

**О неподделываемости схем
подписи вслепую Эль-Гамала
при атаке с последовательными
сеансами**

Бабуева Александра Алексеевна

Махонин Илья Владимирович

Смышляев Станислав Витальевич

Утехина Мария Павловна

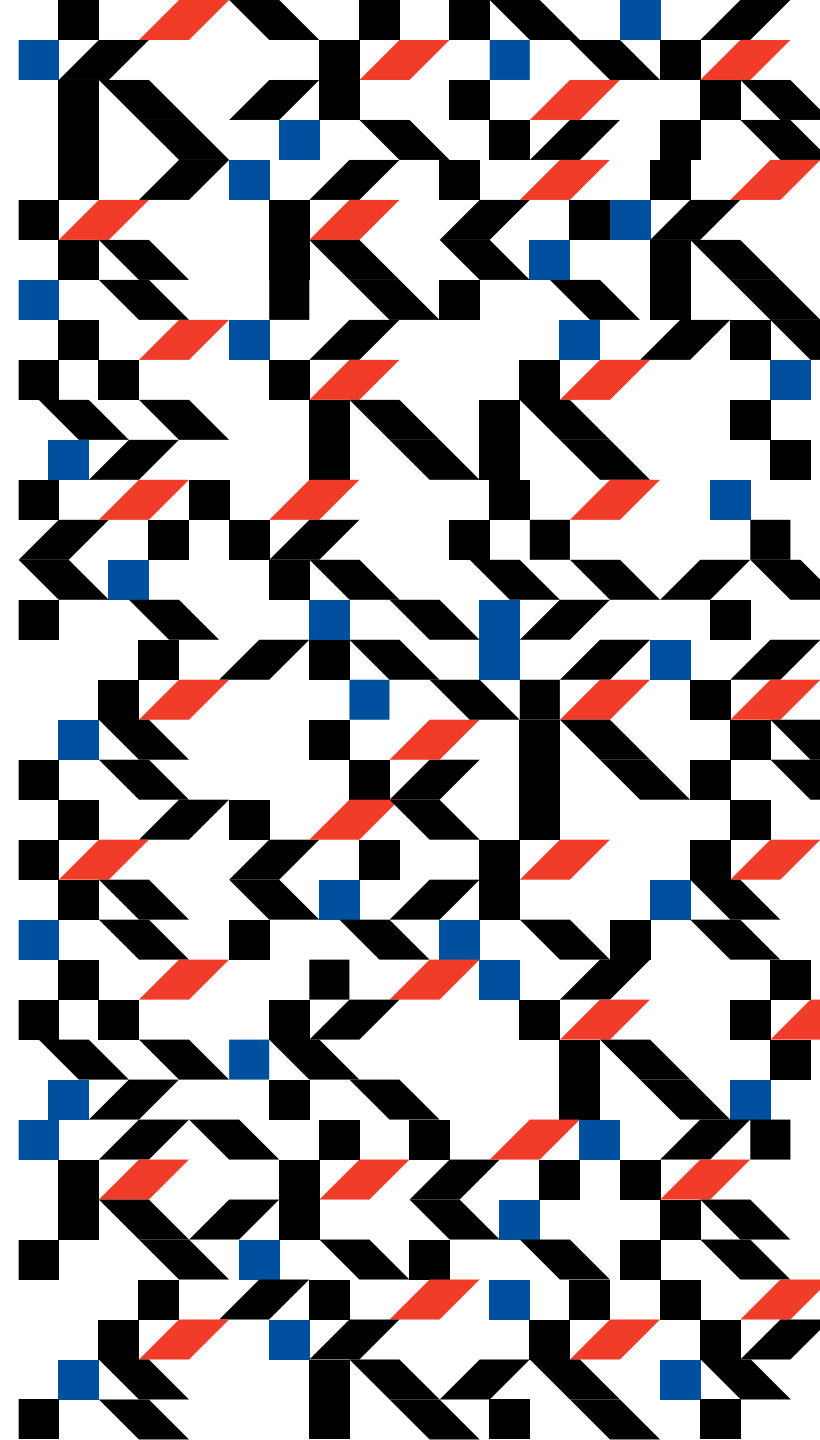
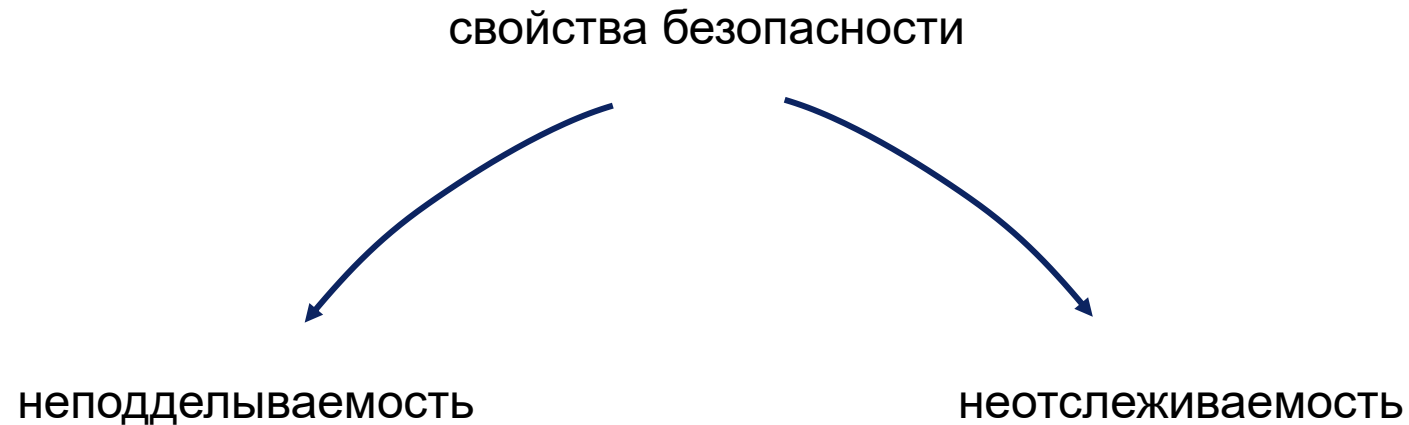


Схема подписи вслепую

- $(sk, pk) \leftarrow KeyGen()$: алгоритм генерации ключей
- $(b, \sigma) \leftarrow \langle Signer(sk), User(pk, m) \rangle$: интерактивный протокол, выполняемый между подписывающей стороной, владеющей ключом подписи sk , и клиентом, владеющим сообщением m
- $b \leftarrow Verify(pk, m, \sigma)$: алгоритм проверки подписи

Схема подписи вслепую

- $(sk, pk) \leftarrow \text{KeyGen}()$: алгоритм генерации ключей
- $(b, \sigma) \leftarrow \langle \text{Signer}(sk), \text{User}(pk, m) \rangle$: интерактивный протокол, выполняемый между подписывающей стороной, владеющей ключом подписи sk , и клиентом, владеющим сообщением m
- $b \leftarrow \text{Verify}(pk, m, \sigma)$: алгоритм проверки подписи

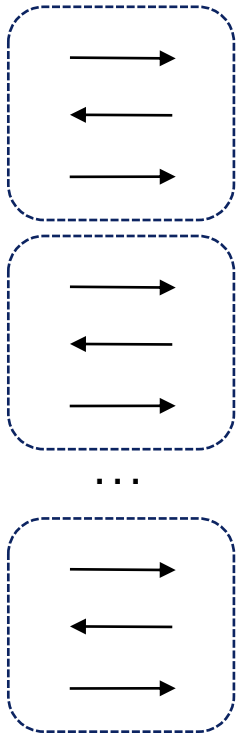


Свойство неподдельности

знать все данные
честного клиента

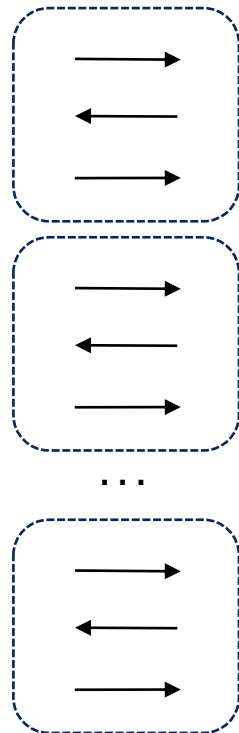
Signer

User



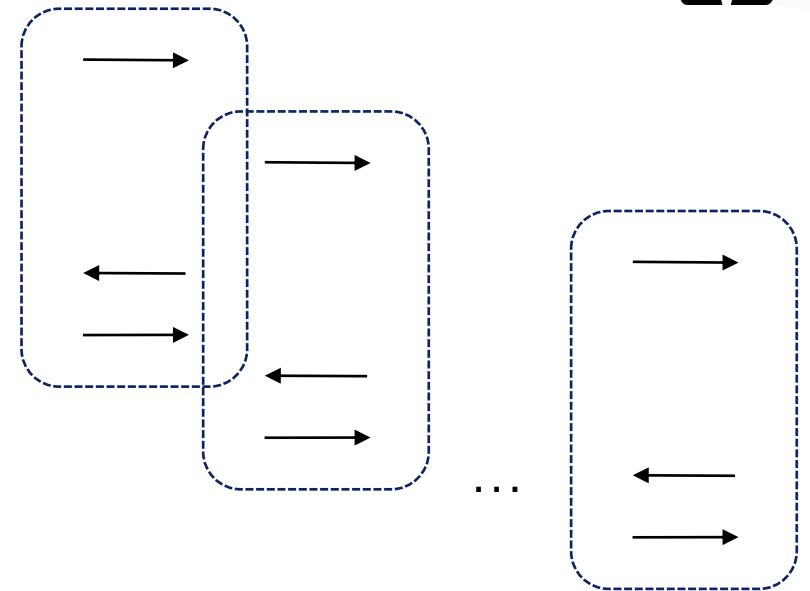
открывать
последовательные
сеансы

Signer



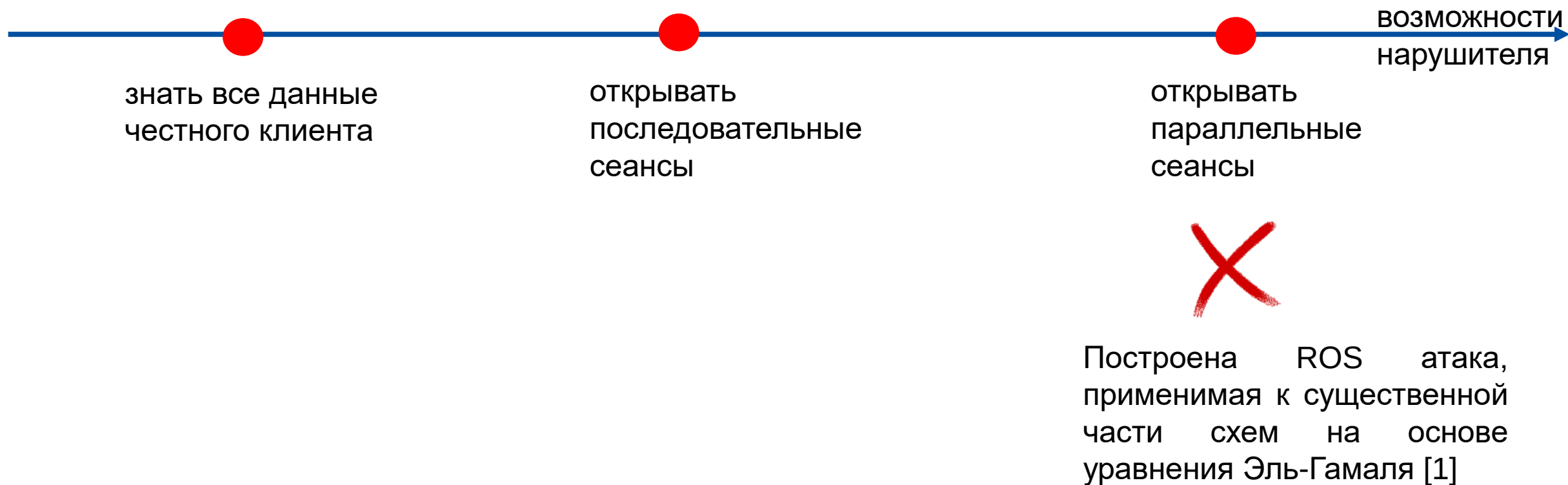
открывать
параллельные
сеансы

Signer



ВОЗМОЖНОСТИ
нарушителя

Схемы подписи вслепую Эль-Гамала: в предыдущих сериях



[1] Akhmetzyanova L. R., Alekseev E. K., Babueva A. A., Smyshlyaev S. V. «On the (im)possibility of secure ElGamal blind signatures», 2023

Схемы подписи вслепую Эль-Гамала: в предыдущих сериях

знать все данные
честного клиента



Схемы, являющиеся слепыми модификациями классических схем Эль-Гамала, обеспечивают свойство неподделываемости, если базовая схема Эль-Гамала обеспечивает свойство неподделываемости [2].

открывать
последовательные
сеансы

открывать
параллельные
сеансы



Построена ROS атака, применяемая к существенной части схем на основе уравнения Эль-Гамала [1].

ВОЗМОЖНОСТИ
нарушителя

[1] Akhmetzyanova L. R., Alekseev E. K., Babueva A. A., Smyshlyaev S. V. «On the (im)possibility of secure ElGamal blind signatures», 2023

 [2] Akhmetzyanova L. R., Babueva A. A., Bozhko A. A., «Blind signature as a shield against backdoors in smart-cards», 2024

Схемы подписи вслепую Эль-Гамала: в предыдущих сериях

знать все данные
честного клиента



Схемы, являющиеся слепыми модификациями классических схем Эль-Гамала, обеспечивают свойство неподделываемости, если базовая схема Эль-Гамала обеспечивает свойство неподделываемости [2].

открывать
последовательные
сеансы



открывать
параллельные
сеансы



Построена ROS атака, применяемая к существенной части схем на основе уравнения Эль-Гамала [1].

ВОЗМОЖНОСТИ
нарушителя

[1] Akhmetzyanova L. R., Alekseev E. K., Babueva A. A., Smyshlyaev S. V. «On the (im)possibility of secure ElGamal blind signatures», 2023

[2] Akhmetzyanova L. R., Babueva A. A., Bozhko A. A., «Blind signature as a shield against backdoors in smart-cards», 2024

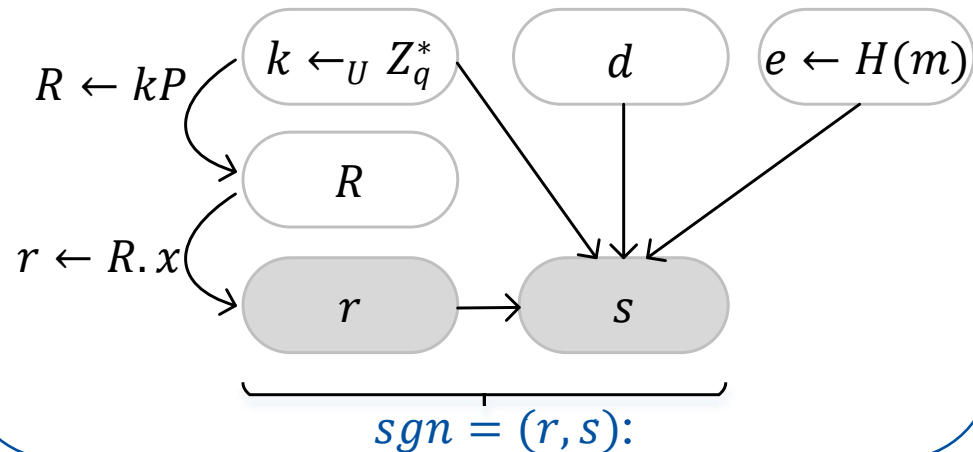
Схемы Эль-Гамала

Схема подписи Эль-Гамала

KeyGen():

$d \leftarrow_U \mathbb{Z}_q^*$
 $Q \leftarrow dP$
return (d, Q)

Sign(d, m):



Уравнение подписи Эль-Гамала:

$$\underbrace{G_d(r, e, s) \cdot d + G_k(r, e, s) \cdot k + G_0(r, e, s)}_{EG(d, k, r, e, s)} = 0$$

q – простой порядок подгруппы группы точек эллиптической кривой

P – точка кривой порядка q

p – порядок поля, над которым определена эллиптическая кривая

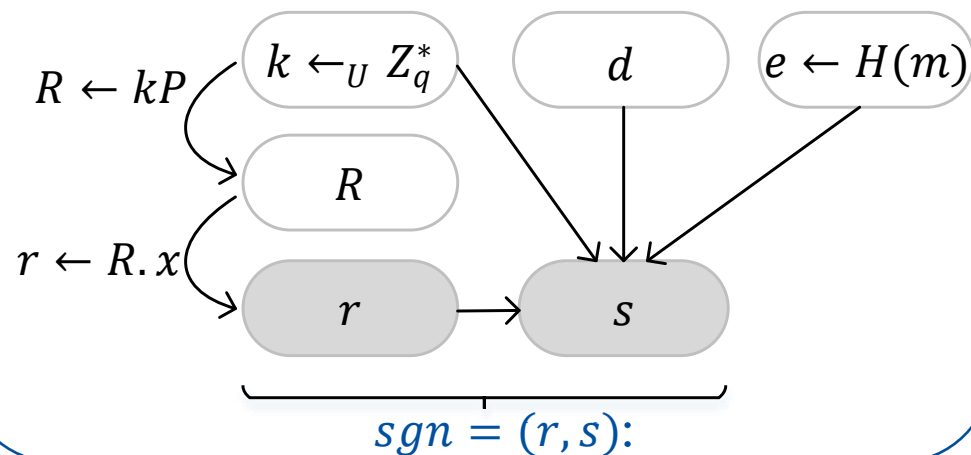
$H: \{0,1\}^* \rightarrow \mathbb{Z}_q$ – криптографическая хэш-функция

Схема подписи Эль-Гамала

KeyGen():

$d \leftarrow_U \mathbb{Z}_q^*$
 $Q \leftarrow dP$
 return (d, Q)

Sign(d, m):



Список допустимых уравнений [3]:

- | | | |
|-------------------|---------------------|--------------------------|
| 1 : $ed = rk + s$ | 7 : $red = k + s$ | 13 : $(r + e)d = k + s$ |
| 2 : $ed = sk + r$ | 8 : $d = rek + s$ | 14 : $d = (r + e)k + s$ |
| 3 : $rd = ek + s$ | 9 : $sd = k + re$ | 15 : $sd = k + (r + e)$ |
| 4 : $rd = sk + e$ | 10 : $d = sk + re$ | 16 : $d = sk + (r + e)$ |
| 5 : $sd = rk + e$ | 11 : $red = sk + 1$ | 17 : $(r + e)d = sk + 1$ |
| 6 : $sd = ek + r$ | 12 : $sd = rek + 1$ | 18 : $sd = (r + e)k + 1$ |



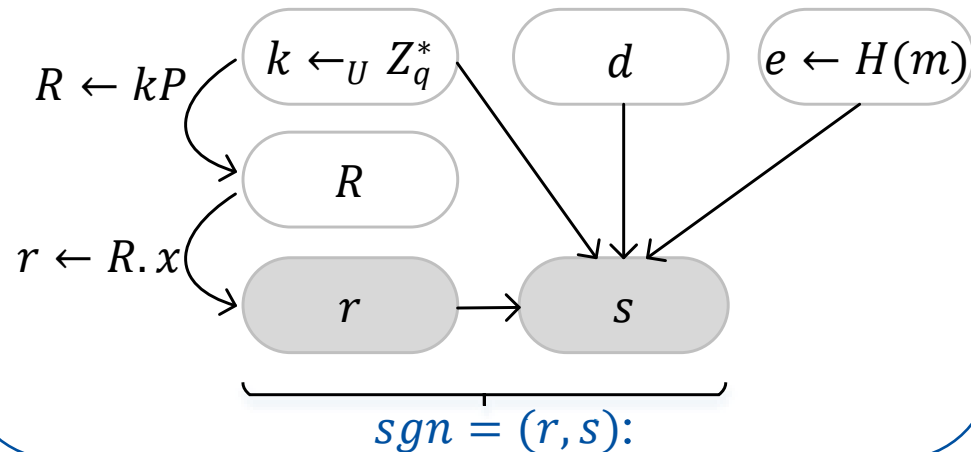
[3] Harn X. «Design of generalised ElGamal type digital signature schemes based on discrete logarithm», 1994

Схема подписи Эль-Гамала

KeyGen():

$d \leftarrow_U \mathbb{Z}_q^*$
 $Q \leftarrow dP$
 return (d, Q)

Sign(d, m):



Список допустимых уравнений [3]:

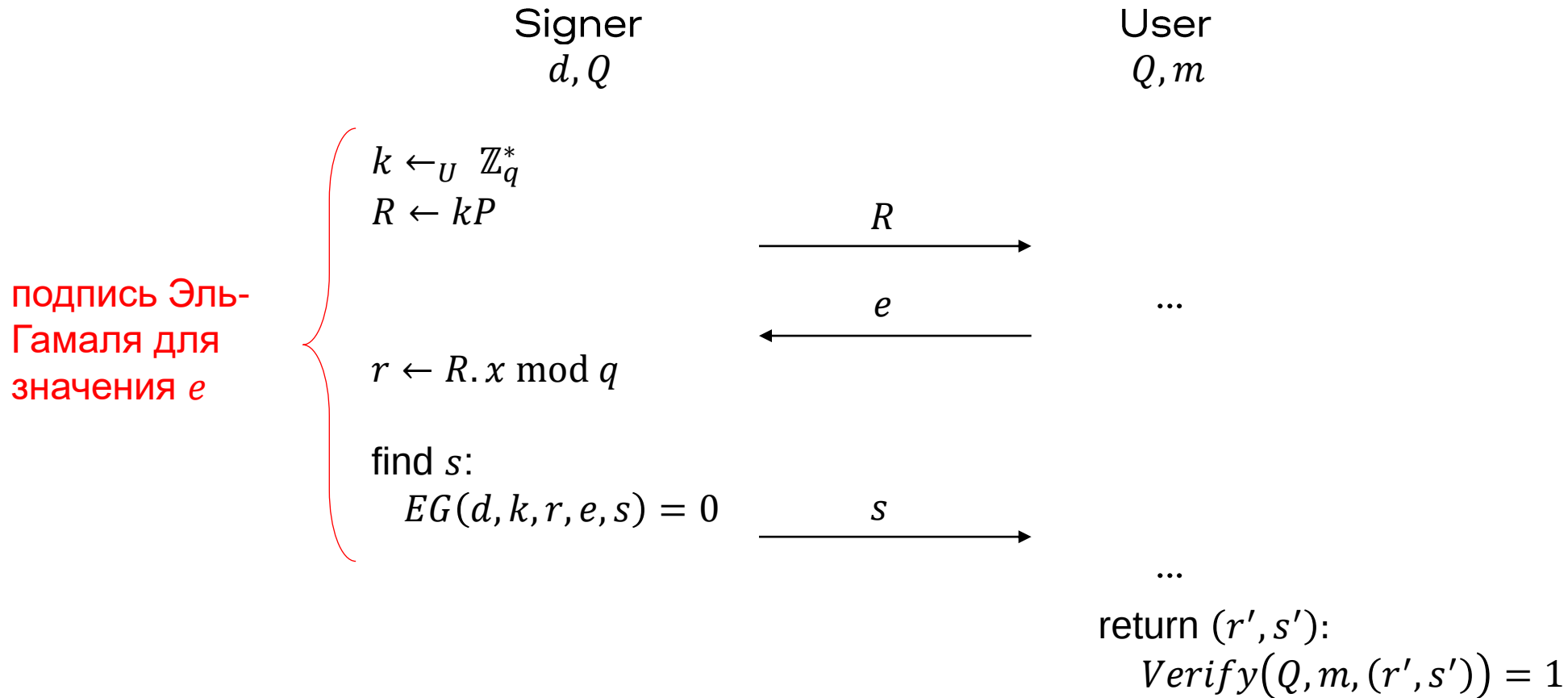
- | | | |
|-------------------|---------------------|--------------------------|
| 1 : $ed = rk + s$ | 7 : $red = k + s$ | 13 : $(r + e)d = k + s$ |
| 2 : $ed = sk + r$ | 8 : $d = rek + s$ | 14 : $d = (r + e)k + s$ |
| 3 : $rd = ek + s$ | 9 : $sd = k + re$ | 15 : $sd = k + (r + e)$ |
| 4 : $rd = sk + e$ | 10 : $d = sk + re$ | 16 : $d = sk + (r + e)$ |
| 5 : $sd = rk + e$ | 11 : $red = sk + 1$ | 17 : $(r + e)d = sk + 1$ |
| 6 : $sd = ek + r$ | 12 : $sd = rek + 1$ | 18 : $sd = (r + e)k + 1$ |

ГОСТ

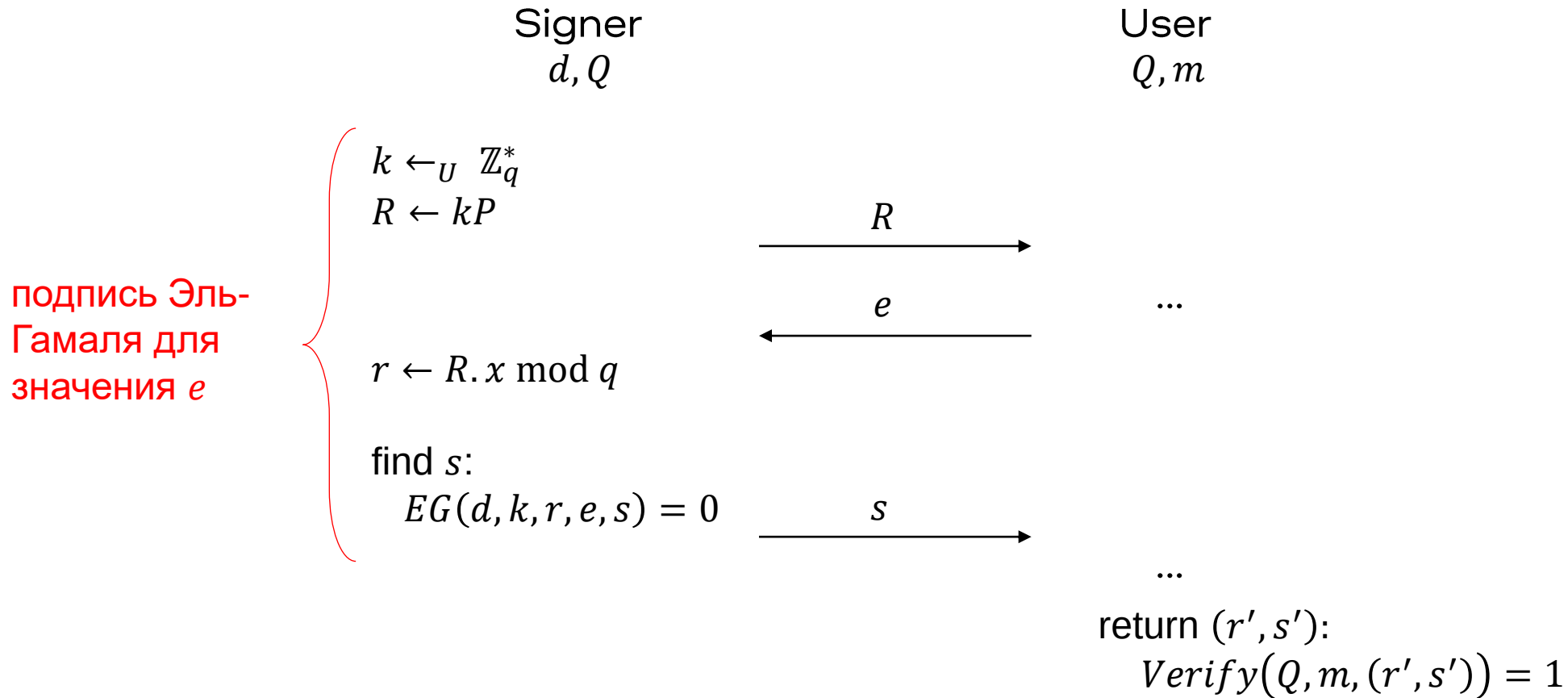


[3] Harn X. «Design of generalised ElGamal type digital signature schemes based on discrete logarithm», 1994

Схемы подписи вслепую Эль-Гамала (класс GenEG-BS [1])



Схемы подписи вслепую Эль-Гамала (класс GenEG-BS)



Схемы на основе различных уравнений EG имеют одинаковые характеристики (скорость генерации подписи, размер подписи).



Схемы GenEG-BS типа I (класс GenEG-BSI)

Уравнение подписи:

$$G_d(r, e, s) \cdot d + G_k(r, e, s) \cdot k + G_0(r, e, s) = 0$$

НЕ ЗАВИСИТ ОТ s

ЗАВИСИТ ОТ s

Условие: уравнение подписи может быть представлено в виде

$$k + Y_1(r, e) \cdot G_1(d) + Y_2(r, e, s) \cdot G_2(d) = 0,$$

где функции G_1 и G_2 аффинны по d , функция Y_1 существенно зависит от e , и функция Y_2 является дробно-линейной по s .

Схемы такого типа не обеспечивают свойство неподделываемости при атаке с параллельными сеансами [1].

Целевая модель безопасности



Модель безопасности SEQ-UF

Возможности нарушителя:

выступать в роли клиента, открывать сеансы протокола формирования подписи последовательным образом

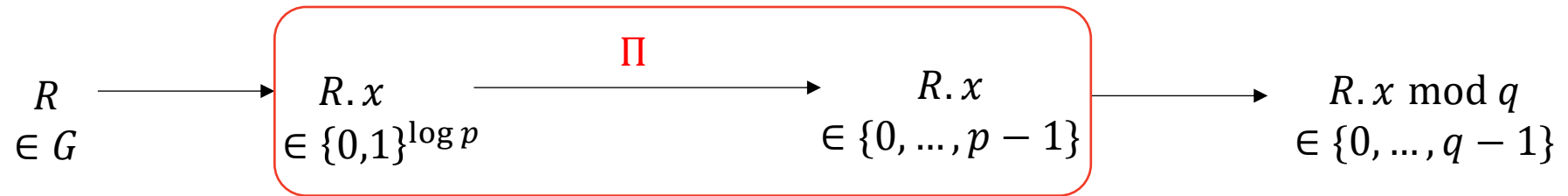
Угроза: сформировать подделку подписи

Идеализации:

- модель со случайным оракулом (хэш-функция H моделируется как случайная функция)
- модель с алгебраической группой и биективным случайным оракулом

Модель BRO (bijective random oracle) [4]

Идеализация способа вычисления значения r :

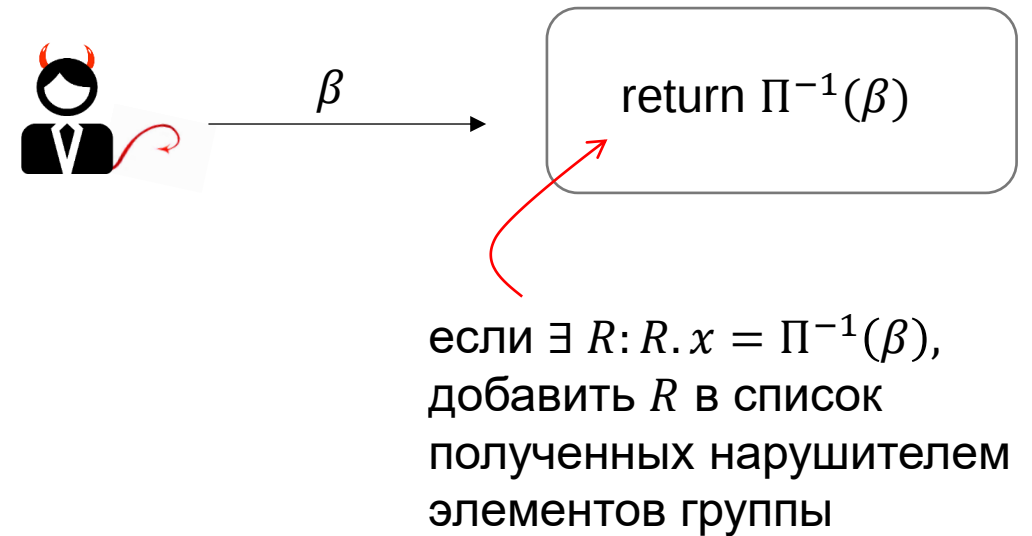
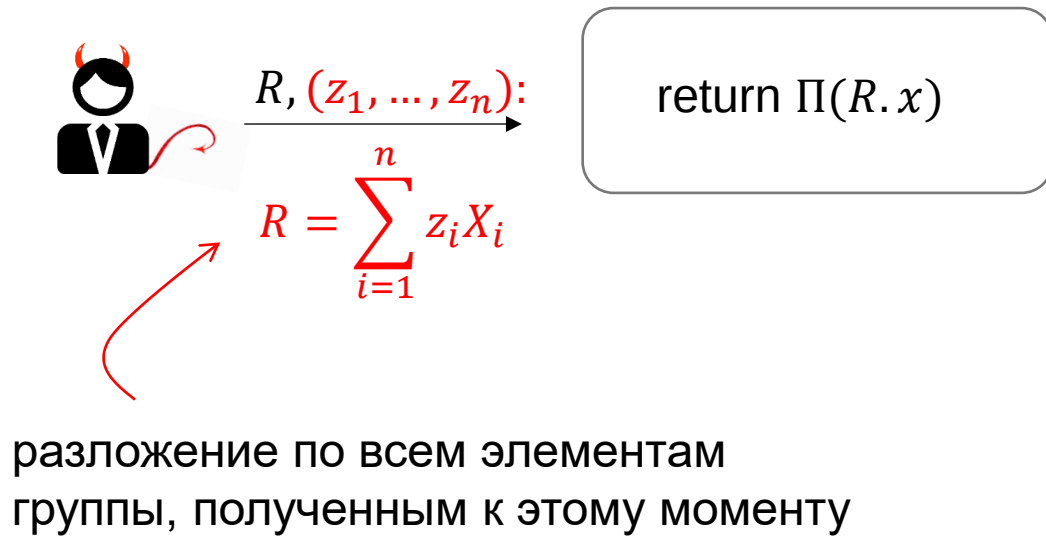


Π – случайное биективное преобразование

Нарушитель имеет доступ к прямому и обратному преобразованию Π :



Модель **ABRO** (**algebraic bijective random oracle**) [5]

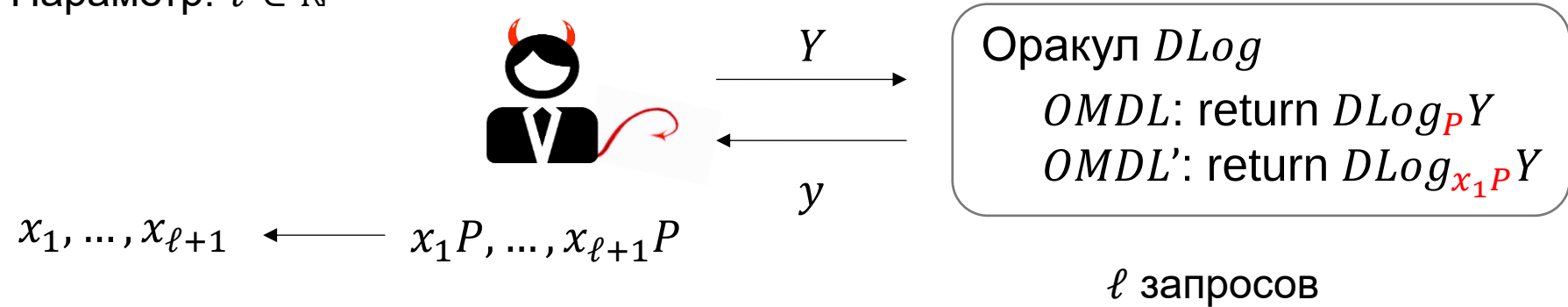


Базовые задачи



Задачи $OMDL$ и $OMDL'$ (One-More Discrete Logarithm)

Параметр: $\ell \in \mathbb{N}$

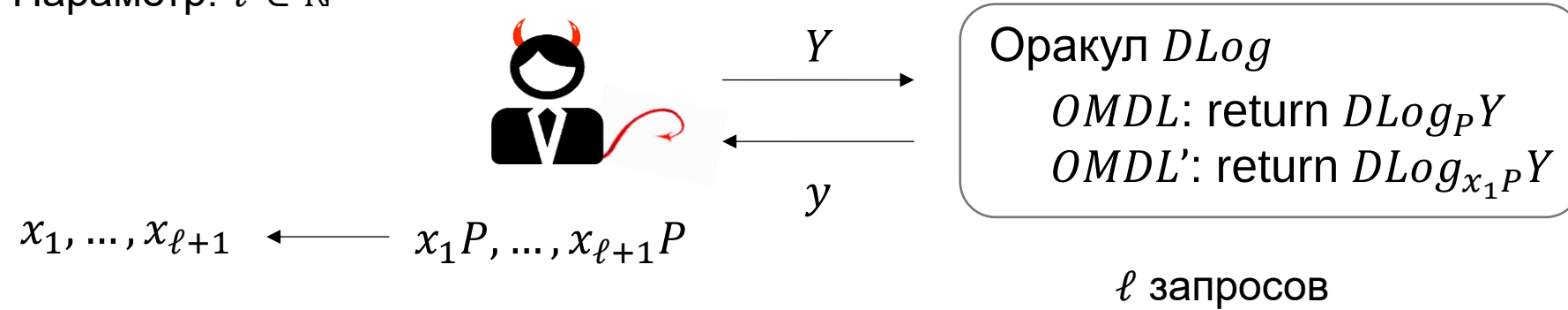


$$Adv_{G,\ell}^{OMDL}(\mathcal{A}) = \Pr \left(\begin{array}{l} x'_1, \dots, x'_{\ell+1} \leftarrow \mathcal{A}^{DLog}(x_1 P, \dots, x_{\ell+1} P): \\ x'_1 = x_1, \dots, x'_{\ell+1} = x_{\ell+1} \end{array} \middle| x_1, \dots, x_{\ell+1} \leftarrow_U \mathbb{Z}_q^* \right)$$

Задача $OMDL$ введена в [6]. Не известно методов решения этой задачи лучших, чем решение задачи дискретного логарифмирования для одной из входных точек.

Задачи $OMDL$ и $OMDL'$ (One-More Discrete Logarithm)

Параметр: $\ell \in \mathbb{N}$

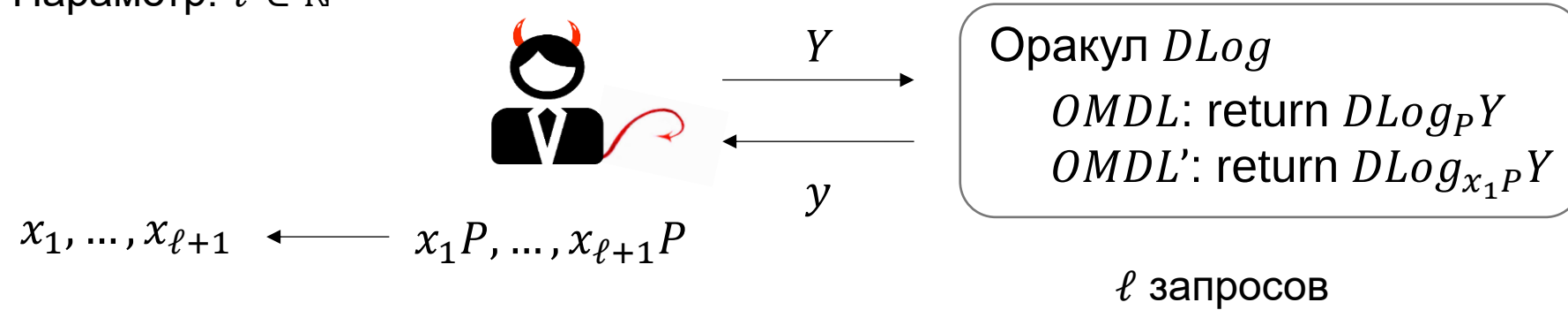


Задача $OMDL'$ с параметром ℓ не сложнее, чем задача $OMDL$ с параметром $(\ell - 1)$:

$$Adv_{G, \ell-1}^{OMDL}(\mathcal{A}) \leq Adv_{G, \ell}^{OMDL'}(\mathcal{B})$$

Задачи $OMDL$ и $OMDL'$ (One-More Discrete Logarithm)

Параметр: $\ell \in \mathbb{N}$



Если образующая точка P не фиксированная, а выбирается случайно равномерно и подается на вход нарушителю, то задача $OMDL'$ не сложнее задачи $OMDL$:

$$Adv_{G,\ell}^{OMDL'}(\mathcal{A}) \leq Adv_{G,\ell}^{OMDL}(\mathcal{B})$$

Основной результат

Схемы GenEG-BS типа I (класс GenEG-BSI)

Уравнение подписи:

$$k + Y_1(r, e) \cdot G_1(d) + Y_2(r, e, s) \cdot G_2(d) = 0$$

схемы типа А

$$k + Y_1(r, e) \cdot d + Y_2(r, e, s) = 0$$

схемы типа В

$$k + Y_1(r, e) + Y_2(r, e, s) \cdot d = 0$$

Оценка стойкости

$$Adv_{GenEG-BS_I}^{SEQ-UF}(\mathcal{A}) \leq Adv_{G,t}^{TASK}(\mathcal{B}) + \frac{(q_{\Pi} + 2q_{\Pi^{-1}} + 3t + 2)^2}{q} + \frac{4q_H^2}{q},$$

где

- $TASK = OMDL$ для схем типа А и $TASK = OMDL'$ для схем типа В
- t – количество открытых сеансов протокола формирования подписи
- q_H – количество запросов к случайному оракулу H
- q_{Π} – количество вычислений преобразования Π
- $q_{\Pi^{-1}}$ – количество вычислений преобразования Π^{-1}

Оценка стойкости

$$Adv_{GenEG-BS_I}^{SEQ-UF}(\mathcal{A}) \leq Adv_{G,t}^{TASK}(\mathcal{B}) + \frac{(q_{\Pi} + 2q_{\Pi^{-1}} + 3t + 2)^2}{q} + \frac{4q_H^2}{q},$$

где

- $TASK = OMDL$ для схем типа А и $TASK = OMDL'$ для схем типа В
- t – количество открытых сеансов протокола формирования подписи
- q_H – количество запросов к случайному оракулу H
- q_{Π} – количество вычислений преобразования Π
- $q_{\Pi^{-1}}$ – количество вычислений преобразования Π^{-1}

атаки, направленные на восстановление ключа подписи d или эфемерных секретов $k_1, \dots, k_t$ в одном из t сеансов

Оценка стойкости

$$Adv_{GenEG-BS_I}^{SEQ-UF}(\mathcal{A}) \leq Adv_{G,t}^{TASK}(\mathcal{B}) + \frac{(q_{\Pi} + 2q_{\Pi^{-1}} + 3t + 2)^2}{q} + \frac{4q_H^2}{q},$$

где

- $TASK = OMDL$ для схем типа А и $TASK = OMDL'$ для схем типа В
- t – количество открытых сеансов протокола формирования подписи
- q_H – количество запросов к случайному оракулу H
- q_{Π} – количество вычислений преобразования Π
- $q_{\Pi^{-1}}$ – количество вычислений преобразования Π^{-1}

атаки, предполагающие накопление большого количества пар (сообщение, подпись) и переходов отображения Π и использующие возникновение каких-либо связей между этими значениями

Оценка стойкости

$$Adv_{GenEG-BS_I}^{SEQ-UF}(\mathcal{A}) \leq Adv_{G,t}^{TASK}(\mathcal{B}) + \frac{(q_{\Pi} + 2q_{\Pi^{-1}} + 3t + 2)^2}{q} + \frac{4q_H^2}{q},$$

где

- $TASK = OMDL$ для схем типа А и $TASK = OMDL'$ для схем типа В
- t – количество открытых сеансов протокола формирования подписи
- q_H – количество запросов к случайному оракулу H
- q_{Π} – количество вычислений преобразования Π
- $q_{\Pi^{-1}}$ – количество вычислений преобразования Π^{-1}

атаки, использующие общие методы взлома хэш-функции H

Какие методы криптоанализа не учитывает оценка?

- Методы, основанные на структурных свойствах конкретной хэш-функции H .

Необходимые свойства хэш-функции H :

- сложность поиска коллизий с точностью до знака;
- сложность поиска различных m_1, m_2 для некоторого случайного значения r :
 $H(m_1) + H(m_2) = r$.

- Методы, предполагающие использование знания о связи между битовыми строками, кодирующими координаты точек эллиптической кривой, и целыми числами.
- Методы, использующие структурные особенности конкретной группы точек эллиптической кривой для формирования новых элементов группы.

Выбор параметров

Положим $q_H, q_{BRO}, q_{BRO}^{-1}, t \leq T$, где T – вычислительные ресурсы нарушителя.

В предположении, что лучшим методом решения задачи $OMDL$ ($OMDL'$) является ро-метод Полларда, имеем:

$$Adv_{GenEG-BS_I}^{SEQ-UF}(\mathcal{A}) \leq \frac{T^2}{q} + \frac{(T + 2T + 3T + 2)^2}{q} + \frac{4T^2}{q} \leq \frac{42T^2}{q}$$



Выводы

- Доказано, что достаточным условием стойкости схем подписи вслепую Эль-Гамала в модели SEQ-UF при соответствующих значениях параметров является сложность решения задачи $OMDL$ ($OMDL'$) в базовой группе точек эллиптической кривой.
- Схемы подписи вслепую Эль-Гамала потенциально можно использовать в прикладных системах, где организационно-техническими мерами обеспечивается отсутствие параллельных сеансов протокола формирования подписи.
- Разные уравнения Эль-Гамала – разные гарантии безопасности.