конференция
РусКрипто

Ежегодная международная научно-практическая конференция
«РусКрипто'2022»

О перспективных для стандартизации схемах подписи вслепую

Бабуева А. А., ведущий инженер-аналитик, КриптоПро
Алексеев Е. К., к.ф.-м.н., начальник отдела криптографических исследований, КриптоПро
Ахметзянова Л. Р., зам. начальника отдела криптографических исследований, КриптоПро

Мотивация

ноябрь 2020 г

разработка Методических Рекомендаций
«Протоколы формирования и проверки электронной подписи вслепую»
в РГ СКАиП ТК26

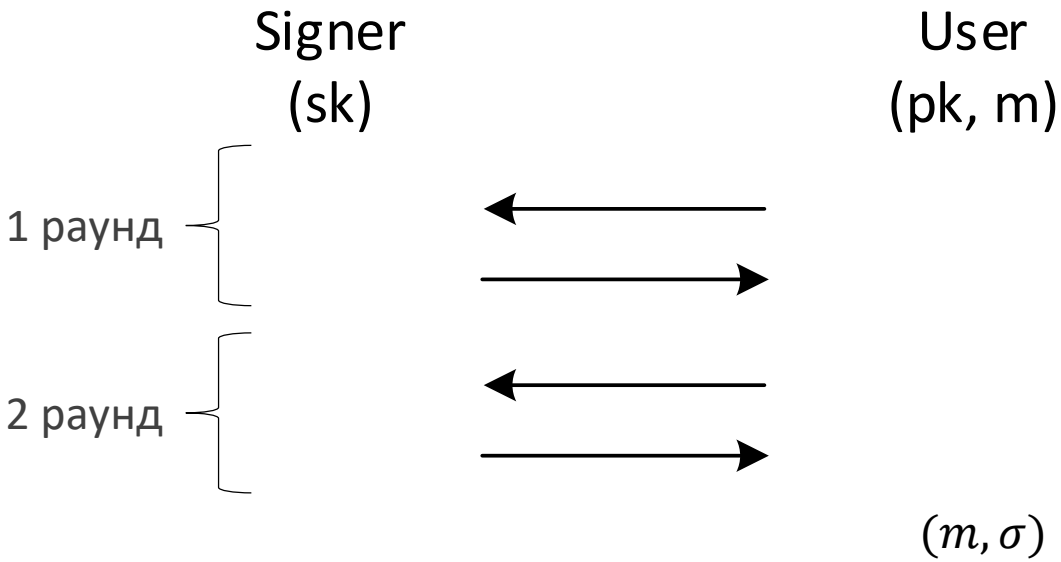
Область применения

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

Схема подписи вслепую

- Алгоритмы генерации ключей и проверки подписи – аналогичны алгоритмам для стандартных схем подписи

- Алгоритм подписи – интерактивный протокол:



Свойства безопасности

неподделываемость
(unforgeability)

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

противник – клиент

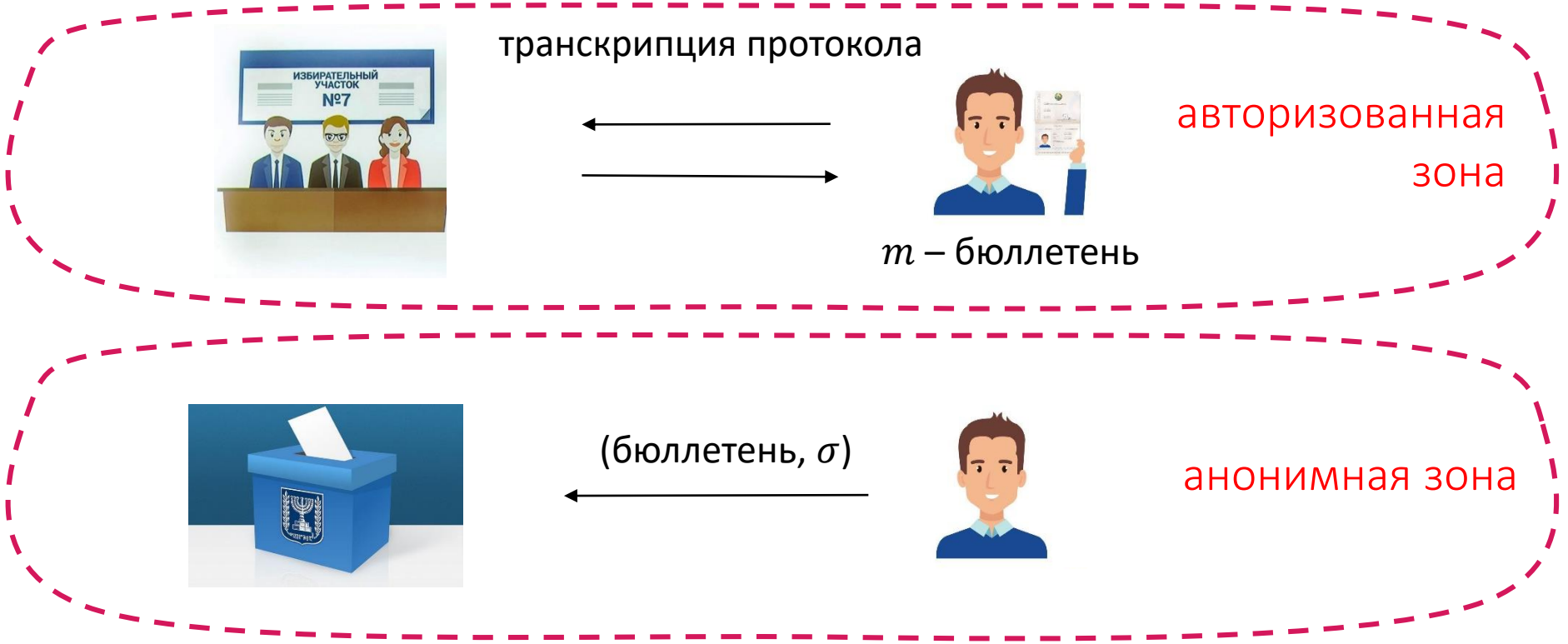
неотслеживаемость
(blindness)

подписывающий не может связать полученную клиентом пару (сообщение, подпись) с конкретной транскрипцией протокола

противник – подписывающий

Неотслеживаемость: пример (голосование)

подписывающий не может связать полученную клиентом пару (m, σ) с конкретной транскрипцией протокола



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

Требования к перспективным схемам

- стандартные базовые механизмы (эллиптические кривые, хэш-функция)
- неподделываемость (большое количество параллельных сессий, возможность провоцировать сбои, слабая угроза)
- 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-03
  - ✓ 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)

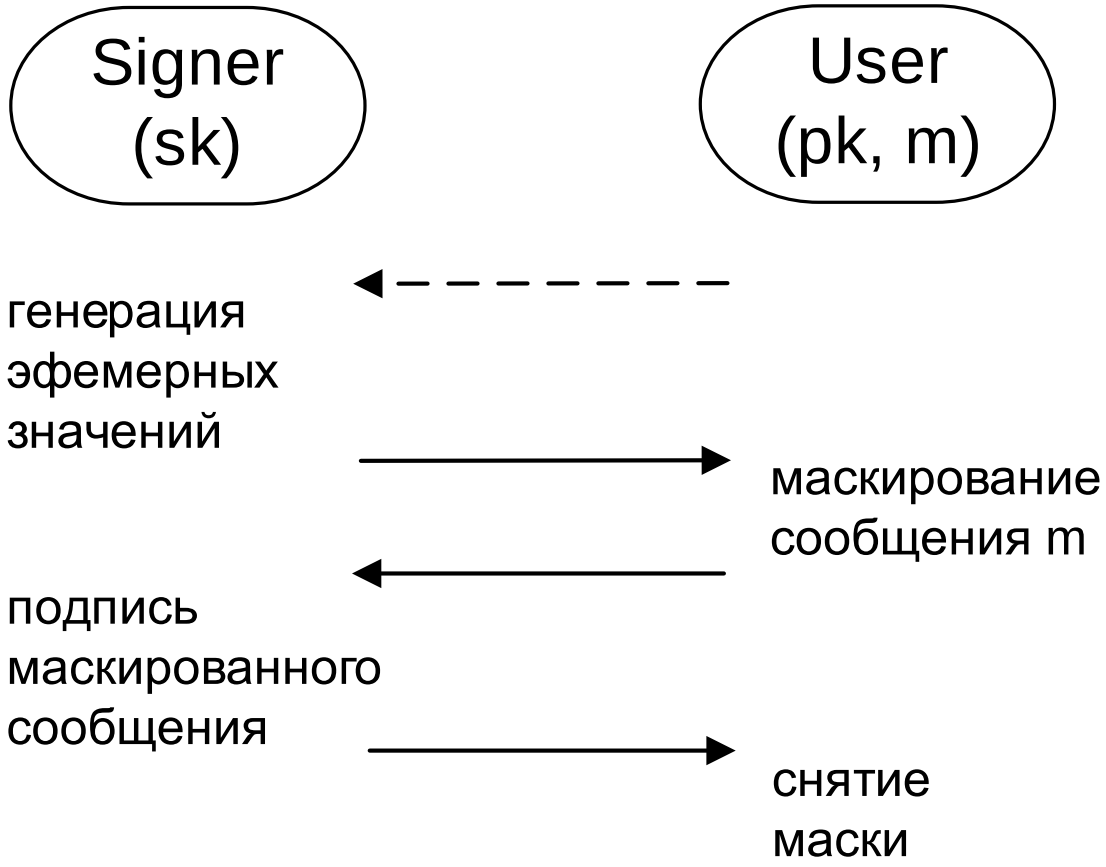
  Chaum D., Pedersen T. P. «Wallet databases with observers», 1992

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

- Схема Тессаро-Жу

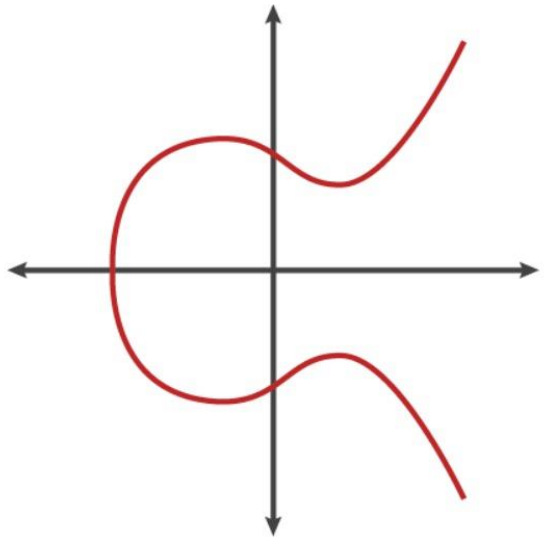
  Tessaro S., Zhu C. «Short Pairing-Free Blind Signatures with Exponential Security», 2022

Общая структура протокола подписи



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)

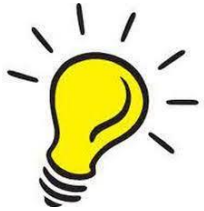


Подходы к построению $\mathcal{H}$ на основе стандартной хэш-функции:
https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hash-to-curve-13

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

Модель с алгебраической группой

Для любого элемента группы, который появляется на выходе алгоритма противника в процессе его работы, противник должен предоставить коэффициенты разложения данного элемента в линейную комбинацию всех элементов, пришедших ему на вход к данному моменту.

$X_1, \dots, X_n$ →  → $Z, (z_1, \dots, z_n)$

$$Z = \sum_{i=1}^{n} z_i X_i$$

- генерическая ≤ алгебраическая ≤ стандартная
- учитывает структурные атаки на схему подписи, например, ROS-атаки

Неподделываемость

Схема Абе

сведение в стандартной модели к задаче Dlog (Abe)

найдена ошибка в доказательстве, получена оценка в модели с генерической группой (Ohkubo, Abe)

сведение в модели с алгебраической группой к задаче Dlog (Kastner, Loss, Xu)

Схема Шаума-Педерсена

2021, КриптоПро:

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

Схема Тессаро-Жу

2022, Tessaro, Zhu:

- сведение в модели с алгебраической группой к задаче Dlog

Сравнение схем: свойства безопасности

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

Сравнение схем: свойства безопасности

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

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

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

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')

Схема Тессаро-Жу

Генерация ключей:

KeyGen( )

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

$Q \leftarrow dP, Z \leftarrow zP$

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

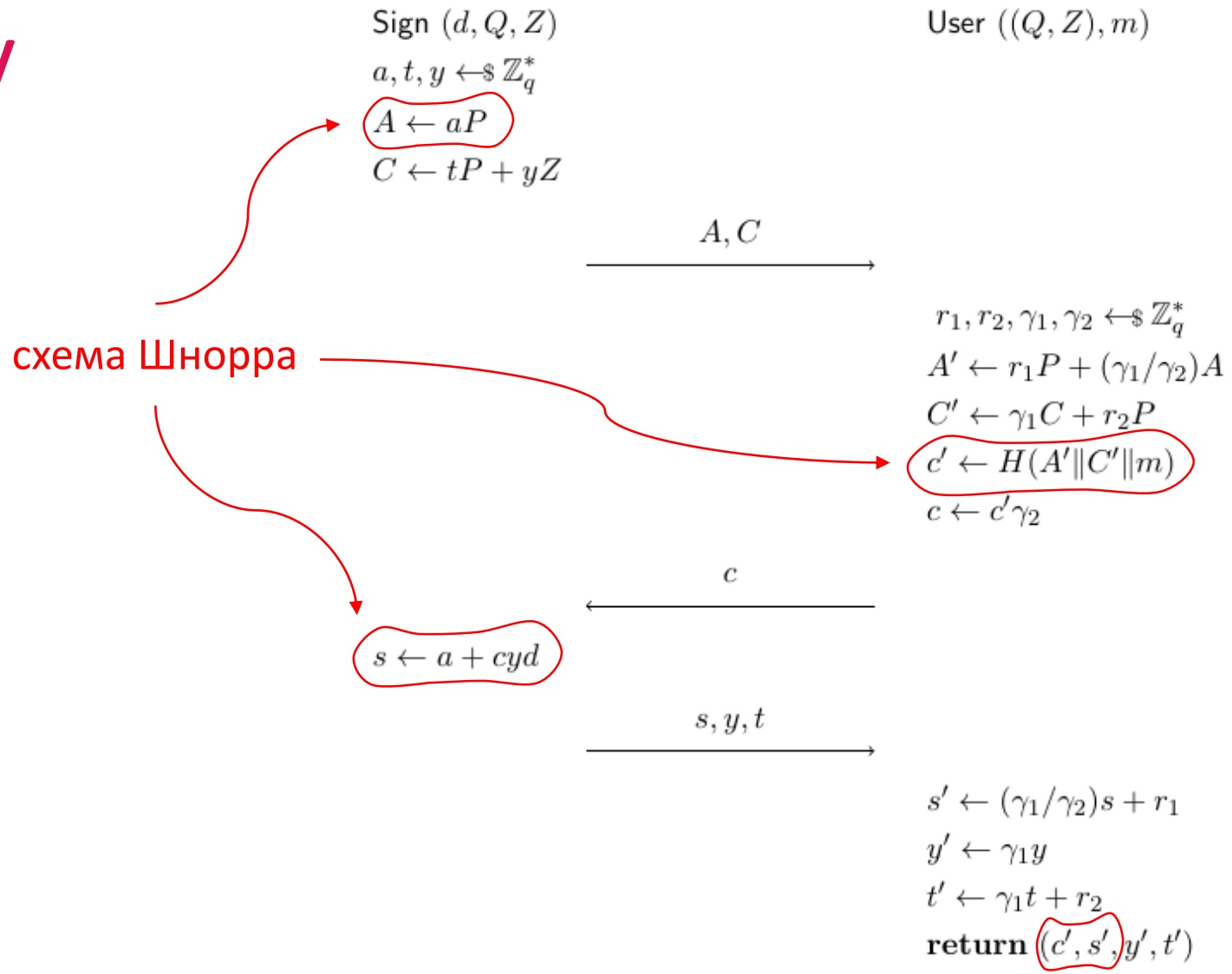


Схема Тессаро-Жу

Генерация ключей:

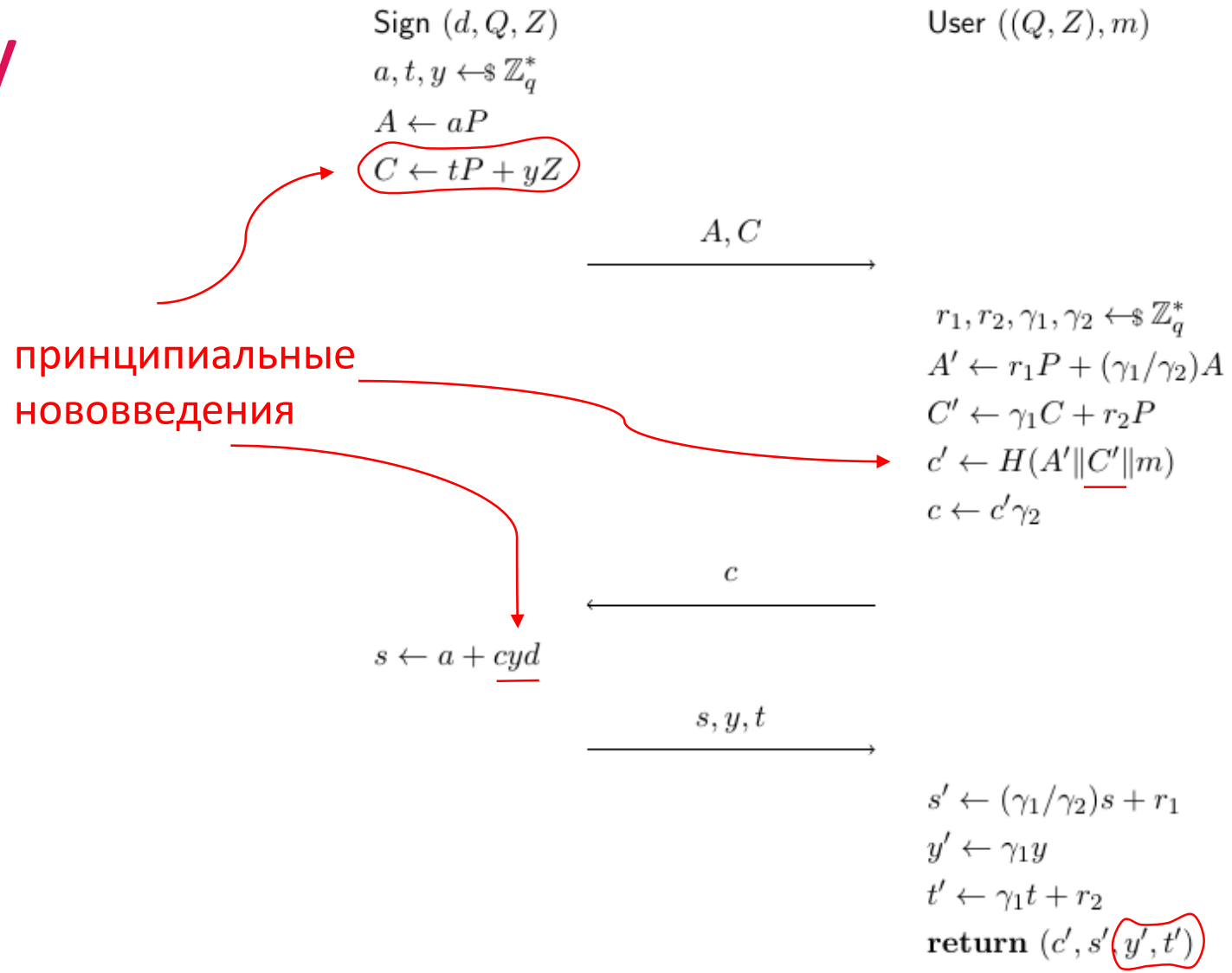
KeyGen( )

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

$Q \leftarrow dP, Z \leftarrow zP$

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

принципиальные нововведения



Резюме

- схема Тессаро-Жу является наиболее перспективной для стандартизации схемой подписи вслепую
- необходима всесторонняя и полномасштабная верификация!

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

Спасибо за внимание!

Контактная информация:

babueva@cryptopro.ru

Схема Абе

KeyGen( )

$d, z \leftarrow_{\$} \mathbb{Z}_q^*$
$Q \leftarrow dP, Z \leftarrow zP$
$G \leftarrow \mathcal{H}_1(p\|q\|P\|Z\|Q)$
if $G = 0$ **then return** $\perp$
return $(d, (Q, Z, G))$

Sign(d, P, Z, G)
$rnd \leftarrow_{\$} \{0,1\}^{\lceil \log_2 q \rceil}$
$G_1 \leftarrow \mathcal{H}_2(rnd)$
$G_2 \leftarrow G - G_1$
$u, s_1, s_2, f \leftarrow_{\$} \mathbb{Z}_q^*$
$A \leftarrow uP$
$B_1 \leftarrow s_1 P + fG_1$
$B_2 \leftarrow s_2 Z + fG_2$

$\xrightarrow{rnd, A, B_1, B_2}$

User(Q, P, Z, G, m)
$G_1 \leftarrow \mathcal{H}_2(rnd)$
$\gamma \leftarrow_{\$} \mathbb{Z}_q^*$
$E \leftarrow \gamma G, E_1 \leftarrow \gamma G_1, E_2 \leftarrow E - E_1$
$t_1, t_2, t_3, t_4, t_5 \leftarrow_{\$} \mathbb{Z}_q^*$
$\alpha \leftarrow A + t_1 P + t_2 Q$
$\beta_1 \leftarrow \gamma B_1 + t_3 P + t_4 E_1$
$\beta_2 \leftarrow \gamma B_2 + t_5 Z + t_4 E_2$
$\tau \leftarrow_{\$} \mathbb{Z}_q^*, T \leftarrow \tau G$
$\varepsilon \leftarrow H(E\|E_1\|\alpha\|\beta_1\|\beta_2\|T\|m)$
$e \leftarrow \varepsilon - t_2 - t_4$

$\xleftarrow{e}$

$c \leftarrow e - f$
$r \leftarrow u - cd$

$\xrightarrow{r, c, s_1, s_2, f}$

$\rho \leftarrow r + t_1$
$w \leftarrow c + t_2$
$\sigma_1 \leftarrow \gamma s_1 + t_3$
$\sigma_2 \leftarrow \gamma s_2 + t_5$
$\delta \leftarrow f + t_4$
$\mu \leftarrow \tau - \delta\gamma$
return $(E, E_1, \rho, w, \sigma_1, \sigma_2, \delta, \mu)$

Схема Шаума-Педерсена

KeyGen( )

$d \leftarrow_{\$} \mathbb{Z}_q^*$

$Q \leftarrow dP$

return (d, Q)

Signer (d)		User (Q, m)
		$M' \leftarrow \mathcal{H}(m)$
		$\alpha \leftarrow_{\$} \mathbb{Z}_q, M \leftarrow \alpha^{-1} M'$
	$\xleftarrow{M}$	
$Z \leftarrow dM$		
$k \leftarrow_{\$} \mathbb{Z}_q$		
$A \leftarrow kP,\ B \leftarrow kM$		
	$\xrightarrow{Z, A, B}$	
		$Z' \leftarrow \alpha Z$
		$u, v \leftarrow_{\$} \mathbb{Z}_q$
		$A' \leftarrow uA + vP$
		$B' \leftarrow u\alpha B + vM'$
		$c' \leftarrow H(M' \Vert Z' \Vert A' \Vert B'),\ c \leftarrow c' u^{-1}$
	$\xleftarrow{c}$	
$s \leftarrow k + cd$		
	$\xrightarrow{s}$	
		$s' \leftarrow us + v$
		$sgn \leftarrow (s', c', Z')$
return 1		**return** sgn