КРИПТОНИТ

Схема постквантовой электронной подписи на основе протокола идентификации Штерна

Конференция «РусКрипто»

Высоцкая Виктория, Чижов Иван

25 марта 2021 г.

Введение

Термины и определения

Определение
Пусть $r, n \in \mathbb{N}$, $r < n$ и H — двоичная $(r \times n)$-матрица полного ранга. Тогда кодом $\mathcal{C}$ над полем из двух элементов называется множество векторов $c \in \{0,1\}^n$, кодовых слов, удовлетворяющих уравнению

$$Hc^T = 0.$$

При этом матрица H называется проверочной матрицей кода $\mathcal{C}$, n — длиной кода, r — числом проверочных символов кода, $k = n - r$ — размерностью кода.

Определение
Минимальный вес Хэмминга ненулевых кодовых слов $\mathcal{C}$ называется кодовым расстоянием ω, т.е.

$$\omega = \min_{c \in \mathcal{C}, c \neq 0} \mathrm{wt}(c).$$

Термины и определения

Определение

Пусть H — проверочная $(r \times n)$-матрица кода $\mathcal{C}$, а $y \in \{0,1\}^n$ — произвольный вектор. Тогда синдромом вектора y называется вектор $S(y) \in \{0,1\}^r$:

$$S(y) = y \cdot H^T.$$

Определение (задача распознавания)
Пусть H — проверочная $(r \times n)$-матрица кода $\mathcal{C}$, $s \in \{0,1\}^r$ — произвольный вектор и t — натуральное число. Тогда задачей синдромного декодирования $SD(H,s,t)$ называется задача проверки существования вектора $y \in \{0,1\}^n$, для которого выполнены условия

$$S(y) = s, \mathrm{wt}(y) = t. \tag{1}$$

Определение (задача поиска)

Задача синдромного декодирования $SD^\star(H,s,t)$ заключается в поиске вектора y, удовлетворяющего условиям (1).

Теорема
Задача $SD(H,s,t)$ является NP-полной. Задача $SD^\star(H,s,t)$ является NP-трудной[1].

[1] Berlekamp E., McEliece R., van Tilborg H. «On the inherent intractability of certain coding problems (Corresp.)» IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 384–386, 1978.

Схема идентификации

Схема идентификации Штерна[2]

Системные параметры:

n	—	длина кода,
k	—	размерность кода,
ω	—	кодовое расстояние,
$H \in \{0,1\}^{(n-k)\times n}$	—	проверочная матрица,
$h(\cdot) : \{0,1\}^* \to \{0,1\}^{\ell}$	—	хэш-функция,
$f(\cdot) : \{0,1\}^* \to \{0,1,2\}^{\delta}$	—	хэш-функция,
λ	—	параметр стойкости,
δ	—	параметр, зависящий от параметра стойкости.

[2] Stern J. «A new identification scheme based on syndrome decoding». Stinson D.R. (eds) Advances in Cryptology — CRYPTO' 93. CRYPTO 1993. Lecture Notes in Computer Science, vol. 773, pp. 13-21, 1994.

P

V

$u \in_R \{0,1\}^n,\ \sigma \in_R S_n,$
$c_0 := h\left(\sigma \| Hu^T\right),$
$c_1 := h(\sigma(u)),$
$c_2 := h(\sigma(u \oplus s)).$

c_0, c_1, c_2

$b \in_R \{0,1,2\}.$

b

$(r_0, r_1) := (\sigma, u),\ b = 0;$
$(r_0, r_1) := (\sigma, u \oplus s),\ b = 1;$
$(r_0, r_1) := (\sigma(u),\ \sigma(s)),\ b = 2.$

r_0, r_1

$s \in_R \{0,1\}^n : \mathrm{wt}(s) = \omega;$
$y^T = Hs^T;$
(s, y) –(секр.кл., откр.кл.)

Выполняет проверки:
$b = 0 :\ c_0 = h\left(r_0 \| Hr_1^T\right),\ c_1 = h(r_0(r_1));$
$b = 1 :\ c_0 = h\left(r_0 \| Hr_1^T \oplus y\right),\ c_2 = h(r_0(r_1));$
$b = 2 :\ c_1 = h(r_0),\ c_2 = h(r_0 \oplus r_1),\ \mathrm{wt}(r_1) = \omega.$

Вероятность подделки

Противник не знает секретный ключ!

P $b \neq 1$ V

$u \in_R \{0,1\}^n,\ \sigma \in_R S_n,$
$t \in_R \{0,1\}^n : \mathrm{wt}(t) = \omega,$
$c_0 := h\left(\sigma \| Hu^T\right),$
$c_1 := h(\sigma(u)),$
$c_2 := h(\sigma(u \oplus t)).$

c_0, c_1, c_2 →

$b \in_R \{0,1,2\}.$

← b

$(r_0, r_1) := (\sigma, u),\ b = 0;$
~~$(r_0, r_1) := (\sigma, u \oplus s),\ b = 1;$~~
$(r_0, r_1) := (\sigma(u),\ \sigma(t)),\ b = 2.$

r_0, r_1 →

Выполняет проверки:
$b = 0 :\ c_0 = h\left(r_0 \| Hr_1^T\right),\ c_1 = h(r_0(r_1));$
~~$b = 1 :\ c_0 = h\left(r_0 \| Hr_1^T \oplus y\right),\ c_2 = h(r_0(r_1));$~~
$b = 2 :\ c_1 = h(r_0),\ c_2 = h(r_0 \oplus r_1),\ \mathrm{wt}(r_1) = \omega.$

Противник не знает секретный ключ!

P $b \neq 1$ V

$u \in_R \{0,1\}^n,\ \sigma \in_R S_n,$
$t \in_R \{0,1\}^n : \mathrm{wt}(t) = \omega,$
$c_0 := h\left(\sigma \| Hu^T\right),$
$c_1 := h(\sigma(u)),$
$c_2 := h(\sigma(u \oplus t)).$

c_0, c_1, c_2 →

$b \in_R \{0,1,2\}.$

← b

$(r_0, r_1) := (\sigma, u),\ b = 0;$
~~$(r_0, r_1) := (\sigma, u \oplus s),\ b = 1;$~~
$(r_0, r_1) := (\sigma(u),\ \sigma(t)),\ b = 2.$

r_0, r_1 →

Вероятность успеха 2/3

Выполняет проверки:
$b = 0 :\ c_0 = h\left(r_0 \| Hr_1^T\right),\ c_1 = h(r_0(r_1));$
~~$b = 1 :\ c_0 = h\left(r_0 \| Hr_1^T \oplus y\right),\ c_2 = h(r_0(r_1));$~~
$b = 2 :\ c_1 = h(r_0),\ c_2 = h(r_0 \oplus r_1),\ \mathrm{wt}(r_1) = \omega.$

Аналогично он может поступить в предположении $b \neq 0$ и $b \neq 2$.

Аналогично он может поступить в предположении $b \neq 0$ и $b \neq 2$.

При любой стратегии вероятность успеха противника — $2/3$.

Аналогично он может поступить в предположении $b \neq 0$ и $b \neq 2$.

При любой стратегии вероятность успеха противника — $2/3$.

Что делать?

Аналогично он может поступить в предположении $b \neq 0$ и $b \neq 2$.

При любой стратегии вероятность успеха противника — $2/3$.

Что делать?

Повторять схему на одной паре ключей много раз!

Аналогично он может поступить в предположении $b \neq 0$ и $b \neq 2$.

При любой стратегии вероятность успеха противника — $2/3$.

Что делать?

Повторять схему на одной паре ключей много раз!

Повторяем δ раз. Тогда вероятность успеха противника $\leqslant \left(\frac{2}{3}\right)^{\delta}$.

Схема подписи

Преобразование Фиата-Шамира

(Fiat A., Shamir A., CRYPTO' 86.)

P (подписывает) V (проверяет)

$u^i \in_R \{0,1\}^n,\ \sigma^i \in_R S_n,$
$c_0^i := h\left(\sigma \| Hu^T\right),$
$c_1^i := h(\sigma(u)),$
$c_2^i := h(\sigma(u \oplus s)).$

δ

c_0, c_1, c_2 →

$b \in_R \{0,1,2\}.$

b ←

$b = f\left(m \| c_0^0 \| c_1^0 \| c_2^0 \| \ldots \| c_2^{\delta-1}\right).$

$(r_0^i, r_1^i) := (\sigma^i, u^i),\ b_i = 0;$
$(r_0^i, r_1^i) := (\sigma^i, u^i \oplus s^i),\ b_i = 1;$
$(r_0^i, r_1^i) := (\sigma^i(u^i),\ \sigma^i(s^i)),\ b_i = 2.$

δ

r_0, r_1 →

$c_0^0 \| c_1^0 \| c_2^0 \| \ldots \| c_2^{\delta-1} \| r_0^0 \| r_1^0 \| \ldots \| r_1^{\delta-1}$

$s \in_R \{0,1\}^n : \mathrm{wt}(s) = \omega;$
$y^T = Hs^T;$
(s, y) –(секр.кл., откр.кл.)

$b = f\left(m \| c_0^0 \| c_1^0 \| c_2^0 \| \ldots \| c_2^{\delta-1}\right).$
Выполняет проверки:

δ
$b_i = 0 :\ c_0^i = h\left(r_0^i \| Hr_1^{iT}\right),\ c_1 = h\left(r_0^i(r_1^i)\right);$
$b_i = 1 :\ c_0^i = h\left(r_0^i \| Hr_1^{iT} \oplus y\right),\ c_2 = h\left(r_0^i(r_1^i)\right);$
$b_i = 2 :\ c_1^i = h\left(r_0^i\right),\ c_2 = h\left(r_0^i \oplus r_1^i\right),\ \mathrm{wt}\left(r_1^i\right) = \omega.$

Параметры схемы

- Для заданного λ выбираем δ из условия $\left(\frac{2}{3}\right)^{\delta} < 2^{-\lambda}$.

[3] May A., Ozerov I. «On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes». Advances in Cryptology – EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science, vol. 9056, pp. 203–228, 2015.

- Для заданного λ выбираем δ из условия $\left(\frac{2}{3}\right)^{\delta} < 2^{-\lambda}$.
- Оценка лучшего известного алгоритма решения задачи синдромного декодирования есть $O(2^{0.0966n})$ битовых операций[3].

[3] May A., Ozerov I. «On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes». Advances in Cryptology – EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science, vol. 9056, pp. 203–228, 2015.

- Для заданного λ выбираем δ из условия $\left(\frac{2}{3}\right)^{\delta} < 2^{-\lambda}$.
- Оценка лучшего известного алгоритма решения задачи синдромного декодирования есть $O(2^{0.0966n})$ битовых операций[3].
- Граница Варшамова–Гилберта:

$$\frac{k}{n} \leqslant 1 - H\left(\frac{\omega}{n}\right),$$

где $H(x) = -x\log(x) - (1-x)\log(1-x)$.

[3] May A., Ozerov I. «On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes». Advances in Cryptology – EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science, vol. 9056, pp. 203–228, 2015.

- Для заданного λ выбираем δ из условия $\left(\frac{2}{3}\right)^{\delta} < 2^{-\lambda}$.
- Оценка лучшего известного алгоритма решения задачи синдромного декодирования есть $O(2^{0.0966n})$ битовых операций[3].
- Граница Варшамова–Гилберта:

$$\frac{k}{n} \leqslant 1 - H\left(\frac{\omega}{n}\right),$$

  где $H(x) = -x\log(x) - (1-x)\log(1-x)$.
- $k = \left\lceil \frac{n}{2} \right\rceil$ и $\omega \approx 0,11n$.

[3] May A., Ozerov I. «On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes». Advances in Cryptology – EUROCRYPT 2015. EUROCRYPT 2015. Lecture Notes in Computer Science, vol. 9056, pp. 203–228, 2015.

λ	n	k	ω	δ	откр. дан., МБ	разм. подп., МБ	время выч., мс	время пров., мс
128	1326	663	146	219	0.05	0.43	15.90	15.53
256	2651	1326	292	438	0.21	1.79	33.68	31.20
512	5301	2651	538	876	0.84	7.56	105.96	100.06

Таблица 1: Параметры схемы без учёта результатов доказуемой стойкости

λ	n	k	ω	δ	откр. дан., МБ	разм. подп., МБ	время выч., мс	время пров., мс
128	4841	2421	533	219	0.70	1.75	32.50	31.15
256	8841	4421	973	438	2.33	6.78	98.52	93.60
512	16818	8409	1850	876	8.43	27.43	391.03	372.29

Таблица 2: Параметры схемы с учётом результатов доказуемой стойкости

(время приведено для сообщения размера 1МБ)

Схема подписи CFS[4]

$\mathcal{C}$ — (n, k, d)-код, принадлежащий заданному классу и имеющий эффективный алгоритм декодирования Dec_H.

Алгоритм формирования подписи:

1. Выбрать случайное i.
2. Декодировать: $x = Dec_H(\cdots h(h(m)||i))$. В случае неуспеха вернуться на Шаг 1.
3. ...

[4] Courtois N., Finiasz M., Sendrier N. «How to achieve a McEliece-based digital signature scheme». Advances in Cryptology — ASIACRYPT 2001. ASIACRYPT 2001. Lecture Notes in Computer Science, vol. 2248, pp. 157–174, 2001.

	Штерн		Штерн + стойк.		CFS (Гоппа)	
λ	откр. дан., Мб	разм. подп., МБ	откр. дан., МБ	разм. подп., МБ	откр. дан.	разм. подп., бит
80	0.02	0.17	0.33	0.72	1.37 МБ	178
128	0.05	0.43	0.70	1.75	143 МБ	289
256	0.21	1.79	2.33	6.78	155 ГБ	623

	Штерн		Штерн + стойк.		CFS (Гоппа)	
λ	время выч., мс	время пров., мс	время выч., мс	время пров., мс	время выч.	время пров., нс
80	12.69	12.54	19.59	19.00	3.51 с	1.89
128	15.90	15.53	32.50	31.15	28.06 мин	3.63
256	33.68	31.20	98.52	93.60	$\approx$ 90 000 лет	12.11

Спасибо за внимание!

Высоцкая Виктория, v.vysotskaya@kryptonite.ru

Чижов Иван, i.chizhov@kryptonite.ru