КОД безопасности

MIPT

21 марта 2024 г.

Электронные цифровые криптографические пороговые подписи

Курочкин А.В.

kurochkin.av@phystech.edu

Тема доклада

Рассказать про пороговые подписи, их недостатки, преимущества
и получить обратную связь о целесообразности их внедрения в банковскую сферу.

Сказка о тройке: «Говорят, говорят, и сами не знают, что говорят. . . »

Что такое пороговая подпись формально?

Протокол пороговой подписи (пороговая подпись) — протокол цифровой подписи, в котором подписывающий заменяется любой правомочной коалицией участников таким образом, что корректная подпись может быть сформирована только при участии всех членов коалиции.

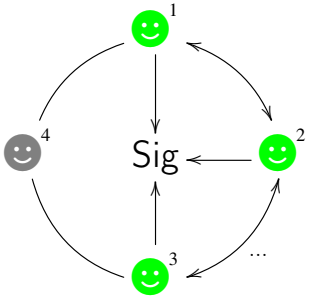
Что такое цифровая подпись?

Для того, чтобы перейти к классической криптографической подписи нажмите:

▸ Открыть воспоминания

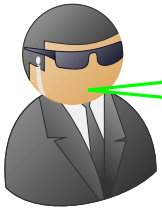
Что такое пороговая подпись «простым» языком?

Пусть есть $n \in \mathbb{N}$ участников протокола, и параметр $t \in \overline{1, n}$ который называется **порогом**. Тогда пороговой (n, t) подписью называется такая подпись которую может сформировать любая группа участников протокола, состоящая из t или более участников.



Пороговая $(3, 4)$ подпись

Трудно быть богом: «Назад идти нельзя»



Общая модель пороговой подписи:

- *проверяемое разделение секрета*
- *выявление нарушителей*
- *формирование подписи*

Более подробно:

КОД безопасности

«В отделе Вечной Молодости после долгой и продолжительной болезни скончалась модель бессмертного человека.»

Общая математическая модель пороговой подписи:

Проверяемое разделение секрета	*Схема разделения секрета Шамира*
	Проверяемое разделение секрета Фелдмана
	Генерация ключа Педерсена
Выявление нарушителей	*Проверяемое разделение секрета Фелдмана*
	Доказательства с нулевым разглашением
Формирование подписи	*Проверяемые случайные функции*
	Адаптированные криптографические подписи

Области применения пороговых подписей

- аутентификация финансовых транзакций в криптовалютах;
- обеспечение безопасности информации, хранимой в системах данных;
- подписание сетевого консенсуса;
- подписание смарт-контрактов в блокчейн структурах, например в Ethereum;

Подробнее о применении пороговых подписей

Предположим, что некоторым электронным кошельком владеют 5 человек и, что для любого перевода с этого кошелька нужны как минимум подписи 3-х владельцев.

Каждая подпись это отдельная транзакция и для того, чтобы верифицировать подписи, и как следствие совершить необходимое действие с переводом денег с кошелька, необходимо оплатить добавление трёх транзакций в блокчейн.

Вместо вычисления 3-х подписей владельцы кошелька могут вычислить одну пороговую подпись, это одна транзакция, добавление которой в блокчейн требует меньшего количества затрат.

КОД безопасности

Великий Гэтсби: «...вспомни, что не все люди на свете обладают теми преимуществами, которыми обладал ты.»

Преимущества пороговых подписей

Экономически выгодное применения в некоторых блокчейн-задачах;

Анонимность с точностью до группы подписантов;

Для подписи необязательно присутствие всех подписантов.

Недостатки пороговых подписей

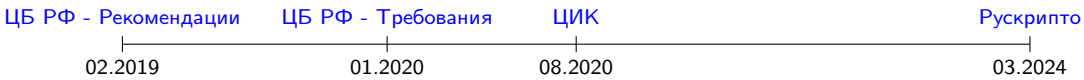
В общем случае пороговые подписи «тяжелы» в реализации;

В общем случае не эффективны;

В общем случае сложные конструкции.

О дивный новый мир: «Как бы интересно стало жить на свете, если бы можно было отбросить заботу о .... *криптографии*»

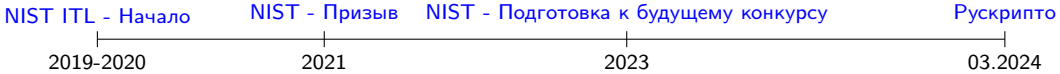
Ситуация в Российской Федерации в области пороговых механизмов.



- рекомендуется использовать аппаратные модули безопасности (HSM) сертифицированные ФСБ РФ;
- требуется использовать пороговые механизмы для защиты ключей в HSM;
- дистанционное голосование в котором реализовано проверяемое разделение секрета.

О дивный новый мир: «Как бы интересно стало жить на свете, если бы можно было отбросить заботу о .... *криптографии*»

Ситуация за рубежом в области пороговых механизмов.

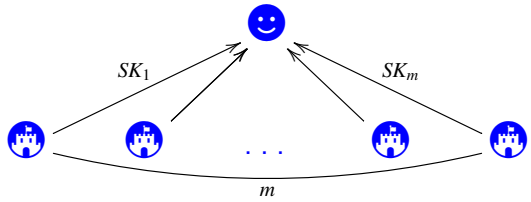


- документ «Threshold Schemes for Cryptographic Primitives Challenges and Opportunities in Standardization and Validation of Threshold Cryptography»;
- документ «Call 2021a for Feedback on Criteria for Threshold Schemes»;
- документ «NIST First Call for Multi-Party Threshold Schemes 13».

Идея для дальнейшего применения :

Формирование сертификатов несколькими организациями.

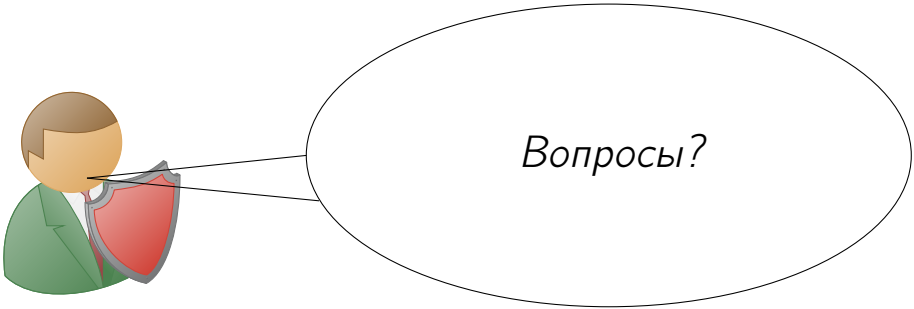
Для формирования публичного ключа и сертификата физическое лицо может обратиться в несколько организаций



Заключение

Предлагается обсудить актуальность развития пороговых подписей с целью дальнейшего внедрения в банковскую сферу.

В случае положительного ответа на предыдущий вопрос, предлагается выяснить степень развития и внедрения.


Вопросы?