РусКрипто

Об одной схеме динамической групповой подписи

Утехина Мария,
Московский государственный университет имени М. В. Ломоносова,
инженер-аналитик, КриптоПро

В прошлом докладе

РусКрипто

- Описаны отличия схемы динамической групповой подписи.
- Метод построения из базовых механизмов.
- Была найдена одна схема, основывающаяся на задаче дискретного логарифмирования*, в работе:

  [1] Fuw-Yi Yang and Jinn-Ke Jan.
  «An efficient group signature based on the discrete logarithm problem». 2004.

- Была построена атака на свойство анонимности схемы.

*для мультипликативной группы конечного поля вычетов.

Схема динамической групповой подписи

РусКрипто

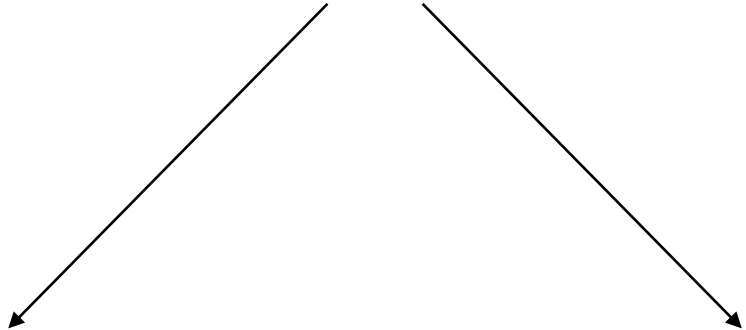
- Каждый пользователь обладает своим секретным ключом, один открытый ключ на группу пользователей.
- Пользователей в группу добавляет Издатель.
- По подписи невозможно установить, кто из участников группы её создал.
- Менеджер со своим секретным ключом, устанавливает, кто из участников группы создал подпись.

Схема динамической групповой подписи

РусКрипто

- $Kgen(\,) \rightarrow (sk_M, sk_I\,, gpk)$: генерация ключей
- $Sign\left(sk_U^i, gpk, m\right) \rightarrow \sigma$: формирование подписи
- $Verify(gpk, m, \sigma) \rightarrow b$: проверка подписи
- $Open(sk_M, m, \sigma) \rightarrow i$: раскрытие подписи
- $Join < User(i, gpk), Iss(i, gpk, sk_I) > \rightarrow (sk_U^i; reg[i])$: добавление нового пользователя

Свойства безопасности



Отслеживаемость (traceability)

Только участники группы могут создавать подписи и менеджер всегда может их раскрыть.

Анонимность (anonymity)

Никто кроме менеджера не может установить, кто из участников подписал сообщение.

РусКрипто

Схема из работы [1]

РусКрипто

Базовые механизмы:

- Схема шифрования с открытым ключом Эль-Гамаля $(KGen^M, Enc, Dec)$
- Алгоритм генерации ключей пользователей $KGen^U$
- Схема подписи $(KGen^I, Sign^I, Verify^I)$ из работы [2]:
  по подписи можно восстановить сообщение

[2] Rainer A. Rueppel Kaisa Nyberg «Message recovery for signature schemes based on the discretelogarithm», Designs, Codes and Cryptography, 1996

Схема из работы [1]

РусКрипто

Генерация ключей $KGen$

Издатель

$(sk_I, pk_I) \leftarrow KGen^I()$ — ключи подписи

Менеджер

$(sk_M, pk_M) \leftarrow KGen^M()$ — ключи шифрования

$gpk = (pk_I, pk_M)$

Схема из работы [1]

РусКрипто

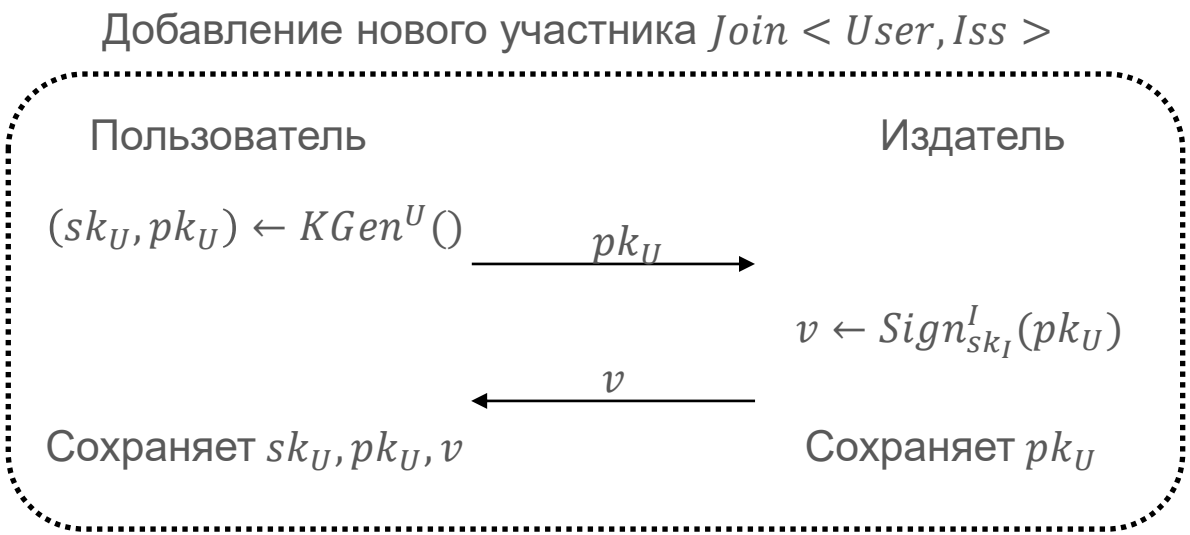


Схема из работы [1]

РусКрипто

Формирование подписи $Sign$

Вход: (sk_U, pk_U, v), (pk_M, pk_I), m

$c \leftarrow Enc_{pk_M}(pk_U)$

$\pi \leftarrow$ подпись m с доказательством знания sk_U, v, таких что:

1. $Dec_{sk_M}(c) = pk_U$
2. pk_U соответствует sk_U
3. $Verify^{I}_{pk_I}(pk_U, v) = 1$

Подпись = (c, π)

Signature of knowledge

Схема из работы [1]

РусКрипто

Проверка подписи $Verify$

Проверяющий Вход: $(pk_I, pk_M), m, (c, \pi)$

Проверяется корректность π

Раскрытие подписи $Open$

Менеджер Вход: $sk_M, m, (c, \pi)$

$pk_U \leftarrow Dec_{sk_M}(c)$

РусКрипто

Задача: построить алгоритм доказательства знания sk_U, v таких, что

1. $Dec_{sk_M}(c) = pk_U$;
2. pk_U соответствует sk_U;
3. $Verify^I_{pk_I}(pk_U, v) = 1$;

с нулевым разглашением pk_U, v, sk_U.

Принципы построения доказательства знания

РусКрипто

1. Доказываемое утверждение → последовательность базовых операций.
2. Промежуточное значение последовательности → обязательство/коммитмент (с помощью схемы обязательства).
3. Базовая операция → доказательство (с помощью ZKP), что за обязательствами «скрываются» значения, для которых выполняются соотношения.
4. Итоговое доказательство: обязательства и доказательства базовых операций.

[3] Khanh Quoc Nguyen, Feng Bao, Yi Mu, Vijay Varadharajan. «Zero-Knowledge Proofs of Possession of Digital Signatures and Its Applications». Information and Communication Security. ICICS. 1999

Принципы построения доказательства знания

$Dec_{sk_M}(c) = pk_U$

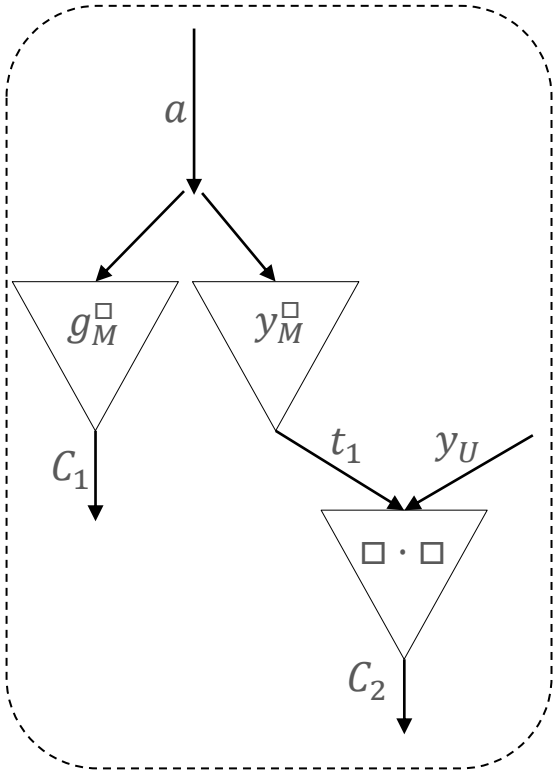
pk_U соответствует sk_U

$Verify^I_{pk_I}(pk_U, v) = 1$

- Схема обязательства Педерсена.
- Схемы ZKP: возведение в степень по известному основанию, умножение.

Принципы построения доказательства знания

РусКрипто



pk_U соответствует sk_U

$Verify_{pk_I}^{I}(pk_U, v) = 1$

Схема шифрования Эль-Гамаля:

KGen$^{\mathbf{M}}$:
$x_M \leftarrow Z_q^*$
$y_M \leftarrow g_M^{x_M}$
$return\ (x_M, y_M)$

Enc(y_M, y_U):
$a \leftarrow Z_q^*$
$C_1 \leftarrow g_M^a$
$C_2 \leftarrow y_U \cdot y_M^a$
$return\ (C_1, C_2)$

Dec$(x_M, (C_1, C_2))$:
$return\ C_2 \cdot C_1^{-x_M}$

Принципы построения доказательства знания

РусКрипто

$Dec_{sk_M}(c) = pk_U$

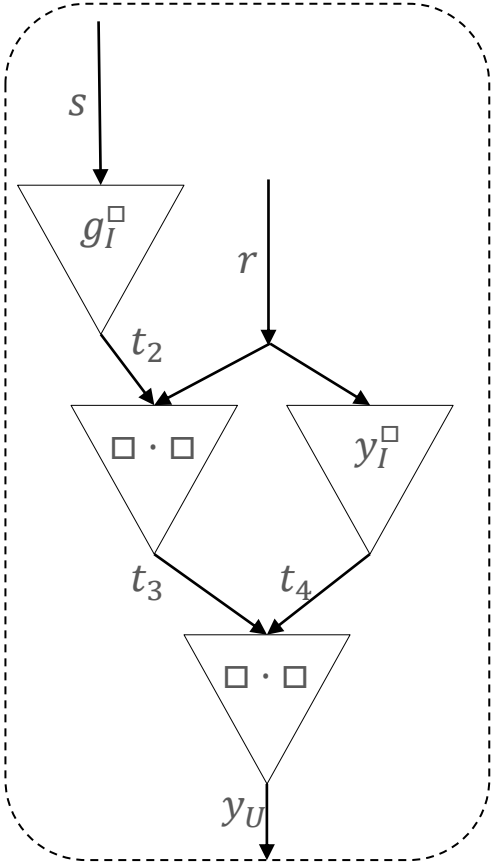
pk_U соответствует sk_U

Схема подписи издателя:

KGen$^{\mathbf{I}}$:
$x_I \leftarrow Z_q^*$
$y_I \leftarrow g_I^{x_I}$
$return\ (x_I, y_I)$

Sign(x_I, y_U):
$k \leftarrow Z_q^*$
$r \leftarrow y_U \cdot g_I^{-k}$
$s \leftarrow k\ - r \cdot x_I$
$return\ (r, s)$

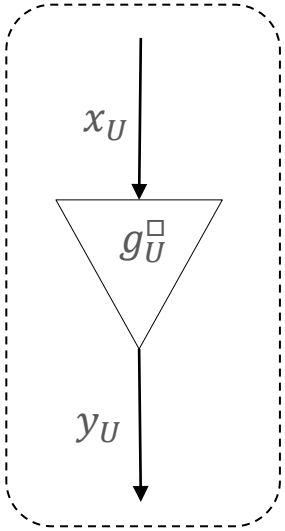
Verify$(y_I, y_U, (r, s))$:
$if\ y_U = r \cdot g_I^s \cdot y_I^r$:
    $return\ 1$
$return\ 0$



Принципы построения доказательства знания

РусКрипто

$Dec_{sk_M}(c) = pk_U$

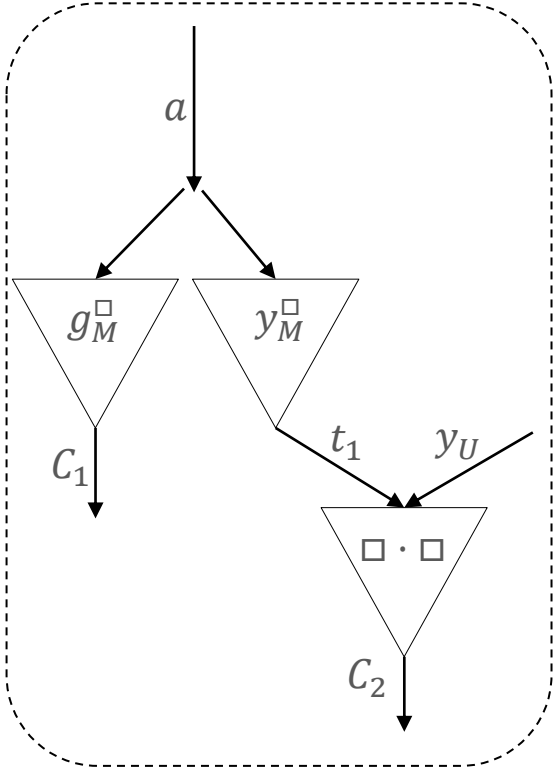


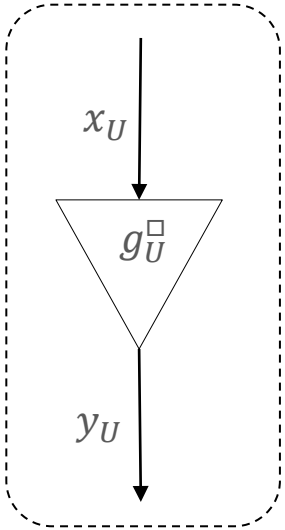
$Verify_{pk_I}^{I}(pk_U, v) = 1$

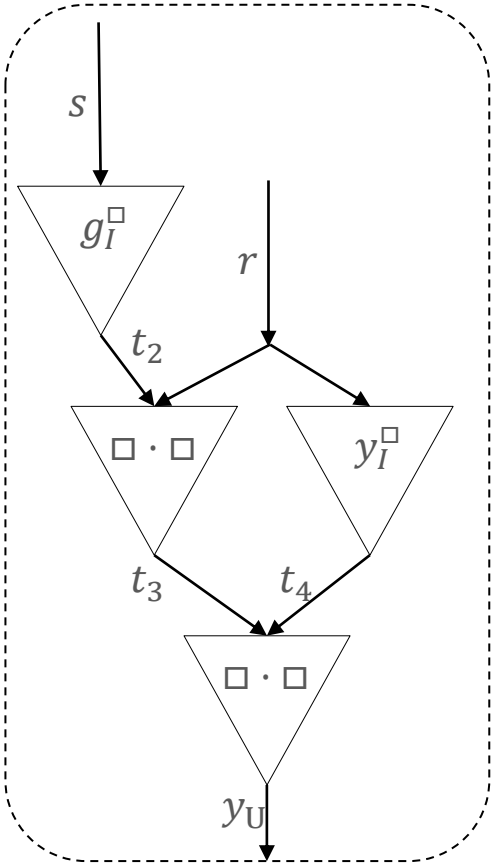
Алгоритм генерации ключей пользователя:

$\mathbf{KGen}^{U}$:
$x_U \leftarrow Z_q^*$
$y_U \leftarrow g_U^{x_U}$
$return\ (x_U, y_U)$

Принципы построения доказательства знания

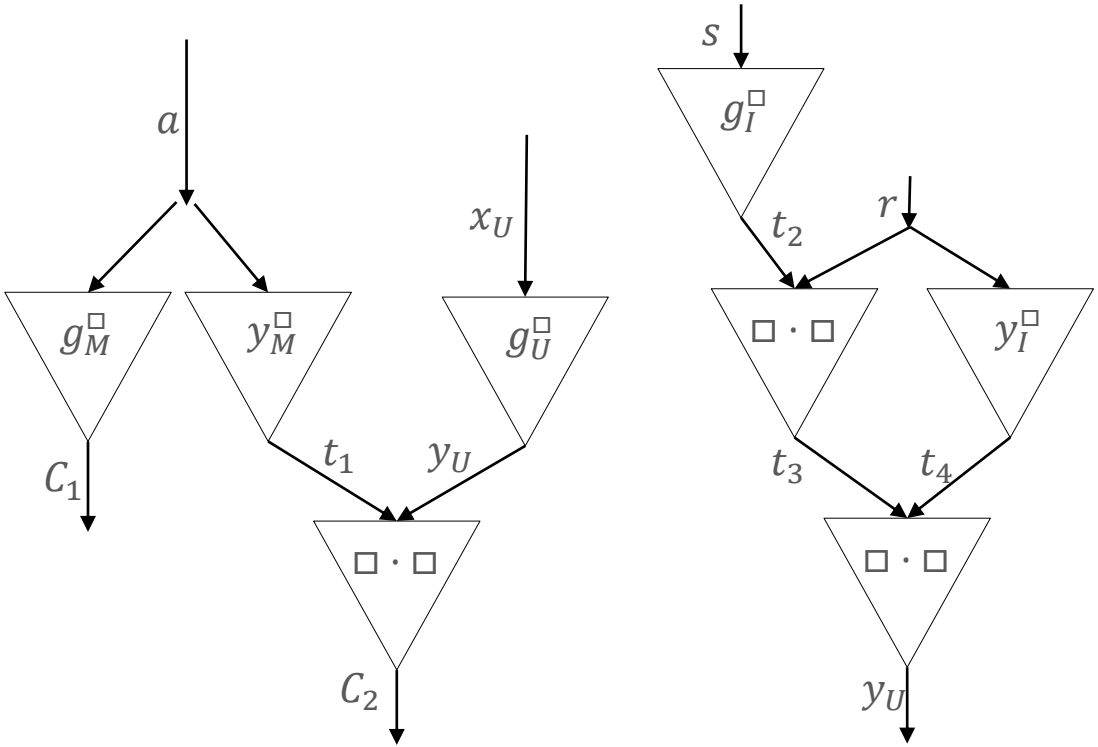






РусКрипто

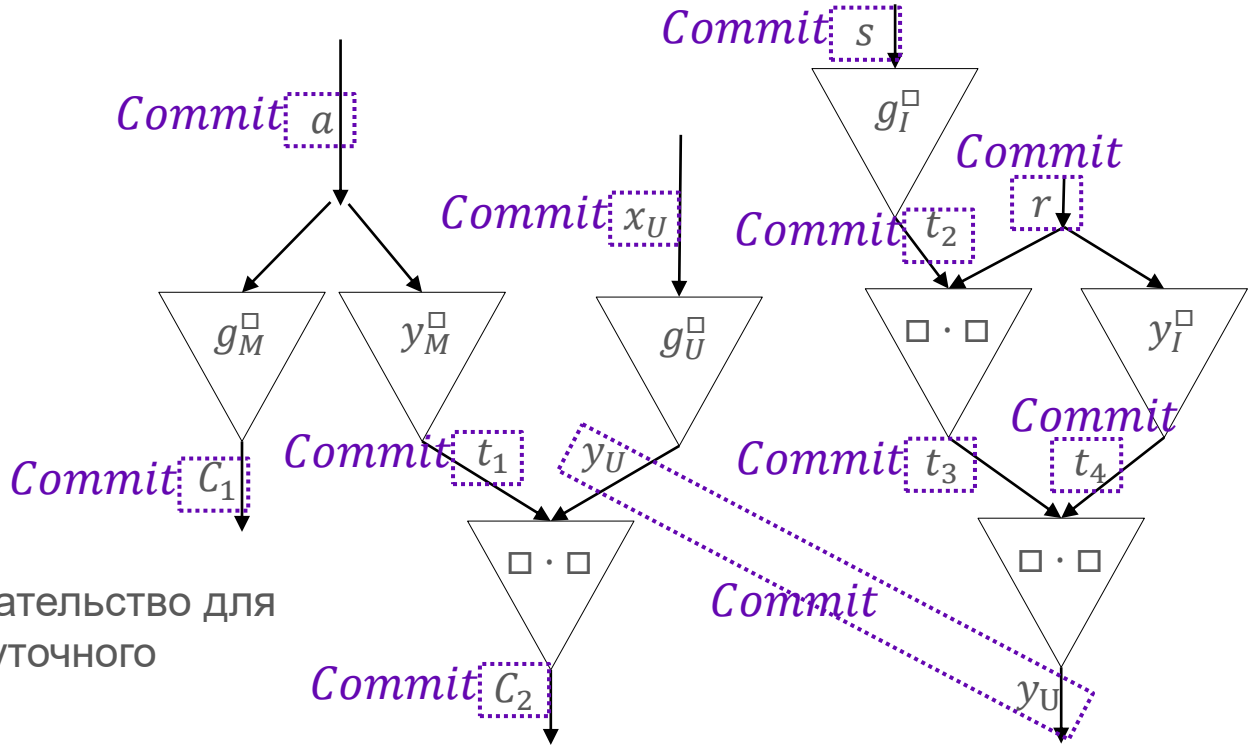
Принципы построения доказательства знания



1. Представляем доказываемое утверждение как последовательность базовых операций.

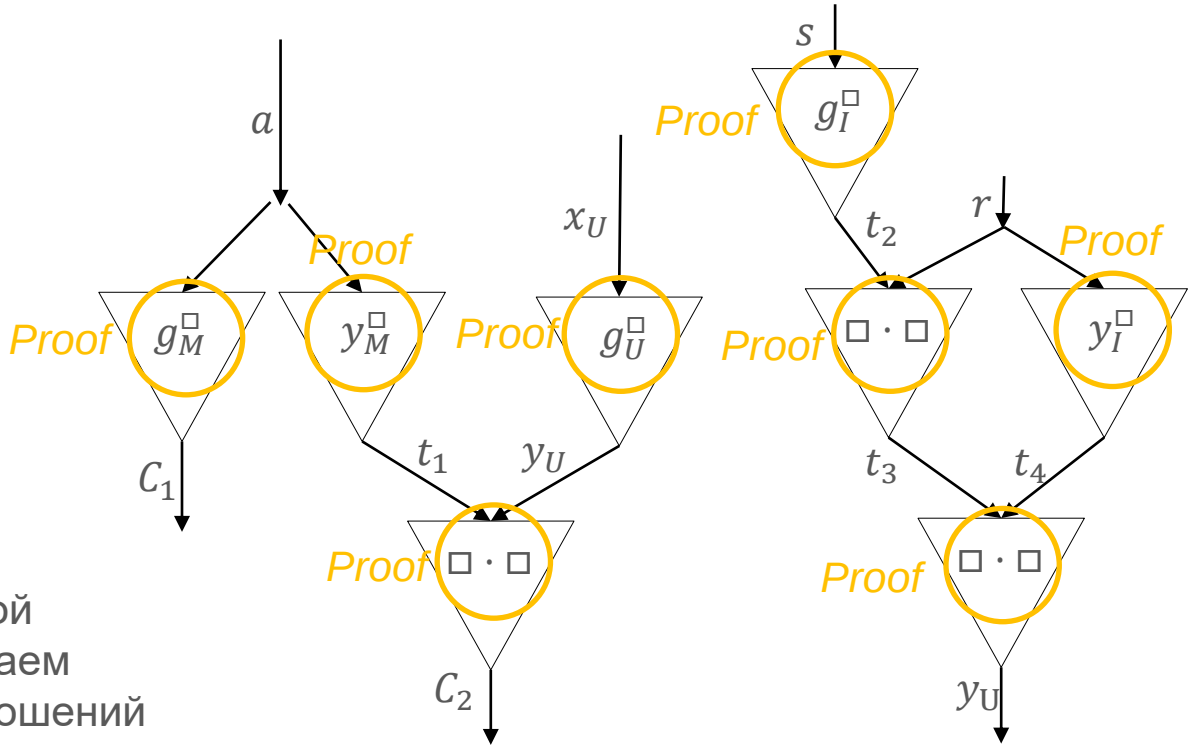
РусКрипто

Принципы построения доказательства знания



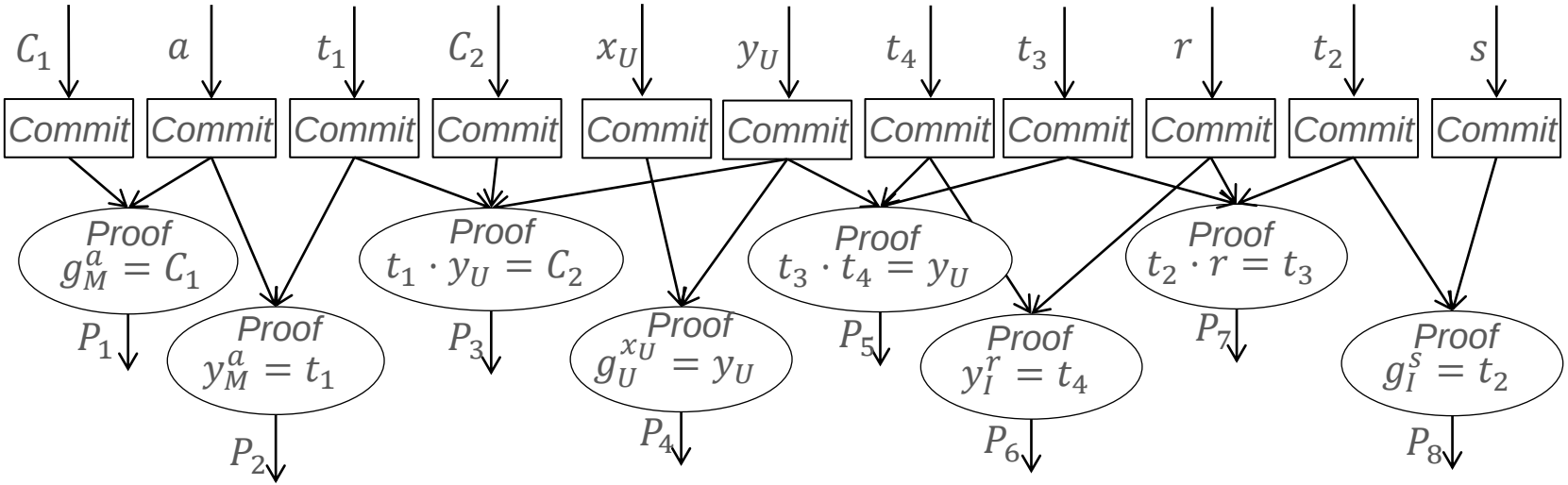
2. Вычисляем обязательство для каждого промежуточного значения.

Принципы построения доказательства знания



3. Для каждой базовой операции доказываем выполнение соотношений для обязательств.

Принципы построения доказательства знания



4. Итоговое доказательство состоит из обязательств и доказательств базовых операций.

$$\pi = (Comm_1, \dots, Comm_{11}, P_1, \dots, P_8)$$

Принципы построения доказательства знания

РусКрипто

- Схема обязательства Педерсена обладает свойством привязки (binding).
- Доказательства базовых операций обладают soundness (построены по преобразованию Фиата-Шамира).

Целевая схема подписи знания обладает свойством неподделываемости.

Принципы построения доказательства знания

РусКрипто

- Схема обязательства Педерсена обладает свойством сокрытия (hiding).
- Доказательства базовых операций обладают нулевым разглашением (построены по преобразованию Фиата-Шамира).

Целевая схема подписи знания обладает свойством нулевого разглашения.

Будущие исследования

РусКрипто

- Построить формальное обоснование свойств.

- Адаптировать алгоритмы для группы точек эллиптической кривой.

РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ