

Совместная стойкость схемы выработки общего ключа VKO и подписи GOST в эвристике обобщённой группы для эллиптических кривых

2 июня 2026 г.

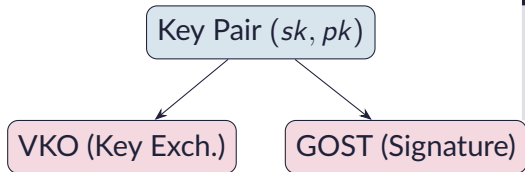
А. О. Бахарев, А. А. Дрынкин,
К. Д. Царегородцев

1. Постановка задачи
2. Известные результаты
3. Эвристика обобщённой группы
4. Модели безопасности
5. Основные результаты
6. Техники доказательства
7. Заключение

[1/7] Постановка задачи

Во многих реальных системах (TLS 1.2, S/MIME) используется **одна** ключевая пара для разных целей:

- ▶ **выработка общего секрета;**
- ▶ **цифровая подпись**
(аутентификация сторон).



Вопрос: приводит ли использование одной статической ключевой пары для двух разных примитивов к ослаблению какого-либо из них?

Задача: показать (в некоторых эвристических предположениях), что использование **одной статической ключевой пары** в российской схеме подписи совместно с алгоритмом выработки ключа VKO безопасно.

Комбинированная схема выработки общего ключа и подписи

Четверка (вероятностных) алгоритмов $CS = (\text{PairGen}, \text{Comb}, \text{Sign}, \text{Verify})$:

- ▶ $(sk, pk) \xleftarrow{\$} CS.\text{PairGen}()$: алгоритм генерации ключевой пары.
- ▶ $K \leftarrow CS.\text{Comb}(sk, epk)$: алгоритм выработки ключа, вырабатывает K на основе двух ключей (статического sk и эфемерного epk).
- ▶ $\sigma \xleftarrow{\$} CS.\text{Sign}(sk, m)$: алгоритм формирования подписи, возвращает подпись σ для сообщения m на ключе sk или ошибку $\perp$.
- ▶ $b \leftarrow CS.\text{Verify}(pk, m, \sigma)$: алгоритм проверки подписи: проверяет корректность подписи σ для сообщения m на открытом ключе pk , возвращает 1, если подпись верна, 0 иначе.

Корректность: для всех m , $(sk, pk) \xleftarrow{\$} CS.\text{PairGen}$, $(esk, epk) \xleftarrow{\$} CS.\text{PairGen}$

$$CS.\text{Comb}(sk, epk) = CS.\text{Comb}(esk, pk), \quad CS.\text{Verify}(pk, m, CS.\text{Sign}(sk, m)) = 1.$$

CS — комбинированная схема выработки общего ключа и подписи.

- ▶ Пару алгоритмов $KE = (CS.PairGen, CS.Comb)$ будем называть **схемой выработки ключей**.
- ▶ Тройку алгоритмов $SS = (CS.PairGen, CS.Sign, CS.Verify)$ будем называть **схемой подписи**.

ГОСТ Р 34.10-2018

- ▶ Схема подписи на эллиптической кривой.
- ▶ Параметры: циклическая подгруппа $G = \langle P \rangle$ простого порядка q .
- ▶ Использует статическую ключевую пару (sk, pk) , где $sk \in \mathbb{Z}_q^*$, $pk = sk \cdot P$.

ВКО (Р 50.1.113-2016)

- ▶ Схема выработки ключей, полустатический неинтерактивный протокол Диффи-Хеллмана.
- ▶
Общий ключ $K = \text{Hash}(\alpha \cdot sk \cdot epk)$,
 sk — статический ключ,
 epk — эфемерный (сеансовый).
- ▶ $\alpha \in \mathbb{Z}_q^*$: кофактор, зависящий от подгруппы.

Комбинированный механизм: **VKOST = VKO + GOST.**

Пример: схема VKOST

VKOST = (PairGen, Comb, Sign, Verify)

VKOST.PairGen

$sk \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$

$pk \leftarrow sk \cdot P$

return (sk, pk)

VKOST.Comb(sk, pk)

return $\text{Hash}_1(\alpha \cdot sk \cdot pk)$

VKOST.Sign(sk, m)

$h \leftarrow \text{Hash}_2(m)$

$r \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$

$R \leftarrow r \cdot P$

$t \leftarrow f(R)$

if $(t = 0)$: return $\perp$

$s \leftarrow (h \cdot r + t \cdot sk)$

if $(s = 0)$: return $\perp$

return (s, t)

VKOST.Verify($pk, m, (s, t)$)

if $(s = 0) \vee (t = 0)$: return 0

$h \leftarrow \text{Hash}_2(m)$

$R \leftarrow (s \cdot h^{-1})P - (t \cdot h^{-1})pk$

if $(R = \mathcal{O})$: return 0

if $(f(R) \neq t)$: return 0

return 1

[2/7] Известные результаты

- ▶ Работа¹: показано, что по xP , yP трудно найти значение $\text{Hash}(xyP)$ в предположении о сложности распознавательной задачи Диффи-Хеллмана в группе точек Э.К.
- ▶ Работа²: введена модель mODH (переформулировка в терминах задачи различения, допускается множество запросов); показано, что она сводится к уже известной³ модели ODH.

¹Е. Алексеев и др. О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012. МВК, 2016.

²К. Царегородцев. Свойства конфиденциальности и целостности схемы ECIES // МВК, 2024.

³М. Abdalla et. al. The oracle Diffie-Hellman assumptions and an analysis of DHIES // LNCS, vol.2020, 2001.

- ▶ ECDSA: показана⁴ стойкость в эвристике EC – GGM.
- ▶ GOST: известны⁵ результаты в эвристике биективного случайного оракула BRO.
- ▶ Модифицированная схема GOST: показана⁶ стойкость в эвристике случайного оракула RO.
- ▶ GOST со связанными ключами: исследована стойкость в различных предположениях⁷.

⁴Groth J., Shoup V. On the Security of ECDSA with Additive Key Derivation and Presignatures // EUROCRYPT 2022.

⁵Fersch M. The provable security of ElGamal-type signature schemes // Doctoral thesis, 2018.

⁶L. Akhmetzyanova et.al. On methods of shortening ElGamal-type signatures //MBK, 2021.

⁷A. Babueva, S. Kyazhin. Additively related keys for signature: security models and results for Schnorr, GOST, ECDSA, and SM2 //MBK, 2025.

- ▶ Инкапсуляция ключа + схема подписи; показано⁸, что схема подписи является стойкой относительно противника с дополнительным доступом к оракулу декапсуляции в эвристике BRO; для схемы инкапсуляции с дополнительными подписями показана сводимость к ODH.
- ▶ VKO + схема подписи — аналогичный результат для схемы подписи⁹.
- ▶ Смежная тематика: signcryption¹⁰.

⁸A. Babueva et.al. Joint security of encryption and signature in RuCMS: two keys are better, but one is also fine //MBK, 2025.

⁹А. Бахарев, К. Царегородцев. О стойкости некоторых алгоритмов над группой точек эллиптических кривых //ПДМ. Приложение, 2025.

¹⁰А. Гуселев. О безопасности одного класса механизмов одновременного шифрования и формирования подписи //MBK, 2025.

[3/7] Эвристика обобщённой группы

- ▶ **Основная идея:** спрятать алгебраическую структуру группы G с помощью **биективного кодирования** элементов групп $\tau: G \rightarrow S_q \subseteq \{0, 1\}^{\lceil \log_2(G) \rceil}$.
- ▶ Противник видит только *метки* групповых элементов $\tau(xP)$.
- ▶ Групповые операции возможны только с помощью обращения к оракулу $\mathcal{O}_{\text{group}}$.
- ▶ Никакие структурные особенности группы не могут быть использованы.

EC-GGM (Groth & Shoup, EUROCRYPT 2022) частный случай GGM, где $S_q = E$ — группа точек эллиптической кривой.

Пример: задача DDH в EC-GGM

$$\text{Exp}_G^{\text{gen-DDH}-b}(\mathcal{A})$$
$$\tau \xleftarrow{\$} \{G \rightarrow E\}$$
$$P \leftarrow \tau(1)$$
$$x \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*, y \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$$
$$X \leftarrow \tau(x), Y \leftarrow \tau(y)$$
$$Z \leftarrow \tau(x \cdot y)$$
$$\text{if } (b = 0) : Z \xleftarrow{\mathcal{U}} E$$
$$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\text{group}}}(P, X, Y, Z)$$
$$\text{return } b'$$
$$\mathcal{O}_{\text{group}}(\mathcal{P}_1, \mathcal{P}_2)$$
$$\text{return } \tau(\tau^{-1}(\mathcal{P}_1) + \tau^{-1}(\mathcal{P}_2))$$

В работе^a показано, что для стандартизированных российских кривых нет лучше методов для решения DDH, CDH, DSLP, чем общие.

^aAlekseev E. K., Nikolaev V. D., Smyshlyaev S. V. On the security properties of Russian standardized elliptic curves //Математические вопросы криптографии. – 2018. – Т. 9. – №. 3. – С. 5-32.

EC-GGM vs. произвольной GGM

M — модель, в которой противник имеет доступ только к оракулу O_{group} в эвристике EC-GGM. M' — аналогичная модель, но в эвристике GGM.

$$\text{InSec}_M^{\mathcal{K}}(t, q_{group}) \leq \text{InSec}_{M'}^{\mathcal{K}'}(t, 4q_{group} + k + 2)$$

DDH в EC-GGM

Адаптированный результат для EC-GGM, утверждение 1:

$$\text{InSec}^{\text{gen-DDH}}(t, q_{grp}) \leq \frac{(4q_{grp} + 5)^2}{q}$$

Любой противник, делающий не более q_{grp} запросов, не может решить DDH с вероятностью больше, чем указанная граница.

[4/7] Модели безопасности

Модели безопасности

Для выработки ключа (VKO)

- ▶ **ODH**: Неотличимость одного выработанного ключа от случайного
- ▶ **mODH**: Неотличимость нескольких ключей
- ▶ **mODH-sig**: mODH *плюс* противник получает доступ к подписывающему оракулу

Для подписи (GOST)

- ▶ **SUF-CMA**: Неподделываемость подписи
- ▶ **SUF-CMA-comb**: SUF-CMA *плюс* противник получает доступ к комбинирующему оракулу

Неформальная задача

Показать, что для VKOST:

$$\text{InSec}_{\text{VKOST}}^{\text{mODH-sig}} \approx \text{InSec}_{\text{VKO}}^{\text{mODH}} \quad \text{и}$$

$$\text{InSec}_{\text{VKOST}}^{\text{SUF-CMA-comb}} \approx \text{InSec}_{\text{GOST}}^{\text{SUF-CMA}}$$

$\text{Exp}_{\text{VKOST}}^{\text{mODH-sig-b}}(\mathcal{A})$

1. Сгенерировать $(sk, pk) \leftarrow \text{PairGen}$
2. Противник $\mathcal{A}$ получает pk и доступ к:
 - ▶ $\mathcal{O}_{\text{kgen}}^b$ — возвращает пару $pk + \text{key}$ (настоящие, если $b = 1$, случайные если $b = 0$)
 - ▶ $\mathcal{O}_{\text{comb}}(\text{epk})$ — возвращает $\text{Comb}(sk, \text{epk})$
 - ▶ $\mathcal{O}_{\text{sig}}(m)$ — возвращает $\text{Sign}(sk, m)$
3. $\mathcal{A}$ пытается угадать b' ; успех, если $b' = b$

Требования стойкости

$\mathcal{A}$ не может отличить настоящие VKO ключи от случайных даже имея доступ к:

- ▶ Множеству генераций ключей
- ▶ Подписи произвольных сообщений

Эксперимент mODH-sig

$\text{Exp}_{\text{CS}}^{\text{mODH-sig-b}}(\mathcal{A})$

$(sk, pk) \xleftarrow{\$} \text{CS.PairGen}$

$\text{Keys} \leftarrow []$

$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\text{kgen}}^b, \mathcal{O}_{\text{comb}}, \mathcal{O}_{\text{sig}}}(pk)$

return b'

$\mathcal{O}_{\text{comb}}(\text{epk})$

if $\text{Keys}[\text{epk}] = \perp$

 return $\text{CS.Comb}(sk, \text{epk})$

fi

return $\text{Keys}[\text{epk}]$

$\mathcal{O}_{\text{kgen}}^b$

$(\text{esk}, \text{epk}) \xleftarrow{\$} \text{CS.PairGen}$

if $\text{Keys}[\text{epk}] = \perp$

$K \leftarrow \text{CS.Comb}(sk, \text{epk})$

 if $(b = 0) : K \xleftarrow{\mathcal{U}} \{0, 1\}^{|K|}$

$\text{Keys}[\text{epk}] \leftarrow K$

fi

return $(\text{epk}, \text{Keys}[\text{epk}])$

$\mathcal{O}_{\text{sig}}(m)$

$\sigma \xleftarrow{\$} \text{CS.Sign}(sk, m)$

return σ

$\text{Exp}_{\text{VKOST}}^{\text{SUF-CMA-comb}}(\mathcal{A})$

1. Сгенерировать $(sk, pk) \leftarrow \text{PairGen}$
2. Противник $\mathcal{A}$ получает pk и доступ к:
 - ▶ $\mathcal{O}_{\text{comb}}(epk)$ — возвращает $\text{Comb}(sk, epk)$
 - ▶ $\mathcal{O}_{\text{sig}}(m)$ — возвращает $\text{Sign}(sk, m)$
3. $\mathcal{A}$ возвращает (m^*, σ^*)
4. **Успех** если $\text{Verify}(pk, m^*, \sigma^*) = 1$ и σ^* не возвращался оракулом $\mathcal{O}_{\text{sig}}$

Требования стойкости

Даже имея доступ к двум оракулам подписи и выработки ключа, $\mathcal{A}$ не может создать **свежую подделку подписи**.

Замечание: Strong Unforgeability

SUF требует, чтобы пара (m^*, σ^*) была полностью новая — не только сообщение. Строже, чем просто UF-CMA.

Эксперимент SUF-CMA-comb

$$\text{Exp}_{\text{CS}}^{\text{SUF-CMA-comb}}(\mathcal{A})$$
$$(sk, pk) \xleftarrow{\$} \text{CS.PairGen}$$
$$L \leftarrow []$$
$$(m, \sigma) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\text{comb}}, \mathcal{O}_{\text{sig}}}(pk)$$
$$\text{if } ((m, \sigma) \notin L) \wedge (\text{CS.Verify}(pk, m, \sigma) = 1)$$
$$\quad \text{return } 1$$
$$\text{else}$$
$$\quad \text{return } 0$$
$$\mathcal{O}_{\text{comb}}(\text{epk})$$
$$K \leftarrow \text{CS.Comb}(sk, \text{epk})$$
$$\text{return } K$$
$$\mathcal{O}_{\text{sig}}(m)$$
$$\sigma \xleftarrow{\$} \text{CS.Sign}(sk, m)$$
$$L \leftarrow L \cup (m, \sigma)$$
$$\text{return } \sigma$$

[5/7] Основные результаты

Теорема

В модели EC – GGM выполнено неравенство:

$$\text{InSec}_{\text{VKO}}^{\text{gen-ODH}}(t, q_{\text{com}}, q_{\text{group}}) \leq 2 \cdot \text{InSec}^{\text{gen-DDH}}(t, q_{\text{group}}) + \text{InSec}_{\text{Hash}_1}^{\text{PRH}}(t) + \\ + \frac{3 \cdot q_{\text{group}} \cdot q_{\text{com}}}{(q - q_{\text{com}})} + \text{InSec}_{\text{Hash}_1}^{\text{FRP}}(t, q_{\text{com}}),$$

- модель PRH – различение значений функции на случайно выбранном входе от случайной строки:

$$\text{Adv}_{\text{F}}^{\text{PRH}}(\mathcal{A}) = \mathbb{P}\left[\mathcal{A}^{\text{O}_F}(F(x)) \rightarrow 1 \mid x \xleftarrow{\mathcal{U}} X, F \xleftarrow{\mathcal{U}} \mathcal{F}\right] - \mathbb{P}\left[\mathcal{A}^{\text{O}_F}(\text{res}) \rightarrow 1 \mid \text{res} \xleftarrow{\mathcal{U}} Y, F \xleftarrow{\mathcal{U}} \mathcal{F}\right];$$

- модель FRP – поиск прообраза хотя бы одной из множества точек:

$$\text{Adv}_{\text{F}}^{\text{FRP}}(\mathcal{A}) = \mathbb{P}\left[\mathcal{A}^{\text{O}_F}(F(x_1), \dots, F(x_k)) \rightarrow m, \exists i \ m = x_i \mid F \xleftarrow{\mathcal{U}} \mathcal{F}, x_i \xleftarrow{\mathcal{U}} Y, x_i \neq x_j, i \neq j\right].$$

Теорема

В эвристике EC-GGM верно неравенство

$$\begin{aligned} \text{InSec}_{\text{GOST}}^{\text{gen-SUF-CMA}}(t, q_{\text{sign}}, q_{\text{group}}) \leq & \text{InSec}_{\text{Hash}_2}^{\pm\text{Coll}}(t) + \\ & + (4 + o(1)) \cdot (q_{\text{sign}} + q_{\text{group}}) \cdot \text{InSec}_{\text{Hash}_2}^{\text{RP}}(t) + \frac{(q_{\text{sign}} + q_{\text{group}})^2}{q}. \end{aligned}$$

- ▶ модель $\pm\text{Coll}$ — поиск коллизии с точностью до знака:

$$\text{Adv}_{\text{F}}^{\pm\text{Coll}}(\mathcal{A}) = \mathbb{P}\left[\mathcal{A}^{\text{O}_F} \rightarrow (x, y), (x \neq y) \wedge (F(x) = \pm F(y)) \mid F \xleftarrow{\mathcal{U}} \text{F}\right];$$

- ▶ модель RP — поиск прообраза случайной точки:

$$\text{Adv}_{\text{F}}^{\text{RP}}(\mathcal{A}) = \mathbb{P}\left[\mathcal{A}^{\text{O}_F}(h) \rightarrow m, F(m) = h \mid h \xleftarrow{\mathcal{U}} Y, F \xleftarrow{\mathcal{U}} \text{F}\right].$$

Теорема (Теорема 3 работы)

В эвристике EC-GGM выполнено неравенство:

$$\begin{aligned} \text{InSec}_{\text{VKOST}}^{\text{gen-mODH-sig}}(t, q_{\text{gen}}, q_{\text{com}}, q_{\text{sign}}, q_{\text{grp}}) \\ \leq \text{InSec}_{\text{VKO}}^{\text{gen-mODH}}(q_{\text{gen}}, q_{\text{com}}, q_{\text{sign}} \cdot (2 \log_2 q + 2) + q_{\text{grp}}) \\ + \frac{q_{\text{sign}}(2q_{\text{com}} + 2q_{\text{gen}} + 6q_{\text{grp}} + 2q_{\text{sign}})}{q - 1} \end{aligned}$$

Теорема (Теорема 5 работы)

В эвристике EC-GGM выполнено неравенство:

$$\begin{aligned} \text{InSec}_{\text{VKOST}}^{\text{gen-SUF-CMA-comb}} \leq & \text{InSec}_{\text{GOST}}^{\text{gen-SUF-CMA}}(t, q_{\text{sign}}, q_{\text{grp}} + q_{\text{com}} + q_{\text{sign}}(2 \log q + 1)) \\ & + \frac{q_{\text{com}}(3q_{\text{grp}} + q_{\text{sign}})}{q - q_{\text{com}}} + \text{InSec}_{\text{Hash}_1}^{\text{FRP}}(t, q_{\text{com}}). \end{aligned}$$

[6/7] Техники доказательств

Стратегия сведения

1. Пусть $\mathcal{A}$ — противник в модели mODH — sig, построим противника $\mathcal{B}$ в модели mODH (без подписывающего оракула)
2. $\mathcal{B}$ **симулирует** оракул подписи с помощью *подмены меток*:
 - ▶ Выбрать $R \xleftarrow{U} E, s \xleftarrow{U} \mathbb{Z}_q^*$ равномерно
 - ▶ Подменить метки $(sh^{-1})P$ и $R + (th^{-1})pk$ в массиве Rep1
 - ▶ Подпись (s, t) корректна по построению
3. Симуляция прерывается, если $\mathcal{A}$ пытается получить информацию о подменниных точках; вероятность $\leq \frac{q_{\text{sign}}(\dots)}{q-1}$

- ▶ **Ключевой аспект:** распределение троек (R, s, t) , полученное при симуляции, **идентично** настоящему — $\mathcal{A}$ не заметит подмену.
- ▶ **Быстрое возведение в степень:** умножение в EC-GGM требует $\log_2 q$ запросов к групповому оракулу, что объясняет значение $q_{\text{sign}} \cdot 2 \log_2 q$ в оценке.

Символическая симуляция

Расширим кодирование до
полиномов $a + b \cdot D$ над $\mathbb{Z}_q$, где D
формальная переменная,
представляющая sk .

Два случая подделки (m^*, s^*, t^*) :

Случай 1: $R^* = \pm R_i$ для некоторого запроса

Пусть $h^* = \pm h_i$ и $s^* = s_i$

$\Rightarrow$ **sign-collision** в Hash_2

Сводится к $\text{InSec}_{\text{Hash}_2}^{\pm \text{Coll}}$

Случай 2: R^* свежая

R^* должна была появиться из
запроса к оракулу; противник
должен “узнать” конкретный
 $t^* = f(R^*) \Rightarrow$ сводится к задаче
по поиску **прообраза** $\text{InSec}_{\text{Hash}_2}^{\text{RP}}$

Это повторяет анализ ECDSA
Groth & Shoup (EUROCRYPT 2022),
адаптированный для уравнения в
GOST $s = h \cdot r + t \cdot sk$.

[7/7] Заключение

0100000

01 0100000
0100000

11 1 0 1 0 0 11 0
0100000
11 1 0 1 0 0 11 0
01
0100000 0100000

0100000 0100000 0100000 0100000



Оценки

VKO с подписывающим оракулом:

$$\text{InSec}_{\text{VKOST}}^{\text{mODH-sig}} \leq \text{InSec}_{\text{VKO}}^{\text{mODH}} + \varepsilon_1$$

GOST с комбинирующим оракулом:

$$\text{InSec}_{\text{VKOST}}^{\text{SUF-CMA-comb}} \leq \text{InSec}_{\text{GOST}}^{\text{SUF-CMA}} + \varepsilon_2$$

где $\varepsilon_1, \varepsilon_2 = O\left(\frac{\text{poly}(q_{\text{queries}})}{q}\right)$
являются незначительными для $q \approx 2^{256}$.

Конкретные параметры

Для стандартной кривой
(например id-tc26-gost-3410-
2012-512-paramSetA) с $q \approx 2^{512}$,
перевешивает для миллиона
запросов:

$$\frac{10^6 \cdot 10^6}{2^{512}} \approx 2^{-490}$$

Основной вывод

Использование VKO и GOST с
одной **ключевой парой**
безопасно в модели EC-GGM.

Было показано

1. **VKO ключ** неотличим от случайного даже имея доступ к подписывающему оракулу
2. **GOST подпись** неподделываема даже с доступом к выработке общего ключа VKO

Практический смысл

VKO + GOST могут быть использованы вместе на одной общей ключевой паре.

Готов ответить на вопросы

Дрынкин Алексей Антонович

Математик лаборатории криптографии



al.drynkin@kryptonite.ru