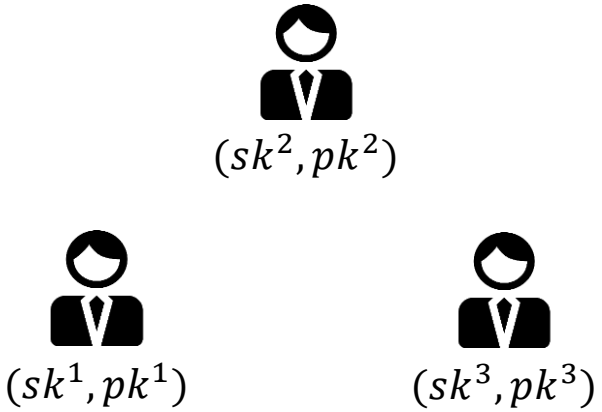
конференция
РусКрипто

Ежегодная международная научно-практическая конференция
«РусКрипто’2024»

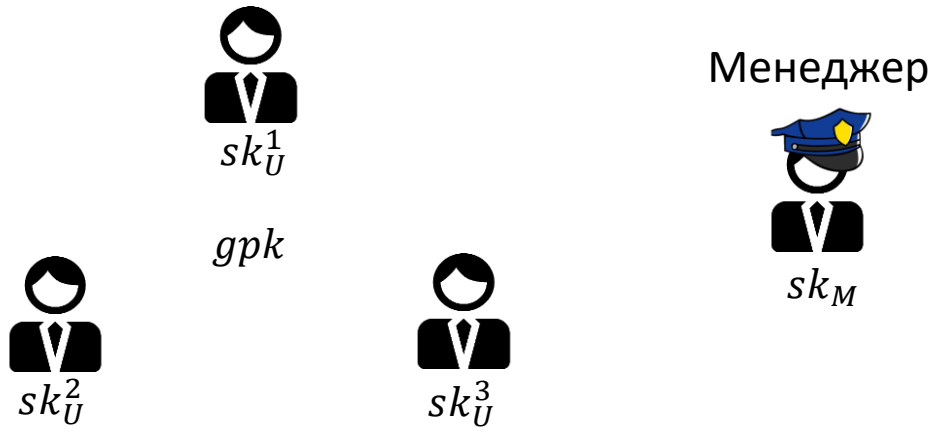
О методах построения схем динамической групповой подписи и атаках на одну схему

Утехина М. П., студентка факультета вычислительной математики и кибернетики МГУ имени М. В. Ломоносова

Схема групповой подписи



- Каждый пользователь обладает своей парой ключей.
- Подпись по корректному открытому ключу однозначно сопоставляется с пользователем.
- Все пользователи равнозначны.



- Каждый пользователь обладает свои секретным ключом, один открытый ключ на группу пользователей.
- По подписи невозможно установить, кто из участников группы её создал.
- Доверенный пользователь – Менеджер со своим секретным ключом, который может устанавливать, кто из участников группы создал подпись.

Применение в прикладных системах

Анонимные платежи:

- Пользователи банка могут совершать анонимные платежи: по транзакции невозможно установить, кто её совершил.
- Банк может узнавать, кто совершил транзакцию по требованию правоохранительных органов (для ПОД/ФТ).

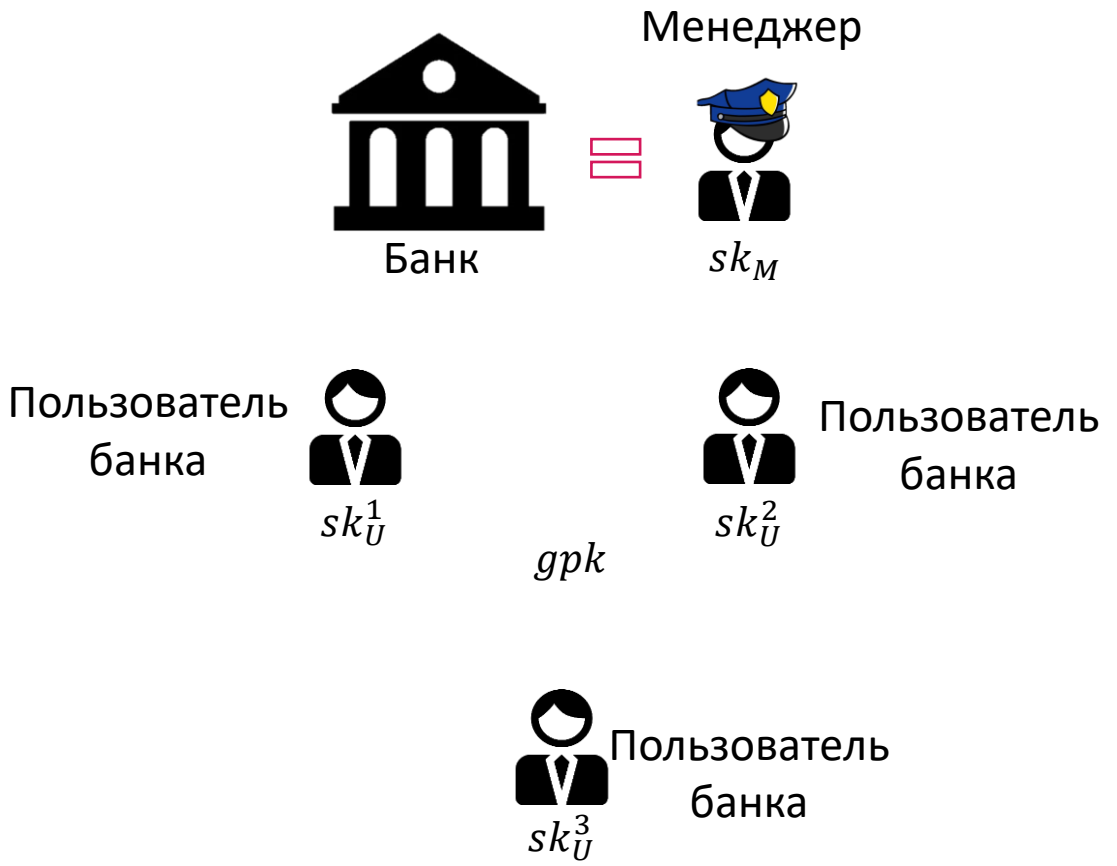


Схема подписи

- $Kgen() \rightarrow (sk, pk)$: генерация ключей
- $Sign(sk, m) \rightarrow \sigma$: формирование подписи
- $Verify(pk, m, \sigma) \rightarrow b$: проверка подписи

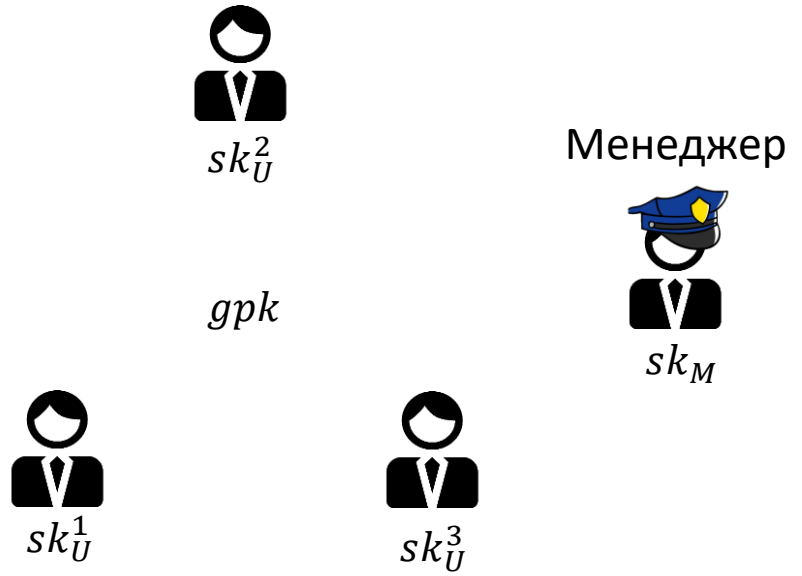
(sk^2, pk^2)

(sk^1, pk^1)

(sk^3, pk^3)

Схема групповой подписи

- $Kgen(n) \rightarrow (sk_M, \{sk_U^i\}, gpk)$: генерация ключей
- $Sign(sk_U^i, gpk, m) \rightarrow \sigma$: формирование подписи
- $Verify(gpk, m, \sigma) \rightarrow b$: проверка подписи
- $Open(sk_M, m, \sigma) \rightarrow i$: раскрытие подписи



Свойства безопасности

Стандартная схема подписи: неподделываемость

Модель нарушителя: нарушитель может являться легитимным пользователем (обладать собственной ключевой парой), получать подписи от честных пользователей.

Модель угрозы: нарушитель создает корректную пару (сообщение, подпись), которая не была создана честным пользователем.

Свойства безопасности

Схема групповой подписи: отслеживаемость (traceability)

Модель нарушителя: нарушитель может являться легитимным участником группы (обладать собственным ключом), получать подписи от честных участников группы.

- полная (full): нарушителем может быть менеджер.

Модель угрозы: нарушитель создаёт корректную пару (сообщение, подпись), которая не была создана честным участником группы и для которой выполняется одно из двух условий:

1. Алгоритм раскрытия возвращает ошибку.
2. Алгоритм раскрытия возвращает номер честного участника.

Свойства безопасности

Схема групповой подписи: анонимность (anonymity)

Модель нарушителя: нарушитель может являться легитимным участником группы (обладать собственным ключом), получать подписи от честных участников группы.

- полная (full): нарушитель может компрометировать честных участников.

Модель угрозы: нарушитель устанавливает, кто из честных участников подписал сообщение.

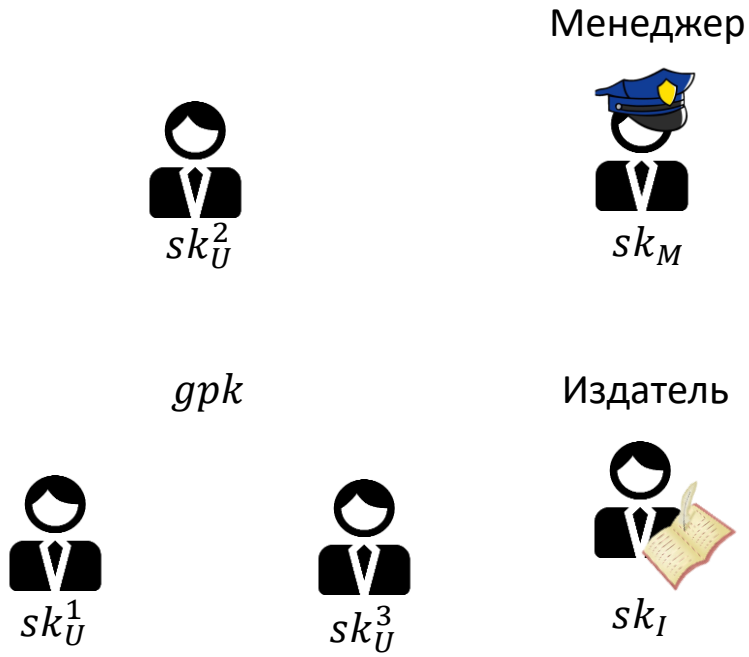
Недостатки групповой подписи

- Фиксированное количество участников.
- Размер подписи.

Схема динамической групповой подписи

1. Новый доверенный пользователь – Издатель со своим секретным ключом.
2. Протокол добавления нового участника группы.

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



Свойства безопасности

Групповая подпись	Отслеживаемость	Анонимность
Менеджер		

Динамическая групповая подпись	Отслеживаемость	Анонимность
Менеджер		
Издатель		

Методы построения

- Метод, использующий рандомизируемые подписи [1].

- Метод, использующий схему шифрования с открытым ключом [2].

[1] Patrik Bichsel, Jan Camenisch, Gregory Neven, Nigel Smart, and Bogdan Warinschi.
«Get shorty via group signatures without encryption», 2010.

[2] Jan Camenisch. «Group signature schemes and payment systems based on the discrete logarithm problem».
ETH Series in Information Security and Cryptography, 1998.

Метод, использующий схему шифрования с открытым ключом

Базовые механизмы:

- Схема шифрования с открытым ключом $(KGen^M, Enc, Dec)$
- Схема подписи пользователя $(KGen^U, Sign^U, Verify^U)$
- Схема подписи издателя $(KGen^I, Sign^I, Verify^I)$

Метод, использующий схему шифрования с открытым ключом

Генерация ключей $KGen$

Издатель

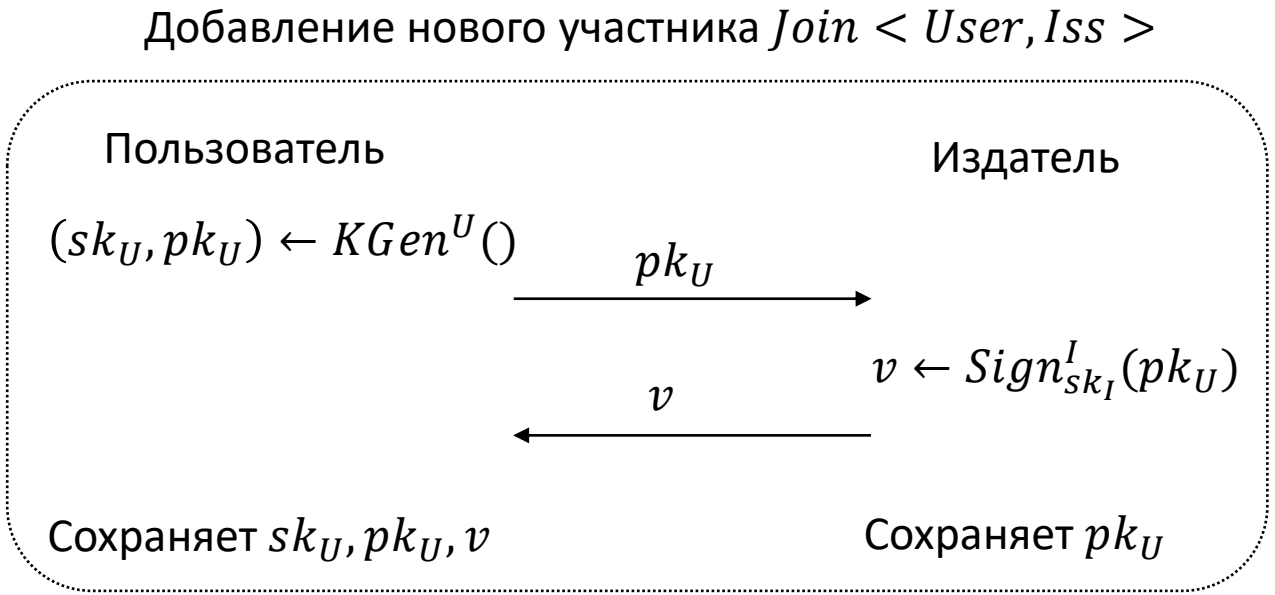
$(sk_I, pk_I) \leftarrow KGen^I()$ — ключи подписи

Менеджер

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

$$gpk = (pk_I, pk_M)$$

Метод, использующий схему шифрования с открытым ключом



Метод, использующий схему шифрования с открытым ключом

Формирование подписи $Sign$

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

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

$\sigma \leftarrow Sign^U_{sk_U}(m)$

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

1. $Dec_{sk_M}(c) = pk_U$
2. pk_U соответствует sk_U
3. $Verify^I_{pk_I}(pk_U, v) = 1$
4. $Verify^U_{pk_U}(m, \sigma) = 1$

Подпись = (c, π)

Отслеживаемость:

Доказательство знания sk_U, σ, v, таких что

1. известный шифртекст c расшифровывается в открытый ключ pk_U,
2. pk_U соответствует sk_U,
3. v является корректным сертификатом для pk_U,
4. подпись σ является корректной для сообщения m и ключа pk_U.

Метод, использующий схему шифрования с открытым ключом

Формирование подписи $Sign$

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

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

$\sigma \leftarrow Sign^U_{sk_U}(m)$

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

1. $Dec_{sk_M}(c) = pk_U$
2. pk_U соответствует sk_U
3. $Verify^I_{pk_I}(pk_U, v) = 1$
4. $Verify^U_{pk_U}(m, \sigma) = 1$

Подпись = (c, π)

Анонимность:

По pk_U можно установить участника группы.

- По sk_U вычисляется pk_U.
- Сертификат v однозначно соответствует участнику группы.
- По подписи σ и сообщению m возможно найти pk_U.

Метод, использующий схему шифрования с открытым ключом

Формирование подписи $Sign$

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

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

$\sigma \leftarrow Sign^U_{sk_U}(m)$

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

1. $Dec_{sk_M}(c) = pk_U$
2. pk_U соответствует sk_U
3. $Verify^I_{pk_I}(pk_U, v) = 1$
4. $Verify^U_{pk_U}(m, \sigma) = 1$

Подпись = (c, π)

Метод описан в общем виде. Реализация метода для конкретных схем требует построения специфических доказательств знания.

Метод, использующий схему шифрования с открытым ключом

Проверка подписи $Verify$

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

Проверяется корректность π

Раскрытие подписи $Open$

Менеджер Вход: $sk_M, m, (c, \pi)$

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

Поставленная задача

- Существуют схемы динамической групповой подписи, основывающиеся на задачах LWE, RSA; использующие группы с неизвестным порядком; использующие «pairing friendly» кривые…
- Была найдена одна схема, основывающаяся на задаче дискретного логарифмирования, в работе:

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!

Базовые механизмы

- Схема шифрования с открытым ключом $(KGen^M, Enc, Dec)$ → Схема шифрования Эль-Гамаля.
- Схема подписи пользователя $(KGen^U, Sign^U, Verify^U)$ → Схема подписи Шнорра.
- Схема подписи издателя $(KGen^I, Sign^I, Verify^I)$ → Схема подписи из работы [3], позволяющая по подписи и ключу восстановить сообщение.

  Сертификат v является парой (r, s).

[3] Rainer Rueppel, Kaisa Nyberg. «Message recovery for signature schemes based on the discrete logarithm.» Designs, Codes and Cryptography, 1996

Особенности схемы, требующиеся для атаки

Алгоритм формирования подписи $Sign$.

$\mathsf{Sign}(\mathsf{usk}, \mathsf{gpk}, m)$

$(\mathsf{sk}, \mathsf{pk}, r, s) \leftarrow \mathsf{usk}$

$(\mathsf{pk_I}, \mathsf{pk_M}) \leftarrow \mathsf{gpk}$

$a \xleftarrow{U} \mathbb{Z}_q^*$

$C_1 \leftarrow h_{\mathsf{M}}^a \mod p$

$C_2 \leftarrow \mathsf{pk} \cdot \mathsf{pk_M}^a \mod p$

$C_3 \leftarrow g^{-a} h_{\mathsf{I}}^s \mod p$

$W \leftarrow g^a \cdot \mathsf{pk_I}^r \cdot \mathsf{pk_M}^a \mod p$

$M \leftarrow m \| g \| h_{\mathsf{I}} \| \hat{h} \| \mathsf{pk_I} \| \mathsf{pk_M} \| C_1 \| C_2 \| C_3 \| W$

$r_a, r_s, r_x \xleftarrow{U} \mathbb{Z}_q^*$

$r_r \xleftarrow{U} \mathbb{Z}_p^*$

$c \leftarrow \mathsf{H}(M \| h_{\mathsf{M}}^{r_a} \| g^{r_x} \cdot \mathsf{pk_M}^{r_a} \| g^{-r_a} \cdot h_{\mathsf{I}}^{r_s} \| g^{r_a} \cdot \mathsf{pk_I}^{r_r} \cdot \mathsf{pk_M}^{r_a} \| \hat{h}^{r_r})$

$s_a \leftarrow r_a - c \cdot a \mod q$

$s_s \leftarrow r_s - c \cdot s \mod q$

$s_r \leftarrow r_r - c \cdot r \mod p$

$s_x \leftarrow r_x - c \cdot \mathsf{sk} \mod q$

return $(C_1, C_2, C_3, W, c, s_a, s_r, s_s, s_x)$

Для любой честно сформированной подписи:

$$C_3 W\, r = C_2$$

Атака на анонимность

1. Участник i создаёт подпись $\sigma = (C_1, C_2, C_3, W, s_a, s_r, s_x, s_s)$.

2. Нарушитель восстанавливает значение $r = C_2(C_3 W)^{-1}$.

a) Нарушителем является издатель.
   Во время добавления новых участников в группу нарушитель может вместе с открытыми ключами сохранять значения (r, s). Тогда по подписи нарушитель однозначно устанавливает участника.

b) Нарушителем является внешний наблюдатель/участник группы.
   Если нарушитель знает, что некоторую подпись σ сформировал участник i, то нарушитель может деанонимизировать все подписи, созданные участником i.

Будущие исследования

Дано: схема шифрования с открытым ключом $(KGen_1, Enc, Dec)$ и схема подписи $(KGen_2, Sign, Verify)$.

$$(sk_E, pk_E) = KGen_1();$$
$$(sk_S, pk_S) = KGen_2();$$
$$\sigma = Sign(sk_S, m).$$

Построить: шифртекст c и соответствующее ему доказательство знания m и σ с нулевым разглашением, таких что

$$Dec(sk_E, c) = m,$$
$$Verify(pk_S, m, \sigma) = 1.$$

Спасибо за внимание!