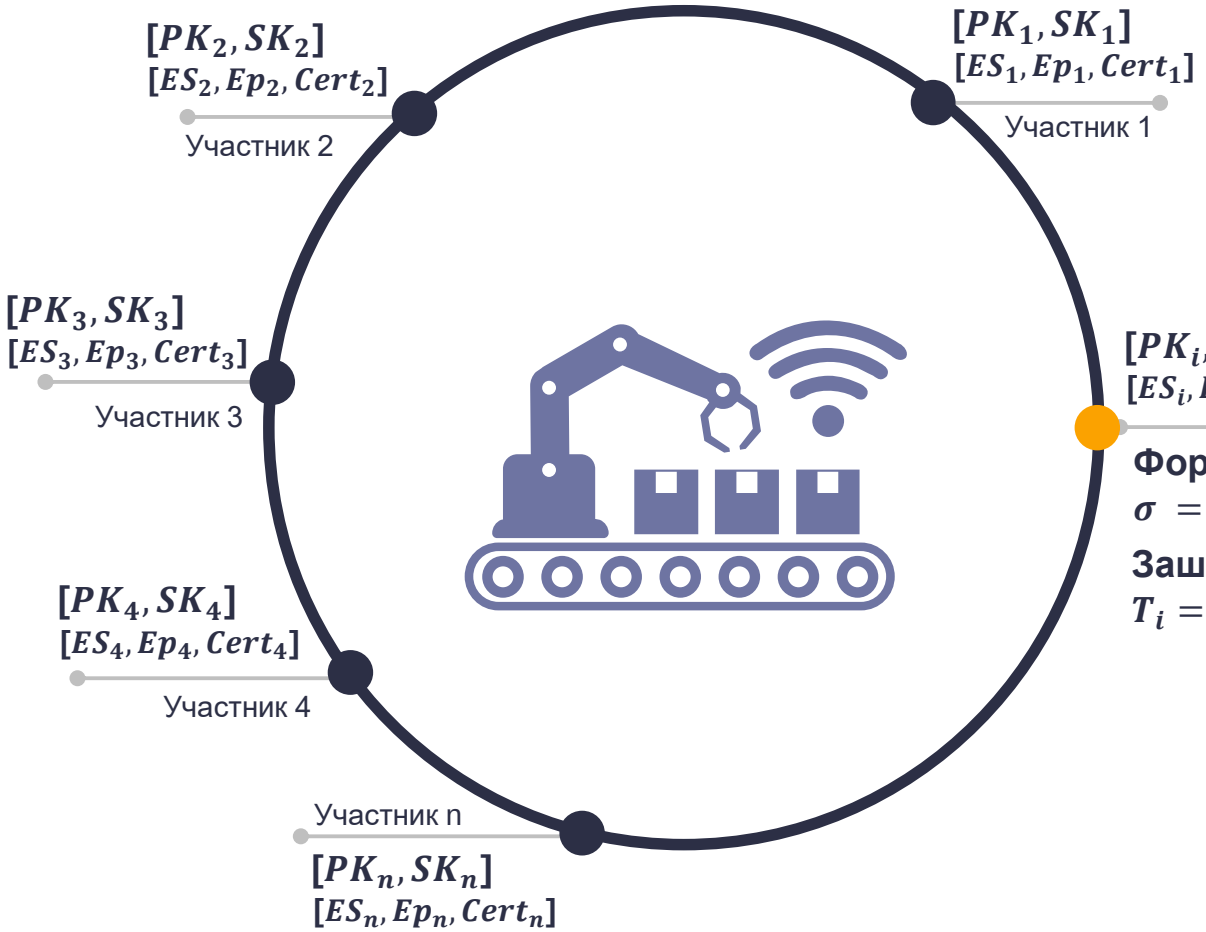
Центр отзыва хранит подписи отозванных участников и, владея ключом связывания, определяет, были ли две подписи сформированы одним автором



Шифрование с открытым ключом с тестами на равенство PKEET

Позволяет по двум шифртекстам определить, зашифровывают ли они один и тот же текст, не раскрывая его содержания

Схема кольцевой подписи с отзывом со связыванием

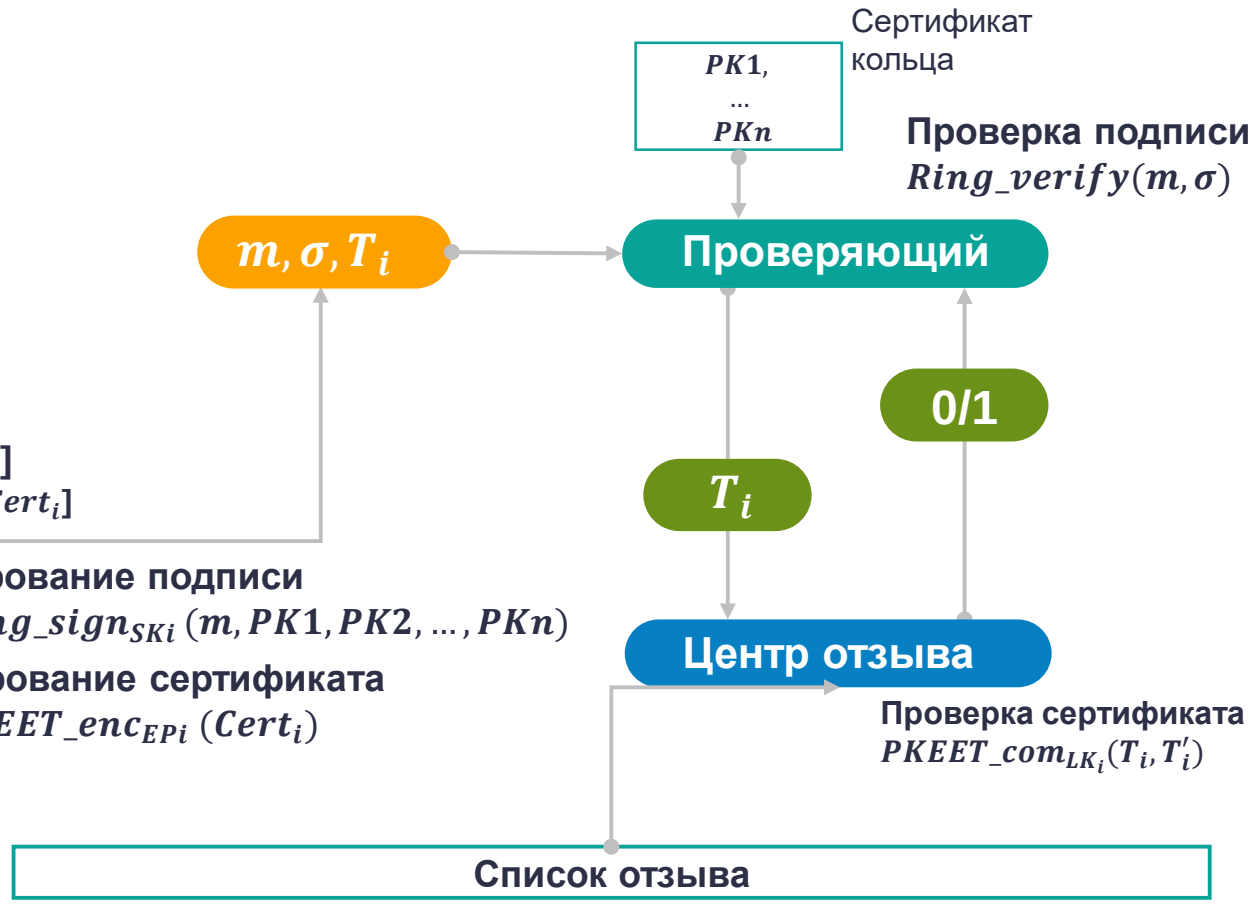


Формирование подписи

$\sigma = Ring\_sign_{SKi}(m, PK1, PK2, \dots, PKn)$

Зашифрование сертификата

$T_i = PKEET\_enc_{EPi}(Cert_i)$



Черный список:

+ Более эффективный поиск за счет меньшего размера списка

– Требует дополнительных вычислений от автора подписи и проверяющего для доказательства того, что зашифрованный сертификат действителен

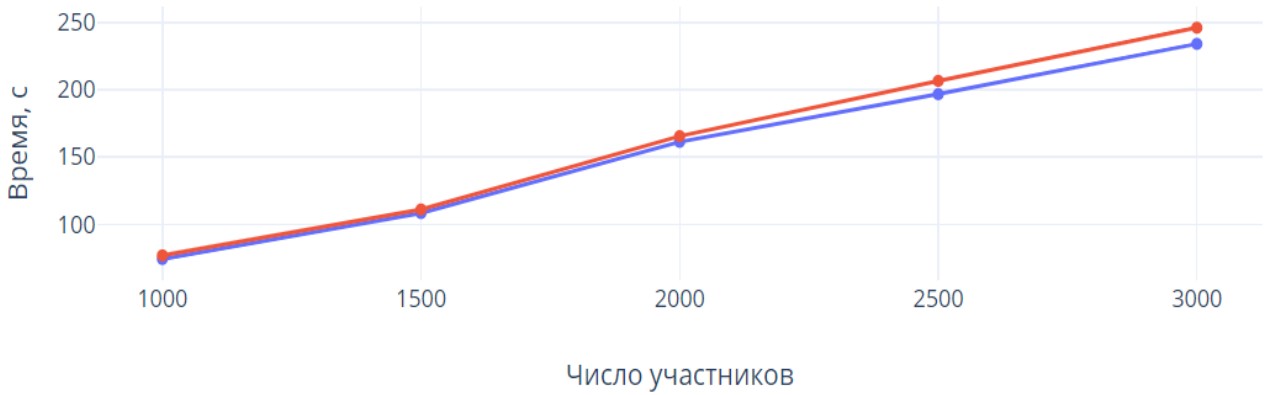
Белый список:

+ Не требует дополнительных вычислений от автора подписи или проверяющего

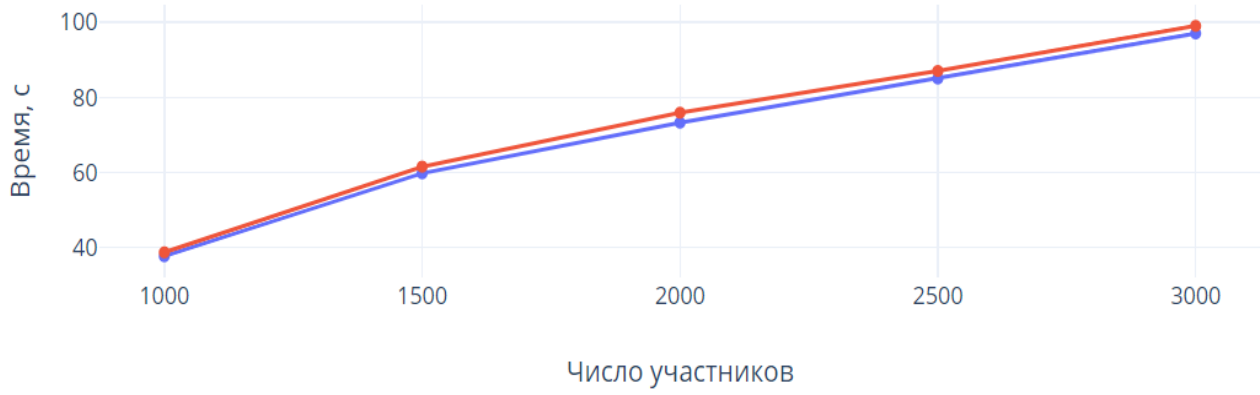
– Неэффективен для схем с большим количеством активных участников

Оценка времени работы разработанной схемы

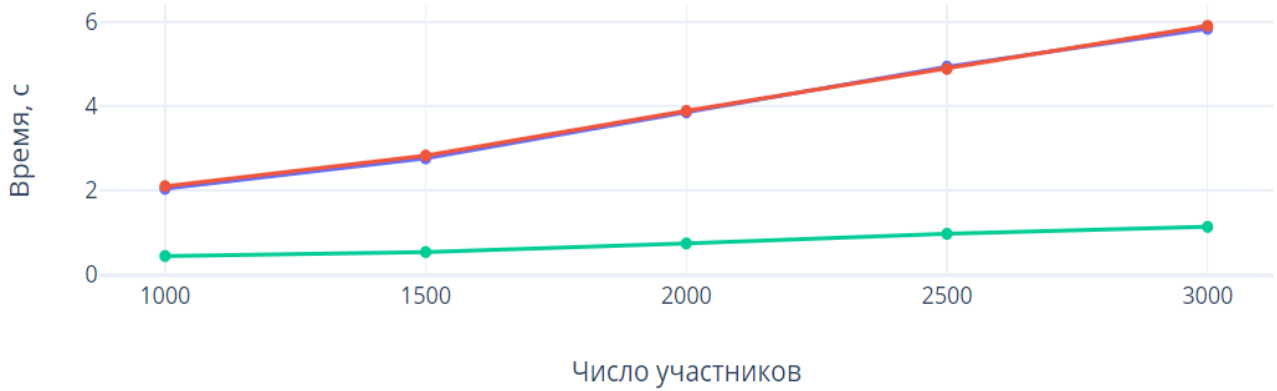
Генерация ключей



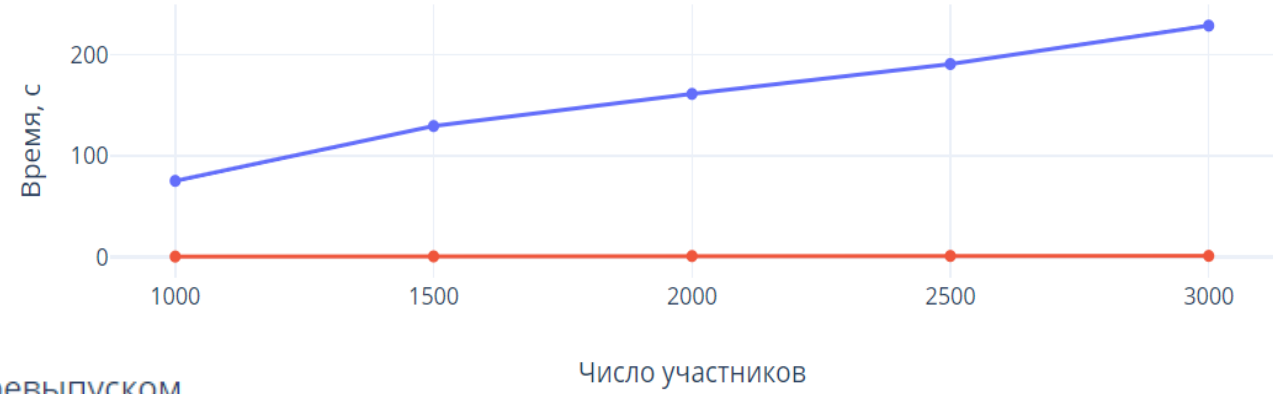
Формирование подписи

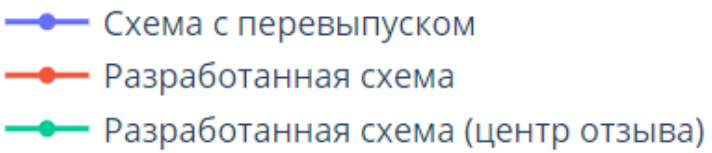


Проверка подписи



Отзыв права подписи

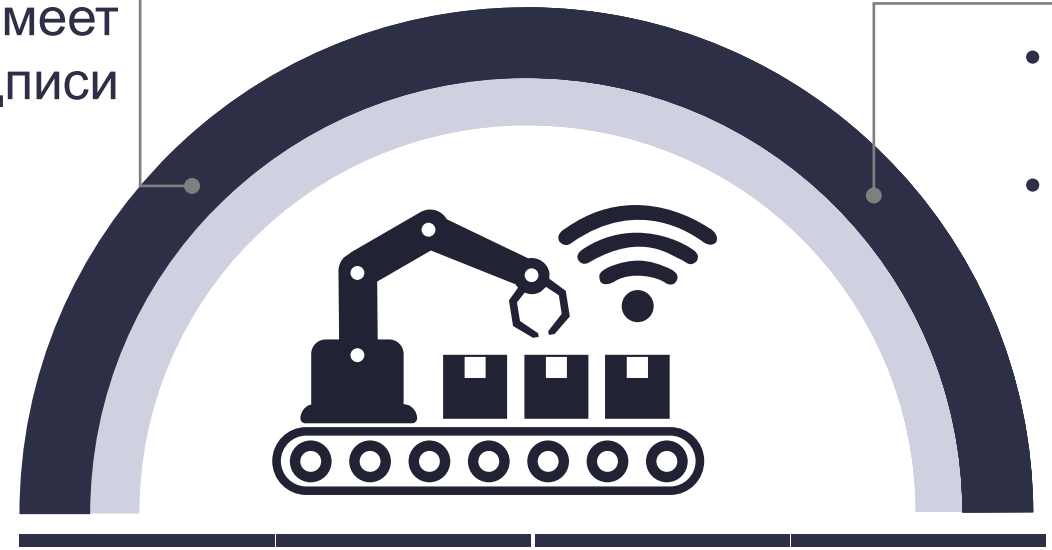




Заключение

Решеточная схема кольцевой подписи

Выбранная схема имеет наименьший размер подписи



Механизм отзыва со связыванием

- не требует обновлений для пользователей
- позволяет производить проверку подписи за время, не зависящее от списка отзыва

Увеличение скорости вычислений

Использование online/offline-вычислений, аутсорс-вычисления

Обеспечение безопасности в случае компрометации центра отзыва

Разделение ключа связывания между несколькими центрами связывания с помощью (t, k)-пороговой схемы разделения секрета

Лаборатория кибербезопасности

г. Санкт-Петербург
ул. Гжатская д. 21, лит. Г

+7 (812) 535-88-84
info@cyberslab.ru

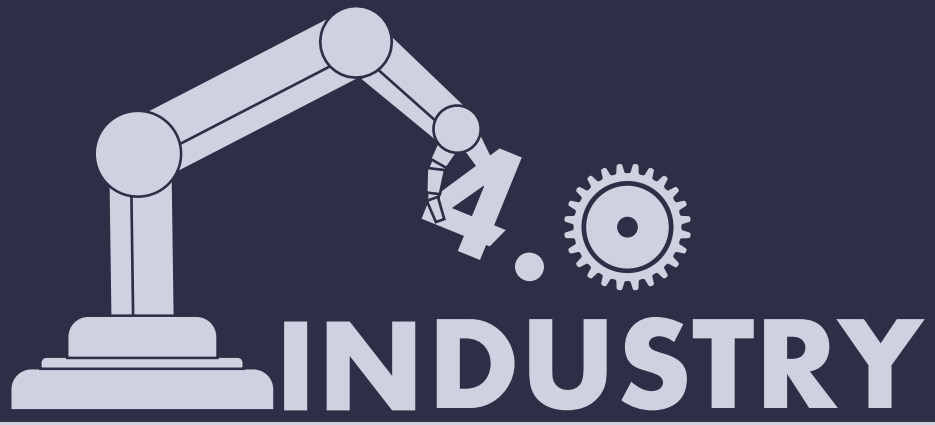
Ярмак
Анастасия Викторовна

yarmak.av@ibks.spbstu.ru

Высшая школа кибербезопасности и защиты информации СПбПУ Петра Великого

г. Санкт-Петербург
Главный учебный корпус, к. 173
Политехническая ул., 29

+7 (812) 552-76-32



Спасибо за внимание!