



5 июня 2025 г.

Пороговые подписи и их приложения: Three green icons: a document with a checkmark, a stylized signature, and a key.



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

Что обсудим? 



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

Что обсудим? 

- ▶ Кратко, что такое пороговые механизмы (подписи) и зачем они нужны;



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

Что обсудим? 

- ▶ Кратко, что такое пороговые механизмы (подписи) и зачем они нужны;
- ▶ Пороговые аналоги Schnorr, ГОСТ, ECDSA;



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

Что обсудим?

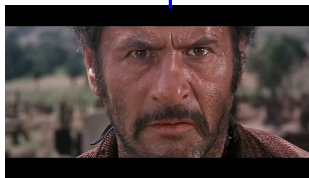
- ▶ Кратко, что такое пороговые механизмы (подписи) и зачем они нужны;
- ▶ Пороговые аналоги Schnorr, ГОСТ, ECDSA;
- ▶ Открытые вопросы.



«Понять - значит упростить»

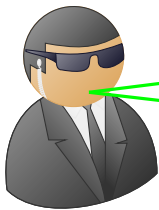
Что такое пороговая подпись «простым» языком? 🎓

Пороговой (n, t) подписью называется такая подпись которую может сформировать любая группа, состоящая из t или более участников протокола. Проверить подпись может любой желающий.





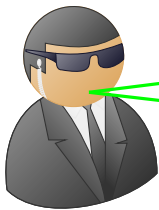
Трудно быть богом: «Назад идти нельзя»



А зачем?



Трудно быть богом: «Назад идти нельзя»

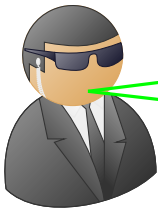


А зачем?

Для участников которые недоверяют друг другу



Трудно быть богом: «Назад идти нельзя»



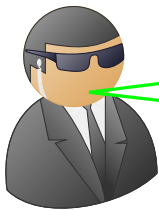
А зачем?

Для участников которые недоверяют друг другу

Для защиты от атак по побочным каналам



Трудно быть богом: «Назад идти нельзя»



А зачем?

Для участников которые недоверяют друг другу

Для защиты от атак по побочным каналам

Для выполнения требований



«Иногда не меняя ничего — самый эффективный способ изменить всё..»

Пороговая подпись Шнорра:

Доля подписи: $k_i + \lambda_i \cdot s_i \cdot e$

λ_i - нужный коэффициент

k_i - случайное число

s_i - доля ключа

e - хэш сообщения



«Иногда не меняя ничего — самый эффективный способ изменить всё..»

Пороговая подпись ГОСТ:

Доля подписи: $R \cdot \lambda_i \cdot s_i + k_i \cdot e$

λ_i - нужный коэффициент

k_i - случайное число, $R = (\sum k_i)_x$

s_i - доля ключа

e - хэш сообщения



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

Пороговая подпись ECDSA:

<i>Доля подписи: $(*) \cdot R \cdot \lambda_i \cdot f(s_i) + k_i \cdot e$</i>	<i>λ_i - нужный коэффициент</i>
	<i>k_i - случайное число, $R = (\sum f(k_i))_x$</i>
	<i>s_i - доля ключа</i>
	<i>e - хэш сообщения</i>



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

Пороговая подпись ECDSA:



λ_i - нужный коэффициент

k_i - случайное число, $R = (\sum f(k_i))_x$

s_i - доля ключа

e - хэш сообщения



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

Открытые вопросы 

- ▶ Вместе подробно изучить пороговые механизмы;



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

Открытые вопросы

- ▶ Вместе подробно изучить пороговые механизмы;
- ▶ Пороговые блочные алгоритмы шифрования;



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

Открытые вопросы

- ▶ Вместе подробно изучить пороговые механизмы;
- ▶ Пороговые блочные алгоритмы шифрования;
- ▶ Полноценный, масштабируемый пороговый ГОСТ (обновление ключей, выявление нарушителей, постквантовый согласованная деривация и так далее);



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

Открытые вопросы

- ▶ Вместе подробно изучить пороговые механизмы;
- ▶ Пороговые блочные алгоритмы шифрования;
- ▶ Полноценный, масштабируемый пороговый ГОСТ (обновление ключей, выявление нарушителей, постквантовый согласованная деривация и так далее);
- ▶ Агрегируемые пороговые мультиподписи;



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

Открытые вопросы

- ▶ Вместе подробно изучить пороговые механизмы;
- ▶ Пороговые блочные алгоритмы шифрования;
- ▶ Полноценный, масштабируемый пороговый ГОСТ (обновление ключей, выявление нарушителей, постквантовый согласованная деривация и так далее);
- ▶ Агрегируемые пороговые мультиподписи;
- ▶ Криптоанализ, криптоанализ и еще раз криптоанализ.



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

Открытые вопросы

- ▶ Вместе подробно изучить пороговые механизмы;
- ▶ Пороговые блочные алгоритмы шифрования;
- ▶ Полноценный, масштабируемый пороговый ГОСТ (обновление ключей, выявление нарушителей, постквантовый согласованная деривация и так далее);
- ▶ Агрегируемые пороговые мультиподписи;
- ▶ Криптоанализ, криптоанализ и еще раз криптоанализ.
- ▶ Нормативные документы.