О стандартизации в Российской Федерации схемы подписи вслепую

Алексеев Евгений Константинович,
к.ф.-м.н., Академия криптографии Российской Федерации,
начальник отдела криптографических исследований ООО «КРИПТО-ПРО»,
эксперт РОСЭУ

Ахметзянова Лилия Руслановна, к.ф.-м.н., ООО «КРИПТО-ПРО»,

Бабуева Александра Алексеевна, ООО «КРИПТО-ПРО»

КРИПТОПРО

PKI-Форум Россия 2022

Мотивация

ноябрь 2020 г

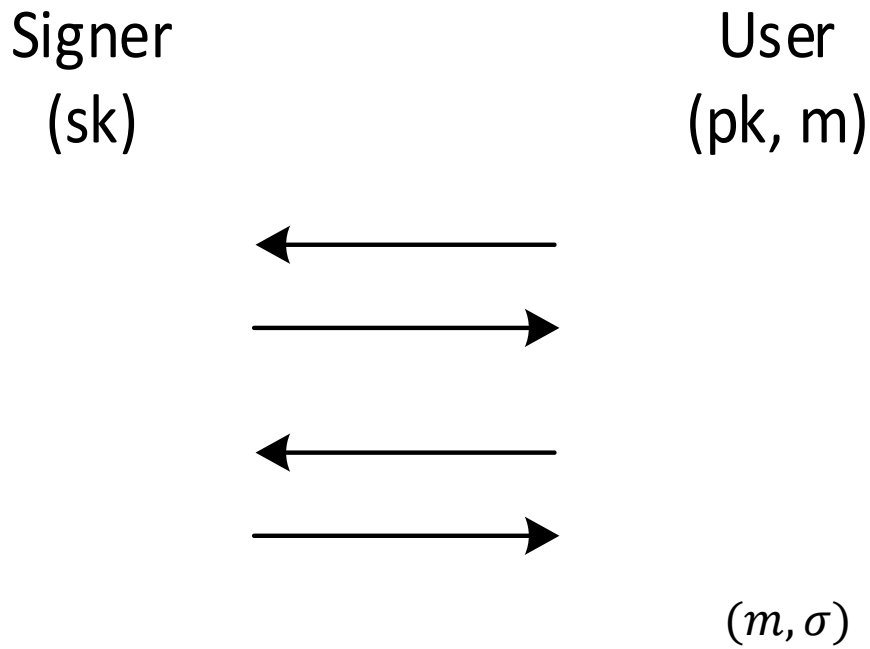
начало разработки МР «Протоколы формирования и проверки электронной подписи вслепую» в РГ СКАиП ТК26

июль 2022 г

сформирован и отправлен на экспертизу пакет документов

Сравнение с электронной подписью

- По процессам:
  - Создание ключей – **алгоритм**
  - Формирование подписи – **интерактивный протокол**
  - Проверка подписи – **алгоритм**
- По свойствам:
  - **Неподделываемость**
  - **Неотслеживаемость**



Свойства безопасности

неподделываемость
(unforgeability)

клиент может сформировать валидную подпись только в результате **успешного** взаимодействия с подписывающим

противник – клиент

неотслеживаемость
(blindness)

подписывающий не может связать сформированную клиентом пару (сообщение, подпись) с конкретным логом работы протокола

противник – подписывающий

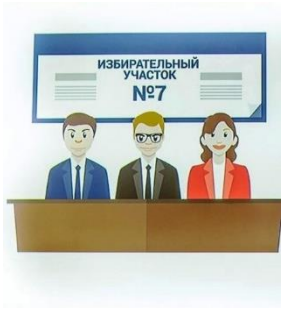
КРИПТОПРО

Область применения

- системы электронных платежей
- системы дистанционного электронного голосования
- … другие приложения, где надо обеспечивать анонимность пользователей

Неотслеживаемость: пример (голосование)

Подписывающий не может связать полученную клиентом пару (m, σ) с конкретным логом работы протокола



лог работы протокола

авторизованная зона

m – бюллетень

σ – подпись, полученная вслепую

(бюллетень, σ)

анонимная зона

КРИПТОПРО

Требования к перспективным схемам

- Стандартные базовые механизмы (эллиптические кривые, хэш-функция)
- Неподделываемость
- Неотслеживаемость
- Наличие формальных обоснований стойкости (в предположении сложности стандартных задач)
- Эффективность (не более 2х раундов, кол-во вычислений)

А что за рубежом?

- IETF: draft-irtf-cfrg-rsa-blind-signatures-04
  - ✓ схема подписи вслепую RSA
  - ✓ на стадии разработки

- ISO: ISO/IEC 18370-1:2016 «Information technology — Security techniques — Blind digital signatures»
  - ✓ 3 схемы подписи вслепую
  - ✓ ни одна схема не обеспечивает требуемые свойства безопасности

Три перспективные схемы

- Схема Абе

  Abe M. «A secure three-move blind signature scheme for polynomially many signatures», 2001

- Схема Шаума-Педерсена (Брандса)

  Chaum D., Pedersen T. P. «Wallet databases with observers», 1992

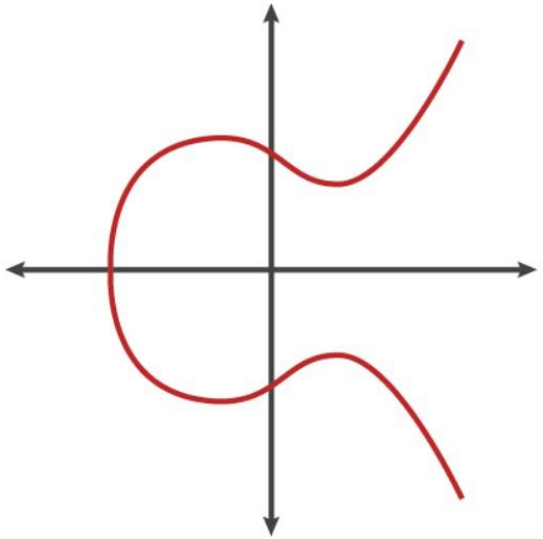
  Brands S. «An efficient off-line electronic cash system based on the representation problem», 1993

- Схема Тессаро-Жу

  Tessaro S., Zhu C. «Short Pairing-Free Blind Signatures with Exponential Security», 2022

Базовые механизмы

- группа точек эллиптической кривой простого порядка q
- H – стандартная хэш-функция
- $\mathcal{H}$ – хэш-функция, переводящая строки произвольной длины в точки ЭК (нужна не для всех схем)



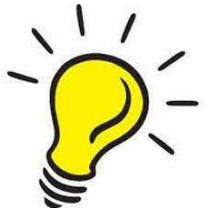
Подходы к построению $\mathcal{H}$ на основе стандартной хэш-функции:
https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hash-to-curve-16

КРИПТОПРО

Неподделываемость

Отрицательный результат о возможности построения сведения в стандартной модели противника (даже со случайным оракулом) для схем подписи вслепую Шнорра и Брандса

Baldimtsi, Lysyanskaya «On the Security of One-Witness Blind Signature Schemes», 2013



Модель с алгебраической группой

Fuchsbauer, Kiltz, Loss «The Algebraic Group Model and its Applications», 2018

КРИПТОПРО

Неподделываемость

Схема Абе

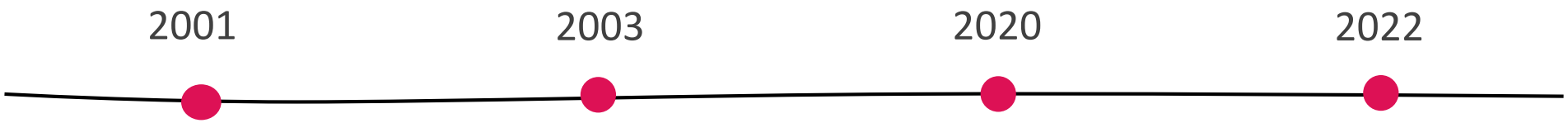


Схема Шаума-Педерсена

2021, КриптоПро:

- атака (сильная модель безопасности)
- сведение в модели с алгебраической группой к нестандартной задаче CP problem (слабая модель безопасности)

Схема Тессаро-Жу

2022, Tessaro, Zhu:

- сведение в модели с алгебраической группой к задаче Dlog

КРИПТОПРО

Сравнение схем: свойства безопасности

	Схема Абе	**Схема Шаума-Педерсена**	**Схема Тессаро-Жу**
Неподделываемость	сильная модель (DLog) – **под вопросом**	слабая модель (CP problem)	сильная модель (DLog)
Неотслеживаемость	вычислительная (DDH)	абсолютная	абсолютная

КРИПТОПРО

Сравнение схем: свойства безопасности

	Схема Абе	**Схема Шаума-Педерсена**	**Схема Тессаро-Жу**
Неподделываемость	сильная модель (DLog) – **под вопросом**	слабая модель (CP problem)	сильная модель (DLog)
Неотслеживаемость	вычислительная (DDH)	абсолютная	абсолютная

КРИПТОПРО

Сравнение схем: эксплуатационные свойства

	Схема Абе	Схема Шаума-Педерсена	Схема Тессаро-Жу
Количество пересылок	3	4	3
Длина подписи (бит)	$8\log_2 q + 2$	$3\log_2 q + 1$	$4\log_2 q$
Количество вычислений кратных точек на клиенте/сервере	11 + 5	9 + 3	8 + 3
Использование хэш-функции на кривую	да (клиент и сервер)	да (клиент)	нет

КРИПТОПРО

Сравнение схем: эксплуатационные свойства

	Схема Абе	Схема Шаума-Педерсена	Схема Тессаро-Жу
Количество пересылок	3	4	3
Длина подписи (бит)	$8\log_2 q + 2$	$3\log_2 q + 1$	$4\log_2 q$
Количество вычислений кратных точек на клиенте/сервере	11 + 5	9 + 3	8 + 3
Использование хэш-функции на кривую	да (клиент и сервер)	да (клиент)	нет

КРИПТОПРО

Схема Тессаро-Жу

Генерация ключей:

KeyGen( )

$d, z \leftarrow\$ \mathbb{Z}_q^*$

$Q \leftarrow dP, Z \leftarrow zP$

return $(d, (Q, Z))$

Sign (d, Q, Z)		User $((Q, Z), m)$
$a, t, y \leftarrow\$ \mathbb{Z}_q^*$		
$A \leftarrow aP$		
$C \leftarrow tP + yZ$		
	$\xrightarrow{A, C}$	
		$r_1, r_2, \gamma_1, \gamma_2 \leftarrow\$ \mathbb{Z}_q^*$
		$A' \leftarrow r_1 P + (\gamma_1/\gamma_2)A$
		$C' \leftarrow \gamma_1 C + r_2 P$
		$c' \leftarrow H(A' \Vert C' \Vert m)$
		$c \leftarrow c'\gamma_2$
	$\xleftarrow{c}$	
$s \leftarrow a + cyd$		
	$\xrightarrow{s, y, t}$	
		$s' \leftarrow (\gamma_1/\gamma_2)s + r_1$
		$y' \leftarrow \gamma_1 y$
		$t' \leftarrow \gamma_1 t + r_2$
		return (c', s', y', t')

КРИПТОПРО

Резюме

- Схема Тессаро-Жу осталась единственной схемой, представленной в проекте методических рекомендаций ТК26 «Протоколы формирования и проверки электронной подписи вслепую»

- Документ находится на стадии экспертизы

Tessaro S., Zhu C. «Short Pairing-Free Blind Signatures with Exponential Security», 2022, https://eprint.iacr.org/2022/047 (Section 5, схема BS_3)

Eurocrypt 2022: «Short Pairing-Free Blind Signatures with Exponential Security»

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

Неподделываемость

Угроза: противник создает $(l+1)$ корректную пару (сообщение, подпись) в результате l взаимодействий с подписывающим

- сильная: все сообщения различны
- слабая: все пары (сообщение, подпись) различны

Тип атаки: противник может получать от подписывающего корректные подписи для адаптивно выбираемых им сообщений

- атаки с последовательными/параллельными сессиями
- атаки с/без провоцирования сбоев

КРИПТОПРО