К. Д. Царегородцев, Свойства конфиденциальности и целостности схемы ECIES,
Матем. вопр. криптогр., 2024, том 15, выпуск 2, 101–136

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2024 Т. 15 № 2 С. 101–136

УДК 519.719.2 DOI https://doi.org/10.4213/mvk472

Свойства конфиденциальности и целостности схемы ECIES

К. Д. Царегородцев

АО «НПК Криптонит», Москва

Получено 06.IX.2023

Аннотация. Схема ECIES анализируется с помощью техники теоретико-сложностных сведéний («доказуемая стойкость»). Показано, что если схема ECIES задается при помощи схемы выработки общего секретного ключа KE и схемы аутентифицированного шифрования AE, то преимущества противника относительно схемы ECIES в стандартных моделях LOR-CCA и INT-CTXT могут быть ограничены сверху через преимущества противников относительно схемы KE в модели mODH (задача Диффи – Хеллмана с доступом к оракулу) и схемы AE в моделях LOR-CCA и INT-CTXT соответственно.

Ключевые слова: схема ECIES, доказуемая стойкость

Privacy and integrity properties of ECIES scheme

K. D. Tsaregorodtsev

JSC «NPK Kryptonite», Moscow

Abstract. We analyze ECIES scheme in the provable security framework. The object of study (ECIES) is an asymmetric (hybrid) authenticated encryption scheme based on the key exchange scheme KE and AE(AD)-scheme AE. The encryption process consists of two steps: (a) generating ephemeral pair and session secret key K using KE, (b) encrypting the message m under the key K using AE and sending results to the recipient.

We show that the adversarial advantage against ECIES scheme in the (standard) LOR-CCA and INT-CTXT models can be upper bounded by the adversarial advantage against KE in the mODH model (Oracle Diffie-Hellman Model with multiple queries) and against AE in the (standard) LOR-CCA and INT-CTXT models respectively. The security in these models implies the following informal properties: (a) the adversary is unable to extract any useful information about plaintext from the given ciphertext (except for its length); (b) if the adversary is given some ephemeral public key (chosen by the honest party), it is unable to form the ciphertext that may be correctly decrypted under this key (for instance, it cannot modify messages formed by honest senders).

Citation: Matematicheskie Voprosy Kriptografii, 2024, v. 15, № 2, pp. 101–136 (Russian)

We point out some differences in our analysis compared to the previous ones: (a) only the confidentiality of the ECIES scheme was analyzed; integrity of the scheme (either in the INT-CTXT or INT-PTXT models) is not considered; (b) the confidentiality model in previous analysis (LOR-CCA-fg/IND-CCA2) allows only one encryption challenge query to the $\mathcal{O}^b_{\text{enc}}$ oracle; generalization to the case of q_e queries to the encryption oracle seems not to be the immediate consequence; however, the possibility to do a number of queries can make a difference in practice; (c) the analysis given in the previous papers could be slightly more general: it allows any AE(AD)-scheme to be used instead of concrete Encrypt-then-MAC approach.

Hence, we show that it is possible to separate key generation step and encryption process in generic ECIES scheme and study them independently, which allows one to develop more modular security solutions. The scheme can be used as a building block of more involved protocols (e.g., as a part of user anonymous authentication in 5G-AKA protocol).

Keywords: ECIES, provable security

Введение

Схема ECIES (**E**lliptic **C**urve **I**ntegrated **E**ncryption **S**cheme) является стандартизованной схемой гибридного шифрования, которая обеспечивает конфиденциальность и неподделываемость пересылаемых сообщений (см. [1–3]). Схема была проанализирована ранее в [3–5] в модели LOR-CCA (**L**eft-**O**r-**R**ight **C**hosen **C**iphertext **A**ttack) для изучения свойства неотличимости шифртекстов при доступе противника к оракулам зашифрования и расшифрования. Проведенному в указанных работах анализу были присущи следующие особенности: (a) анализ не затрагивал свойство целостности информации, (b) модель позволяла сделать только один тестовый запрос на зашифрование сообщения, (c) доказательство рассматривало только один конкретный «тип» ECIES-схемы (стандартизованный режим с композицией вида **“Encrypt-then-MAC”**, подробнее см. [6]).

В этой работе мы изучаем стойкость «обобщенной» схемы ECIES (см. раздел 1.4) в (адаптированных) моделях безопасности: LOR-CCA для изучения свойства конфиденциальности и INT-CTXT (**INT**egrity of **C**ipher**t**e**xt**) для изучения свойства целостности. Безопасность схемы ECIES в указанных моделях влечет следующие неформальные свойства:

– противник не может извлечь никакой полезной информации об открытом тексте из шифртекста (кроме длины открытого текста);

– если противнику дан некоторый эфемерный открытый ключ (выбранный честным участником схемы ECIES), то ему трудно сформировать новый шифртекст таким образом, чтобы он был корректно расшифрован на выбранном ключе (в частности, противник не может модифицировать сообщения, сформированные честными участниками).

Отметим отдельно, что указанные свойства **не гарантируют** аутентичность отправителя: получатель сообщения может лишь убедиться в том, что сообщение не было модифицировано, но не способен восстановить источник сообщения. Рассматриваемая схема также **не может быть использована** сама по себе в качестве протокола выработки общего ключа (так называемого AKE-протокола, **a**uthenticated **k**ey **e**xchange), поскольку не обеспечивает многие требуемые свойства подобных протоколов (подробнее см., например, [7, 8]): аутентификацию сторон, защиту от чтения назад, подтверждение и аутентификацию ключа, защиту от UKS- и KCI-атак и др. При этом схема может быть использована как «строительный блок» более сложных протоколов, в частности протоколов аутентификации и выработки общего ключа в технологии 5G [9].

Работа построена следующим образом. В разделе 1 приводятся основные определения и обозначения, раздел 2 посвящен формальному введению моделей безопасности для рассматриваемых криптографических механизмов. В разделе 3 получено сведение моделей с несколькими участниками к случаю модели с одним участником/запросом. Раздел 4 посвящен доказательству стойкости схемы ECIES в соответствующих моделях безопасности. Наконец, в разделе 5 кратко перечислены результаты работы.

Иерархия введенных ниже моделей изображена на рис. 1. Стрелка от модели A к модели B означает, что преимущество противника в модели A может быть «нетривиально» ограничено с помощью преимущества некоторого другого противника в модели B.

1. Основные определения и обозначения

1.1. Обозначения

Длина сообщения x (в блоках) обозначается через $|x|$. Под $x \leftarrow y$ подразумеваем присвоение значения y переменной x; $x \xleftarrow{\$} \mathcal{O}$ символизирует процесс запуска вероятностного алгоритма $\mathcal{O}$ с присвоением результата работы алгоритма переменной x; если M — конечное

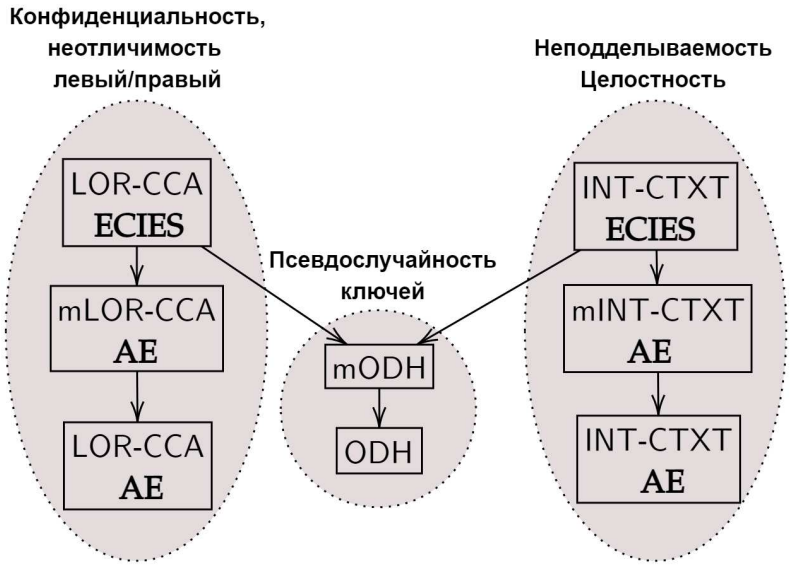

Рис. 1. Иерархия моделей безопасности для схемы ECIES

множество, то под $x \xleftarrow{\mathcal{U}} M$ подразумеваем процесс выбора значения y в соответствии с равномерным распределением на M с последующим присвоением значения y переменной x. Пустой словарь (ассоциативный массив) обозначается $[\,]$. Символ $\perp$ — это либо символ ошибки (например, ошибка расшифрования), либо специальный символ, означающий отсутствие элемента в словаре по заданному индексу. Если в наборе $(x, y, z, \ldots)$ конкретное значение некоторого элемента нам не важно, то будем писать вместо такого элемента символ $\cdot$; например $(x, \cdot, \cdot)$ означает набор из трех элементов, в которых первым элементом набора является x.

1.2. Схема аутентифицированного шифрования

Пусть задано три непустых множества $Keys, Msg, Ctxt \subseteq \{0,1\}^*$. Элементы $K \in Keys$ будем называть «ключами», $m \in Msg$ — «открытыми текстами», $ct \in Ctxt$ — «шифртекстами».

Определение 1. Схема аутентифицированного шифрования $\mathsf{AE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ — это тройка (вероятностных) алгоритмов:

– алгоритм генерации ключа схемы шифрования KGen, алгоритм возвращает случайный ключ K из множества ключей $Keys$ (далее

предполагаем, что ключ выбирается случайно равновероятно среди элементов множества $Keys = \{0,1\}^{klen}$);

– (вероятностный) алгоритм зашифрования Enc, принимающий на вход ключ $K \in \{0,1\}^{klen}$ и открытый текст $m \in Msg$ и возвращающий шифртекст $ct \in Ctxt$;

– (детерминированный) алгоритм расшифрования Dec, принимающий на вход ключ $K \in \{0,1\}^{klen}$ и шифртекст $ct \in Ctxt$ для расшифрования и возвращающий открытый текст $m \in Msg$ или специальный символ ошибки $\perp$.

Алгоритмы зашифрования и расшифрования должны удовлетворять стандартному требованию корректности: для любых $m \in Msg$

$$K \xleftarrow{\$} \mathsf{AE.KGen} \;\Rightarrow\; \mathsf{AE.Dec}(K, \mathsf{AE.Enc}(K, m)) = m.$$

Если на некотором входе $ct \in Ctxt$ на ключе K алгоритм расшифрования возвращает ошибку $\mathsf{AE.Dec}(K, ct) = \perp$, то шифртекст ct называется некорректным (для данного ключа K, который предполагается ясным из контекста). Примером схемы аутентифицированного шифрования может служить режим аутентифицированного шифрования **MGM** [10, 11] или режим шифрования **CTR** совместно с выработкой имитовставки **MAC** [12] на независимых ключах в композиции вида **Encrypt-then-MAC** (подробнее см. [6]). В таких схемах $Msg = Ctxt = \{0,1\}^*$.

1.3. Схема выработки общего ключа

В этой работе под схемой выработки общего ключа подразумевается криптографический механизм, который позволяет двум сторонам взаимодействия (неаутентифицированно) выработать общий секретный ключ, используя для этого две ключевые пары (эфемерную (esk, epk) и долговременную (sk, pk)).

Определение 2. Схемой выработки общего ключа будем называть пару (вероятностных) алгоритмов $\mathsf{KE} = (\mathsf{PairGen}, \mathsf{Comb})$:

– алгоритм генерации ключевой пары $\mathsf{PairGen}$ возвращает случайно выбранную ключевую пару (sk, pk);

– алгоритм выработки ключа Comb на основе двух ключей — открытого pk и секретного sk — вырабатывает ключ $K \in Keys$.

При этом должно выполняться стандартное требование корректности выработки ключей:

$$(sk, pk) \xleftarrow{\$} \mathsf{KE.PairGen}, \quad (esk, epk) \xleftarrow{\$} \mathsf{KE.PairGen}$$
$$\Rightarrow \mathsf{KE.Comb}(sk, epk) = \mathsf{KE.Comb}(esk, pk).$$

Примером схемы выработки общего ключа является алгоритм «выработки ключа обмена» [13] в полустатическом режиме, анализ схемы приведен в работе [14, раздел 3.7].

1.4. Описание схемы ECIES

Введем в рассмотрение основной объект изучения настоящей работы — схему ECIES, по сути являющуюся гибридной системой аутентифицированного шифрования. Процесс зашифрования сообщения m в схеме ECIES состоит из двух шагов (см. псевдокод схемы на рис. 2):

– генерации эфемерной ключевой пары и секретного ключа K с помощью схемы KE;

– зашифрования сообщения m на ключе K с помощью схемы AE.

$\underline{\mathsf{ECIES.Enc}(pk, m)}$	$\underline{\mathsf{ECIES.Dec}(sk, (epk, ct))}$
$(esk, epk) \xleftarrow{\$} \mathsf{KE.PairGen}$	$K \leftarrow \mathsf{KE.Comb}(sk, epk)$
$K \leftarrow \mathsf{KE.Comb}(esk, pk)$	**return** $\mathsf{AE.Dec}(K, ct)$
$ct \leftarrow \mathsf{AE.Enc}(K, m)$	
return (epk, ct)	

Рис. 2. Псевдокод схемы ECIES

Отметим некоторые особенности схемы ECIES:

– для выработки каждого шифртекста используется новая эфемерная ключевая пара (esk, epk);

– алгоритм KE.Comb может выдавать пару ключей (например, ключ шифрования и ключ выработки имитовставки), основным требованием к совместимости схем KE и AE является совпадение множества значений алгоритма KE.Comb с множеством ключей $Keys$ схемы AE;

– в схему могут быть добавлены ассоциированные данные, их защита может осуществляться с помощью AEAD-схемы [15, раздел 5.2.1].

2. Модели безопасности

В настоящем разделе опишем основные модели безопасности посредством соответствующих экспериментов, каждый из которых формализует некоторое интуитивно понятное свойство безопасности, в рамках парадигмы «доказуемой стойкости» [15,16]. Для этого в каждом эксперименте опишем набор оракулов (интерфейсов), доступных противнику, а также зададим меру успеха противника (преимущество). Противник может делать адаптивные запросы к оракулам и получать от них ответы, которые могут содержать какую-либо информацию о секретных (неизвестных противнику) значениях (например, значениях ключей схемы шифрования). Задачей противника является либо подделка какого-либо значения в ходе эксперимента, либо различение поведения оракулов в двух различных ситуациях.

Замечание 1. Далее под временной сложностью противника понимается количество шагов работы программы, описывающей противника, в некоторой фиксированной модели вычислений вместе с размером кода для описания программы (это необходимо, чтобы исключить ситуации, в которых в код противника вписываются очень большие предвычисленные таблицы).

2.1. Свойство конфиденциальности для схемы шифрования

Приведем описание модели mLOR-CCA (**m**ulti-user LOR-CCA) для формализации свойства конфиденциальности режима аутентифицированного шифрования AE. Пусть $D \in \mathbb{N}$ — количество участников в рассматриваемой модели. В ходе эксперимента противник $\mathcal{A}$ взаимодействует с двумя оракулами (см. псевдокод эксперимента на рис. 3):

– $\mathcal{O}^b_{\text{enc}}$ принимает на вход тройки (i, m_0, m_1), состоящие из пар сообщений (m_0, m_1) одинаковой длины ($|m_0| = |m_1|$) и номера ключа $i \in \{1, \ldots, D\}$, оракул зашифровывает сообщение m_b на ключе K_i с помощью алгоритма AE.Enc и возвращает итоговый шифртекст противнику;

– $\mathcal{O}_{\text{dec}}$ принимает на вход номер $i \in \{1, \ldots, D\}$ и шифртекст ct; если ct не возвращался ранее противнику в качестве ответа оракула $\mathcal{O}^b_{\text{enc}}$ на запрос вида $(i, \cdot, \cdot)$, то $\mathcal{O}_{\text{dec}}$ расшифровывает ct на ключе K_i с помощью алгоритма AE.Dec и возвращает результат противнику, в противном случае возвращается символ ошибки $\perp$.

Задачей противника является корректное определение бита b, зафиксированного внутри оракула $\mathcal{O}^b_{\text{enc}}$. Высокое преимущество в указанной задаче свидетельствует о том, что противник может восстановить частичную информацию об открытом тексте из шифртекстов.

Определение 3. Преимуществом противника $\mathcal{A}$ в модели mLOR-CCA с D участниками для схемы AE называется следующая величина:

$$\mathbf{Adv}^{\mathsf{mLOR\text{-}CCA}}_{\mathsf{AE}}(\mathcal{A}) = \mathbb{P}\big[\mathbf{Exp}^{\mathsf{mLOR\text{-}CCA\text{-}1}}_{\mathsf{AE}}(\mathcal{A}) \to 1\big] - \mathbb{P}\big[\mathbf{Exp}^{\mathsf{mLOR\text{-}CCA\text{-}0}}_{\mathsf{AE}}(\mathcal{A}) \to 1\big],$$

псевдокод эксперимента $\mathbf{Exp}^{\mathsf{mLOR\text{-}CCA\text{-}}b}_{\mathsf{AE}}$, $b \in \{0,1\}$, приведен на рис. 3.

$\mathbf{Exp}^{\mathsf{mLOR\text{-}CCA\text{-}}b}_{\mathsf{AE}}(\mathcal{A})$	$\mathcal{O}^b_{\text{enc}}(i, m_0, m_1)$	$\mathcal{O}_{\text{dec}}(i, ct)$
for $1 \leqslant i \leqslant D$ **do**	$ct \xleftarrow{\$} \mathsf{AE.Enc}(K_i, m_b)$	**if** $((i, ct) \in sent)$
$\quad K_i \xleftarrow{\mathcal{U}} \{0,1\}^{klen}$	$sent \leftarrow sent \cup \{(i, ct)\}$	$\quad$ **return** $\perp$
endfor	**return** ct	**fi**
$sent \leftarrow \varnothing$		**return** $\mathsf{AE.Dec}(K_i, ct)$
$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}^b_{\text{enc}}, \mathcal{O}_{\text{dec}}}$		
return b'		

Рис. 3. Псевдокод эксперимента $\mathbf{Exp}^{\mathsf{mLOR\text{-}CCA\text{-}}b}_{\mathsf{AE}}$

Определение 4. Обозначим через

$$\mathbf{InSec}^{\mathsf{mLOR\text{-}CCA}}_{\mathsf{AE}}(t, Q_e, L_e, M_e, Q_d, L_d, M_d, D)$$

максимум среди преимуществ противников $\mathcal{A}$ в эксперименте $\mathbf{Exp}^{\mathsf{mLOR\text{-}CCA}}_{\mathsf{AE}}$ с D участниками, где противник $\mathcal{A}$ имеет ограничение t на вычислительные ресурсы и следующие ограничения на обращения к оракулам ($1 \leqslant i \leqslant D$):

– общее число запросов вида $(i, \cdot, \cdot)$ к оракулу $\mathcal{O}^b_{\text{enc}}$ (вида $(i, \cdot)$ к оракулу $\mathcal{O}_{\text{dec}}$) не превышает $Q_e[i]$ ($Q_d[i]$ соответственно);

– общая длина сообщений в запросах вида $(i, \cdot, \cdot)$ к оракулу $\mathcal{O}^b_{\text{enc}}$ (в запросах вида $(i, \cdot)$ к оракулу $\mathcal{O}_{\text{dec}}$) не превышает $L_e[i]$ ($L_d[i]$ соответственно);

– максимальная длина сообщения в запросах вида $(i, \cdot, \cdot)$ к оракулу $\mathcal{O}^b_{\text{enc}}$ (в запросах вида $(i, \cdot)$ к оракулу $\mathcal{O}_{\text{dec}}$) не превышает $M_e[i]$ ($M_d[i]$ соответственно).

Замечание 2. Заметим, что в случае $D = 1$ получается «обычная» модель LOR-CCA для конфиденциальности режима аутентифицированного шифрования [6]. Если противник не имеет доступа к оракулу $\mathcal{O}_{\text{dec}}$, то получаем модель LOR-CPA (**L**eft-**O**r-**R**ight **C**hosen **P**laintext **A**ttack).

2.2. Свойство целостности для схемы шифрования

Введем модель mINT-CTXT (**m**ulti-user INT-CTXT) для изучения свойства целостности схемы шифрования. Пусть $D \in \mathbb{N}$ — количество участников в рассматриваемой модели. В ходе эксперимента противник $\mathcal{A}$ взаимодействует с двумя оракулами:

– $\mathcal{O}_{\text{enc}}$ принимает на вход номер $i \in \{1, \ldots, D\}$ и сообщение m, зашифровывает сообщение m на ключе K_i с помощью алгоритма AE.Enc и выдает полученный шифртекст ct противнику;

– $\mathcal{O}_{\text{vfy}}$ принимает на вход номер $i \in \{1, \ldots, D\}$ и шифртекст ct, расшифровывает $m \leftarrow \mathsf{AE.Dec}(K_i, ct)$ и возвращает m противнику.

Задачей противника является подделка (создание) шифртекста ct, который корректно расшифровывается на одном из неизвестных ключей K_i (см. псевдокод эксперимента на рис. 4).

Определение 5. Преимуществом противника $\mathcal{A}$ в модели mINT-CTXT с D участниками для схемы AE называется следующая величина:

$$\mathbf{Adv}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}(\mathcal{A}) = \mathbb{P}\big[\mathbf{Exp}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}(\mathcal{A}) \to 1\big],$$

псевдокод эксперимента $\mathbf{Exp}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}$ приведен на рис. 4.

$\mathbf{Exp}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}(\mathcal{A})$	$\mathcal{O}_{\text{enc}}(i, m)$	$\mathcal{O}_{\text{vfy}}(i, ct)$
for $1 \leqslant i \leqslant D$ **do**	$ct \xleftarrow{\$} \mathsf{AE.Enc}(K_i, m)$	$m \leftarrow \mathsf{AE.Dec}(K_i, ct)$
$K_i \xleftarrow{\mathcal{U}} \{0,1\}^{klen}$	$sent \leftarrow sent \cup \{(i, ct)\}$	**if** $((i, ct) \notin sent)\,\&\,(m \neq \perp)$
endfor	**return** ct	$win \leftarrow 1$
$sent \leftarrow \varnothing$		**fi**
$win \leftarrow 0$		**return** m
$\mathcal{A}^{\mathcal{O}_{\text{enc}}, \mathcal{O}_{\text{vfy}}}$		
return win		

Рис. 4. Псевдокод эксперимента $\mathbf{Exp}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}$

Определение 6. Обозначим через

$$\mathbf{InSec}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}(t, Q_e, L_e, M_e, Q_v, L_v, M_v, D)$$

максимум среди преимуществ противников $\mathcal{A}$ в эксперименте $\mathbf{Exp}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}$ с D участниками, где противник $\mathcal{A}$ имеет ограничение t на вычислительные ресурсы и следующие ограничения на обращения к оракулам ($1 \leqslant i \leqslant D$):

– общее число запросов вида $(i, \cdot)$ к оракулу $\mathcal{O}_{\text{enc}}$ ($(i, \cdot)$ к оракулу $\mathcal{O}_{\text{vfy}}$) не превышает $Q_e[i]$ ($Q_v[i]$ соответственно);

– общая длина сообщений в запросах вида $(i, \cdot)$ к оракулу $\mathcal{O}_{\text{enc}}$ (в запросах вида $(i, \cdot)$ к оракулу $\mathcal{O}_{\text{vfy}}$) не превышает $L_e[i]$ ($L_v[i]$ соответственно);

– максимальная длина сообщения в запросах вида $(i, \cdot)$ к оракулу $\mathcal{O}_{\text{enc}}$ (к оракулу $\mathcal{O}_{\text{vfy}}$) не превышает $M_e[i]$ ($M_v[i]$ соответственно).

Замечание 3. В случае $D = 1$ получается «обычная» модель INT-CTXT [6] для свойства целостности режима аутентифицированного шифрования.

2.3. Модели безопасности для схемы выработки ключей

Рассмотрим две модели для изучения безопасности схемы выработки ключей KE: модель ODH из работы [4] (**O**racle **D**iffie **H**ellman) и mODH (**m**ultiple **ODH**).

В модели ODH противнику предоставляется тройка (pk, epk, K), где K — либо ключ, полученный с помощью алгоритма KE.Comb (на ключах (sk, epk)), либо случайно равновероятно выбранная двоичная строка аналогичной длины. Также противник имеет доступ к оракулу $\mathcal{O}_{\text{comb}}$, который принимает на вход ключ $epk' \neq epk$ и возвращает ответ $\mathsf{KE.Comb}(epk', sk)$. Задачей противника является определение, является ли ключ K «честно выработанным» согласно схеме KE ключом или случайным равновероятным ключом такой же битовой длины. Более подробно псевдокод эксперимента ODH описан на рис. 5.

Определение 7. Преимуществом противника $\mathcal{A}$ в модели ODH для схемы выработки ключей KE называется следующая величина:

$$\mathbf{Adv}^{\mathsf{ODH}}_{\mathsf{KE}}(\mathcal{A}) = \mathbb{P}\big[\mathbf{Exp}^{\mathsf{ODH\text{-}1}}_{\mathsf{KE}}(\mathcal{A}) \to 1\big] - \mathbb{P}\big[\mathbf{Exp}^{\mathsf{ODH\text{-}0}}_{\mathsf{KE}}(\mathcal{A}) \to 1\big],$$

псевдокод эксперимента $\mathbf{Exp}^{\mathsf{ODH}\text{-}b}_{\mathsf{KE}}$, $b \in \{0, 1\}$, приведен на рис. 5.

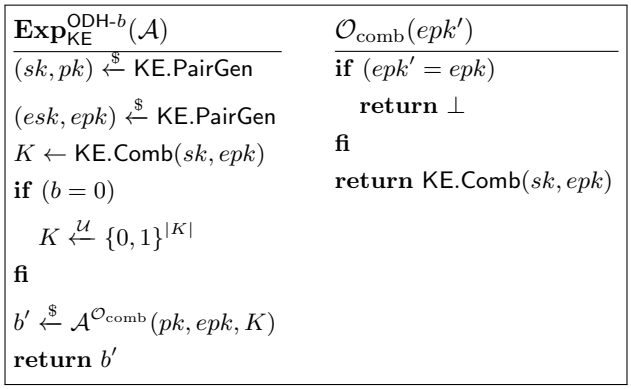

Рис. 5. Псевдокод эксперимента $\mathbf{Exp}^{\mathsf{ODH}\text{-}b}_{\mathsf{KE}}$

Определение 8. Обозначим через $\mathbf{InSec}^{\mathsf{ODH}}_{\mathsf{KE}}(t, q_{com})$ максимум среди преимуществ вида $\mathbf{Adv}^{\mathsf{ODH}}_{\mathsf{KE}}(\mathcal{A})$, где максимум берется по всем противникам $\mathcal{A}$ с ограничением t на вычислительные ресурсы и делающим не более q_{com} запросов к оракулу $\mathcal{O}_{\mathrm{comb}}$.

Модель mODH является обобщением модели ODH на случай нескольких ключей K. В модели mODH противник $\mathcal{A}$ имеет доступ к двум оракулам:

– $\mathcal{O}^b_{\mathrm{kgen}}$ генерирует либо случайные равновероятные ключи заданной длины (при $b = 0$), либо ключи, сгенерированные с помощью схемы KE (при $b = 1$), с некоторыми ограничениями, исключающими возможность тривиальных атак, см. псевдокод эксперимента 6 ниже;

– $\mathcal{O}_{\mathrm{comb}}(epk)$ генерирует общий ключ с помощью алгоритма KE.Comb, используя предоставленный ему на вход открытый ключ epk (кроме тех случаев, когда ключ epk возвращался ранее оракулом $\mathcal{O}_{\mathrm{kgen}}$).

Задачей противника является корректное определение бита b, зафиксированного внутри оракула $\mathcal{O}^b_{\mathrm{kgen}}$.

Замечание 4. Отличительной особенностью модели mODH является не только возможность запросить несколько ключей K от оракула $\mathcal{O}^b_{\mathrm{kgen}}$, но и возможность делать запросы к оракулу $\mathcal{O}_{\mathrm{comb}}$ до всех запросов к оракулу $\mathcal{O}^b_{\mathrm{kgen}}$.

Определение 9. Преимуществом противника $\mathcal{A}$ в модели mODH для схемы выработки ключей KE называется следующая величина:

$$\mathbf{Adv}^{\mathsf{mODH}}_{\mathsf{KE}}(\mathcal{A}) = \mathbb{P}\big[\mathbf{Exp}^{\mathsf{mODH\text{-}1}}_{\mathsf{KE}}(\mathcal{A}) \to 1\big] - \mathbb{P}\big[\mathbf{Exp}^{\mathsf{mODH\text{-}0}}_{\mathsf{KE}}(\mathcal{A}) \to 1\big],$$

псевдокод эксперимента $\mathbf{Exp}^{\mathsf{mODH}\text{-}b}_{\mathsf{KE}}$, $b \in \{0,1\}$, приведен на рис. 6.

$\mathbf{Exp}^{\mathsf{mODH}\text{-}b}_{\mathsf{KE}}(\mathcal{A})$	$\mathcal{O}_{\mathrm{comb}}(epk)$	$\mathcal{O}^b_{\mathrm{kgen}}$
$(sk, pk) \xleftarrow{\$} \mathsf{KE.PairGen}$	**if** $Gen[epk] = \bot$	$(esk, epk) \xleftarrow{\$} \mathsf{KE.PairGen}$
$Gen \leftarrow [\,]$	**return** $\mathsf{KE.Comb}(sk, epk)$	**if** $Gen[epk] = \bot$
$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}^b_{\mathrm{kgen}}, \mathcal{O}_{\mathrm{comb}}}(pk)$	**fi**	$K \leftarrow \mathsf{KE.Comb}(sk, epk)$
return b'	**return** $Gen[epk]$	**if** $(b = 0)$
		$K \xleftarrow{\mathcal{U}} \{0,1\}^{\lvert K\rvert}$
		fi
		$Gen[epk] \leftarrow K$
		fi
		return $(epk, Gen[epk])$

Рис. 6. Псевдокод эксперимента $\mathbf{Exp}^{\mathsf{mODH}\text{-}b}_{\mathsf{KE}}$

Определение 10. Обозначим через $\mathbf{InSec}^{\mathsf{mODH}}_{\mathsf{KE}}(t, q_{gen}, q_{com})$ максимум среди преимуществ вида $\mathbf{Adv}^{\mathsf{mODH}}_{\mathsf{KE}}(\mathcal{A})$, где максимум берется по всем противникам $\mathcal{A}$ с ограничением t на вычислительные ресурсы и делающим не более q_{gen} (q_{com}) запросов к оракулу $\mathcal{O}^b_{\mathrm{kgen}}$ (к оракулу $\mathcal{O}_{\mathrm{comb}}$).

2.4. Модели безопасности для схемы ECIES

В настоящем разделе введем модели безопасности для изучения свойств конфиденциальности и целостности для схемы ECIES. По сути, введенные ниже модели сходны по своей структуре с моделями, введенными для аналогичных свойств схемы шифрования (см. подразделы 2.1 и 2.2) с добавлением генерации эфемерных ключей с помощью схемы KE.

Определение 11. Преимуществом противника $\mathcal{A}$ в модели $\mathsf{LOR\text{-}CCA}$ для схемы ECIES называется следующая величина:

$$\mathbf{Adv}^{\mathsf{LOR\text{-}CCA}}_{\mathrm{ECIES}}(\mathcal{A}) = \mathbb{P}\big[\mathbf{Exp}^{\mathsf{LOR\text{-}CCA\text{-}1}}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\big] - \mathbb{P}\big[\mathbf{Exp}^{\mathsf{LOR\text{-}CCA\text{-}0}}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\big],$$

псевдокод эксперимента $\mathbf{Exp}^{\mathsf{LOR\text{-}CCA}\text{-}b}_{\mathrm{ECIES}}$, $b \in \{0,1\}$, приведен на рис. 7.

$\mathbf{Exp}^{\mathsf{LOR\text{-}CCA}\text{-}b}_{\mathrm{ECIES}}(\mathcal{A})$	$\mathcal{O}^b_{\mathrm{enc}}(m_0, m_1)$	$\mathcal{O}_{\mathrm{dec}}(epk, ct)$
$(sk, pk) \xleftarrow{\$} \mathsf{KE.PairGen}$	$(epk, esk) \xleftarrow{\$} \mathsf{KE.PairGen}$	**if** $(epk, ct) \in sent$
$sent \leftarrow \varnothing$	$K \leftarrow \mathsf{KE.Comb}(sk, epk)$	**return** $\perp$
$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}^b_{\mathrm{enc}}, \mathcal{O}_{\mathrm{dec}}}(pk)$	$ct \xleftarrow{\$} \mathsf{AE.Enc}(K, m_b)$	**fi**
return b'	$sent \leftarrow sent \cup \{(epk, ct)\}$	$K \leftarrow \mathsf{KE.Comb}(sk, epk)$
	return (epk, ct)	**return** $\mathsf{AE.Dec}(K, ct)$

Рис. 7. Псевдокод эксперимента $\mathbf{Exp}^{\mathsf{LOR\text{-}CCA}\text{-}b}_{\mathrm{ECIES}}$

Определение 12. Пусть $\mathbf{InSec}^{\mathsf{LOR\text{-}CCA}}_{\mathrm{ECIES}}(t, q_e, \ell_e, \mu_e, q_d, \ell_d, \mu_d)$ обозначает максимум среди преимуществ вида $\mathbf{Adv}^{\mathsf{LOR\text{-}CCA}}_{\mathrm{ECIES}}(\mathcal{A})$, где противник $\mathcal{A}$ имеет ограничение t на вычислительные ресурсы и делает:

– не более q_e запросов к оракулу $\mathcal{O}^b_{\mathrm{enc}}$, суммарная длина запросов не превышает ℓ_e, максимальная длина запроса не превышает μ_e;

– не более q_d запросов к оракулу $\mathcal{O}_{\mathrm{dec}}$, суммарная длина запросов не превышает ℓ_d, максимальная длина запроса не превышает μ_d.

Определение 13. Преимуществом противника $\mathcal{A}$ в модели $\mathsf{INT\text{-}CTXT}$ для схемы ECIES называется следующая величина:

$$\mathbf{Adv}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}(\mathcal{A}) = \mathbb{P}\big[\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\big],$$

псевдокод эксперимента $\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}$ приведен на рис. 8.

$\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}(\mathcal{A})$	$\mathcal{O}_{\mathrm{enc}}(m)$	$\mathcal{O}_{\mathrm{vfy}}(epk, ct)$
$(sk, pk) \xleftarrow{\$} \mathsf{KE.PairGen}$	$(epk, esk) \xleftarrow{\$} \mathsf{KE.PairGen}$	$K \leftarrow \mathsf{KE.Comb}(sk, epk)$
$sent \leftarrow \varnothing$	$EGen \leftarrow EGen \cup \{epk\}$	$m \leftarrow \mathsf{AE.Dec}(K, ct)$
$EGen \leftarrow \varnothing$	$K \leftarrow \mathsf{KE.Comb}(sk, epk)$	$t_1 \leftarrow (m \neq \perp)$
$win \leftarrow 0$	$ct \xleftarrow{\$} \mathsf{AE.Enc}(K, m)$	$t_2 \leftarrow (epk \in EGen)$
$\mathcal{A}^{\mathcal{O}_{\mathrm{enc}}, \mathcal{O}_{\mathrm{vfy}}}(pk)$	$sent \leftarrow sent \cup \{(epk, ct)\}$	$t_3 \leftarrow ((epk, ct) \notin sent)$
return win	**return** (epk, ct)	**if** $t_1 \& t_2 \& t_3$
		$win \leftarrow 1$
		fi
		return m

Рис. 8. Псевдокод эксперимента $\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}$

Определение 14. Обозначим через

$$\mathbf{InSec}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}(t, q_e, \ell_e, \mu_e, q_v, \ell_v, \mu_v)$$

максимум среди преимуществ вида $\mathbf{Adv}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}(\mathcal{A})$, где противник $\mathcal{A}$ имеет ограничение t на вычислительные ресурсы и делает:

– не более q_e запросов к оракулу $\mathcal{O}_{\mathrm{enc}}$, суммарная длина запросов не превышает ℓ_e, максимальная длина запроса не превышает μ_e;

– не более q_v запросов к оракулу $\mathcal{O}_{\mathrm{vfy}}$, суммарная длина запросов не превышает ℓ_v, максимальная длина запроса не превышает μ_v.

3. Анализ моделей с несколькими участниками

В настоящем разделе покажем, что модели mLOR-CCA, mINT-CTXT и mODH сводятся к моделям LOR-CCA, INT-CTXT и ODH соответственно. Каждая из сводимостей следует из так называемого «гибридного аргумента»: по сути, мы показываем, что для всякого противника $\mathcal{A}$ в модели с D участниками существует набор из D противников $\mathcal{B}_1, \ldots, \mathcal{B}_D$ в соответствующих моделях с одним участником (в случае модели mODH — с одним запросом), сумма преимуществ которых не меньше, чем преимущество $\mathcal{A}$. Дополнительно для модели ODH в ходе доказательства нам необходимо отдельно рассмотреть событие, состоящее в совпадении значения epk, генерируемого оракулом $\mathcal{O}^b_{\mathrm{kgen}}$, с каким-либо из значений epk', запрашиваемых противником у оракула $\mathcal{O}_{\mathrm{comb}}$. При условии равномерной распределенности значений epk вероятность указанного события ограничивается сверху величиной $\frac{q_{gen}\, q_{com}}{|EpkSet|}$.

Утверждение 1. *Выполнено следующее неравенство*:

$$\mathbf{InSec}^{\mathsf{mLOR\text{-}CCA}}_{\mathsf{AE}}(t, Q_e, L_e, M_e, Q_d, L_d, M_d, D) \leqslant D \cdot \mathbf{InSec}^{\mathsf{LOR\text{-}CCA}}_{\mathsf{AE}}(t + T_{\mathsf{mLOR\text{-}CCA}}, q_e, \ell_e, \mu_e, q_d, \ell_d, \mu_d),$$

где использованы следующие обозначения:

$$T_{\mathsf{mLOR\text{-}CCA}} = D + \sum_{i=1}^{D} \left(Q_e[i] + Q_d[i] + L_e[i] + L_d[i]\right),$$

$$q_x = \max_{1 \leqslant i \leqslant D} Q_x[i], \ell_x = \max_{1 \leqslant i \leqslant D} L_x[i], \mu_x = \max_{1 \leqslant i \leqslant D} M_x[i], x \in \{e, d\}.$$

Утверждение 2. *Выполнено следующее неравенство*:

$$\mathbf{InSec}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}(t, Q_e, L_e, M_e, Q_v, L_v, M_v, D) \leqslant D \cdot \mathbf{InSec}^{\mathsf{INT\text{-}CTXT}}_{\mathsf{AE}}(t + T_{\mathsf{mINT\text{-}CTXT}}, q_e, \ell_e, \mu_e, q_v, \ell_v, \mu_v),$$

где использованы следующие обозначения:

$$T_{\mathsf{mINT\text{-}CTXT}} = D + \sum_{i=1}^{D} \left(Q_e[i] + Q_v[i] + L_e[i] + L_v[i]\right),$$

$$q_x = \max_{1 \leqslant i \leqslant D} Q_x[i], \ell_x = \max_{1 \leqslant i \leqslant D} L_x[i], \mu_x = \max_{1 \leqslant i \leqslant D} M_x[i], x \in \{e, v\}.$$

Утверждение 3. *Пусть алгоритм* KE.PairGen *порождает равномерное распределение на множестве открытых ключей* $EpkSet$. *Тогда выполняется следующее неравенство*:

$$\mathbf{InSec}^{\mathsf{mODH}}_{\mathsf{KE}}(t, q_{gen}, q_{com}) \leqslant q_{gen} \cdot \mathbf{InSec}^{\mathsf{ODH}}_{\mathsf{KE}}(t + q_{gen} + q_{com}, q_{com}) + \frac{2\, q_{gen}\, q_{com}}{|EpkSet|}.$$

Доказательства приведенных выше утверждений содержатся в приложении А.

4. Анализ моделей безопасности для схемы ECIES

Преимущество противника для схемы ECIES в моделях LOR-CCA и INT-CTXT может быть ограничено сверху через преимущества противников в модели mODH для схемы KE и моделях mLOR-CCA и mINT-CTXT для схемы AE соответственно. Доказательство построено аналогично рассуждениям, приведенным в работе [6]: первым шагом ключи, сгенерированные с помощью схемы KE, заменяются случайными равновероятными. Далее в полученной модели анализируется схема ECIES . В силу независимости используемых ключей мы можем свести ситуацию к рассмотрению моделей mLOR-CCA и mINT-CTXT. При этом в ходе доказательства особое внимание уделяется оценке вероятности коллизий, возникновение которых препятствует корректному моделированию всех входящих в эксперименты случайных величин. «Фундаментальная игровая лемма» [17], стандартный результат из техники теоретико-сложностных сводимостей, позволяет перейти от исходной модели к модифицированной, в которой упомянутые коллизии не дают «вклада» в оценку преимущества.

Теорема 1. *Пусть алгоритм* KE.PairGen *порождает равномерное распределение на множестве открытых ключей* $EpkSet$. *Тогда выполнено неравенство*

$$\begin{aligned}\mathbf{InSec}^{\mathsf{LOR\text{-}CCA}}_{\mathrm{ECIES}}(t, q_e, \ell_e, \mu_e, q_d, \ell_d, \mu_d) \\ \leqslant \mathbf{InSec}^{\mathsf{mLOR\text{-}CCA}}_{\mathsf{AE}}(t+T, Q_e, L_e, M_e, Q_d, L_d, M_d, q_e) \\ + 2 \cdot \mathbf{InSec}^{\mathsf{mODH}}_{\mathsf{KE}}(t+T, q_e, q_d) + \frac{q_e \cdot (q_e + 2\, q_d)}{|EpkSet|},\end{aligned}$$

где использованы обозначения $(1 \leqslant i \leqslant q_e)$

$$T = q_e + q_d + \ell_e + \ell_d, Q_e[i] = 1, L_e[i] = M_e[i] = \mu_e,$$
$$Q_d[i] = q_i, M_d[i] = \mu_d, L_d[i] = q_i \cdot \mu_d, \sum_{i=1}^{q_e} q_i = q_d.$$

Теорема 2. *Пусть алгоритм* KE.PairGen *порождает равномерное распределение на множестве открытых ключей* $EpkSet$. *Тогда*

$$\begin{aligned}\mathbf{InSec}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}(t, q_e, \ell_e, \mu_e, q_v, \ell_v, \mu_v) \\ \leqslant \mathbf{InSec}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}(t+T, Q_e, L_e, M_e, Q_v, L_v, M_v, q_e) \\ + \mathbf{InSec}^{\mathsf{mODH}}_{\mathsf{KE}}(t+T, q_e, q_v) + \frac{q_e^2}{|EpkSet|},\end{aligned}$$

где использованы обозначения $(1 \leqslant i \leqslant q_e)$

$$T = q_e + q_v + \ell_e + \ell_v, Q_e[i] = 1, L_e[i] = M_e[i] = \mu_e,$$
$$Q_v[i] = q_i, M_v[i] = \mu_v, L_v[i] = q_i \cdot \mu_v, \sum_{i=1}^{q_e} q_i = q_v.$$

Доказательства теорем вынесены в приложения B и C.

5. Заключение

В настоящей работе изучена стойкость схемы ECIES в моделях LOR-CCA и INT-CTXT для конфиденциальности и целостности соответственно. Показано, что стойкость схемы ECIES основывается на стойкости схемы выработки ключа KE в модели mODH и стойкости используемого режима аутентифицированного шифрования AE в моделях LOR-CCA и INT-CTXT. В качестве направлений дальнейших исследований можно указать следующие: (1) изучение стойкости различных

схем выработки общего ключа KE в моделях ODH и mODH с использованием различных идеализаций, например моделей случайного оракула [4], обобщенной группы [18, 19] и т. д.; (2) расширение модели mODH на более общие ситуации, возникающие при изучении конкретных реализаций схемы ECIES [3] (использование только X-координаты точки эллиптической кривой, хэширование координат точки эллиптической кривой и т. д.); (3) рассмотрение схемы аутентифицированного шифрования с присоединенными данными совместно с анализом свойств безопасности.

Автор благодарит рецензентов за внимательное отношение к работе и множество полезных комментариев, позволивших значительно улучшить изложение.

Список литературы

[1] Martínez G. V., Encinas L. H., "A comparison of the standardized versions of ECIES", Sixth Int. Conf. Inf. Assurance and Security, 2010, 1–4.

[2] Martínez G. V., Encinas L. H., Dios A. Q., "Security and practical considerations when implementing the elliptic curve integrated encryption scheme", *Cryptologia*, **39**:3 (2015), 244–269.

[3] Shoup V., "A proposal for an ISO standard for public key encryption", *IACR Cryptology ePrint Archive, Paper 2001/112*, 2001, `https://eprint.iacr.org/2001/112`.

[4] Abdalla M., Bellare M., Rogaway P., "The Oracle Diffie-Hellman assumptions and an analysis of DHIES", CT-RSA 2001, Lect. Notes Comput. Sci., **2020**, 2001, 143–158.

[5] Smart N., "The exact security of ECIES in the generic group model", Cryptography and Coding, Lect. Notes Comput. Sci., **2260**, 2001, 73–84.

[6] Bellare M., Namprempre C., "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm", *J. Cryptology*, **21**:4 (2008), 469–491.

[7] Boyd C., Mathuria A., Stebila D., *Protocols for authentication and key establishment*, 2nd edition, Springer, Berlin, Heidelberg, 2020, 521 pp.

[8] Нестеренко А. Ю., Семенов А. М., "Методика оценки безопасности криптографических протоколов", *Прикл. дискр. матем.*, 2022, №56, 33–82.

[9] 3GPP, *Technical specification (TS). Security architecture and procedures for 5G System (3GPP TS 33.501 version 17.5.0 Release 17)*, 2022.

[10] *Рекомендации по стандартизации Р*1323565.1.026-2019. *Информационная технология* (*ИТ*). *Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование*, М.: Стандартинформ, 2019, 12+IV с.

[11] Nozdrunov V., "Parallel and double block cipher mode of operation (PD-mode) for authenticated encryption", Preproceedings, 6th Workshop on Current Trends in Cryptology (CTCrypt 2017), 2017, 36–45.

[12] *Межгосударственный стандарт ГОСТ* 34.13-2018. *Информационная технология* (*ИТ*). *Криптографическая защита информации. Режимы работы блочных шифров*, М.: Стандартинформ, 2018, 24+V с.

[13] *Рекомендации по стандартизации Р* 50.1.113-2016. *Информационная технология (ИТ). Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования*, М.: Стандартинформ, 2016, 24+IV с.

[14] Алексеев Е. К., Ошкин И. Б., Попов В. О., Смышляев С. В., "О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012", *Математические вопросы криптографии*, **7**:1 (2016), 5–38.

[15] Katz J., Lindell Y., *Introduction to modern cryptography*, CRC press, Boca Raton, Florida, 2020, 626 pp.

[16] Guo F., Susilo W., Mu Y., *Introduction to security reduction*, Springer, Cham, Switzerland, 2018, 253 pp.

[17] Bellare M., Rogaway P., "The security of triple encryption and a framework for code-based game-playing proofs", EUROCRYPT 2006, Lect. Notes Comput. Sci., **4004**, 2006, 409–426.

[18] Нечаев В. И., "К вопросу о сложности детерминированного алгоритма для дискретного логарифма", *Матем. заметки*, **55**:2 (1994), 91–101.

[19] Shoup V., "Lower bounds for discrete logarithms and related problems", EUROCRYPT 1997, Lect. Notes Comput. Sci., **1233**, 1997, 256–266.

[20] *Межгосударственный стандарт ГОСТ* 34.12-2018. *Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры*, М.: Стандартинформ, 2018, 13+IV с.

[21] Bellare M., Goldreich O., Mityagin A., "The power of verification queries in message authentication and authenticated encryption", *IACR Cryptology ePrint Archive, Paper 2004/309*, 2004 `https://eprint.iacr.org/2004/309`.

[22] Rogaway P., "Evaluation of some blockcipher modes of operation", *Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan*, 2011.

[23] Iwata T., Kurosawa K., "Stronger security bounds for OMAC, TMAC, and XCBC", INDOCRYPT 2003, Lect. Notes Comput. Sci., **2904**, 2003, 402–415.

[24] Nandi M., "Improved security analysis for OMAC as a pseudorandom function", *J. Math. Cryptology*, **3**:2 (2009), 133–148.

[25] Chattopadhyay S., Jha A., Nandi M., "Towards tight security bounds for OMAC, XCBC and TMAC", ASIACRYPT 2022, Lect. Notes Comput. Sci., **13791**, 2023, 348–378.

[26] Ahmetzyanova L., Alekseev E., Oshkin I., Smyshlyaev S., Sonina L., "On the properties of the CTR encryption mode of Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing", *Математические вопросы криптографии*, **8**:2 (2017), 39–50.

[27] Bellare M., Rogaway P., "Random oracles are practical: A paradigm for designing efficient protocols", 1st ACM Conf. Computer Communic. Security, 1993, 62–73.

[28] Koblitz N., Menezes A., "The random oracle model: a twenty-year retrospective", *Designs, Codes and Cryptography*, **77** (2015), 587–610.

A. Сводимость моделей с несколькими участниками к случаю одного участника

A.1. Доказательство утверждения 1

Будем использовать технику гибридного аргумента. Обозначим через $\mathbf{Exp}_{b_1 \ldots b_D}$, $b_i \in \{0, 1\}$ эксперимент $\mathsf{mLOR\text{-}CCA}$ с таким набором ора-

кулов, что на запросы вида (i, m_0, m_1) оракул $\mathcal{O}_{\text{enc}}$ выбирает сообщение m_{b_i} для зашифрования. В таком случае преимущество противника $\mathcal{A}$ может быть представлено следующим образом:

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mLOR\text{-}CCA}}_{\mathsf{AE}}(\mathcal{A}) &= \mathbb{P}[\mathbf{Exp}_{11\ldots1}(\mathcal{A}) \to 1] - \mathbb{P}[\mathbf{Exp}_{00\ldots0}(\mathcal{A}) \to 1] \\ &= (\mathbb{P}[\mathbf{Exp}_{11\ldots1}(\mathcal{A}) \to 1] - \mathbb{P}[\mathbf{Exp}_{11\ldots0}(\mathcal{A}) \to 1]) \\ \ldots + \left(\mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{s}\underbrace{0\ldots0}_{D-s}}(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{s-1}\underbrace{0\ldots0}_{D-s+1}}(\mathcal{A}) \to 1\right]\right) \\ \ldots + (\mathbb{P}[\mathbf{Exp}_{10\ldots0}(\mathcal{A}) \to 1] - \mathbb{P}[\mathbf{Exp}_{00\ldots0}(\mathcal{A}) \to 1])\,.\end{aligned}$$

Каждое из слагаемых вида

$$\left(\mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{s}\underbrace{0\ldots0}_{D-s}}(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{s-1}\underbrace{0\ldots0}_{D-s+1}}(\mathcal{A}) \to 1\right]\right)$$

ограничивается сверху величиной

$$\mathbf{InSec}^{\mathsf{LOR\text{-}CCA}}_{\mathsf{AE}}(t + T_{\mathsf{mLOR\text{-}CCA}}, Q_e[s], L_e[s], M_e[s], Q_d[s], L_d[s], M_d[s]), \quad (1)$$

где $T_{\mathsf{mLOR\text{-}CCA}}$ — время, необходимое на моделирование эксперимента $\mathsf{mLOR\text{-}CCA}$. Покажем это, построив противников $\mathcal{B}_s$, $1 \leqslant s \leqslant D$, в модели $\mathsf{LOR\text{-}CCA}$ (с одним участником). Противник $\mathcal{B}_s$ генерирует ключи K_i, $1 \leqslant i \leqslant D$, $i \neq s$, отвечает специальным образом на запросы противника $\mathcal{A}$ (см. табл. 1) и выдает тот же бит b', что и $\mathcal{A}$.

Таблица 1. Обработка запросов $\mathcal{A}$ на зашифрование противником $\mathcal{B}_s$

$(1, m_0, m_1), \ldots$ $\ldots, (s-1, m_0, m_1)$	(s, m_0, m_1)	$(s+1, m_0, m_1), \ldots$ $\ldots, (D, m_0, m_1)$
Выбрать m_1 и зашифровать на ключе K_i, $1 \leqslant i \leqslant s-1$	Перенаправить оракулу $\mathcal{O}^b_{\text{enc}}(m_0, m_1)$	Выбрать m_0 и зашифровать на ключе K_i, $s+1 \leqslant i \leqslant D$

По определению экспериментов

$$\mathbb{P}\left[\mathbf{Exp}^{\mathsf{LOR\text{-}CCA\text{-}1}}_{\mathsf{AE}}(\mathcal{B}_s) \to 1\right] = \mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{s}\underbrace{0\ldots0}_{D-s}}(\mathcal{A}) \to 1\right],$$

$$\mathbb{P}\left[\mathbf{Exp}^{\mathsf{LOR\text{-}CCA\text{-}0}}_{\mathsf{AE}}(\mathcal{B}_s) \to 1\right] = \mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{s-1}\underbrace{0\ldots0}_{D-s+1}}(\mathcal{A}) \to 1\right],$$

откуда следует оценка (1). Количество тактов вычислений $T_{\mathsf{mLOR\text{-}CCA}}$ может быть ограничено сверху следующим образом (генерация ключей, обработка запросов):

$$T_{\mathsf{mLOR\text{-}CCA}} \leqslant D + \sum_{i=1}^{D} \left(Q_e[i] + Q_d[i] + L_e[i] + L_d[i]\right).$$

A.2. Доказательство утверждения 2

Пусть $\mathcal{A}$ — противник в модели $\mathsf{mINT\text{-}CTXT}$ с D участниками. Построим противника $\mathcal{B}$ в модели $\mathsf{mINT\text{-}CTXT}$ (с одним участником), который использует $\mathcal{A}$ как подпроцедуру и достигает преимущества, равного $\frac{1}{D}\,\mathbf{Adv}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}(\mathcal{A})$:

– $\mathcal{B}$ выбирает случайный номер $s \xleftarrow{\mathcal{U}} \{1,\ldots,D\}$;

– генерирует $K_i \xleftarrow{\mathcal{U}} \{0,1\}^{klen}$, $1 \leqslant i \leqslant D$, $i \neq s$;

– обрабатывает запросы $\mathcal{A}$ вида $(i,\cdot)$, $1 \leqslant i \leqslant D$, $i \neq s$, согласно описанию эксперимента $\mathsf{mINT\text{-}CTXT}$; запросы вида $(s,\cdot)$ перенаправляются собственным оракулам $\mathcal{B}$.

Противник $\mathcal{B}$ успешно подделывает шифртекст тогда и только тогда, когда $\mathcal{A}$ успешно подделывает шифртекст для s-го ключа. Поскольку s было выбрано случайно равновероятно, и ключи K_i, $1 \leqslant i \leqslant D$, независимы и одинаково распределены, имеем:

$$\mathbf{Adv}^{\mathsf{INT\text{-}CTXT}}_{\mathsf{AE}}(\mathcal{B}) = \frac{1}{D}\,\mathbf{Adv}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}(\mathcal{A}).$$

Ресурсы противника $\mathcal{B}$ относительно оракулов и временные ресурсы не превосходят указанных в условиях утверждения.

A.3. Доказательство утверждения 3

Обозначим через $\mathbf{Exp}_{b_1 b_2 \ldots b_D}$, $b_i \in \{0,1\}$, эксперимент $\mathbf{Exp}^{\mathsf{mODH}}_{\mathsf{KE}}$, в котором на i-й запрос к оракулу $\mathcal{O}_{\mathrm{kgen}}$ возвращается ответ, сформированный в соответствии с тем, как если бы в оракуле $\mathcal{O}_{\mathrm{kgen}}$ был зафиксирован бит b_i (т. е. на i-й запрос к оракулу $\mathcal{O}_{\mathrm{kgen}}$ возвращается $\mathsf{KE.Comb}(sk, epk)$, если $b_i = 1$, и случайный равновероятный ключ из множества $\{0,1\}^{klen}$ в случае $b_i = 0$). Положим $D = q_{gen}$. Тогда преимущество противника $\mathcal{A}$ выражается следующим образом:

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mODH}}_{\mathsf{KE}}(\mathcal{A}) &= \mathbb{P}[\mathbf{Exp}_{11\ldots1}(\mathcal{A}) \to 1] - \mathbb{P}[\mathbf{Exp}_{00\ldots0}(\mathcal{A}) \to 1] \\ &= \sum_{i=0}^{D-1} \left(\mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{D-i}\underbrace{0\ldots0}_{i}}(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{D-i-1}\underbrace{0\ldots0}_{i+1}}(\mathcal{A}) \to 1\right] \right).\end{aligned}$$

Ограничим каждое из слагаемых вида

$$\left(\mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{s}\underbrace{0\ldots0}_{D-s}}(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{s-1}\underbrace{0\ldots0}_{D-s+1}}(\mathcal{A}) \to 1\right] \right).$$

Для корректного моделирования эксперимента необходимо исключить возможность возникновения коллизии выделенного генерируемого значения epk' с каким-либо из значений epk, запрошенных противником $\mathcal{A}$ у оракула $\mathcal{O}_{\mathrm{comb}}$ до генерации выделенного значения. Рассмотрим модификацию эксперимента $\mathbf{Exp}_{\underbrace{1\ldots1}_{s-1}\,b\,\underbrace{0\ldots0}_{D-s}}$, в которой эксперимент прерывается при возникновении подобной коллизии (см. псевдокод эксперимента $\widetilde{\mathbf{Exp}}^{b}_{s}$ на рис. 9; измененные по сравнению с экспериментом $\mathbf{Exp}_{\underbrace{1\ldots1}_{s-1}\,b\,\underbrace{0\ldots0}_{D-s}}$ места выделены пунктирной рамкой). По фундаментальной игровой лемме (см., например, [17, лемма 1]) выполнено неравенство

$$\begin{aligned}&\left(\mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{s}\underbrace{0\ldots0}_{D-s}}(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\mathbf{Exp}_{\underbrace{1\ldots1}_{s-1}\underbrace{0\ldots0}_{D-s+1}}(\mathcal{A}) \to 1\right] \right) \\ &\qquad \leqslant \mathbb{P}\left[\widetilde{\mathbf{Exp}}^{1}_{s}(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\widetilde{\mathbf{Exp}}^{0}_{s}(\mathcal{A}) \to 1\right] + 2\,\mathbb{P}[\mathbf{Bad}],\end{aligned}$$

где $\mathbb{P}[\mathbf{Bad}]$ — вероятность того, что флаг *bad* в эксперименте $\widetilde{\mathbf{Exp}}^{b}_{s}$ будет установлен значением True. Вероятность события **Bad** ограничивается

сверху: $\mathbb{P}[\mathbf{Bad}] \leqslant q_{com}/|EpkSet|$, что следует из условия равномерности распределения ключей epk на множестве $EpkSet$.

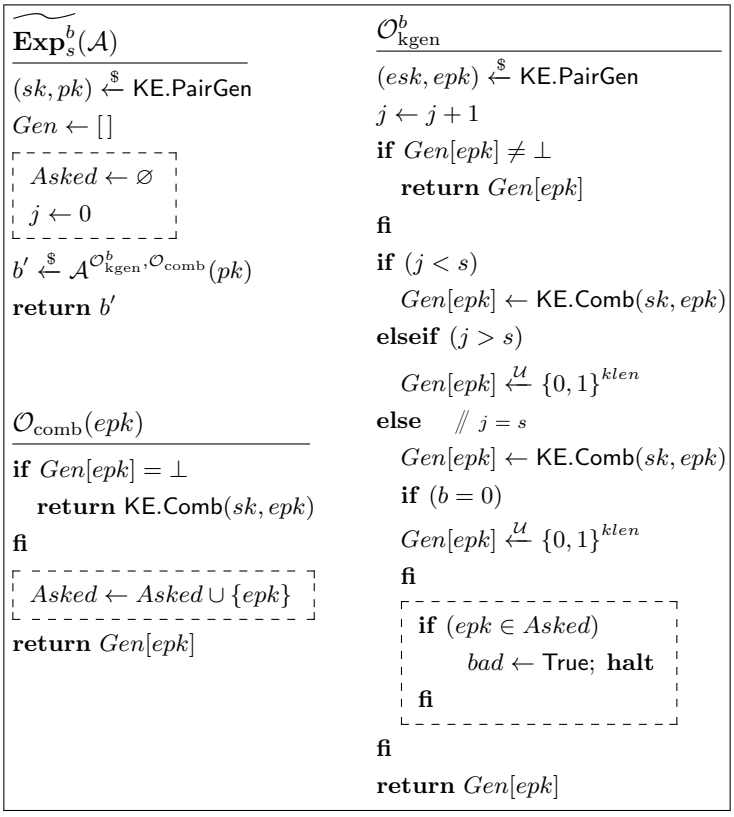

Рис. 9. Псевдокод модифицированного эксперимента $\widetilde{\mathbf{Exp}}^b_s$: добавлено прерывание в случае, когда сгенерированный оракулом $\mathcal{O}_{\mathrm{kgen}}$ на s-м шаге ключ ранее запрашивался у оракула $\mathcal{O}_{\mathrm{comb}}$

Разность $\varepsilon = \mathbb{P}\left[\widetilde{\mathbf{Exp}}^1_s(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\widetilde{\mathbf{Exp}}^0_s(\mathcal{A}) \to 1\right]$ ограничим сверху при помощи следующих соображений. Пусть $\mathcal{B}_s$ — противник в модели ODH, который моделирует для противника $\mathcal{A}$ условия эксперимента $\widetilde{\mathbf{Exp}}^b_s$ и достигает преимущества ε. Противник $\mathcal{B}_s$ в рамках эксперимента $\mathbf{Exp}^{\mathsf{ODH}\text{-}b}_{\mathsf{KE}}$ получает тройку значений (pk, epk', K'), где K' — либо случайно равновероятно выбранный ключ (при $b = 0$), либо ключ, сформированный с помощью алгоритма $\mathsf{KE.Comb}$ на значениях (sk, epk').

Противник $\mathcal{B}_s$ заводит пустой словарь Gen, счетчик j и отвечает на запросы $\mathcal{A}$ следующим образом.

1) Запросы epk противника $\mathcal{A}$ к оракулу $\mathcal{O}_{\text{comb}}$:
   - если $epk = epk'$ и $j < s$: прервать эксперимент (**halt**);
   - если $Gen[epk] = \perp$: перенаправить запрос к оракулу $\mathcal{O}_{\text{comb}}$ противника $\mathcal{B}_s$: $K \leftarrow \mathcal{O}_{\text{comb}}(epk)$;
   - вернуть $Gen[epk]$ противнику $\mathcal{A}$.

2) Запросы $\mathcal{A}$ к оракулу $\mathcal{O}_{\text{kgen}}$:
   - увеличить счетчик $j \leftarrow j + 1$;
   - сгенерировать $(esk, epk) \xleftarrow{\$} \mathsf{KE.PairGen}$;
   - если $j < s$ и $Gen[epk] = \perp$: положить $Gen[epk] \leftarrow \mathsf{KE.Comb}(esk, pk)$;
   - если $j = s$: положить $epk \leftarrow epk'$, если $Gen[epk] = \perp$: положить $Gen[epk] \leftarrow K'$;
   - если $j > s$ и $Gen[epk] = \perp$: положить $Gen[epk] \xleftarrow{\mathcal{U}} \{0,1\}^{klen}$;
   - вернуть $Gen[epk]$ противнику $\mathcal{A}$.

Противник $\mathcal{B}_s$ возвращает тот же бит b', что и $\mathcal{A}$. Заметим, что $\mathcal{B}_s$ в рамках эксперимента $\mathbf{Exp}_{\mathsf{KE}}^{\mathsf{ODH}\text{-}b}$ моделирует для $\mathcal{A}$ условия эксперимента $\widetilde{\mathbf{Exp}}_s^b$:

- проверка условия $epk' \in Asked$ на s-м запросе к оракулу $\mathcal{O}_{\text{kgen}}$ эквивалентна проверке пары условий $(epk = epk')$ и $(j < s)$ при обработке обращений к оракулу $\mathcal{O}_{\text{comb}}$ (эксперименты прерываются при одних и тех же условиях); распределение ответов противника $\mathcal{B}_s$ при запросах $\mathcal{A}$ к оракулу $\mathcal{O}_{\text{comb}}$ в исходах, при которых эксперимент не прерывается, идентично описанному в эксперименте на рис. 9;

- распределение ответов противника $\mathcal{B}_s$ при запросах $\mathcal{A}$ к оракулу $\mathcal{O}_{\text{kgen}}$ идентично распределению ответов в эксперименте $\widetilde{\mathbf{Exp}}_s^b$: на первые $s - 1$ запросов к $\mathcal{O}_{\text{kgen}}$ противник $\mathcal{B}_s$ возвращает «честно сгенерированные» (с помощью алгоритма $\mathsf{KE.Comb}$) ключи, на последние $D - s$ запросов — случайно выбранные ключи; на s-м шаге при $b = 0$ используется случайно равновероятно выбранный ключ K', при $b = 1$ — ключ, сгенерированный с помощью алгоритма $\mathsf{KE.Comb}$.

Поскольку $\mathcal{B}_s$ выдает тот же бит b', что и $\mathcal{A}$, выполняется равенство:

$$\mathbb{P}\Big[\widetilde{\mathbf{Exp}}_s^b(\mathcal{A}) \to 1\Big] = \mathbb{P}\big[\mathbf{Exp}_{\mathsf{KE}}^{\mathsf{ODH}\text{-}b}(\mathcal{B}_s) \to 1\big],$$

а значит, выполняется неравенство

$$\mathbf{Adv}_{\mathsf{KE}}^{\mathsf{mODH}}(\mathcal{A}) \leqslant \sum_{s=0}^{D-1} \left(\mathbf{Adv}_{\mathsf{KE}}^{\mathsf{ODH}}(\mathcal{B}_s) + \frac{2\, q_{com}}{|EpkSet|} \right),$$

откуда (при переходе к максимумам по всем противникам с ограничением на вычислительные ресурсы и число запросов к оракулам) следует утверждение теоремы.

B. Доказательство теоремы 1

Пусть $\mathcal{A}$ — противник в модели $\mathsf{LOR\text{-}CCA}$ для схемы ECIES. Доказательство состоит из двух шагов: (1) заменить ключи, сгенерированные с помощью алгоритма $\mathsf{KE.Comb}$, случайными равновероятными ключами из множества $\{0,1\}^{klen}$; (2) проанализировать схему ECIES со случайно выбираемыми ключами, сведя задачу к изучению схемы AE в модели $\mathsf{mLOR\text{-}CCA}$. Введем промежуточную модель $\widetilde{\mathsf{LOR\text{-}CCA}}$, в которой все ключи, вырабатываемые в ходе зашифрования сообщений в оракуле $\mathcal{O}_{\text{enc}}$, выбираются случайно равновероятно из множества $\{0,1\}^{klen}$ (см. псевдокод на рис. 10; измененные фрагменты псевдокода выделены пунктирными рамками). Тогда преимущество $\mathcal{A}$ может быть представлено следующим образом:

$$\begin{aligned}
\mathbf{Adv}_{\text{ECIES}}^{\mathsf{LOR\text{-}CCA}}(\mathcal{A}) &= \mathbb{P}\big[\mathbf{Exp}_{\text{ECIES}}^{\mathsf{LOR\text{-}CCA\text{-}1}}(\mathcal{A}) \to 1\big] - \mathbb{P}\big[\mathbf{Exp}_{\text{ECIES}}^{\mathsf{LOR\text{-}CCA\text{-}0}}(\mathcal{A}) \to 1\big] \\
&= \Big(\mathbb{P}\big[\mathbf{Exp}_{\text{ECIES}}^{\mathsf{LOR\text{-}CCA\text{-}1}}(\mathcal{A}) \to 1\big] - \mathbb{P}\Big[\mathbf{Exp}_{\text{ECIES}}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}1}(\mathcal{A}) \to 1\Big]\Big) \\
&+ \Big(\mathbb{P}\Big[\mathbf{Exp}_{\text{ECIES}}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}1}(\mathcal{A}) \to 1\Big] - \mathbb{P}\Big[\mathbf{Exp}_{\text{ECIES}}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}0}(\mathcal{A}) \to 1\Big]\Big) \\
&+ \Big(\mathbb{P}\Big[\mathbf{Exp}_{\text{ECIES}}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}0}(\mathcal{A}) \to 1\Big] - \mathbb{P}\big[\mathbf{Exp}_{\text{ECIES}}^{\mathsf{LOR\text{-}CCA\text{-}0}}(\mathcal{A}) \to 1\big]\Big). \quad (2)
\end{aligned}$$

Оценим первое слагаемое в формуле (2). Для этого построим противника $\mathcal{B}$ в модели mODH, который действует следующим образом.

1) При запросе $\mathcal{A}$ вида (m_0, m_1) к оракулу $\mathcal{O}_{\text{enc}}^1$:

   – запрашивает $(epk, K) \xleftarrow{\$} \mathcal{O}_{\text{kgen}}^b$;

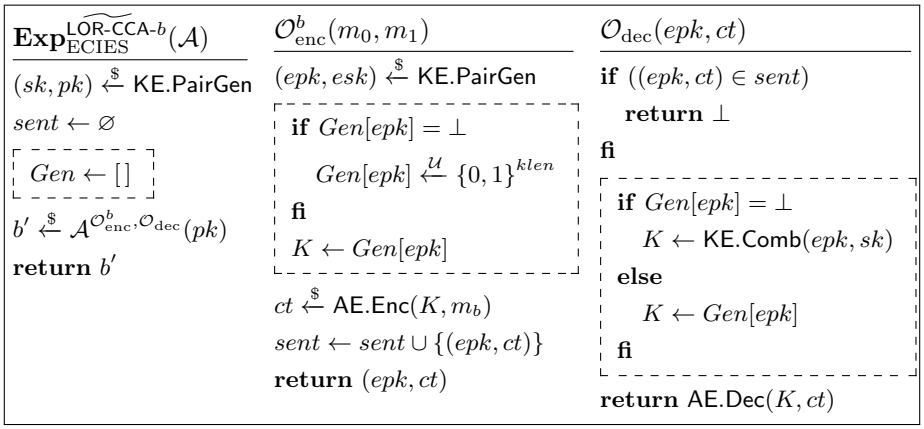

Рис. 10. Псевдокод эксперимента $\mathbf{Exp}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}b}_{\mathrm{ECIES}}$: основное отличие от исходного эксперимента $\mathbf{Exp}^{\mathsf{LOR\text{-}CCA}\text{-}b}_{\mathrm{ECIES}}$ заключается в том, что ключи в оракуле $\mathcal{O}^b_{\mathrm{enc}}$ выбираются случайно равновероятно из множества $\{0,1\}^{klen}$

– обрабатывает m_1 на ключе K: $ct \xleftarrow{\$} \mathsf{AE.Enc}(K, m_1)$;
– сохраняет значение $sent \leftarrow sent \cup \{(epk, ct)\}$;
– возвращает (epk, ct).

2) При запросе $\mathcal{A}$ к оракулу $\mathcal{O}_{\mathrm{dec}}$ вида (epk, ct):

– если $(epk, ct) \in sent$: возвращает $\bot$;
– в противном случае запрашивает $K \leftarrow \mathcal{O}_{\mathrm{comb}}(epk)$ и возвращает результат расшифрования $m \leftarrow \mathsf{AE.Dec}(K, ct)$.

Противник $\mathcal{B}$ выдает тот же бит, что и противник $\mathcal{A}$. В случае фиксации бита $b = 1$ в модели mODH (т. е. $\mathcal{B}$ делает запросы к оракулу $\mathcal{O}^1_{\mathrm{kgen}}$) $\mathcal{B}$ симулирует условия эксперимента $\mathbf{Exp}^{\mathsf{LOR\text{-}CCA}\text{-}1}_{\mathrm{ECIES}}$ для $\mathcal{A}$ (ключи в оракуле $\mathcal{O}^1_{\mathrm{kgen}}$ вырабатываются в соответствии со схемой выработки ключа KE). Если в модели mODH зафиксирован бит $b = 0$ (т. е. $\mathcal{B}$ делает запросы к оракулу $\mathcal{O}^0_{\mathrm{kgen}}$), то $\mathcal{B}$ воспроизводит условия эксперимента $\mathbf{Exp}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}1}_{\mathrm{ECIES}}$ для $\mathcal{A}$. Таким образом, имеем:

$$\mathbb{P}\big[\mathbf{Exp}^{\mathsf{mODH}\text{-}1}_{\mathsf{KE}}(\mathcal{B}) \to 1\big] = \mathbb{P}\big[\mathbf{Exp}^{\mathsf{LOR\text{-}CCA}\text{-}1}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\big],$$
$$\mathbb{P}\big[\mathbf{Exp}^{\mathsf{mODH}\text{-}0}_{\mathsf{KE}}(\mathcal{B}) \to 1\big] = \mathbb{P}\Big[\mathbf{Exp}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}1}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\Big].$$

Аналогичным образом (с заменой m_1 на m_0) строится противник и для третьего слагаемого в формуле (2). Таким образом, первое и тре-

тье слагаемые в формуле (2) оцениваются сверху величиной

$$\mathbf{InSec}^{\mathsf{mODH}}_{\mathsf{KE}}\left(t + T_{\mathsf{LOR\text{-}CCA}}, q_e, q_d\right),\ T_{\mathsf{LOR\text{-}CCA}} = q_e + q_d + \ell_e + \ell_d.$$

Теперь рассмотрим второе слагаемое в формуле (2). Покажем, что его можно оценить сверху через преимущество противника относительно режима шифрования AE в модели $\mathsf{mLOR\text{-}CCA}$ с $D = q_e$ участниками **с одним запросом на зашифрование на каждом из ключей**. Для этого рассмотрим еще одну модификацию исходного эксперимента (см. псевдокод на рис. 11; измененные фрагменты псевдокода выделены пунктирными рамками). Эксперимент прерывается в двух случаях:

– либо epk генерировался ранее в рамках моделирования поведения оракула $\mathcal{O}_{\text{enc}}$ (условие $epk \in EGen$) — в таком случае для некоторого индекса i может возникнуть более одного запроса на зашифрование сообщений, и в таком случае итоговая оценка окажется хуже;

– либо epk генерировался ранее в рамках моделирования поведения оракула $\mathcal{O}_{\text{dec}}$ (условие $epk \in DGen$) — в таком случае противник $\mathcal{B}$ должен обработать сообщение m_b на ключе $\mathsf{KE.Comb}(epk, sk)$, не зная бит b; указанная коллизия также нежелательна.

По фундаментальной игровой лемме (см. [17, лемма 1]) имеем:

$$\begin{aligned}\mathbf{Adv}^{\widetilde{\mathsf{LOR\text{-}CCA}}}_{\text{ECIES}}(\mathcal{A}) &= \mathbb{P}\Big[\mathbf{Exp}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}1}_{\text{ECIES}}(\mathcal{A}) \to 1\Big] - \mathbb{P}\Big[\mathbf{Exp}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}0}_{\text{ECIES}}(\mathcal{A}) \to 1\Big] \\ &\leqslant \mathbb{P}\Big[\mathbf{Exp}^{\mathsf{LOR\text{-}CCA'}\text{-}1}_{\text{ECIES}}(\mathcal{A}) \to 1\Big] - \mathbb{P}\Big[\mathbf{Exp}^{\mathsf{LOR\text{-}CCA'}\text{-}0}_{\text{ECIES}}(\mathcal{A}) \to 1\Big] + 2\,\mathbb{P}[\mathbf{Bad}],\end{aligned}$$

где $\mathbb{P}[\mathbf{Bad}]$ — вероятность того, что флаг bad будет установлен значением True. Вероятность $\mathbb{P}[\mathbf{Bad}]$ может быть ограничена сверху следующим образом. При выборе случайного равновероятного ключа $epk \xleftarrow{\mathcal{U}} EpkSet$:

– вероятность события $epk \in EGen$ не превышает $\frac{|EGen|}{|EpkSet|}$,

– вероятность события $epk \in DGen$ не превышает $\frac{|DGen|}{|EpkSet|}$.

Следовательно, если количество запросов противника $\mathcal{A}$ к оракулу $\mathcal{O}_{\text{enc}}$ не превышает q_e, к $\mathcal{O}_{\text{dec}}$ — не превышает q_d, то для вероятности события $\mathbf{Bad}$ справедлива оценка

$$\mathbb{P}[\mathbf{Bad}] \leqslant \frac{q_e \cdot (q_e - 1)}{2|EpkSet|} + \frac{q_e\, q_d}{|EpkSet|} \leqslant \frac{q_e \cdot (q_e/2 + q_d)}{|EpkSet|}.$$

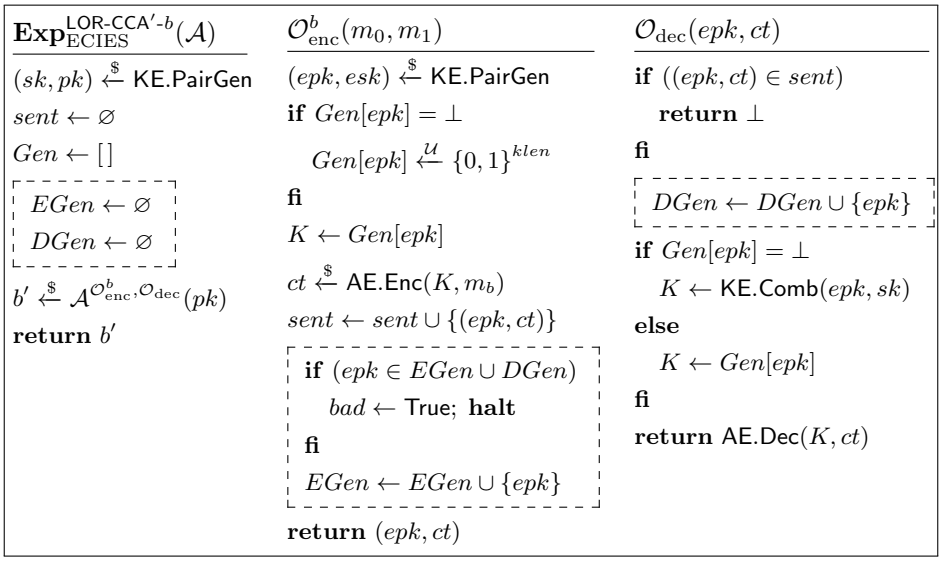

Рис. 11. Псевдокод эксперимента $\mathbf{Exp}^{\mathsf{LOR\text{-}CCA'\text{-}}b}_{\mathrm{ECIES}}$: добавлены прерывания при возникновении коллизий

Разность $\mathbb{P}\Big[\mathbf{Exp}^{\mathsf{LOR\text{-}CCA'\text{-}1}}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\Big] - \mathbb{P}\Big[\mathbf{Exp}^{\mathsf{LOR\text{-}CCA'\text{-}0}}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\Big]$ оценивается следующим образом. Построим противника $\mathcal{B}$ в модели mLOR-CCA, который генерирует ключевую пару $(sk, pk) \xleftarrow{\$} \mathsf{KE.PairGen}$ и предоставляет pk противнику $\mathcal{A}$. Также он заводит пустой словарь Gen, пустые множества $EGen$, $DGen$ и счетчик $i \leftarrow 1$.

1) При запросе $\mathcal{A}$ к оракулу $\mathcal{O}^b_{\mathrm{enc}}$ вида (m_0, m_1) противник $\mathcal{B}$:
   - генерирует $(esk, epk) \xleftarrow{\$} \mathsf{KE.PairGen}$;
   - если $epk \in EGen \cup DGen$: прерывает эксперимент;
   - обновляет значения
   $$Gen[epk] \leftarrow i,\ i \leftarrow i + 1,\ EGen \leftarrow EGen \cup \{epk\};$$
   - делает запрос $ct \xleftarrow{\$} \mathcal{O}^b_{\mathrm{enc}}(Gen[epk], m_0, m_1)$;
   - возвращает пару (epk, ct) противнику $\mathcal{A}$.
2) При запросе $\mathcal{A}$ к оракулу $\mathcal{O}_{\mathrm{dec}}$ вида (epk, ct) противник $\mathcal{B}$:
   - обновляет значение $DGen \leftarrow DGen \cup \{epk\}$;

– если $Gen[epk] \neq \perp$: запрашивает свой собственный оракул $m \leftarrow \mathcal{O}_{\mathrm{dec}}(Gen[epk], ct)$ и возвращает m;

– в противном случае вычисляет $K \leftarrow \mathsf{KE.Comb}(epk, sk)$, обрабатывает ct на ключе K согласно алгоритму $\mathsf{AE.Dec}$ и возвращает результат обработки противнику $\mathcal{A}$.

В конце эксперимента противник $\mathcal{B}$ выдает тот же бит, что и $\mathcal{A}$. Противник $\mathcal{B}$ в рамках эксперимента $\mathsf{mLOR\text{-}CCA}$ для схемы AE моделирует для противника $\mathcal{A}$ условия эксперимента $\mathsf{LOR\text{-}CCA'}$ для схемы ECIES:

– если эксперимент не прервался, то генерируемые в оракуле $\mathcal{O}_{\mathrm{enc}}$ ключи epk гарантированно не повторились, а значит, всякий раз выполняется условие $Gen[epk] = \perp$; в таком случае противник $\mathcal{B}$ обращается с запросом на зашифрование к своему оракулу $\mathcal{O}_{\mathrm{enc}}$ на i-м ключе и наращивает счетчик i; при этом на каждом ключе происходит единственное обращение к оракулу $\mathcal{O}_{\mathrm{enc}}$;

– моделирование условий работы оракула $\mathcal{O}_{\mathrm{dec}}$ полностью соответствует псевдокоду эксперимента $\mathbf{Exp}_{\mathrm{ECIES}}^{\mathsf{LOR\text{-}CCA'}\text{-}b}$, а значит, распределения ответов также идентичны.

Таким образом, выполнены равенства

$$\mathbb{P}\Big[\mathbf{Exp}_{\mathrm{ECIES}}^{\mathsf{LOR\text{-}CCA'}\text{-}b}(\mathcal{A}) \to 1\Big] = \mathbb{P}\big[\mathbf{Exp}_{\mathsf{AE}}^{\mathsf{mLOR\text{-}CCA}\text{-}b}(\mathcal{B}) \to 1\big],\ b \in \{0,1\},$$

а значит, для второго слагаемого в формуле (2) справедливо:

$$\begin{aligned}
&\Big(\mathbb{P}\Big[\mathbf{Exp}_{\mathrm{ECIES}}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}1}(\mathcal{A}) \to 1\Big] - \mathbb{P}\Big[\mathbf{Exp}_{\mathrm{ECIES}}^{\widetilde{\mathsf{LOR\text{-}CCA}}\text{-}0}(\mathcal{A}) \to 1\Big]\Big) \\
&\leqslant \mathbb{P}\Big[\mathbf{Exp}_{\mathrm{ECIES}}^{\mathsf{LOR\text{-}CCA'}\text{-}1}(\mathcal{A}) \to 1\Big] - \mathbb{P}\Big[\mathbf{Exp}_{\mathrm{ECIES}}^{\mathsf{LOR\text{-}CCA'}\text{-}0}(\mathcal{A}) \to 1\Big] + 2\,\mathbb{P}[\mathbf{Bad}] \\
&\leqslant \mathbf{InSec}_{\mathsf{AE}}^{\mathsf{mLOR\text{-}CCA}}(t + T, Q_e, L_e, M_e, Q_d, L_d, M_d, q_e) + \frac{q_e \cdot (q_e + 2\,q_d)}{|EpkSet|},
\end{aligned}$$

где использованы следующие обозначения ($1 \leqslant i \leqslant q_e$):

$$T = q_e + q_d + \ell_e + \ell_d, \quad Q_e[i] = 1, \quad L_e[i] = M_e[i] = \mu_e,$$
$$Q_d[i] = q_i, \quad M_d[i] = \mu_d, \quad L_d[i] = q_i \cdot \mu_d, \quad \sum_{i=1}^{q_e} q_i = q_d.$$

C. Анализ модели INT-CTXT для схемы ECIES

Доказательство теоремы 2 аналогично рассмотренному выше и состоит из двух шагов: (1) заменить ключи, сгенерированные с помощью алгоритма $\mathsf{KE.Comb}$, случайными равновероятными ключами из множества $\{0,1\}^{klen}$; (2) проанализировать схему ECIES со случайно выбираемыми ключами, сведя задачу к изучению схемы AE модели mINT-CTXT.

Введем модель $\widetilde{\mathsf{INT\text{-}CTXT}}$ для схемы ECIES, в которой ключи в оракуле $\mathcal{O}_{\mathrm{enc}}$ выбираются случайно равновероятно (см. псевдокод на рис. 12, измененные фрагменты псевдокода выделены пунктирными рамками). Тогда для преимущества противника $\mathcal{A}$ справедлива формула:

$$\begin{aligned}\mathbf{Adv}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}(\mathcal{A}) &= \mathbb{P}\big[\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\big] \\ &= \Big(\mathbb{P}\big[\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\big] - \mathbb{P}\Big[\mathbf{Exp}^{\widetilde{\mathsf{INT\text{-}CTXT}}}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\Big]\Big) \\ &\quad + \mathbb{P}\Big[\mathbf{Exp}^{\widetilde{\mathsf{INT\text{-}CTXT}}}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\Big]. \quad (3)\end{aligned}$$

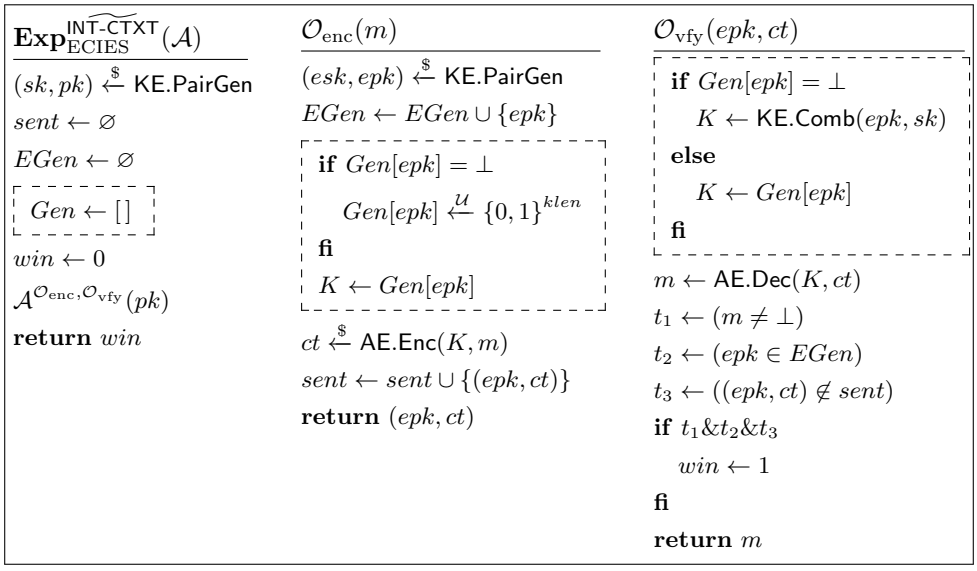

Рис. 12. Псевдокод эксперимента $\mathbf{Exp}^{\widetilde{\mathsf{INT\text{-}CTXT}}}_{\mathrm{ECIES}}$: основное отличие от исходного эксперимента $\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}}_{\mathrm{ECIES}}$ заключается в том, что ключи в оракуле $\mathcal{O}_{\mathrm{enc}}$ выбираются случайно равновероятно из множества $\{0,1\}^{klen}$

Оценим первое слагаемое в формуле (3). Для этого построим противника $\mathcal{B}$ в модели mODH следующим образом.

1) При запросе $\mathcal{A}$ к оракулу $\mathcal{O}_{\text{enc}}$ вида m противник $\mathcal{B}$:
   - запрашивает $(epk, K) \xleftarrow{\$} \mathcal{O}^b_{\text{kgen}}$;
   - обрабатывает m на ключе K: $ct \xleftarrow{\$} \mathsf{AE.Enc}(K, m)$;
   - запоминает значения
   $$sent \leftarrow sent \cup \{(epk, ct)\}, EGen \leftarrow EGen \cup \{epk\};$$
   - возвращает пару (epk, ct).
2) При запросе $\mathcal{A}$ к оракулу $\mathcal{O}_{\text{vfy}}$ вида (epk, ct) противник $\mathcal{B}$:
   - запрашивает $K \leftarrow \mathcal{O}_{\text{comb}}(epk)$;
   - расшифровывает ct: $m \leftarrow \mathsf{AE.Dec}(K, ct)$;
   - возвращает m; если условия t_1, t_2 и t_3 выполнены, то выполняет присваивание $win \leftarrow 1$.

Противник $\mathcal{B}$ возвращает бит win. В случае фиксации бита $b = 1$ в модели mODH (т. е. $\mathcal{B}$ делает запросы к оракулу $\mathcal{O}^1_{\text{kgen}}$) $\mathcal{B}$ симулирует условия эксперимента $\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}}_{\text{ECIES}}$ для $\mathcal{A}$ (ключи в оракуле $\mathcal{O}^1_{\text{kgen}}$ вырабатываются в соответствии со схемой выработки ключа KE). Если в модели mODH зафиксирован бит $b = 0$ (т. е. $\mathcal{B}$ делает запросы к оракулу $\mathcal{O}^0_{\text{kgen}}$), то $\mathcal{B}$ воспроизводит условия эксперимента $\mathbf{Exp}^{\widetilde{\mathsf{INT\text{-}CTXT}}}_{\text{ECIES}}$ для $\mathcal{A}$. Таким образом, имеем:

$$\mathbb{P}\big[\mathbf{Exp}^{\mathsf{mODH\text{-}1}}_{\mathsf{KE}}(\mathcal{B}) \to 1\big] = \mathbb{P}\big[\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}}_{\text{ECIES}}(\mathcal{A}) \to 1\big],$$
$$\mathbb{P}\big[\mathbf{Exp}^{\mathsf{mODH\text{-}0}}_{\mathsf{KE}}(\mathcal{B}) \to 1\big] = \mathbb{P}\Big[\mathbf{Exp}^{\widetilde{\mathsf{INT\text{-}CTXT}}}_{\text{ECIES}}(\mathcal{A}) \to 1\Big],$$

следовательно, для первого слагаемого в оценке (3) выполнена оценка

$$\Big(\mathbb{P}\big[\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}}_{\text{ECIES}}(\mathcal{A}) \to 1\big] - \mathbb{P}\Big[\mathbf{Exp}^{\widetilde{\mathsf{INT\text{-}CTXT}}}_{\text{ECIES}}(\mathcal{A}) \to 1\Big]\Big) \leqslant \mathbf{InSec}^{\mathsf{mODH}}_{\mathsf{KE}}(t + T, q_e, q_v).$$

Теперь ограничим сверху вероятность $\mathbb{P}\Big[\mathbf{Exp}^{\widetilde{\mathsf{INT\text{-}CTXT}}}_{\text{ECIES}}(\mathcal{A}) \to 1\Big]$. Сначала исключим вероятность коллизий значений epk с помощью уже

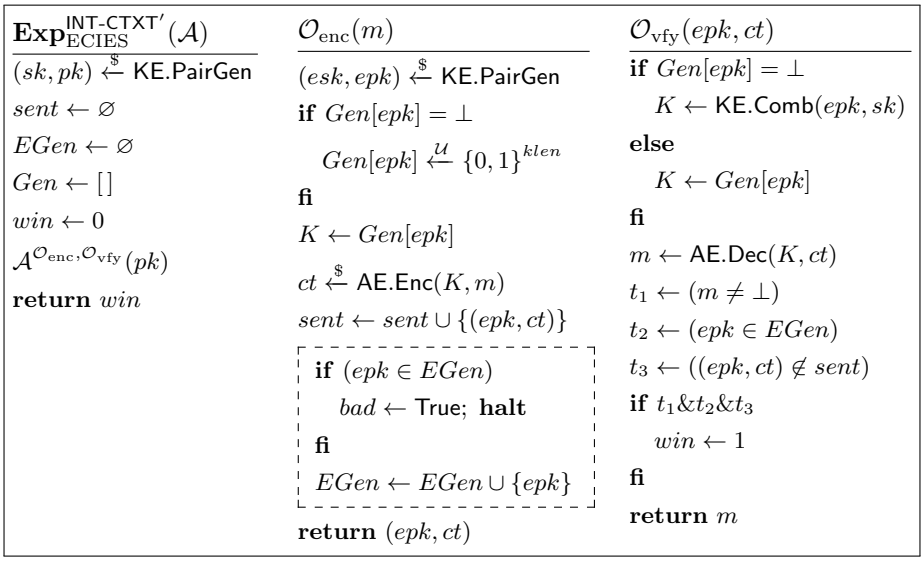

Рис. 13. Псевдокод эксперимента $\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}'}_{\mathrm{ECIES}}$: добавлены прерывания при возникновении коллизий

рассмотренной ранее фундаментальной игровой леммы (см. раздел B). Добавим в псевдокод оракула $\mathcal{O}_{\mathrm{enc}}$ проверку того, что сгенерированный ключ epk не лежит в множестве $EGen$, аналогично тому, как это сделано при рассмотрении модели $\mathsf{LOR\text{-}CCA}'$ (см. псевдокод на рис. 13).

По фундаментальной игровой лемме (см. [17, лемма 1]) имеем:

$$\mathbf{Adv}^{\widetilde{\mathsf{INT\text{-}CTXT}}}_{\mathrm{ECIES}}(\mathcal{A}) \leqslant \mathbb{P}\Big[\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}'}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\Big] + \mathbb{P}[\mathbf{Bad}],$$

где $\mathbb{P}[\mathbf{Bad}]$ — вероятность того, что флаг bad будет установлен значением True. Вероятность $\mathbb{P}[\mathbf{Bad}]$ может быть ограничена сверху: при выборе случайного равновероятного ключа $epk \xleftarrow{\mathcal{U}} EpkSet$ вероятность события $epk \in EGen$ не превышает $\frac{|EGen|}{|EpkSet|}$. Следовательно, если количество запросов противника $\mathcal{A}$ к оракулу $\mathcal{O}_{\mathrm{enc}}$ не превышает q_e, то

$$\mathbb{P}[\mathbf{Bad}] \leqslant \frac{q_e^2}{2|EpkSet|}.$$

Для оценки вероятности $\mathbb{P}\Big[\mathbf{Exp}^{\mathsf{INT\text{-}CTXT}'}_{\mathrm{ECIES}}(\mathcal{A}) \to 1\Big]$ построим противника $\mathcal{B}$ в модели $\mathsf{mINT\text{-}CTXT}$ с $D = q_e$ участниками. Противник $\mathcal{B}$ генерирует ключевую пару $(sk, pk) \xleftarrow{\$} \mathsf{KE.PairGen}$ и предоставляет ключ pk

противнику $\mathcal{A}$. Также он генерирует пустой словарь Gen, множество $EGen$ и заводит счетчик $i \leftarrow 1$.

1) При запросе $\mathcal{A}$ к оракулу $\mathcal{O}_{\text{enc}}$ вида m противник $\mathcal{B}$:
   - генерирует пару $(esk, epk) \xleftarrow{\$} \mathsf{KE.PairGen}$;
   - если $epk \in EGen$: прерывает эксперимент;
   - запоминает $EGen \leftarrow EGen \cup \{epk\}$;
   - устанавливает $Gen[epk] \leftarrow i$ и наращивает счетчик $i \leftarrow i + 1$;
   - запрашивает оракул зашифрования $ct \xleftarrow{\$} \mathcal{O}_{\text{enc}}(Gen[epk], m)$;
   - возвращает пару (epk, ct) противнику $\mathcal{A}$.
2) При запросе $\mathcal{A}$ к оракулу $\mathcal{O}_{\text{vfy}}$ вида (epk, ct) противник $\mathcal{B}$:
   - если $Gen[epk] \neq \perp$: запрашивает $m \leftarrow \mathcal{O}_{\text{dec}}(Gen[epk], ct)$ и возвращает m противнику $\mathcal{A}$;
   - иначе вычисляет $K \leftarrow \mathsf{KE.Comb}(epk, sk)$, обрабатывает ct на ключе K и возвращает результат противнику $\mathcal{A}$.

Из определения противников $\mathcal{A}$ и $\mathcal{B}$ следует, что выполнено равенство

$$\mathbb{P}\big[\mathbf{Exp}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}(\mathcal{B}) \to 1\big] = \mathbb{P}\Big[\mathbf{Exp}^{\mathsf{INT\text{-}CTXT'}}_{\text{ECIES}}(\mathcal{A}) \to 1\Big],$$

где $\mathsf{mINT\text{-}CTXT}$ — модель с $D = q_e$ участниками, следовательно,

$$\mathbb{P}\Big[\mathbf{Exp}^{\mathsf{INT\text{-}CTXT'}}_{\text{ECIES}}(\mathcal{A}) \to 1\Big] \leqslant \mathbf{InSec}^{\mathsf{mINT\text{-}CTXT}}_{\mathsf{AE}}(t + T, Q_e, L_e, M_e, Q_v, L_v, M_v, q_e) + \frac{q_e \cdot (q_e/2)}{|EpkSet|},$$

$$T = q_e + q_v + \ell_e + \ell_v, Q_e[i] = 1, L_e[i] = M_e[i] = \mu_e,$$
$$Q_v[i] = q_i, M_v[i] = \mu_v, L_v[i] = q_i \cdot \mu_v, \sum_i q_i = q_v, 1 \leqslant i \leqslant q_e.$$

D. Оценки для схемы ECIES

Для простоты изложения здесь и далее будем опускать некоторые незначительные технические детали, которые не сильно влияют на итоговые конкретные оценки стойкости. Так, будем использовать обозначение $t' = O(t)$ и опускать члены, которые пренебрежимо мало влияют на итоговую оценку (при использовании «хорошего» блочного шифра).

D.1. Описание одной конкретной версии схемы ECIES

Рассмотрим версию схемы ECIES.

В качестве схемы выработки общего ключа KE возьмем следующую конструкцию. Множество открытых эфемерных ключей — циклическая подгруппа $H = \langle P \rangle$ группы точек эллиптической кривой без нулевой точки: $EpkSet = H \backslash \{0\}$, $h \leftarrow |H| - 1$. Алгоритм KE.PairGen генерирует эфемерный секретный ключ $sk \xleftarrow{U} \{1, \ldots, h\}$ и соответствующий ему открытый ключ $pk \leftarrow sk \cdot P$. Алгоритм KE.Comb (а также конкретные параметры эллиптической кривой, группы точек и ее подгруппы) может быть задан согласно описанию алгоритма **VKO**, приведенного в [14, раздел 3.7] (с параметрами $UKM \leftarrow 1$, $t \leftarrow 512$).

В качестве режима аутентифицированного шифрования рассмотрим следующий механизм (так называемая композиция вида **"Encrypt-then-MAC"** [6, раздел 4.3]). Алгоритм AE.KGen генерирует два независимых равномерно распределенных ключа $K_{enc} \xleftarrow{U} \{0,1\}^{256}$, $K_{mac} \xleftarrow{U} \{0,1\}^{256}$ (т. е. $klen = 512$). Сообщение m на ключе $K = K_{enc} \| K_{mac}$ обрабатывается в два этапа:

– m зашифровывается в режиме работы **CTR** [12] алгоритма шифрования E на ключе K_{enc} и векторе инициализации $IV \leftarrow 0 \ldots 0$:

$$c \leftarrow \mathbf{CTR}^{IV}[E](K_{enc}, m);$$

– имитовставка τ вычисляется с помощью режима выработки имитовставки **CMAC** [12] блочного алгоритма шифрования E:

$$\tau \leftarrow \mathbf{CMAC}[E](K_{mac}, c).$$

Результатом зашифрования сообщения m схемой AE является пара (c, τ). Для расшифрования $ct = (c, \tau)$ на ключе $K = K_{enc} \| K_{mac}$ сначала проверяется имитовставка τ путем ее повторного расчета и сравнения со значением τ (если имитовставка некорректна, то возвращается ошибка $\perp$). Затем (в случае корректности имитовставки) расшифровывается c в режиме **CTR**.

D.2. Дополнительные модели безопасности

D.2.1. Описание модели PRF

Семейством (ключевых) функций будем называть множество функций $\mathcal{F} = \{\mathcal{F}_K \colon \mathrm{Dom} \to \{0,1\}^n \mid K \in \{0,1\}^{klen}\}$, индексированных некоторым ключом $K \in \{0,1\}^{klen}$. Примером семейства функций может

служить блочный шифр «Магма» [20] с длиной ключа $klen = 256$ бит и длиной блока $n = 64$ бита ($\mathrm{Dom} = \{0,1\}^{64}$) или функция выработки имитовставки $\mathsf{MAC}_K(\cdot)$ (в таком случае имеем $\mathrm{Dom} = \{0,1\}^*$).

Введем следующую количественную характеристику псевдослучайности семейства функции (см., например, [15, раздел 3.5.1]).

Определение 15. Преимуществом противника $\mathcal{A}$ в модели PRF (**P**seudo**R**andom **F**unction) для семейства функций $\mathcal{F}$ называется величина

$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathcal{F}}(\mathcal{A}) = \mathbb{P}\big[\mathbf{Exp}^{\mathsf{PRF\text{-}1}}_{\mathcal{F}}(\mathcal{A}) \to 1\big] - \mathbb{P}\big[\mathbf{Exp}^{\mathsf{PRF\text{-}0}}_{\mathcal{F}}(\mathcal{A}) \to 1\big],$$

псевдокод эксперимента $\mathbf{Exp}^{\mathsf{PRF}\text{-}b}_{\mathcal{F}}$, $b \in \{0,1\}$, приведен на рис. 14.

$\mathbf{Exp}^{\mathsf{PRF\text{-}1}}_{\mathcal{F}}(\mathcal{A})$	$\mathcal{O}^b_{\mathrm{prf}}(m)$
$K \xleftarrow{\mathcal{U}} \{0,1\}^{klen}$	**if** $(b = 0)$
$Asked \leftarrow [\,]$	**if** $Asked[m] = \perp$
$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}^b_{\mathrm{prf}}}$	$Asked[m] \xleftarrow{\mathcal{U}} \{0,1\}^n$
return b'	**fi**
	return $Asked[m]$
	else // $b = 1$
	return $\mathcal{F}_K(m)$
	fi

Рис. 14. Псевдокод эксперимента $\mathbf{Exp}^{\mathsf{PRF}\text{-}b}_{\mathcal{F}}$

Определение 16. Обозначим через $\mathbf{InSec}^{\mathsf{PRF}}_{\mathcal{F}}(t, q, \ell, \mu)$ максимум среди значений $\mathbf{Adv}^{\mathsf{PRF}}_{\mathcal{F}}(\mathcal{A})$, где противник $\mathcal{A}$ имеет ограничение t на вычислительные ресурсы и делает не более q запросов к $\mathcal{O}^b_{\mathrm{prf}}$, суммарная и максимальная длины запросов не превосходят ℓ и μ соответственно.

D.2.2. Описание модели EUF-CMA

Для изучения свойства целостности (неподделываемости) будем использовать (стандартную) модель подделки кода аутентификации сообщения EUF-CMA (**E**xistential **U**n**F**orgeability under **C**hosen **M**essage **A**ttack) для детерминированной функции выработки имитовставки MAC (см., например, [21]). В рассматриваемой модели противнику дается доступ к оракулу выработки имитовставки $\mathcal{O}_{\mathrm{tag}}$ и оракулу проверки

имитовставки $\mathcal{O}_{\text{vfy}}$. Противник подает адаптивно выбранные сообщения m различной длины на вход оракулу $\mathcal{O}_{\text{tag}}$ и получает код аутентификации τ сообщения m на секретном ключе K. Задача противника — подделать код аутентификации τ для сообщения m, которое не подавалось ранее на вход оракулу $\mathcal{O}_{\text{tag}}$.

Определение 17. Преимуществом противника $\mathcal{A}$ в модели EUF-CMA для схемы выработки имитовставки MAC называется величина

$$\mathbf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{MAC}}(\mathcal{A}) = \mathbb{P}\big[\mathbf{Exp}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{MAC}}(\mathcal{A}) \to 1\big],$$

псевдокод эксперимента $\mathbf{Exp}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{MAC}}$ приведен на рис. 15.

$\mathbf{Exp}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{MAC}}(\mathcal{A})$	$\mathcal{O}_{\text{tag}}(m)$	$\mathcal{O}_{\text{vfy}}(m,\tau)$
$K \xleftarrow{\mathcal{U}} \{0,1\}^{klen}$	$sent \leftarrow sent \cup \{m\}$	**if** $(m \notin sent)$ & $(\tau = \mathsf{MAC}_K(m))$
$sent \leftarrow \varnothing$	**return** $\mathsf{MAC}_K(m)$	$win \leftarrow 1$
$win \leftarrow 0$		**fi**
$\mathcal{A}^{\mathcal{O}_{\text{tag}},\mathcal{O}_{\text{vfy}}}$		**return** res
return win		

Рис. 15. Псевдокод эксперимента $\mathbf{Exp}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{MAC}}$

Определение 18. Обозначим через $\mathbf{InSec}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{MAC}}(t, q_t, \ell_t, \mu_t, q_v, \ell_v, \mu_v)$ максимум среди преимуществ противников $\mathcal{A}$ в эксперименте $\mathbf{Exp}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{MAC}}$, где противник $\mathcal{A}$ имеет ограничение t на вычислительные ресурсы и делает не более q_t запросов к оракулу $\mathcal{O}_{\text{tag}}$ (q_v запросов к $\mathcal{O}_{\text{vfy}}$), суммарная длина запросов не превосходит ℓ_t (ℓ_v для $\mathcal{O}_{\text{vfy}}$), максимальная длина запроса не превосходит μ_t (μ_v для $\mathcal{O}_{\text{vfy}}$).

D.3. Конкретные оценки

Для композиции вида **“Encrypt-then-MAC”** верны следующие оценки [6]:

$$\mathbf{InSec}^{\mathsf{INT\text{-}CTXT}}_{\mathsf{AE}}(t, q_e, \ell_e, \mu_e, q_v, \ell_v, \mu_v) \leqslant \mathbf{InSec}^{\mathsf{EUF\text{-}CMA}}_{\mathbf{CMAC}}(t', q_e, \ell_e, \mu_e, q_v, \ell_v, \mu_v),$$

$$\mathbf{InSec}^{\mathsf{LOR\text{-}CCA}}_{\mathsf{AE}}(t, q_e, \ell_e, \mu_e, q_d, \ell_d, \mu_d) \leqslant \mathbf{InSec}^{\mathsf{LOR\text{-}CPA}}_{\mathsf{AE}}(t', q_e, \ell_e, \mu_e) + 2 \cdot \mathbf{InSec}^{\mathsf{EUF\text{-}CMA}}_{\mathbf{CMAC}}(t', q_e, \ell_e, \mu_e, q_d, \ell_d, \mu_d).$$

Для режима **CTR** в работе [26] приводится оценка

$$\mathbf{InSec}^{\mathsf{LOR\text{-}CPA}}_{\mathsf{AE}}(t, q_e, \ell_e, \mu_e) \leqslant 2 \cdot \mathbf{InSec}^{\mathsf{PRF}}_{E}(t', \ell_e). \tag{4}$$

Для режима **CMAC** в ряде статей [21–25] были получены следующие оценки. В работе [21] получено сведение случая нескольких запросов q_v к оракулу $\mathcal{O}_{\text{vfy}}$ к случаю одного запроса, что совместно с результатами из работы [22] дает оценку:

$$\mathbf{InSec}^{\mathsf{EUF\text{-}CMA}}_{\mathbf{CMAC}}(t, q_e, \ell_e, \mu_e, q_v, \ell_v, \mu_v) \leqslant q_v \cdot \left(\mathbf{InSec}^{\mathsf{PRF}}_{\mathbf{CMAC}}(t', q_e + 1, \ell_e + \ell_v, \max(\mu_e, \mu_v)) + \frac{1}{2^{tlen}}\right),$$

где $tlen$ — длина имитовставки (в битах).

В работах [23–25] приводятся три попарно несравнимые оценки:

$$\mathbf{InSec}^{\mathsf{PRF}}_{\mathbf{CMAC}}(t, q, \ell, \mu) \leqslant \min\left(\frac{4\ell^2}{2^n}, \quad \frac{4q\ell}{2^n} + \frac{8q(q-1)\mu^4}{2^{2n}}, \right.$$
$$\frac{4\ell + 16q^2 + q\mu^2}{2^n} + \frac{8q^2\mu^4 + 32q^3\mu^2 + 2q^2\mu^3}{2^{2n}}$$
$$\left. + \frac{3q^3\mu^5 + 143q^3\mu^6 + 11q^4\mu^3}{2^{3n}} + \frac{17q^4\mu^6 + 5462q^4\mu^8}{2^{4n}}\right),$$

где n — длина блока используемого в режиме **CMAC** блочного шифра E. Для конкретных параметров q, ℓ и μ может быть использована минимальная из указанных оценок.

Для рассматриваемой схемы KE для величины $\mathbf{InSec}^{\mathsf{ODH}}_{\mathsf{KE}}(t, q)$ при **дополнительных предположениях:**

– хеш-функция в алгоритме $\mathsf{KE.Comb}$ моделируется как случайный оракул [27, 28],

– рассматриваются только обобщенные алгоритмы дискретного логарифмирования (так называемая generic group model [18, 19]),

можно получить оценку вида $\mathcal{O}\left(\frac{q^4}{h}\right)$. Более подробный анализ модели ODH требует отдельного рассмотрения и выходит за рамки настоящей работы.