конференция
РусКрипто

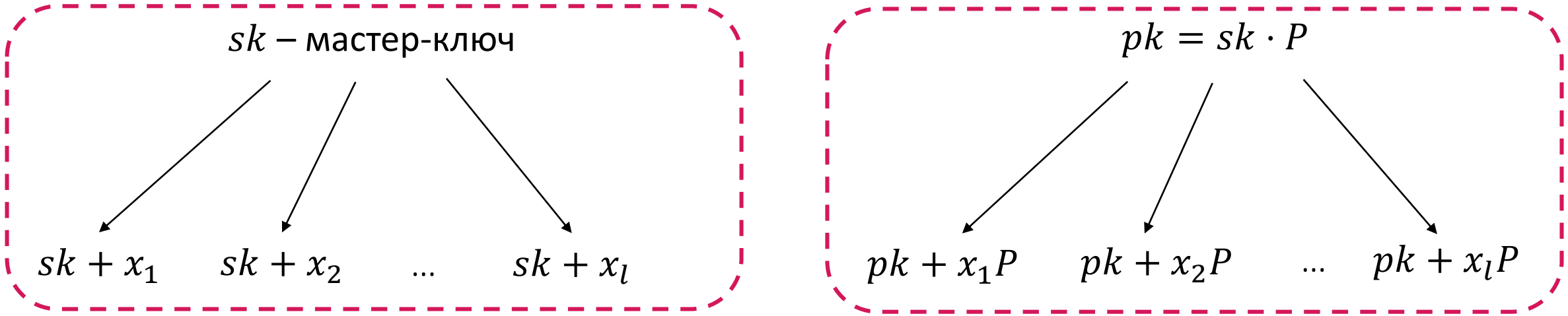
Ежегодная международная научно-практическая конференция
«РусКрипто'2024»

Аддитивно связанные ключи подписи: взломать нельзя использовать

Бабуева А. А., ведущий инженер-аналитик, КриптоПро
Кяжин С. Н., к.ф.-м.н., ведущий инженер-аналитик, КриптоПро

Аддитивно связанные ключи подписи

- $KGen(\,) \rightarrow (sk, pk)$
- $Sign(sk, m) \rightarrow \sigma$
- $Verify(pk, m, \sigma) \rightarrow \ 0/1$



$x_i \in \Omega, 1 \leq i \leq l, \quad \Omega$ – множество допустимых сдвигов

P – образующая точка кривой

Аддитивно связанные ключи подписи: предыстория

1) NSUCRYPTO’2022, открытая задача «Public keys for e-coins»:

   задача диверсификации ключей подписи с возможностью проверки подписи с помощью единого открытого ключа

2) SibeCRYPT’2023: частичное решение задачи и обзор моделей безопасности

   A. A. Babueva, S. N. Kyazhin, “Public keys for e-coins: partially solved problem using signature with rerandomizable keys”

3) TrustCom’2021: «… we proved that GOST is insecure …, but SM2 is secure ... This result well differentiates the security of ECDSA, SM2 and GOST…»

   Cui H. et al. “Security on SM2 and GOST signatures against related key”

Модели безопасности: классическая модель

Возможности нарушителя CMA:

Получать значения подписи для произвольных сообщений m, вычисленные с использованием ключа sk

Угроза (подделка подписи) UF:

Найти такую пару (m, σ), что:

- $Verify(pk, m, \sigma) = 1$
- нарушитель не запрашивал подпись для сообщения m

Модели безопасности, учитывающие связанные ключи

Возможности нарушителя CMA:

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

- (RKA) выбираются нарушителем (из допустимых)
- (KRKA) генерируются «честным образом»

*-RKA ⇒ *-KRKA

Угроза (подделка подписи для мастер-ключа):

Найти такую пару (m, σ), что:

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

UF-* ⇒ wUF-*

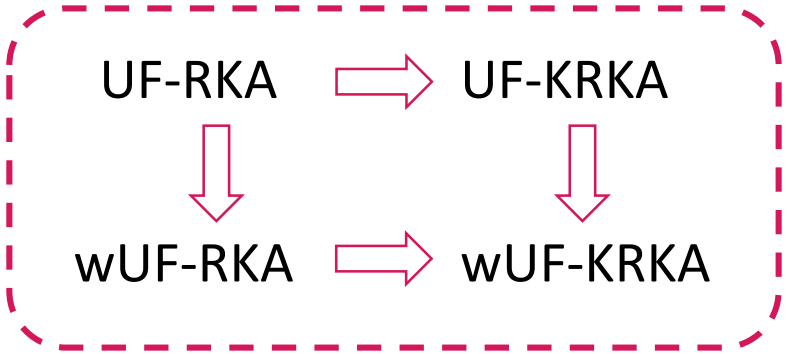
Модели безопасности, учитывающие связанные ключи

Возможности нарушителя CMA:

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

- (RKA) выбираются нарушителем (из допустимых)
- (KRKA) генерируются «честным образом»

*-RKA ⇒ *-KRKA



Угроза (подделка подписи для мастер-ключа):

Найти такую пару (m, σ), что:

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

UF-* ⇒ wUF-*

Модели безопасности, учитывающие связанные ключи

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-*

Модели безопасности, учитывающие связанные ключи

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»

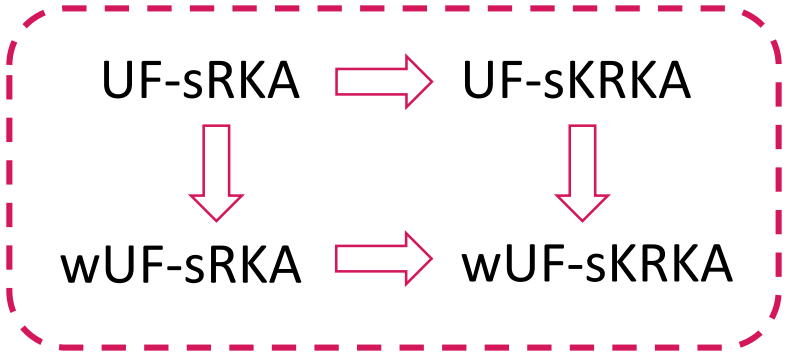
*-sRKA ⇒ *-sKRKA

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-*



Модели безопасности, учитывающие связанные ключи

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-*

Модели *-CM-sRKA учитывают угрозу нарушения свойства DSKS (Duplicate Signature Key Selection) следующего типа:

- нарушитель не знает исходный ключ подписи
- нарушитель не меняет параметры схемы

Анализ схем: существующие результаты

		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	ROM [PS96]								
ГОСТ	BRO [F18]								
ECDSA	BRO [F18]								
SM2	BRO [F18]								

[PS96] Pointcheval D., Stern J. Security proofs for signature, 1996.

[F18] Fersch M., The provable security of Elgamal-type signature schemes, 2018.

Анализ схем: существующие результаты

		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		[M+16]	[M+16]						
ГОСТ									
ECDSA									
SM2									

[M+16] Morita H. et al. On the security of the Schnorr signature scheme and DSA against related-key attacks, 2016.

Анализ схем: существующие результаты

		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				[⇒]	[YY19]		[⇒]		[YY19]
ГОСТ									
ECDSA				[⇒]				[⇒]	ROM [YY19]
SM2									

[YY19] Yuen Y.H., Yiu S.M. Strong Known Related-Key Attacks and the Security of ECDSA, 2019.

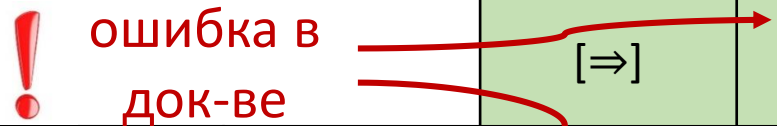
Анализ схем: существующие результаты

		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									
ГОСТ			[C+21]		[C+21]		[C+21]		[C+21]
ECDSA									
SM2		[⇒]	ROM [C+21]	[⇒]	[⇒]			[⇒]	ROM [C+21]

[C+21] Cui H. et al. Security on SM2 and GOST signatures against related key, 2021.

Анализ схем: существующие результаты

		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									
ГОСТ									
ECDSA				[⇒]				[⇒]	ROM [YY19]
SM2		[⇒]	ROM [C+21]	[⇒]	[⇒]			[⇒]	ROM [C+21]



Анализ схем: существующие результаты

		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									
ГОСТ									
ECDSA				[⇒]				[⇒]	GGM [GS22]
SM2									

[GS22] Groth J., Shoup V. On the security of ECDSA with additive key derivation and presignatures, 2022.

Анализ схем: существующие результаты

		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									
ГОСТ									
ECDSA									
SM2									

Анализ схем: новые результаты (ГОСТ)

		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									
ГОСТ		[⇒]		[⇒]		[new]		[⇒]	
ECDSA									
SM2									

Схема ГОСТ является стойкой в моделях со связанными ключами, в которых *подделка* должна быть построена *для нового сообщения*

Анализ схем: новые результаты (схема Шнорра)

		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									
ECDSA									
SM2									

Схема Шнорра является стойкой в моделях со связанными ключами, в которых *подделка* должна быть построена *для нового сообщения*

Анализ схем: новые результаты (ECDSA)

		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									
ГОСТ									
ECDSA									
SM2									

Анализ схем: новые результаты (ECDSA)

Существующие результаты в моделях, где сдвиги выбираются честным образом:

Theorem 2. *Let $\mathcal{A}$ be an adversary attacking $\mathcal{S}_{\mathrm{ecdsa}}$ as in Definition 2 with* ***additive key derivation*** *that makes at most N signing or group queries, of which N_{sig} are signing queries. Then there exist adversaries $\mathcal{B}_{\mathrm{Ia}}$, $\mathcal{B}_{\mathrm{Ib}}$, $\mathcal{B}_{\mathrm{II}}$, and $\mathcal{B}_{\mathrm{III}}$, whose running times are essentially the same as $\mathcal{A}$, such that*

$$\begin{aligned}\mathrm{CMA}^{\mathrm{ggm}}_{\mathrm{akd}}\mathsf{adv}[\mathcal{A}, \mathcal{S}_{\mathrm{ecdsa}}, \mathfrak{E}] \leq\ & \mathrm{CRadv}[\mathcal{B}_{\mathrm{Ia}}, \mathit{Hash}] + \\ & (4 + o(1))N_{\mathrm{sig}}|\mathfrak{E}|\cdot \mathrm{RPRadv}[\mathcal{B}_{\mathrm{Ib}}, \mathit{Hash}] + \\ & (4 + o(1))N|\mathfrak{E}|\cdot \mathrm{RPRadv}[\mathcal{B}_{\mathrm{II}}, \mathit{Hash}] + \\ & \mathrm{ZPRadv}[\mathcal{B}_{\mathrm{III}}, \mathit{Hash}] + \\ & O(N^2/q).\end{aligned}$$

мощность множества сдвигов, генерируемых в рамках эксперимента

Гипотеза: если множество сдвигов, для которых может быть предъявлена подделка, не ограничено, то схема ECDSA не стойкая

Анализ схем: новые результаты (ECDSA)

Атака на ECDSA в моделях *-CM-sRKA

(подделка для хотя бы одного ключа, произвольное значение сдвига)

Нарушитель:

1) Получает подпись (r, s) для произвольного сообщения m_1 на мастер-ключе d:

$$s = k^{-1}(e_1 + rd),$$

где $e_1 = H(m_1)$, k – выбирается случайно равновероятно из $\mathbb{Z}_q^*$.

2) Выдает в качестве подделки подпись (r, s) для произвольного сообщения m_2 и сдвига x_2, такого что

$$e_2 + rx_2 = e_1,$$

где $e_2 = H(m_2)$.

Анализ схем: новые результаты (ECDSA)

		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									
ГОСТ									
ECDSA						[new]	[⇒]		
SM2									

Анализ схем: новые результаты (ECDSA)

		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									
ГОСТ									
ECDSA		BRO [new]							
SM2									

Схема ECDSA является стойкой в моделях со связанными ключами, в которых *подделка* должна быть построена *для мастер-ключа и нового сообщения*

Анализ схем: новые результаты (ECDSA)

		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									
ГОСТ									
ECDSA									
SM2									

Анализ схем: новые результаты (SM2)

Атака на SM2 в моделях *-CM-sRKA

(подделка для хотя бы одного ключа, произвольное значение сдвига)

Нарушитель:

1) Получает подпись (r, s_1) для произвольного сообщения m_1 на мастер-ключе d:

$$s_1(d+1) = k - (r + e_1)d,$$

где $e_1 = H(m_1)$, k – выбирается случайно равновероятно из $\mathbb{Z}_q^*$.

2) Выдает в качестве подделки подпись (r, s_2) для произвольного сообщения m_2 и сдвига x_2, где

$$s_2 = s_1 + e_1 - e_2$$
$$x_2 = (s_1 + r + e_1)^{-1}(e_2 - e_1),$$

где $e_2 = H(m_2)$.

Анализ схем: новые результаты (SM2)

		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									
ГОСТ									
ECDSA									
SM2						[new]	[⇒]		

Анализ схем: новые результаты (SM2)

		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									
ГОСТ									
ECDSA									
SM2		BRO [new]		[⇒]					

Схема SM2 является стойкой в моделях со связанными ключами, в которых *подделка* должна быть построена *для мастер-ключа и нового сообщения*

Анализ схем: новые результаты

		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]	[⇒]		

Выводы для схемы ГОСТ

Если релевантна угроза создания подделки *для произвольного* сообщения:

взломать, нельзя использовать

Если релевантна угроза создания подделки *только для нового* сообщения:

взломать нельзя, использовать