РусКрипто

XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Схема подписи ГОСТ в условиях мультипликативно связанных ключей: о стойкости в модели UF-CM-sKRKA

Бабуева А.А.[1], Кяжин С.Н.[2], Махонин И.В.[1,2]

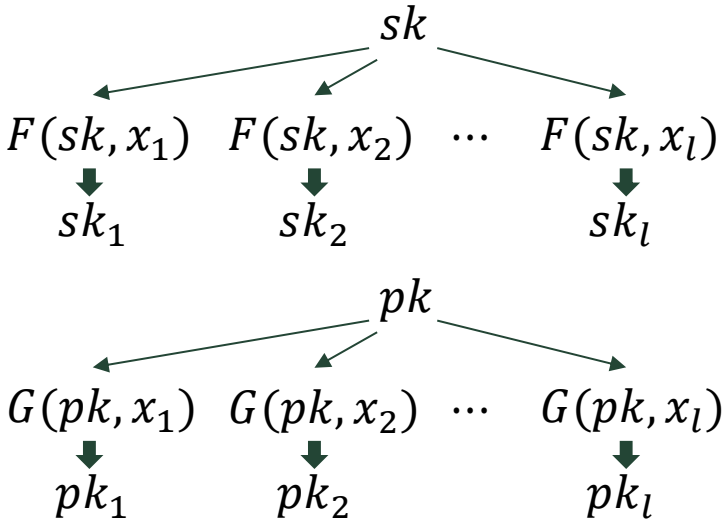
1. ООО «Крипто-Про», 2. НИЯУ МИФИ

Связанные ключи подписи

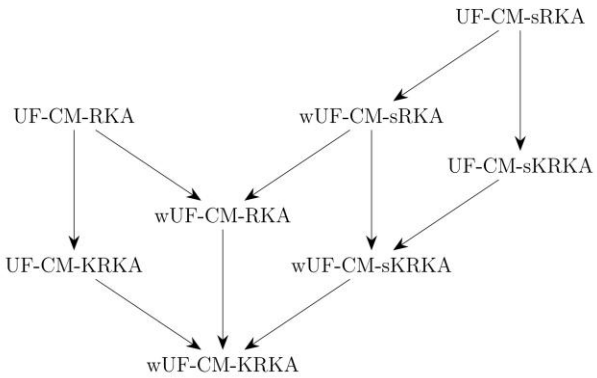
- $Kgen() \rightarrow sk, pk$
- $Sign(sk, m) \rightarrow \sigma$
- $Verify(pk, \sigma, m) \rightarrow 0/1$

- sk (pk) – исходный закрытый (открытый) ключ
- sk_i (pk_i) – производные закр. (откр.) ключи
- x_i – значения сдвигов
- F (G) – функции формирования производных закр. (откр.) ключей

- H – хэш-функция, используемая в алгоритме



Модели безопасности



- *Babueva A.A., Kyazhin S.N. Additively related keys for signature: security models and results for Schnorr, GOST, ECDSA, and SM2 // Математические вопросы криптографии. 2025. Том 16, выпуск 3. С. 101–121.*
- *Бабуева А.А., Кяжин С.Н. Аддитивно связанные ключи подписи: взломать нельзя использовать // РусКрипто'2024.*

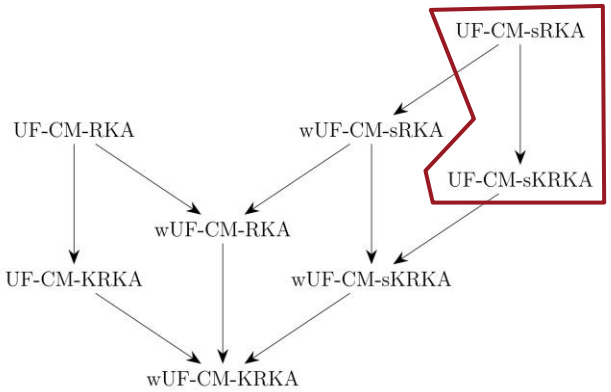
mult-Hash

$$x_i \leftarrow H'(r_i)$$

- H' – хэш-функция
- r_i выбираются нарушителем

- *Бахарев А.О., Царегородцев К.Д. Мультипликативно и линейно связанные ключи подписи // РусКрипто'2025.*

Модели безопасности



- *Babueva A.A., Kyazhin S.N. Additively related keys for signature: security models and results for Schnorr, GOST, ECDSA, and SM2 // Математические вопросы криптографии. 2025. Том 16, выпуск 3. С. 101–121.*
- *Бабуева А.А., Кяжин С.Н. Аддитивно связанные ключи подписи: взломать нельзя использовать // РусКрипто'2024.*

mult-Hash

$$x_i \leftarrow H'(r_i)$$

- H' – хэш-функция
- r_i выбираются нарушителем

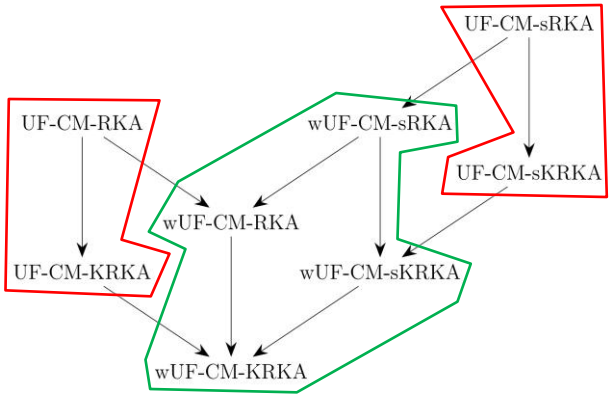
- *Бахарев А.О., Царегородцев К.Д. Мультипликативно и линейно связанные ключи подписи // РусКрипто'2025.*

Сравнение трех моделей

Модель	UF-CM-sRKA	mult-Hash	UF-CM-sKRKA
Выбор сдвига	Нарушитель выбирает x_i	Нарушитель выбирает r_i	Случайный выбор x_i

ГОСТ в условии аддитивно связанных ключей

$$F(sk, x) = sk + x;$$
$$G(pk, x) = pk + xP$$



P – образующая группы точек эллиптической кривой

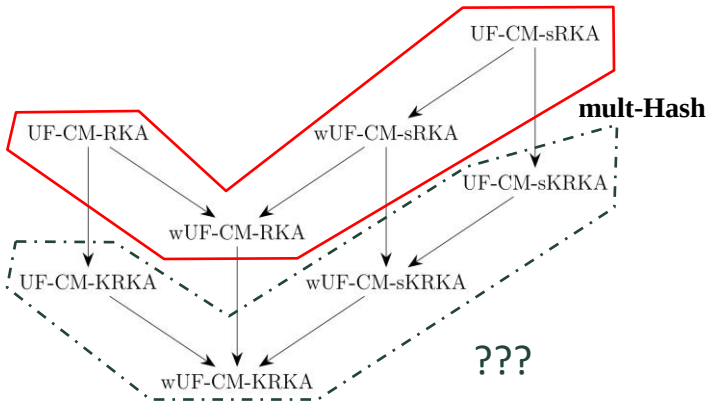
Получены результаты во всех 8 моделях:

- Доказана ***стойкость*** в моделях с подделкой для **нового** сообщения (wUF-).
- Построены ***атаки*** в моделях с подделкой для **произвольного** сообщения (UF-)

- Babueva A.A., Kyazhin S.N. Additively related keys for signature: security models and results for Schnorr, GOST, ECDSA, and SM2 // Математические вопросы криптографии. 2025. Том 16, выпуск 3. С. 101–121.
- Бабуева А.А., Кяжин С.Н. Аддитивно связанные ключи подписи: взломать нельзя использовать // РусКрипто'2024.

ГОСТ в условии мультипликативно связанных ключей

$$F(sk, x) = x \cdot sk;$$
$$G(pk, x) = x \cdot pk$$



Атака в моделях с адаптивным выбором сдвига (-RKA и -sRKA):

- Cui H., Qin X., Cai C., Yuen T.H. Security on SM2 and GOST signatures against related key attacks // 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2021. Pp. 155–163.

Оценка стойкости в модели mult-Hash:

- Бахарев А.О., Царегородцев К.Д. Мультипликативно и линейно связанные ключи подписи // РусКрипто'2025.

В моделях со случайным выбором сдвига (-KRKA и -sKRKA) результаты отсутствуют.

Цель: определить задачи для хэш-функции, сложность которых является необходимым условием стойкости схемы ГОСТ в модели UF-CM-sKRKA

Задачи, сложность которых необходима для стойкости ГОСТ в модели mult-Hash

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

    return 1

return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели mult-Hash

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0)$:

  return 1

return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели mult-Hash

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$
$x \xleftarrow{\$} \mathcal{A}(h)$
if $(\mathsf{H}(x) = h)$:
    return 1
return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}(x) = 0)$:
    return 1
return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:
    return 1
return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели mult-Hash

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

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

  return 1

return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели mult-Hash

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$
$x \xleftarrow{\$} \mathcal{A}(h)$
if $(\mathsf{H}(x) = h)$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}(x) = 0)$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(x \neq y) \wedge \left(\mathsf{H}'(x) = \mathsf{H}'(y)\right)$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}(x) = -\mathsf{H}(y))$:
  return 1
return 0

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge$
  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = \dfrac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:
  return 1
return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели mult-Hash

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$
$x \xleftarrow{\$} \mathcal{A}(h)$
if $(\mathsf{H}(x) = h)$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}(x) = 0)$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}(x) = -\mathsf{H}(y))$:
  return 1
return 0

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge$
  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = \dfrac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:
  return 1
return 0

$\mathbf{Exp}^{\text{4-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge$
  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\dfrac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:
  return 1
return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели mult-Hash

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$
$x \xleftarrow{\$} \mathcal{A}(h)$
if $(\mathsf{H}(x) = h)$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}(x) = 0)$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}(x) = -\mathsf{H}(y))$:
  return 1
return 0

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge$
  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = \dfrac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:
  return 1
return 0

$\mathbf{Exp}^{\text{4-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge$
  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\dfrac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:
  return 1
return 0

$\mathbf{Exp}^{\text{3-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq 1) \wedge$
  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = \mathsf{H}'(z)\right)$:
  return 1
return 0

$\mathbf{Exp}^{\text{3-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq 1) \wedge$
  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\mathsf{H}'(z)\right)$:
  return 1
return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели ~~mult-Hash~~ UF-CM-sKRKA

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

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

  return 1

return 0

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge$

  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = \dfrac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{4-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge$

  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\dfrac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq 1) \wedge$

  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = \mathsf{H}'(z)\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq 1) \wedge$

  $\wedge \left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\mathsf{H}'(z)\right)$:

  return 1

return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели ~~mult-Hash~~ UF-CM-sKRKA

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$ $\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$ $\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

Не зависит от H'

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$
if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:
  return 1
return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

Не зависит от H'

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:
  return 1
return 0

$\mathbf{Exp}^{\text{4-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:
  return 1
return 0

$\mathbf{Exp}^{\text{3-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq 1) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \mathsf{H}'(z)\right)$:
  return 1
return 0

$\mathbf{Exp}^{\text{3-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$
if $(\mathsf{H}'(z) \neq 1) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\mathsf{H}'(z)\right)$:
  return 1
return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели ~~mult-Hash~~ UF-CM-sKRKA

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

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

  return 1

return 0

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{4-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq 1) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \mathsf{H}'(z)\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq 1) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\mathsf{H}'(z)\right)$:

  return 1

return 0

Адаптация задачи COLL для H' к модели UF-CM-sKRKA

Нарушитель в mult-Hash

1. находит x, y: $H'(x) = H'(y)$;
2. для любого сообщения m запрашивает подпись для значения x, определяющего сдвиг, и получает подпись σ
3. возвращает σ в качестве подделки для сообщения m и значения y, определяющего сдвиг

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge \left(\mathsf{H}'(x) = \mathsf{H}'(y)\right)$:

  return 1

return 0

Адаптация задачи COLL для H' к модели UF-CM-sKRKA

Нарушитель в mult-Hash

1. находит x, y: $H'(x) = H'(y)$;
2. для любого сообщения m запрашивает подпись для значения x, определяющего сдвиг, и получает подпись σ
3. возвращает σ в качестве подделки для сообщения m и значения y, определяющего сдвиг

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:

  return 1

return 0

В модели UF-CM-sKRKA каждому новому сдвигу соответствует уникальное значение производного ключа

Атака не применима в модели UF-CM-sKRKA

Задачи, сложность которых необходима для стойкости ГОСТ в модели ~~mult-Hash~~ UF-CM-sKRKA

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

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

  return 1

return 0

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{4-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq 1) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \mathsf{H}'(z)\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq 1) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\mathsf{H}'(z)\right)$:

  return 1

return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели ~~mult-Hash~~ UF-CM-sKRKA

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

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

  return 1

return 0

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{4-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq 1) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \mathsf{H}'(z)\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq 1) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\mathsf{H}'(z)\right)$:

  return 1

return 0

Адаптация задач 3-PMCOLL и 3-NMCOLL к модели UF-CM-sKRKA

$\mathbf{Exp}^{\text{3-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq 1) \wedge$

$\wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \mathsf{H}'(z)\right)$:

return 1

return 0

$\mathbf{Exp}^{\text{3-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq 1) \wedge$

$\wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\mathsf{H}'(z)\right)$:

return 1

return 0

3-PMCOLL / 3-NMCOLL

Нарушитель в mult-Hash

- находит x, y, z: $\frac{H(x)}{H(y)} = H'(z) = \Delta$ $\frac{H(x)}{H(y)} = -H'(z) = \Delta$
- для сообщения y и исходного ключа, запрашивает подпись

$$\sigma = (r = (kP).\mathrm{x}; s = kH(y) + dr)$$

- для сообщения x и значения z, определяющего сдвиг, формирует подделку

$$\sigma^* = (r^* = r\ r^* = -r; s^* = s \cdot \Delta)$$

Адаптация задач 3-PMCOLL и 3-NMCOLL к модели UF-CM-sKRKA

$\mathbf{Exp}_{\mathsf{H}}^{\text{3-PMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = z\right) \wedge (z \in \mathcal{R})$:

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{3-NMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -z\right) \wedge (z \in \mathcal{R})$:

  return 1

return 0

3-PMCOLL' / 3-NMCOLL'

Нарушитель в UF-CM-sKRKA

- находит x, y, z: $\frac{H(x)}{H(y)} = z = \Delta$ $\frac{H(x)}{H(y)} = -z = \Delta$
- для сообщения y и исходного ключа, запрашивает подпись

$$\sigma = (r = (kP).\mathrm{x}; s = kH(y) + dr)$$

- для сообщения x и значения сдвига z формирует подделку

$$\sigma^* = (r^* = r\ r^* = -r; s^* = s \cdot \Delta)$$

Задачи, сложность которых необходима для стойкости ГОСТ в модели ~~mult-Hash~~ UF-CM-sKRKA

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

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

  return 1

return 0

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{4-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-PMCOLL}'}_{\mathsf{H}}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = z\right) \wedge (z \in \mathcal{R})$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-NMCOLL}'}_{\mathsf{H}}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -z\right) \wedge (z \in \mathcal{R})$:

  return 1

return 0

Задачи, сложность которых необходима для стойкости ГОСТ в модели ~~mult-Hash~~ UF-CM-sKRKA

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

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

  return 1

return 0

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{4-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-PMCOLL}'}_{\mathsf{H}}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = z\right) \wedge (z \in \mathcal{R})$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-NMCOLL}'}_{\mathsf{H}}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -z\right) \wedge (z \in \mathcal{R})$:

  return 1

return 0

Адаптация задач 4-PMCOLL и 4-NMCOLL к модели UF-CM-sKRKA

$\mathbf{Exp}^{\text{4-PMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge$

$\wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

return 1

return 0

$\mathbf{Exp}^{\text{4-NMCOLL}}_{\mathsf{H},\mathsf{H}'}(\mathcal{A})$

$x, y, z, w \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}'(z) \neq \mathsf{H}'(w)) \wedge$

$\wedge \left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\frac{\mathsf{H}'(z)}{\mathsf{H}'(w)}\right)$:

return 1

return 0

4-PMCOLL / 4-NMCOLL

Нарушитель в mult-Hash

- находит x, y, z, w: $\frac{H(x)}{H(y)} = \frac{H'(z)}{H'(w)} = \Delta$ $\frac{H(x)}{H(y)} = -\frac{H'(z)}{H'(w)} = \Delta$
- для сообщения y и значения w, определяющего сдвиг, запрашивает подпись

$$\sigma = (r = (kP).\mathrm{x}; s = kH(y) + dH'(w)r)$$

- для сообщения x и значения z, определяющего сдвиг, формирует подделку

$$\sigma^* = (r^* = r\ r^* = -r; s^* = s \cdot \Delta)$$

Адаптация задач 4-PMCOLL и 4-NMCOLL к модели UF-CM-sKRKA

$\mathbf{Exp}_{\mathsf{H}}^{\text{4-PMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z, w \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \frac{z}{w}\right) \wedge (z, w \in \mathcal{R})$:

return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{4-NMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z, w \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\frac{z}{w}\right) \wedge (z, w \in \mathcal{R})$:

return 1

return 0

4-PMCOLL' / 4-NMCOLL'

Нарушитель в UF-CM-sKRKA

- находит x, y, z, w: $\frac{H(x)}{H(y)} = \frac{z}{w} = \Delta$ $\frac{H(x)}{H(y)} = -\frac{z}{w} = \Delta$
- для сообщения y и значения сдвига w запрашивает подпись

$$\sigma = (r = (kP).\mathrm{x}; s = kH(y) + dwr)$$

- для сообщения x и значения сдвига z формирует подделку

$$\sigma^* = (r^* = r\ r^* = -r; s^* = s \cdot \Delta)$$

Задачи, сложность которых необходима для стойкости ГОСТ в модели ~~mult-Hash~~ UF-CM-sKRKA

$\mathbf{Exp}^{\mathsf{RP}}_{\mathsf{H}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{ZP}}_{\mathsf{H}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0)$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{COLL}}_{\mathsf{H}'}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}'(x) = \mathsf{H}'(y))$:

  return 1

return 0

$\mathbf{Exp}^{\mathsf{NC}}_{\mathsf{H}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

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

  return 1

return 0

$\mathbf{Exp}^{\text{4-PMCOLL}'}_{\mathsf{H}}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z, w \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = \frac{z}{w}\right) \wedge (z, w \in \mathcal{R})$:

  return 1

return 0

$\mathbf{Exp}^{\text{4-NMCOLL}'}_{\mathsf{H}}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z, w \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\frac{z}{w}\right) \wedge (z, w \in \mathcal{R})$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-PMCOLL}'}_{\mathsf{H}}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = z\right) \wedge (z \in \mathcal{R})$:

  return 1

return 0

$\mathbf{Exp}^{\text{3-NMCOLL}'}_{\mathsf{H}}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\frac{\mathsf{H}(x)}{\mathsf{H}(y)} = -z\right) \wedge (z \in \mathcal{R})$:

  return 1

return 0

Итоговый список задач, сложность которых необходима для стойкости ГОСТ в UF-CM-sKRKA

$\mathbf{Exp}_{\mathsf{H}}^{\text{4-PMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z, w \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = \dfrac{z}{w}\right) \wedge (z, w \in \mathcal{R})$:

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{4-NMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z, w \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\dfrac{z}{w}\right) \wedge (z, w \in \mathcal{R})$:

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{3-PMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = z\right) \wedge (z \in \mathcal{R})$:

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{3-NMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = -z\right) \wedge (z \in \mathcal{R})$:

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{COLL}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y))$:

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{NC}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

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

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{ZP}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0)$:

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{RP}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h)$:

  return 1

return 0

Итоговый список задач, сложность которых необходима для стойкости ГОСТ в UF-CM-sKRKA

$\mathbf{Exp}_{\mathsf{H}}^{\text{4-PMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z, w \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = \dfrac{z}{w}\right) \wedge (z, w \in \mathcal{R}) :$

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{4-NMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z, w \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = -\dfrac{z}{w}\right) \wedge (z, w \in \mathcal{R}) :$

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{3-PMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = z\right) \wedge (z \in \mathcal{R}) :$

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{3-NMCOLL}'}(\mathcal{A})$

$\mathcal{R} \leftarrow \{r_i \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*\}_{i=1}^k$

$x, y, z \xleftarrow{\$} \mathcal{A}(\mathcal{R})$

if $\left(\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = -z\right) \wedge (z \in \mathcal{R}) :$

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{COLL}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

if $(x \neq y) \wedge (\mathsf{H}(x) = \mathsf{H}(y)) :$

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{NC}}(\mathcal{A})$

$x, y \xleftarrow{\$} \mathcal{A}$

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

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{ZP}}(\mathcal{A})$

$x \xleftarrow{\$} \mathcal{A}$

if $(\mathsf{H}(x) = 0) :$

  return 1

return 0

$\mathbf{Exp}_{\mathsf{H}}^{\text{RP}}(\mathcal{A})$

$h \xleftarrow{\mathcal{U}} \mathbb{Z}_q$

$x \xleftarrow{\$} \mathcal{A}(h)$

if $(\mathsf{H}(x) = h) :$

  return 1

return 0

Связь между задачами

Результат 1

$$\mathsf{Insec}_H^{\text{3-NMCOLL}'}(T,k) = \mathsf{Insec}_H^{\text{3-PMCOLL}'}(T,k)$$

Связь между задачами

Результат 1

$$\mathsf{Insec}_H^{\text{3-NMCOLL}'}(T,k) = \mathsf{Insec}_H^{\text{3-PMCOLL}'}(T,k)$$

Результат 2

$$\mathsf{Insec}_H^{\text{3-PMCOLL}'}(T,k) \leq k \cdot \mathsf{Insec}_H^{\text{RCCOLL}}(T)$$

$\mathbf{Exp}_{\mathsf{H}}^{\text{RCCOLL}}(\mathcal{A})$

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

$x, y \xleftarrow{\$} \mathcal{A}(z)$

if $\dfrac{\mathsf{H}(x)}{\mathsf{H}(y)} = z$:

  return 1

return 0

Спасибо
за внимание!

РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Махонин Илья
ООО «Крипто-Про», НИЯУ МИФИ
makhonin@cryptopro.ru