# Групповые личностные криптосистемы на основе мультилинейных отображений

Косолапов Д.О., к.ф.-м.н.

Московский Государственный Университет им М.В. Ломоносова
Москва, 2015

# План семинара

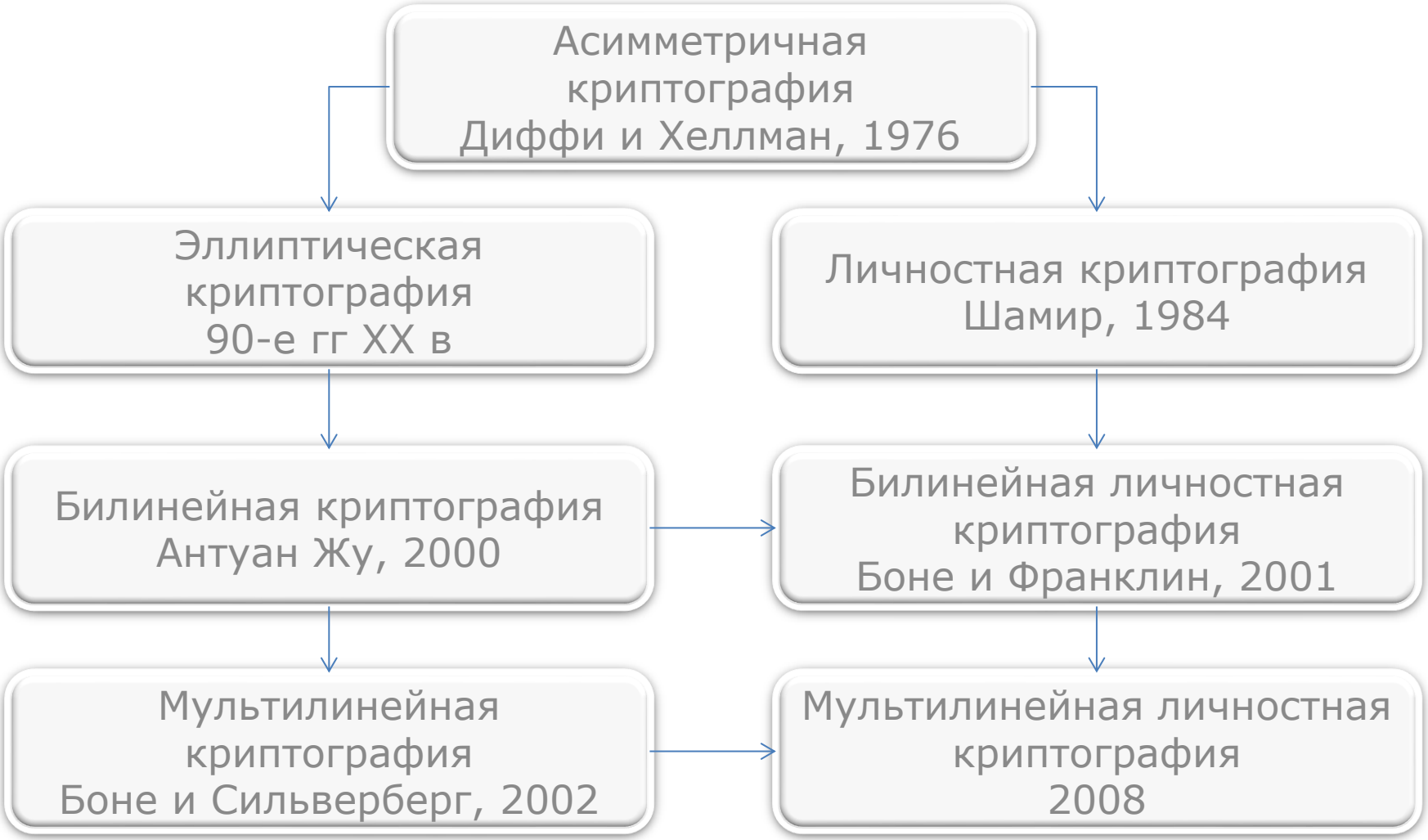
- Личностная криптография как подход к упрощению инфраструктуры открытых ключей
- Математический аппарат билинейных и мультилинейных отображений
- Групповые личностные криптосистемы
- Стойкость групповых личностных криптосистем на примере системы шифрования

# Личностные криптосистемы

- В качестве открытого ключа используется какая-либо идентификационная информация абонента (номер мобильного телефона или адрес электронной почты)
- Закрытый ключ абонент получает у Центра Генерации Ключей (ЦГК), предварительно пройдя процедуру аутентификации
- Главное преимущество личностных криптосистем – упразднение затратной Инфраструктуры Открытых Ключей (ИОК)

# Личностные криптосистемы

# История развития личностных криптосистем



# Личностные криптосистемы

Перспективные для практического использования личностные криптосистемы (криптосистемы на основе идентификационных данных) используют математический аппарат билинейных отображений в группах точек эллиптической кривой

# Билинейное отображение

Отображение вида $e$: $G_1 \times G_1 \to G_2$,

обладающее свойствами аддитивности, невырожденности и эффективной вычислимости

$(G_1, +)$ - циклическая аддитивная группа порядка $p$

$(G_2, *)$ - циклическая мультипликативная группа порядка $p$

$p$ – простое число

# Свойства билинейного отображения

- Аддитивность

$\forall R, S, T \in G_1 : e(R + S, T) = e(R, T)e(S, T)$

$\forall R, S, T \in G_1 : e(R, S + T) = e(R, S)e(R, T)$

- Невырожденность

$\forall R \in G_1^* : e(R, R) \neq 1$

- Эффективная вычислимость

Существует эффективный алгоритм вычисления $e(R, S)$ для $\forall R, S \in G_1$

# Свойства билинейного отображения

Следствием свойства аддитивности является линейность по обоим аргументам, а именно

$\forall a, b \in \mathbb{N}, R = aP \in G_1, S = bP \in G_1$, где

$P$ – образующий элемент группы $G_1$:

$$e(R, S) = e(aP, bP) = e(P, P)^{ab} = e(S, R)$$

# Групповые личностные криптосистемы

В связи с экспоненциальным ростом количества участников информационного обмена возникла необходимость построения групповых личностных криптосистем.

Данные криптосистемы могут быть построены на основе мультилинейных отображений

# Мультилинейное отображение

Отображение вида $\mu: \underbrace{G_1 \times \cdots \times G_1}_{n} \to G_2$,

обладающее свойствами мультилинейности и невырожденности

$(G_1, +)$ - циклическая аддитивная группа порядка $p$

$(G_2, *)$ - циклическая мультипликативная группа порядка $p$

$p$ – простое число

# Свойства мультилинейного отображения

- Мультилинейность

$\forall a_1, \dots, a_n \in \mathbb{Z}, \forall P \in G_1$

$\mu(a_1 P, \dots, a_n P) = \mu(P, \dots, P)^{a_1 \dots a_n}$

- Невырожденность

Если элемент $P$ является образующим элементом группы $G_1$, то $\mu(P, \dots, P)$ является образующим элементом группы $G_2$

# Мультилинейная проблема Диффи-Хеллмана (MDH)

$\langle P, a_1 P, \ldots, a_{n+1} P \rangle$, где $\forall a_1, \ldots, a_{n+1} \in \mathbb{Z}_p^*$,

$\mu$ - $n$-мультилинейное отображение,

$P$ – образующий элемент $G_1$

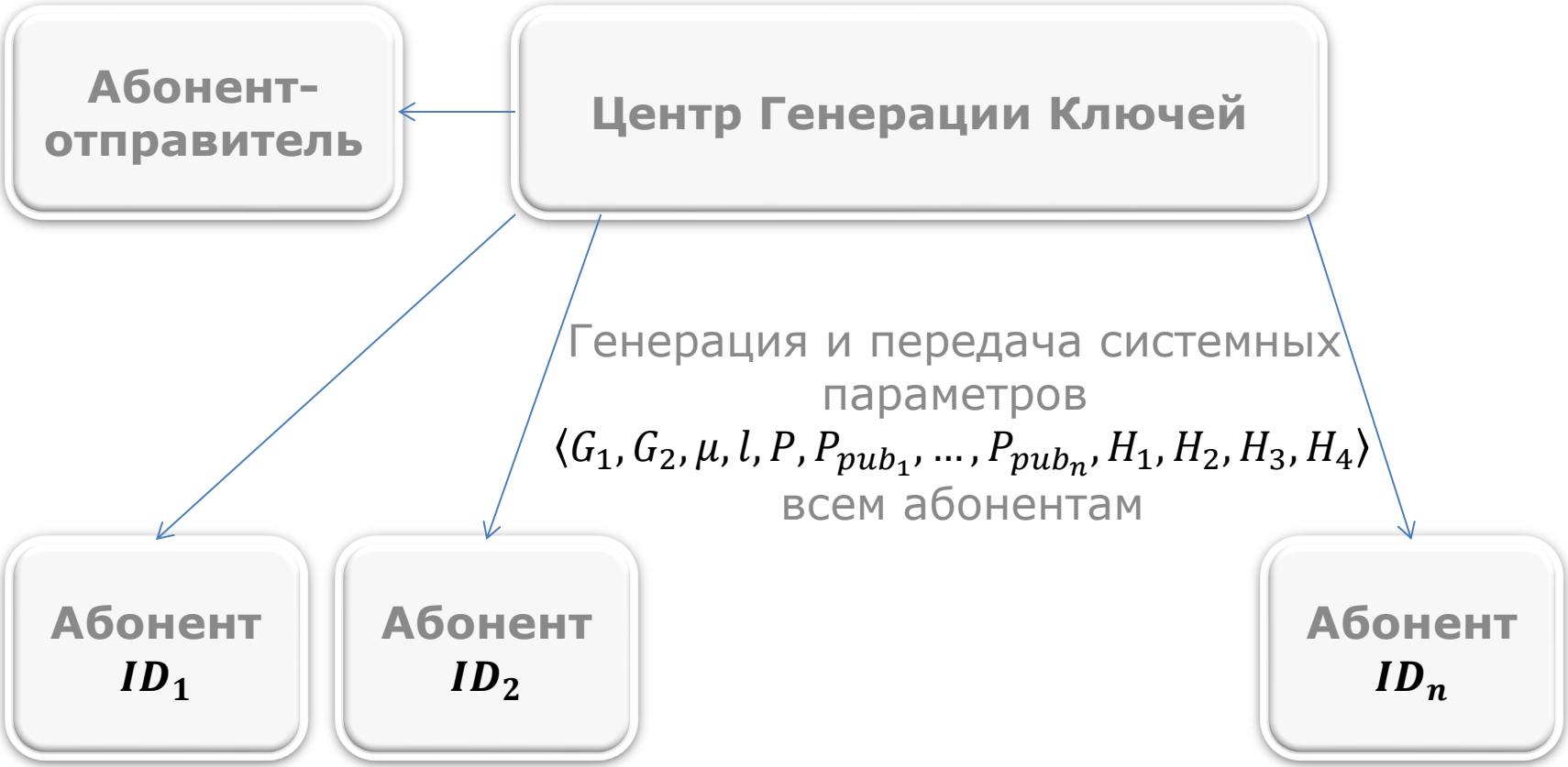
MDH заключается в вычислении $\mu(P, \ldots, P)^{a_1 \ldots a_{n+1}} \in G_2$

# Мультилинейная криптосистема группового личностного шифрования (МГЛШ)

ЦГК – Центр Генерации Ключей

- Инициализация
- Получение закрытого ключа
- Шифрование
- Расшифрование

# МГЛШ - Инициализация



# МГЛШ - Инициализация

ЦГК:

$k$ - параметр стойкости

$G_1$ - аддитивная группа порядка $p$

$G_2$ - мультипликативная группа порядка $p$

$p$ – простое число

$P$ – образующий элемент группы $G_1$

$\mu: \underbrace{G_1 \times \cdots \times G_1}_{2n} \to G_2$ - $2n$-мультилинейное отображение

# МГЛШ - Инициализация

ЦГК:

$s_1, \dots, s_n \in \mathbb{Z}_p^*$ - псевдослучайно выбранные элементы, секретные мастер-ключи абонентов

$P_{pub_1} = s_1 P, \dots, P_{pub_n} = s_n P$, где $P_{pub_i} \in G_1$ - открытые мастер-ключи абонентов

Криптографические хеш-функции:

$H_1: \{0,1\}^* \to G_1^*$

$H_2: G_2 \to \{0,1\}^l$ для некоторого $l \in \mathbb{Z}$

$H_3: \{0,1\}^l \times \{0,1\}^l \to \mathbb{Z}_p^*$

$H_4: \{0,1\}^l \to \{0,1\}^l$

# МГЛШ - Инициализация

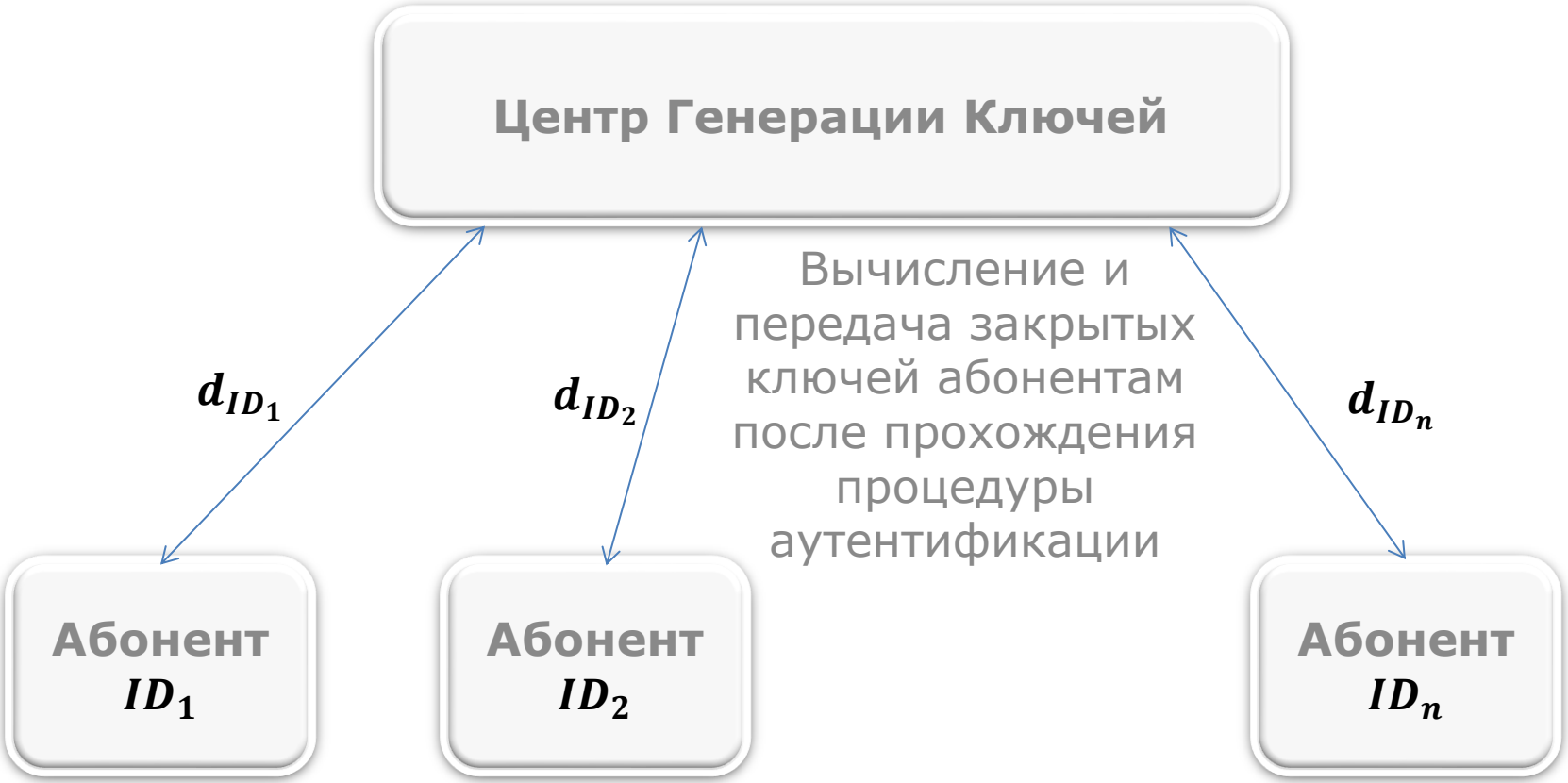
ЦГК:

$\vartheta \in \{0,1\}^l$ - пространство сообщений

$\gamma = G_1^* \times \{0,1\}^l \times \{0,1\}^l$ - пространство шифртекстов

$\langle G_1, G_2, \mu, l, P, P_{pub_1}, \dots, P_{pub_n}, H_1, H_2, H_3, H_4 \rangle$ - системные параметры

# МГЛШ - Получение закрытого ключа



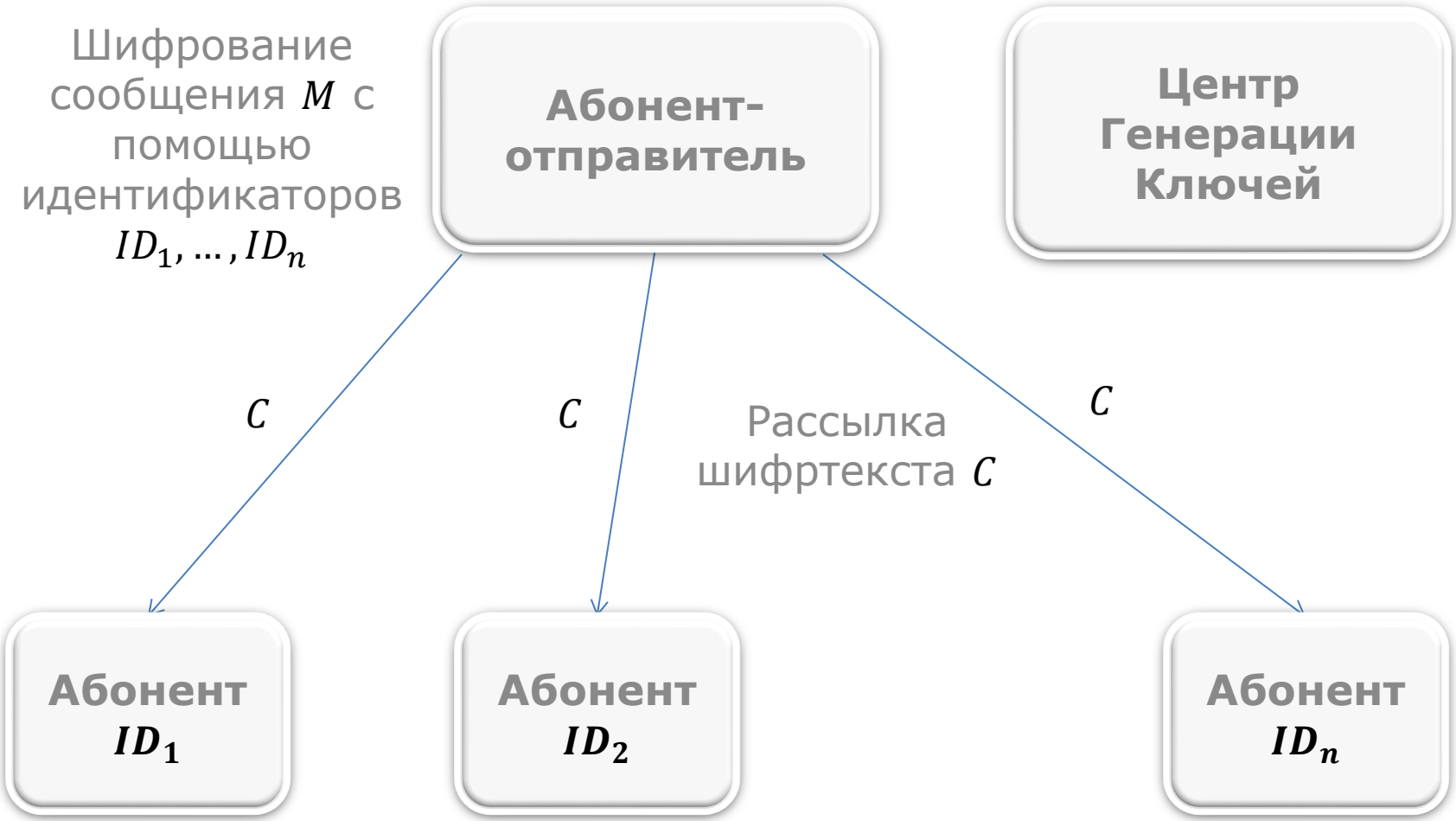
# МГЛШ - Получение закрытого ключа

ЦГК:

$Q_{ID_1} = H_1(ID_1) \in G_1^*, \dots, Q_{ID_n} = H_1(ID_n) \in G_1^*$, где $ID_1, \dots, ID_n \in \{0,1\}^*$ - идентификаторы абонентов

$d_{ID_1} = s_1 Q_{ID_1}, \dots, d_{ID_n} = s_n Q_{ID_n}, d_{ID_i} \in G_1^*$- закрытые ключи абонентов, где $s_1, \dots, s_n$ - секретные мастер-ключи

# МГЛШ - Шифрование



# МГЛШ - Шифрование

$M \in \vartheta$ – сообщение, предназначенное абонентам $ID_1, \dots, ID_n \in \{0,1\}^*$

Отправитель:

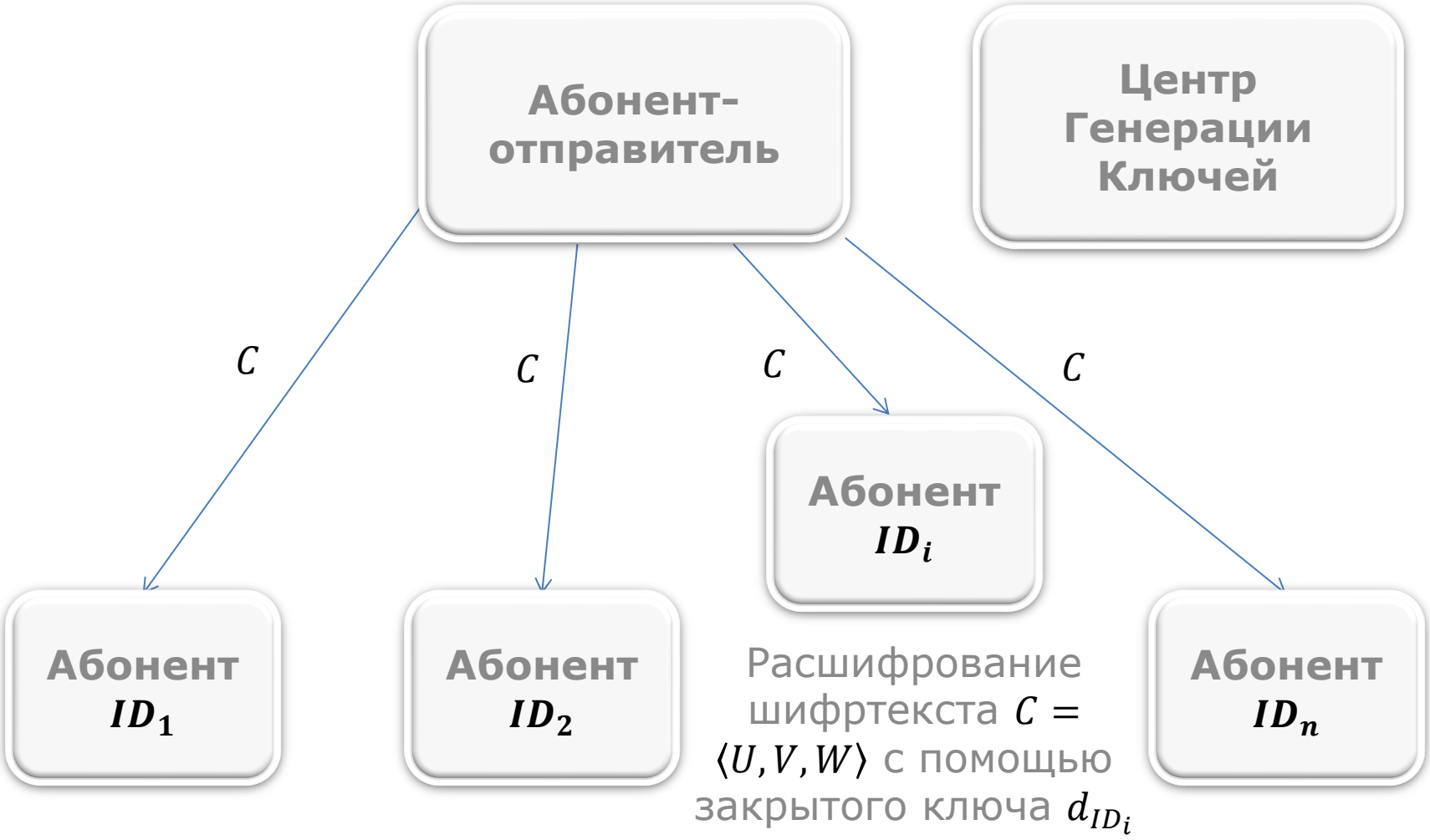
$Q_{ID_1} = H_1(ID_1) \in G_1^*, \dots, Q_{ID_n} = H_1(ID_n) \in G_1^*$

$\sigma \in \{0,1\}^l, l \in \mathbb{Z}$ - псевдослучайно выбранный вектор

$r = H_3(\sigma, M) \in \mathbb{Z}_p^*$

$C = \langle rP, \sigma \oplus H_2(g^r), M \oplus H_4(\sigma) \rangle \in \gamma$ - шифртекст, где $g = \mu(Q_{ID_1}, \dots, Q_{ID_n}, P_{pub_1}, \dots, P_{pub_n}) \in G_2^*$

# МГЛШ - Расшифрование



# МГЛШ - Расшифрование

$C = \langle U, V, W \rangle \in \gamma$ – шифртекст

Абонент $ID_i$:

Проверка $U \in G_1^*$. Если $U \notin G_1^*$, то шифртекст отклоняется.

$$V \oplus H_2\left(\mu(Q_{ID_1}, \dots, Q_{ID_{i-1}}, d_{ID_i}, Q_{ID_{i+1}}, \dots, Q_{ID_n}, P_{pub_1}, \dots, P_{pub_{i-1}}, U, P_{pub_{i+1}}, \dots, P_{pub_n})\right) = \sigma$$

$$W \oplus H_4(\sigma) = M$$

$$r = H_3(\sigma, M), r \in \mathbb{Z}_p^*$$

Проверка $U = rP$. Если равенство не выполняется, то сообщение $M$ отклоняется, в противном случае сообщение $M$ принимается

# МГЛШ - Корректность криптосистемы

$$\mu\left(Q_{ID_1}, \dots, Q_{ID_{i-1}}, d_{ID_i}, Q_{ID_{i+1}}, \dots, Q_{ID_n}, P_{pub_1}, \dots, P_{pub_{i-1}}, U, P_{pub_{i+1}}, \dots, P_{pub_n}\right)$$
$$= \mu\left(Q_{ID_1}, \dots, Q_{ID_n}, P_{pub_1}, \dots, P_{pub_{i-1}}, P, P_{pub_{i+1}}, \dots, P_{pub_n}\right)^{s_i r}$$
$$= \mu\left(Q_{ID_1}, \dots, Q_{ID_n}, P_{pub_1}, \dots, P_{pub_n}\right)^{r} = g^r$$

# Игра злоумышленника и запросчика

# Стойкость криптосистемы - Инициализация

Запросчик, представляющий криптосистему шифрования, принимает параметр стойкости $k \in \mathbb{N}$, запускает процедуру инициализации криптосистемы, передает злоумышленнику $A$ системные параметры $params$ и сохраняет мастер-ключи в секрете

# Стойкость криптосистемы – Этап 1

Злоумышленник $A$ генерирует запросы $q_1, \dots, q_m$ и отправляет их запросчику, где $q_j$ является:

1. Запросом закрытого ключа $\langle ID'_j \rangle$. В данном случае запросчик выполняет алгоритм получения закрытого ключа $d'_j \in G_1$, соответствующего открытому ключу $\langle ID'_j \rangle$ и передает $d'_j$ злоумышленнику

2. Запросом расшифрования $\langle ID'_j, C'_j \rangle$. В данном случае запросчик выполняет алгоритм генерации ключа $d'_j$, соответствующего открытому ключу $\langle ID'_j \rangle$. Далее выполняет алгоритм расшифрования шифртекста $C'_j$ с помощью $d'_j$ и передает полученный открытый текст злоумышленнику

Запросы проводятся адаптивно, т.е. каждый запрос $q_j$ может зависеть от ответов на запросы $q_1, \dots, q_{j-1}$

# Стойкость криптосистемы - Задача

Злоумышленник генерирует 2 открытых текста $M_0, M_1 \in \vartheta$ равной длины и набор идентификаторов абонентов $ID_1, \dots, ID_n$, для которых он проводит атаку.

$ID_i \neq ID'_j$ при $i = 1, \dots, n;\ j = 1, \dots, m$ во время этапа 1

$\vartheta$ - множество текстов произвольной длины

Запросчик псевдослучайно выбирает бит $b \in \{0,1\}$ и отправляет $C_b = Encrypt(params, ID_1, \dots, ID_n, M_b)$ злоумышленнику

# Стойкость криптосистемы – Этап 2

Злоумышленник генерирует запросы $q_{m+1}, \dots, q_s$ и отправляет их запросчику, где $q_j$ является:

1. Запросом закрытого ключа $\langle ID'_j \rangle$. При этом $ID'_j \neq ID_i$ для $j = m+1, \dots, s;\ i = 1, \dots, n$. Запросчик отвечает также как и во время этапа 1
2. Запросом расшифрования $\langle ID'_j, C'_j \rangle$. При этом $\langle ID'_j, C'_j \rangle \neq \langle ID_i, C_i \rangle$ для $j = m+1, \dots, s;\ i = 1, \dots, n$. Запросчик отвечает также, как и во время этапа 1.

Данные запросы могут проводиться адаптивно, как и во время этапа 1

# Стойкость криптосистемы - Результат

Злоумышленник возвращает бит $b' \in \{0,1\}$ и выигрывает игру, если $b = b'$

Выигрышем при проведении атаки на криптосистему шифрования с помощью описанной выше игры является следующая функция параметра стойкости $k \in \mathbb{N}$:

$$Adv_{E,A}(k) = \left|\Pr[b = b'] - \frac{1}{2}\right|$$

# Стойкость к адаптивной атаке с выбором шифртекста

Мультилинейная криптосистема группового личностного шифрования является семантически стойкой к адаптивной атаке с выбором шифртекста (IND-IDB-CCA стойкой), если для всех полиномиальных во времени злоумышленников $A$, способных проводить запросы закрытого ключа и расшифрования (IND-IDB-CCA злоумышленников), функция $Adv_{E,A}(k)$ является пренебрежимо малой

# Стойкость к адаптивной атаке с выбором открытого текста

Мультилинейная криптосистема группового личностного шифрования является семантически стойкой к адаптивной атаке с выбором открытого текста (IND-IDB-CPA стойкой), если для всех полиномиальных во времени злоумышленников $A$, способных проводить только запросы закрытого ключа (IND-IDB-CPA злоумышленников), функция $Adv_{E,A}(k)$ является пренебрежимо малой

# Схема доказательства стойкости

Обозначим построенную криптосистему МГЛШ как MulFullIdent.

Для доказательства IND-IDB-CCA стойкости MulFullIdent необходимо доказать IND-CPA стойкость криптосистемы MulBasicPub, являющейся модификацией криптосистемы MulBasicIdent до стандартной криптосистемы шифрования с открытым ключом

# Теорема о стойкости МГЛШ

**Теорема.** В предположении, что хеш-функции $H_1, H_2, H_3, H_4$ являются случайными оракулами, криптосистема MulFullIdent является IND-IDB-CCA стойкой при предположении сложности проблемы MDH в генерируемых генератором $G$ группах

# Дополнение к теореме о стойкости МГЛШ

Пусть существует IND-IDB-CCA злоумышленник $A$, имеющий для каждого абонента выигрыш $\varepsilon(k) \in \mathbb{R}$

и время выполнения, не превышающее $t(k) \in \mathbb{R}$, где $k \in \mathbb{N}$ - параметр стойкости.

Пусть $A$ выполняет не более $q_E \in \mathbb{N}$ запросов закрытого ключа, не более $q_D \in \mathbb{N}$ запросов расшифрования и не более $q_{H_2}, q_{H_3}, q_{H_4} \in \mathbb{N}$ запросов к хеш-функциям $H_2, H_3, H_4$ соответственно

# Дополнение к теореме о стойкости МГЛШ

Тогда существует алгоритм $B$, решающий MDH для генератора $G$, при этом для его выигрыша $Adv_{G,B}(k)$ и времени выполнения $t_1(k)$ справедливы следующие неравенства:

$$Adv_{G,B}(k) \geq \frac{2nFO_{adv}\left(\frac{\varepsilon(k)}{e(1+q_E+q_D)}, q_{H_4}, q_{H_3}, q_D\right)}{q_{H_2}}$$

$$t_1(k) \leq nFO_{time}\left(t(k), q_{H_4}, q_{H_3}\right)$$

# Дополнение к теореме о стойкости МГЛШ

Функции $FO_{adv}$ и $FO_{time}$ определены следующим образом:

$$FO_{adv}\left(\varepsilon(k), q_{H_4}, q_{H_3}, q_D\right) = \frac{1}{2\left(q_{H_4} + q_{H_3}\right)}\left((\varepsilon(k)+1)(1-2/p)^{q_D} - 1\right)$$

$$FO_{time}\left(t(k), q_{H_4}, q_{H_3}\right) = t(k) + O\left(\left(q_{H_4} + q_{H_3}\right)l\right)$$

$n$ – количество абонентов, $l \in \mathbb{N}$ - длина $\sigma$

# Планы дальнейших исследований

- Построение эффективных мультилинейных отображений
- Реализация групповых личностных криптосистем в сетевых решениях и решениях по обработке данных

Спасибо за внимание!