Мультипликативно и линейно связанные ключи подписи

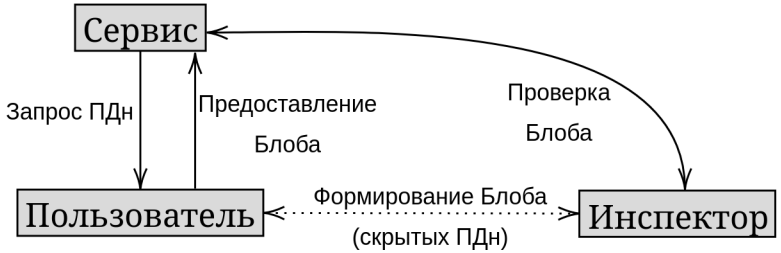
А. О. Бахарев[1], К. Д. Царегородцев[2]

1. АО «НПК«Криптонит»
2. МГУ им. М. В. Ломоносова

20 марта 2025

Мотивация: Протокол ИКС[1]

- Протокол передачи персональных данных (ПДн) без их раскрытия.
- Три роли: **Сервис** (хочет получить ПДн), **Пользователь** (хочет предоставить ПДн, не раскрывая их Сервису), **Инспектор** (некоторая доверенная третья сторона, проводящая верификацию ПДн).



[1]Бельский В. С., Герасимов И. Ю., Царегородцев К. Д., Чижов И. В. (2020). Протокол обмена персональными данными: ИКС. INJOIT, 8 (6), 1-23.

Мотивация: ИКС 2.0

- Протокол не скрывает личность Пользователя.
- Способ формирования Блоба:

$$K = \mathsf{VKO}(esk,\ pk_U)$$

$$BLOB = \Big(\underbrace{epk,\ UID, \mathsf{Enc}_K(Request \parallel SecData)}, \sigma\Big)$$

$Sign + Certificate$

- Нужен альтернативный механизм: «анонимизированная подпись» — трудно подделать за Пользователя, трудно по подписи определить, кто её сформировал, Инспектор должен иметь возможность проверить, кто именно сформировал подпись.
- В работе изучается один из возможных подходов: подпись ГОСТ на связанных ключах.

Модели безопасности: в предыдущих сериях[2]

Возможности нарушителя CMA:

Получать значения подписи для произвольных сообщений m, вычисленные с использованием ключа sk и $sk + x_i$, где сдвиги x_i:

- (sRKA) выбираются нарушителем (из допустимых)
- (sKRKA) генерируются «честным образом»

*-sRKA ⇒ *-sKRKA

Угроза (подделка подписи для хотя бы одного ключа):

Найти такую тройку $(m, \sigma, pk + xP)$, что:

- $Verify(pk + xP, m, \sigma) = 1$
- нарушитель не запрашивал подпись
  - (wUF) для сообщения m
  - (UF) для сообщения m на ключе $sk + x$

UF-* ⇒ wUF-*

[2] Бабуева А. А., Кяжин С. Н. Аддитивно связанные ключи подписи: взломать нельзя использовать // РусКрипто'2024

В предыдущих сериях: что знаем про ГОСТ со связанными ключами?[3]

		Подделка для мастер-ключа				Подделка хотя бы для одного ключа			
		Любой сдвиг		Заданный сдвиг		Любой сдвиг		Заданный сдвиг	
		сбщ	пара (сбщ, м-к)	сбщ	пара (сбщ, м-к)	сбщ	пара (сбщ, ключ)	сбщ	пара (сбщ, ключ)
		1	2	3	4	5	6	7	8
	UF-CMA	wUF-CM-RKA	UF-CM-RKA	wUF-CM-KRKA	UF-CM-KRKA	wUF-CM-sRKA	UF-CM-sRKA	wUF-CM-sKRKA	UF-CM-sKRKA
Шнорр						[new]		[⇒]	
ГОСТ		[⇒]		[⇒]		[new]		[⇒]	
ECDSA		BRO [new]				[new]	[⇒]		
SM2		BRO [new]		[⇒]		[new]	[⇒]		

[3] Бабуева А. А., Кяжин С. Н. Аддитивно связанные ключи подписи: взломать нельзя использовать // РусКрипто'2024

Модель с мультипликативно связанными ключами

$$sk \to sk_e = e \cdot sk, \quad pk \to pk_e = e \cdot pk$$

Возможности нарушителя: получать значения подписей для произвольных сообщений на мастер-ключе sk и ключах sk_{e_i}, вычисленных с использованием множителей e_i, где нарушитель:

- либо выбирает непосредственно e_i (модель без хэширования)

Угроза:

- Найти тройку (m, σ, e), что
  1. $\text{Verify}(pk_e, m, \sigma) = 1$, где pk_e вычислен с использованием множителя e
  2. нарушитель не получал подпись σ на запрос (m, e)

Модель с мультипликативно связанными ключами

$$sk \to sk_e = e \cdot sk, \quad pk \to pk_e = e \cdot pk$$

Возможности нарушителя: получать значения подписей для произвольных сообщений на мастер-ключе sk и ключах sk_{e_i}, вычисленных с использованием множителей e_i, где нарушитель:

- либо выбирает непосредственно e_i (модель без хэширования)
- либо выбирает R_i, которые хэшируются, т.е. $e_i = H'(R_i)$ (модель с хэшированием)

Угроза:

- Найти тройку (m, σ, e), что
  1. $\text{Verify}(pk_e, m, \sigma) = 1$, где pk_e вычислен с использованием множителя e
  2. нарушитель не получал подпись σ на запрос (m, e)
- Найти тройку (m, σ, R), что
  1. $\text{Verify}(pk_e, m, \sigma) = 1$, где $pk_e = pk$ при $R = \perp$, иначе pk_e вычислен с использованием множителя $e = H'(R)$
  2. нарушитель не получал подпись σ на запрос (m, R)

Модель обобщенной группы для эллиптических кривых[4]

Для группы точек ЭК E размера q определяется **функция кодирования** $\pi : \mathbb{Z}_q \to E$:

- функция π инъективна,
- $\pi(0) = \mathcal{O}$,
- $\forall\ i \in \mathbb{Z}_q,\ \pi(-i) = -\pi(i)$.

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

Модель обобщенной группы для эллиптических кривых[4]

Для группы точек ЭК E размера q определяется **функция кодирования** $\pi : \mathbb{Z}_q \to E$:

- функция π инъективна,
- $\pi(0) = \mathcal{O}$,
- $\forall\ i \in \mathbb{Z}_q,\ \pi(-i) = -\pi(i)$.

В рамках модели обобщенной группы для Э.К. противник не имеет прямого доступа к элементам группы, но проводит вычисления с точками только **путем запросов** к групповому оракулу $\mathcal{O}_{\mathrm{grp}}$:

- запрос вида $\mathcal{O}_{\mathrm{grp}}(\mathit{map}, i)$, $i \in \mathbb{Z}_q$: вернуть $\pi(i) \in E$,
- запрос вида $\mathcal{O}_{\mathrm{grp}}(\mathit{add}, \mathcal{P}_1, \mathcal{P}_2)$, где $\mathcal{P}_1, \mathcal{P}_2 \in E$: вернуть $\pi(\pi^{-1}(\mathcal{P}_1) + \pi^{-1}(\mathcal{P}_2))$.

Основная идея: скрыть групповую связь с помощью случайного выбора π.

Модель обобщенной группы используется при изучении сложности задач, связанных с дискретным логарифмированием.

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

Мультипликативно связанные ключи с хэшированием множителя

$$esk \leftarrow e \cdot sk, \quad epk \leftarrow e \cdot pk, \quad e \leftarrow H'(R).$$

Задачи, связанные с поиском коллизий

Задачи, связанные с поиском прообразов

Задачи, связанные с поиском алгебраических соотношений на H, H'

Стандартная оценка сложности в обобщенной группе

$$\mathbf{InSec}^{\mathsf{mult-Hash}}_{GOST}(t, N_{sign}, N_{group}) \leq$$

$$\leq \mathbf{InSec}^{\mathsf{Coll}}_{H}(t) + \mathbf{InSec}^{\mathsf{Coll}}_{H'}(t) + \mathbf{InSec}^{\mathsf{NC}}_{H}(t) +$$

$$+\mathbf{InSec}^{\mathsf{ZP}}_{H}(t) \; + \; (4 + o(1)) \cdot (N_{sign} + N_{group}) \cdot \mathbf{InSec}^{\mathsf{RP}}_{H}(t) +$$

$$+\mathbf{InSec}^{\mathsf{4PMColl}}_{H,H'}(t) + \mathbf{InSec}^{\mathsf{4NMColl}}_{H,H'}(t) + \mathbf{InSec}^{\mathsf{3PMColl}}_{\mathbf{H,H'}}(\mathbf{t}) + \mathbf{InSec}^{\mathsf{3NMColl}}_{H,H'}(t) +$$

$$+(4 + o(1)) \cdot (N_{sign} + N_{group}) \cdot \mathbf{InSec}^{\mathsf{2mult}}_{H,H'}(t) +$$

$$+\mathrm{O}\left(\frac{(N_{sign} + N_{group})^2}{q}\right).$$

Мультипликативно связанные ключи без хэширования множителя

Атака на ГОСТ

Нарушитель:

1. Получает подпись (t, s) для сообщения m с хэшем h и множителя e (вообще говоря произвольного).
2. Выдаёт в качестве подделки подпись $(t^* = t, s^* = e^{-1}(s \cdot e^*))$ для сообщения m^* с хэшем h^* и множителя e^*, для которых выполнено равенство $h^* \cdot e = h \cdot e^*$.

Тогда выполнено равенство:

$$(h^*)^{-1}(s^* - t \cdot e^* \cdot sk) = (h^{-1}(e^*)^{-1}e) \cdot (e^{-1}(s \cdot e^*) - t \cdot e^* \cdot sk) = h^{-1}(s - t \cdot e \cdot sk).$$

Иначе говоря, выполняется проверка корректности t.

Линейно связанные ключи без хэширования множителя

У Пользователя есть две пары секретных и открытых ключей:

$$(sk_1, pk_1), \quad (sk_2, pk_2), \quad sk_1 \neq sk_2.$$

Сформируем из них пару (sk, pk) и будем формировать эфемерные пары следующим образом:

$$sk \leftarrow sk_1 + sk_2, \quad pk \leftarrow pk_1 + pk_2$$
$$esk \leftarrow sk_1 + e \cdot sk_2, \quad epk \leftarrow pk_1 + e \cdot pk_2.$$

Линейно связанные ключи без хэширования множителя

У Пользователя есть две пары секретных и открытых ключей:

$$(sk_1, pk_1), \quad (sk_2, pk_2), \quad sk_1 \neq sk_2.$$

Сформируем из них пару (sk, pk) и будем формировать эфемерные пары следующим образом:

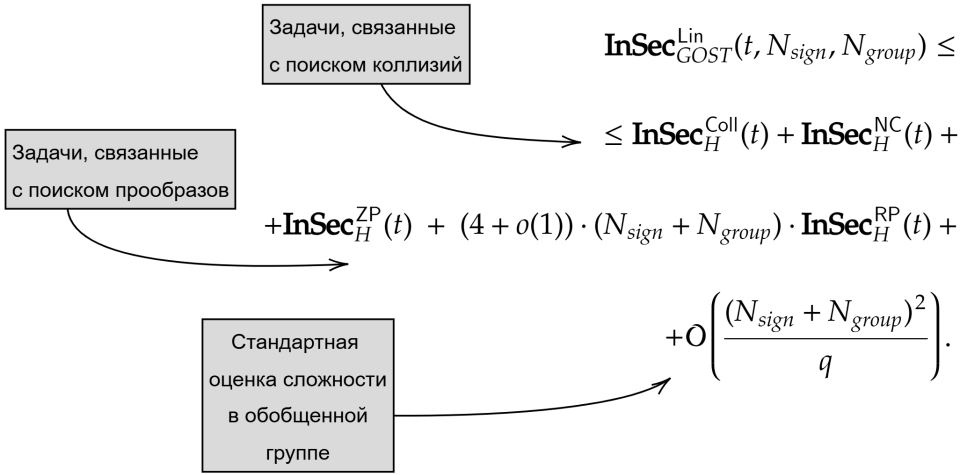
$$sk \leftarrow sk_1 + sk_2, \quad pk \leftarrow pk_1 + pk_2$$
$$esk \leftarrow sk_1 + e \cdot sk_2, \quad epk \leftarrow pk_1 + e \cdot pk_2.$$

Возможности нарушителя: получать значения подписей для произвольных сообщений на мастер-ключе sk и ключах sk_{e_i}, вычисленных с использованием множителей e_i, где нарушитель выбирает непосредственно e_i (модель без хэширования).

Угроза: Найти тройку (m, σ, e), что

1. $\text{Verify}(pk_e, m, \sigma) = 1$, где pk_e вычислен с использованием множителя e,
2. нарушитель не получал подпись σ на запрос (m, e).

Оценка стойкости в модели с линейно связанными ключами



Дальнейшие направления

1. Доказательство анонимности подписи.
2. Изучение полученного «зоопарка» задач для хэш-функций.
3. Альтернативные доказательства в «ослабленных» моделях (алгебраическая группа)?
4. Обобщаются ли результаты на gen – elGamal?
5. Изучение альтернативных конструкций.

Спасибо за внимание!

Задачи, связанные с поиском коллизий и прообразов

$\mathrm{Exp}_{\mathsf{F}}^{\mathrm{COLL}}$

$x, y \xleftarrow{\$} \mathcal{A}^{\mathsf{F}}$

if $(x \neq y)$ & $(\mathsf{F}(x) = \mathsf{F}(y))$

  return 1

return 0

$\mathrm{Exp}_{\mathsf{F}}^{\mathrm{NC}}$

$x, y \xleftarrow{\$} \mathcal{A}^{\mathsf{F}}$

if $(\mathsf{F}(x) = -\mathsf{F}(y))$

  return 1

return 0

$\mathrm{Exp}_{\mathsf{F}}^{\mathrm{ZP}}$

$x \xleftarrow{\$} \mathcal{A}^{\mathsf{F}}$

if $(\mathsf{F}(x) = 0)$

  return 1

return 0

$\mathrm{Exp}_{\mathsf{F}}^{\mathrm{RP}}$

$h \xleftarrow{\mathcal{U}} \mathrm{Rng}$

$x \xleftarrow{\$} \mathcal{A}^{\mathsf{F}}(h)$

if $(\mathsf{F}(x) = h)$

  return 1

return 0

Задачи, связанные с поиском алгебраических соотношений

$\mathrm{Exp}^{\text{4-PMCOLL}}_{\mathsf{F},\mathsf{F}'}$

$x, y, z, v \xleftarrow{\$} \mathcal{A}^{\mathsf{F},\mathsf{F}'}$

if $(\mathsf{F}'(z) \neq \mathsf{F}'(v))$ &

$\& \left(\dfrac{\mathsf{F}(x)}{\mathsf{F}(y)} = \dfrac{\mathsf{F}'(z)}{\mathsf{F}'(v)}\right)$

return 1

return 0

$\mathrm{Exp}^{\text{4-NMCOLL}}_{\mathsf{F},\mathsf{F}'}$

$x, y, z, v \xleftarrow{\$} \mathcal{A}^{\mathsf{F},\mathsf{F}'}$

if $(\mathsf{F}'(z) \neq \mathsf{F}'(v))$ &

$\& \left(\dfrac{\mathsf{F}(x)}{\mathsf{F}(y)} = -\dfrac{\mathsf{F}'(z)}{\mathsf{F}'(v)}\right)$

return 1

return 0

$\mathrm{Exp}^{\text{3-PMCOLL}}_{\mathsf{F},\mathsf{F}'}$

$x, y, z \xleftarrow{\$} \mathcal{A}^{\mathsf{F},\mathsf{F}'}$

if $(\mathsf{F}'(z) \neq 1)$ &

$\& \left(\dfrac{\mathsf{F}(x)}{\mathsf{F}(y)} = \mathsf{F}'(z)\right)$

return 1

return 0

$\mathrm{Exp}^{\text{3-NMCOLL}}_{\mathsf{F},\mathsf{F}'}$

$x, y, z \xleftarrow{\$} \mathcal{A}^{\mathsf{F},\mathsf{F}'}$

if $(\mathsf{F}'(z) \neq 1)$ &

$\& \left(\dfrac{\mathsf{F}(x)}{\mathsf{F}(y)} = -\mathsf{F}'(z)\right)$

return 1

return 0

$\mathrm{Exp}^{\text{2mult}}_{\mathsf{F},\mathsf{F}'}$

$x \xleftarrow{\$} \mathcal{A}^{\mathsf{F},\mathsf{F}'}(), y \xleftarrow{\$} \mathrm{Rng}$

$a, b \xleftarrow{\$} \mathcal{A}^{\mathsf{F},\mathsf{F}'}(y)$

if $\left(y\mathsf{F}'(a) = x\mathsf{F}(b)\right)$

return 1

return 0

Модели безопасности для мультипликативно связанных ключей с хэшированием множителя

$\mathrm{Exp}_{\mathrm{SS}}^{\text{Mult-hash}}(\mathcal{A})$

$(sk, pk) \xleftarrow{\$} \mathrm{SS.PairGen}()$

$L \leftarrow []$

$(m, \sigma, R) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\mathrm{sig}}}(pk)$

$epk' = \mathrm{Hash}(R) \cdot pk$

if $(\mathrm{SS.Verify}(epk', m, \sigma) = 0) \vee ((R, m, \sigma) \in L)$

  return 0

fi

return 1

$\mathcal{O}_{\mathrm{sig}}(m, R)$

if $R = \perp$

  $e \leftarrow 1$

else

  $e \leftarrow \mathrm{Hash}(R)$

fi

$esk \leftarrow sk \cdot e$

$epk \leftarrow e \cdot pk$

$\sigma \xleftarrow{\$} \mathrm{SS.Sign}(esk, epk, m)$

$L \leftarrow L \cup \{(R, m, \sigma)\}$

return σ

Модели безопасности для линейно связанных ключей без хэширования множителя

$\mathrm{Exp}^{\mathsf{Lin}}_{\mathsf{SS}}(\mathcal{A})$

$(sk, pk) \xleftarrow{\$} \mathsf{SS.PairGen}()$

$L \leftarrow []$

$(m, \sigma, e) \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\mathrm{sig}}}(pk)$

$epk' = e \cdot pk$

if $(\mathsf{SS.Verify}(epk', m, \sigma) = 0) \vee ((e, m, \sigma) \in L)$

  return 0

fi

return 1

$\mathcal{O}_{\mathrm{sig}}(m, e)$

$esk \leftarrow sk \cdot e$

$epk \leftarrow e \cdot pk$

$\sigma \xleftarrow{\$} \mathsf{SS.Sign}(esk, epk, m)$

$L \leftarrow L \cup \{(e, m, \sigma)\}$

return σ