КРИПТОНИТ

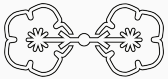
Анализ устойчивости постквантовой электронной подписи «Шиповник» к атакам, нацеленным на хэш-функции

Виктория Высоцкая, Диана Дас

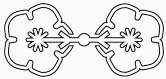
21 марта 2024

Схема подписи

Параметры схемы



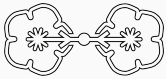
λ	— уровень стойкости,
n	— длина кода,
k	— размерность кода,
ω	— вес вектора ошибки,
$H \in \{0,1\}^{(n-k)\times n}$	— случайная проверочная матрица,
$h(\cdot) : \{0,1\}^* \to \{0,1\}^{512}$	— двоичная хэш-функция,
$h'(\cdot) : \{0,1\}^* \to \{0,1,2\}^{\delta}$	— троичная хэш-функция,
δ	— параметр, отвечающий за длину подписи и зависящий от уровня стойкости.



Двоичная хэш-функция h определена в ГОСТ 34.11-2018 с выходом 512 бит (Стрибог-512).

Троичная хэш-функция $h' : [0; 2^{512} - 1] \to [0; 3^{\delta} - 1]$ принимает на вход выход базовой хэш-функции и определена следующим образом:

$$h'(x) = \left\lfloor \frac{x \cdot 3^{\delta}}{2^{512}} \right\rfloor.$$



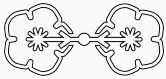
Shipovnik.KeyGen(1^λ)

$s \xleftarrow{u} \{x \in \{0,1\}^n : \mathrm{wt}(x) = \omega\}$

$y \leftarrow Hs^T$

return (y, s)

Сложность поиска секретного ключа основана на сложности решения задачи синдромного декодирования.



Shipovnik.SigGen(s, m)

foreach $0 \leqslant i < \delta$:

$u_i \xleftarrow{u} \{0,1\}^n, \sigma_i \xleftarrow{u} S_n$

$c_{i,0} \leftarrow h(\sigma_i \| H u_i^T)$

$c_{i,1} \leftarrow h(\sigma_i(u_i))$

$c_{i,2} \leftarrow h(\sigma_i(u_i \oplus s))$

$c_i \leftarrow c_{i,0} \| c_{i,1} \| c_{i,2}$

$c \leftarrow c_0 \| \ldots \| c_{\delta-1}$

$b \leftarrow h'(m \| c)$

foreach $0 \leqslant i < \delta$:

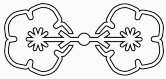
if $b_i = 0$: $r_i \leftarrow \sigma_i \| u_i$

if $b_i = 1$: $r_i \leftarrow \sigma_i \| (u_i \oplus s)$

if $b_i = 2$: $r_i \leftarrow \sigma_i(u_i) \| \sigma_i(s)$

$r \leftarrow r_0 \| \ldots \| r_{\delta-1}$

return $c \| r$



Shipovnik.SigVer$(y, m, c\|\|r)$

$b \leftarrow h'(m\|\|c)$

foreach $0 \leqslant i < \delta$:

  if $\left[b_i = 0\right] \wedge \left[\left[c_{i,0} \neq h(r_{i,0}\|\|Hr_{i,1}^T)\right] \vee \left[c_{i,1} \neq h(r_{i,0}(r_{i,1}))\right]\right]$:

    return 0

  if $\left[b_i = 1\right] \wedge \left[\left[c_{i,0} \neq h(r_{i,0}\|\|(Hr_{i,1}^T \oplus y))\right] \vee \left[c_{i,2} \neq h(r_{i,0}(r_{i,1}))\right]\right]$:

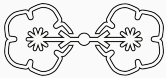
    return 0

  if $\left[b_i = 2\right] \wedge \left[\left[c_{i,1} \neq h(r_{i,0})\right] \vee \left[c_{i,2} \neq h(r_{i,0} \oplus r_{i,1})\right] \vee \left[\mathrm{wt}(r_{i,1}) \neq \omega\right]\right]$:

    return 0

return 1

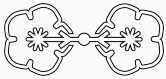
Классическая атака на схему подписи «Шиповник»



Алгоритм $\mathcal{A}(y)$

Вход: $y \in \{0,1\}^n$ — открытый ключ

Выход: (m, ζ) — корректная пара (сообщение, подпись)



$\mathcal{A}(y)$

$t \xleftarrow{u} \{0,1\}^n \ \wedge \ \mathrm{wt}(t) = \omega$

foreach $0 \leqslant i < \delta$:

$u_i \xleftarrow{u} \{0,1\}^n, \sigma_i \xleftarrow{u} S_n$

$c_{i,0} \leftarrow h(\sigma_i \| H u_i^T)$

$c_{i,1} \leftarrow h(\sigma_i(u_i))$

$c_{i,2} \leftarrow h(\sigma_i(u_i \oplus t))$

$c_i \leftarrow c_{i,0} \| c_{i,1} \| c_{i,2}$

$c \leftarrow c_0 \| \ldots \| c_{\delta-1}$

$b \leftarrow h'(m \| c)$

foreach $0 \leqslant i < \delta$:

if $b_i = 0$: $r_i \leftarrow \sigma_i \| u_i$

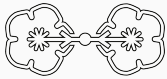
if $b_i = 1$: $r_i \leftarrow \sigma_i \| (u_i \oplus t)$

if $b_i = 2$: $r_i \leftarrow \sigma_i(u_i) \| \sigma_i(t)$

$r \leftarrow r_0 \| \ldots \| r_{\delta-1}$

return $\zeta = c \| r$

$b_i \neq 1$



Подделка не пройдет проверку там, где $b_i = 1$!

Shipovnik.SigVer$(y, m, c\|r)$

$b \leftarrow h'(m\|c)$

foreach $0 \leqslant i < \delta$:

if $\left[b_i = 0\right] \wedge \left[\left[c_{i,0} \neq h(r_{i,0}\|Hr_{i,1}^T)\right] \vee \left[\left[c_{i,1} \neq h(r_{i,0}(r_{i,1}))\right]\right]$:

return 0

if $\left[b_i = 1\right] \wedge \left[\left[c_{i,0} \neq h(r_{i,0}\|(Hr_{i,1}^T \oplus y))\right] \vee \left[c_{i,2} \neq h(r_{i,0}(r_{i,1}))\right]\right]$:

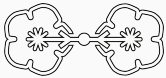
return 0

if $\left[b_i = 2\right] \wedge \left[\left[c_{i,1} \neq h(r_{i,0})\right] \vee \left[c_{i,2} \neq h(r_{i,0} \oplus r_{i,1})\right] \vee \left[\mathrm{wt}(r_{i,1}) \neq \omega\right]\right]$:

return 0

return 1

Атака в модели без известных сообщений



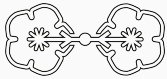
Алгоритм $\mathcal{A}(y, (m, \zeta))$

$$p_{\mathcal{A}} = \left(\frac{2}{3}\right)^{\delta}$$

$$T_{\mathcal{A}} = T_{\text{Shipovnik.SigGen}}$$

$$\frac{T_{\mathcal{A}}}{p_{\mathcal{A}}} \approx 2^{128} \cdot T_{\text{Shipovnik.SigGen}}$$

Атаки на основе поиска прообраза троичной хэш-функции h'

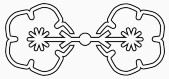


Задача $\mathrm{FSPA}(b, c)$ [Fixed Suffix Preimage Attack]:
Дано: хэш-функция h', строки $b \in \{0,1,2\}^{\delta}$ и $c \in \{0,1\}^{1536 \cdot \delta}$.
Найти: сообщение $m \in \{0,1\}^*$ такое, что $h'(m \| c) = b$.

Алгоритм P решает задачу FSPA.

Алгоритм $\mathcal{A}^{\mathrm{P}}(y)$
Вход: $y \in \{0,1\}^n$ — открытый ключ.
Выход: (m, ζ) — корректная пара (сообщение, подпись).

Атака в модели без известных сообщений



$\mathcal{A}^{\mathsf{P}}(y)$

foreach $0 \leqslant i < \delta$:

$b_i \xleftarrow{u} \{0,1,2\}$

if $b_i = 2$:

$r_i \xleftarrow{u} \{0,1\}^{2n}$:

$\mathrm{wt}(r_{i,1}) = \omega$

else :

$r_i \xleftarrow{u} \{0,1\}^{n(log_2 n+1)}$

$b \leftarrow b_0 \| \ldots \| b_{\delta-1}$

foreach $0 \leqslant i < \delta$:

if $b_i = 0$:

$c_{i,0} = h(r_{i,0} \| Hr_{i,1}^T)$

$c_{i,1} = h(r_{i,0}(r_{i,1}))$

$c_{i,2} \xleftarrow{u} \{0,1\}^{512}$

if $b_i = 1$:

$c_{i,0} = h(r_{i,0} \| (Hr_{i,1}^T \oplus y))$

$c_{i,1} \xleftarrow{u} \{0,1\}^{512}$

$c_{i,2} = h(r_{i,0}(r_{i,1}))$

if $b_i = 2$:

$c_{i,0} \xleftarrow{u} \{0,1\}^{512}$

$c_{i,1} = h(r_{i,0})$

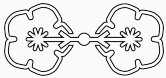
$c_{i,2} = h(r_{i,0} \oplus r_{i,1})$

$c_i \leftarrow c_{i,0} \| c_{i,1} \| c_{i,2}$

$\zeta = (c_0 \| \ldots \| c_{\delta-1} \| r_0 \| \ldots \| r_{\delta-1})$

$m \leftarrow\!\$\ \mathsf{P}(b, c_0 \| \ldots \| c_{\delta-1})$

return (m, ζ)



Shipovnik.SigVer$(y, m, c\|\|r)$

$b \leftarrow h'(m\|\|c)$

foreach $0 \leqslant i < \delta$:

if $\left[b_i = 0\right] \wedge \left[\left[c_{i,0} \neq h(r_{i,0}\|\|Hr_{i,1}^T)\right] \vee \left[\left[c_{i,1} \neq h(r_{i,0}(r_{i,1}))\right]\right]$:

return 0

if $\left[b_i = 1\right] \wedge \left[\left[c_{i,0} \neq h(r_{i,0}\|\|(Hr_{i,1}^T \oplus y))\right] \vee \left[c_{i,2} \neq h(r_{i,0}(r_{i,1}))\right]\right]$:

return 0

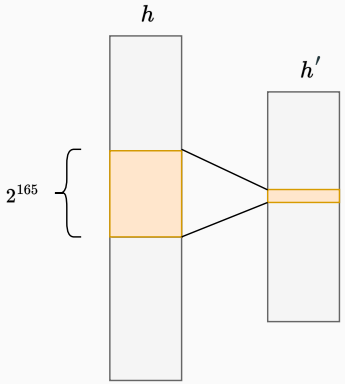
if $\left[b_i = 2\right] \wedge \left[\left[c_{i,1} \neq h(r_{i,0})\right] \vee \left[c_{i,2} \neq h(r_{i,0} \oplus r_{i,1})\right] \vee \left[\mathrm{wt}(r_{i,1}) \neq \omega\right]\right]$:

return 0

return 1

Атака в модели без известных сообщений

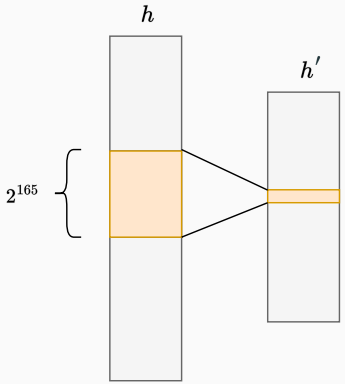
$$p_{\mathsf{P}} = 2^{-347}$$
$$T_{\mathsf{P}} = T_{\mathsf{hash}}$$
$$\frac{T_{\mathsf{P}}}{p_{\mathsf{P}}} = 2^{347} \cdot T_{\mathsf{hash}}$$

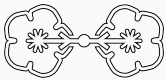


Атака в модели без известных сообщений

$$p_{\mathsf{P}} = 2^{-347}$$
$$T_{\mathsf{P}} = T_{\mathsf{hash}}$$
$$\frac{T_{\mathsf{P}}}{p_{\mathsf{P}}} = 2^{347} \cdot T_{\mathsf{hash}}$$

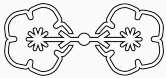
$$p_{\mathcal{A}^{\mathsf{P}}} = 1$$
$$T_{\mathcal{A}^{\mathsf{P}}} = T_{\mathsf{Shipovnik.SigVer}} + \frac{T_{\mathsf{P}}}{p_{\mathsf{P}}}$$
$$\frac{T_{\mathcal{A}^{\mathsf{P}}}}{p_{\mathcal{A}^{\mathsf{P}}}} = T_{\mathsf{Shipovnik.SigVer}} + 2^{347} \cdot T_{\mathsf{hash}}$$





Алгоритм P решает задачу FSPA.

Алгоритм $\mathcal{A}^{\mathrm{P}}(y,(m,\zeta))$
Вход: $y \in \{0,1\}^n$ — открытый ключ, (m,ζ) — корректная пара (сообщение, подпись).
Выход: (m',ζ) — новая корректная пара (сообщение, подпись), $m \neq m'$.



$\mathcal{A}^{\mathrm{P}}(y, (m, c_0 || \ldots || c_{\delta-1} || r_0 || \ldots || r_{\delta-1}))$

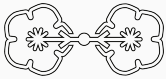
---

1 : $b \leftarrow h'(m || c_0 || \ldots || c_{\delta-1})$

2 : $m' \leftarrow\!\!\$\ P(b, c_0 || \ldots || c_{\delta-1})$

3 : $\mathbf{return}\ (m', c_0 || \ldots || c_{\delta-1} || r_0 || \ldots || r_{\delta-1})$

Атака в модели с известными сообщениями



$$\mathcal{A}^{\mathsf{P}}(y, (m, c_0 \| \ldots \| c_{\delta-1} \| r_0 \| \ldots \| r_{\delta-1}))$$

1 : $b \leftarrow h'(m \| c_0 \| \ldots \| c_{\delta-1})$

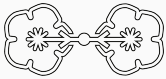
2 : $m' \leftarrow\!\!\$\ P(b, c_0 \| \ldots \| c_{\delta-1})$

3 : $\mathbf{return}\ (m', c_0 \| \ldots \| c_{\delta-1} \| r_0 \| \ldots \| r_{\delta-1})$

При одной известной паре (сообщение, подпись):

$$p_{\mathsf{P}} = 2^{-347}$$
$$T_{\mathsf{P}} = T_{\mathsf{hash}}$$
$$\frac{T_{\mathsf{P}}}{p_{\mathsf{P}}} = 2^{347} \cdot T_{\mathsf{hash}}$$

$$p_{\mathcal{A}^{\mathsf{P}}} = 1$$
$$T_{\mathcal{A}^{\mathsf{P}}} = \frac{T_{\mathsf{P}}}{p_{\mathsf{P}}}$$
$$\frac{T_{\mathcal{A}^{\mathsf{P}}}}{p_{\mathcal{A}^{\mathsf{P}}}} = 2^{347} \cdot T_{\mathsf{hash}}$$



$$\mathcal{A}^{\mathsf{P}}(y, (m, c_0 \| \dots \| c_{\delta-1} \| r_0 \| \dots \| r_{\delta-1}))$$

1 : $b \leftarrow h'(m \| c_0 \| \dots \| c_{\delta-1})$

2 : $m' \leftarrow\!\!\$\ P(b, c_0 \| \dots \| c_{\delta-1})$

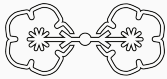
3 : $\mathbf{return}\ (m', c_0 \| \dots \| c_{\delta-1} \| r_0 \| \dots \| r_{\delta-1})$

Если известно не более 2^{219} таких пар:

$$p_{\mathsf{P}} = 2^{-128}$$
$$T_{\mathsf{P}} = T_{\mathsf{hash}}$$
$$\frac{T_{\mathsf{P}}}{p_{\mathsf{P}}} = T_{\mathsf{hash}} \cdot 2^{128}$$

$$p_{\mathcal{A}^{\mathsf{P}}} = 1$$
$$T_{\mathcal{A}^{\mathsf{P}}} = \frac{T_{\mathsf{P}}}{p_{\mathsf{P}}}$$
$$\frac{T_{\mathcal{A}^{\mathsf{P}}}}{p_{\mathcal{A}^{\mathsf{P}}}} \geqslant 2^{128} \cdot T_{\mathsf{hash}}$$

Атаки на основе поиска второго прообраза троичной хэш-функции h'

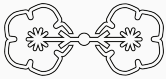


Задача $\mathrm{FSSPA}(m, c)$ [Fixed Suffix Second-Preimage Attack]:
Дано: хэш-функция h', строки $m \in \{0,1\}^*$ и $c \in \{0,1\}^{1536 \cdot \delta}$.
Найти: сообщение $m', m' \neq m$ такое, что $h'(m'||c) = h'(m||c)$.

Алгоритм P решает задачу FSSPA.

Алгоритм $\mathcal{A}^{\mathrm{P}}(y, (m, \zeta))$
Вход: $y \in \{0,1\}^n$ — открытый ключ, (m, ζ) — корректная пара (сообщение, подпись).
Выход: (m', ζ) — новая корректная пара (сообщение, подпись), $m' \neq m$.

Атака в модели с известными сообщениями

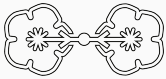


$\mathcal{A}^{P}(y, (m, c_0 || \ldots || c_{\delta-1} || r_0 || \ldots || r_{\delta-1}))$

1 : $m' \leftarrow\$ P(m, c_0 || \ldots || c_{\delta-1})$

2 : **return** $(m', c_0 || \ldots || c_{\delta-1} || r_0 || \ldots || r_{\delta-1})$

Атака в модели с известными сообщениями



$\mathcal{A}^{\mathsf{P}}(y, (m, c_0 || \ldots || c_{\delta-1} || r_0 || \ldots || r_{\delta-1}))$

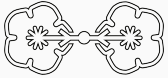
1 : $m' \leftarrow\!\$\ P(m, c_0 || \ldots || c_{\delta-1})$

2 : **return** $(m', c_0 || \ldots || c_{\delta-1} || r_0 || \ldots || r_{\delta-1})$

При одном известном сообщении:

$$p_{\mathsf{P}} = 2^{-347}$$
$$T_{\mathsf{P}} = 2T_{\mathsf{hash}}$$
$$\frac{T_{\mathsf{P}}}{p_{\mathsf{P}}} = 2^{348} \cdot T_{\mathsf{hash}}$$

$$p_{\mathcal{A}^{\mathsf{P}}} = 1$$
$$T_{\mathcal{A}^{\mathsf{P}}} = \frac{T_{\mathsf{P}}}{p_{\mathsf{P}}}$$
$$\frac{T_{\mathcal{A}^{\mathsf{P}}}}{p_{\mathcal{A}^{\mathsf{P}}}} = 2^{348} \cdot T_{\mathsf{hash}}$$



$$\mathcal{A}^{\mathsf{P}}(y, (m, c_0 \| \ldots \| c_{\delta-1} \| r_0 \| \ldots \| r_{\delta-1}))$$

1 : $m' \leftarrow\!\$\ P(m, c_0 \| \ldots \| c_{\delta-1})$

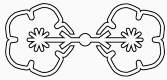
2 : **return** $(m', c_0 \| \ldots \| c_{\delta-1} \| r_0 \| \ldots \| r_{\delta-1})$

Если известно не более 2^{220} сообщений:

$$p_{\mathsf{P}} = 2^{-128}$$
$$T_{\mathsf{P}} = T_{\mathsf{hash}}$$
$$\frac{T_{\mathsf{P}}}{p_{\mathsf{P}}} = 2^{128} \cdot T_{\mathsf{hash}}$$

$$p_{\mathcal{A}^{\mathsf{P}}} = 1$$
$$T_{\mathcal{A}^{\mathsf{P}}} = \frac{T_{\mathsf{P}}}{p_{\mathsf{P}}}$$
$$\frac{T_{\mathcal{A}^{\mathsf{P}}}}{p_{\mathcal{A}^{\mathsf{P}}}} \geqslant 2^{128} \cdot T_{\mathsf{hash}}$$

Атаки на основе поиска коллизии хэш-функции h



Задача $\mathrm{CColl}(H, y)$ [Conditional Collision Attack]:
Дано: хэш-функция h, $(n-k) \times n$-матрица H и строка $y \in \{0,1\}^{n-k}$.
Найти: перестановку $\sigma \in S_n$ и строки $u \in \{0,1\}^n, t \in \{0,1\}^n : \mathrm{wt}(t) = \omega$ такие, что выполняется условие:

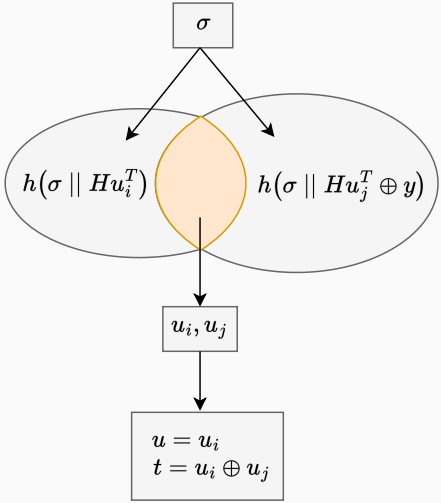
$$h(\sigma || Hu^T) = h(\sigma || H(u \oplus t)^T \oplus y).$$

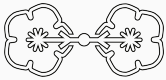
Алгоритм P решает задачу CColl.

Атака в модели без известных сообщений

Алгоритм P ищет σ, u, t, т.ч.
$h(\sigma||Hu^T) = h(\sigma||H(u \oplus t)^T \oplus y)$.

$p_P = 0.63$
$T_P = 2^{256} \cdot T_{\text{hash}}$
$\frac{T_P}{p_P} = 2^{257} \cdot T_{\text{hash}}$
(парадокс дней рождения)



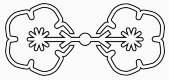


Алгоритм $\mathcal{A}^{\mathrm{P}}(y)$

Вход: $y \in \{0,1\}^n$ — открытый ключ.

Выход: (m, ζ) — корректная пара (сообщение, подпись).

Атака в модели без известных сообщений



$\mathcal{A}^{\mathsf{P}}(y)$

$\sigma, u, t \leftarrow\$\ \mathsf{P}(H, y)$

foreach $0 \leqslant i < \delta$:

$c_{i,0} = h(\sigma \| Hu^T)$

$c_{i,1} = h(\sigma(u))$

$c_{i,2} = h(\sigma(u \oplus t))$

$c \leftarrow c_0 \| \ldots \| c_{\delta-1}$

$b \leftarrow h'(m \| c)$

foreach $0 \leqslant i < \delta$:

if $b_i = 0$: $r_i \leftarrow \sigma \| u$

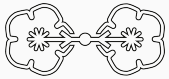
if $b_i = 1$: $r_i \leftarrow \sigma \| (u \oplus t)$

if $b_i = 2$: $r_i \leftarrow \sigma(u) \| \sigma(t)$

$r \leftarrow r_0 \| \ldots \| r_{\delta-1}$

return $c \| r$

Т.е. $\mathcal{A}^{\mathsf{P}}$ подставляет в Shipovnik.SigGen выход P вместо случайных σ_i и u_i, а также t вместо секрета s.



Shipovnik.SigVer$(y, m, (c\|r))$

$b \leftarrow h'(m\|c)$

foreach $0 \leqslant i < \delta$:

if $\left[b_i = 0\right] \wedge \left[\left[c_{i,0} \neq h(r_{i,0}\|Hr_{i,1}^T)\right] \vee \left[c_{i,1} \neq h(r_{i,0}(r_{i,1}))\right]\right]$:

return 0

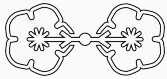
if $\left[b_i = 1\right] \wedge \left[\left[c_{i,0} \neq h(r_{i,0}\|(Hr_{i,1}^T \oplus y))\right] \vee \left[c_{i,2} \neq h(r_{i,0}(r_{i,1}))\right]\right]$:

return 0

if $\left[b_i = 2\right] \wedge \left[\left[c_{i,1} \neq h(r_{i,0})\right] \vee \left[c_{i,2} \neq h(r_{i,0} \oplus r_{i,1})\right] \vee \left[\mathrm{wt}(r_{i,1}) \neq \omega\right]\right]$:

return 0

return 1



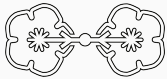
Решение задачи

$$\mathrm{CColl}(H, y) : h(\sigma_i \| H u_i^T) = h(\sigma_i \| H(u_i \oplus t_i)^T \oplus y)$$

пройдет проверку $c_{i,0} = h(r_{i,0} \| (H r_{i,1}^T \oplus y))$.

$$p_{\mathcal{A}^{\mathrm{P}}} = 1$$
$$T_{\mathcal{A}^{\mathrm{P}}} = T_{\mathsf{Shipovnik.SigGen}} + \frac{T_{\mathrm{P}}}{p_{\mathrm{P}}}$$
$$\frac{T_{\mathcal{A}^{\mathrm{P}}}}{p_{\mathcal{A}^{\mathrm{P}}}} = T_{\mathsf{Shipovnik.SigGen}} + 2^{257} \cdot T_{\mathsf{hash}}$$

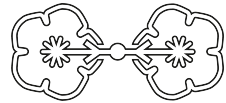
Стойкость схемы «Шиповник»



Параметры «Шиповника» гарантируют стойкость:

- 70 бит (на основе доказуемой стойкости)
- 128 бит (на основе классических атак)

Ни одна из рассмотренных атак не снижает стойкость схемы!



СПАСИБО ЗА ВНИМАНИЕ!

Высоцкая Виктория
v.vysotskaya@kryptonite.ru

Дас Диана
d.das@kryptonite.ru