

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 С называется кодовым расстоянием ω, т.е.

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

1



Определение

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

$$S(y) = s, wt(y) = t.$$
 (1)

Определение (задача поиска)

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

Теорема

Задача SD(H,s,t) является NP-полной. Задача $SD^*(H,s,t)$ является NP-трудной¹.

¹Berlekamp 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.

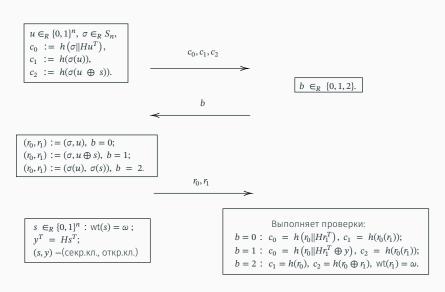
Схема идентификации

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.

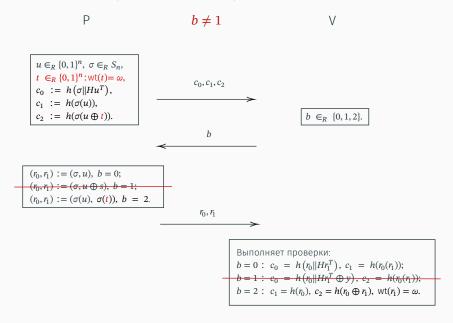
²Stern J. «A new identification scheme based on syndrome decoding». Stinson D.R. (eds) Advances in Cryptology — CRYPTO' 93. CRYPTO 1993. Lecture Notes in Computer Science, vol. 773, pp. 13-21, 1994.

P

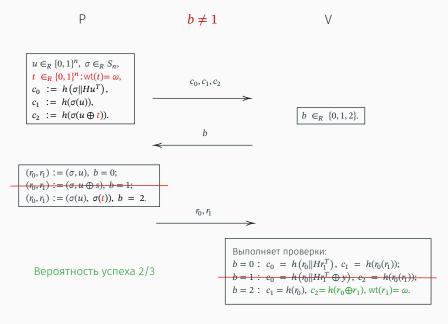


Вероятность подделки

Противник не знает секретный ключ!



Противник не знает секретный ключ!



При любой стратегии вероятность успеха противника -2/3.

При любой стратегии вероятность успеха противника -2/3.

Что делать?

При любой стратегии вероятность успеха противника -2/3.

Что делать?

Повторять схему на одной паре ключей много раз!

При любой стратегии вероятность успеха противника -2/3.

Что делать?

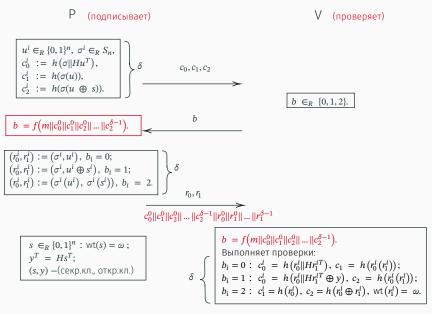
Повторять схему на одной паре ключей много раз!

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.)



Параметры схемы

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

³May 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 операций³.

³May 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 операций³.
- Граница Варшамова-Гилберта:

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

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

³May 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 операций³.
- Граница Варшамова-Гилберта:

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

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

$$\cdot k = \left[\frac{n}{2}\right] \cup \omega \approx 0,11n.$$

³May 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.

				откр.	разм.	время	время	
λ	n	k	ω	δ	дан.,	подп.,	выч.,	пров.,
					МБ	МБ	MC	MC
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

					откр.	разм.	время	время
λ	n	k	ω	δ	дан.,	подп.,	выч.,	пров.,
					МБ	МБ	MC	MC
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 CFS⁴

 $\mathcal{C}-(n,k,d)$ -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. ...

⁴Courtois 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	I + СТОЙК.	CFS (Гоппа)	
	откр.	разм.	откр.	разм.	OTVD	разм.
λ	дан.,	подп.,	дан.,	подп.,	откр. дан.	подп.,
	Мб	МБ	МБ	МБ	дап.	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

	Шт	ерн	Штерн + стойк.		CFS (Гоппа)	
	время	время	время	время	ррома	время
λ	выч.,	пров.,	выч.,	пров.,	время выч.	пров.,
	MC	MC	МС	MC	выч.	НС
80	12.69	12.54	19.59	19.00	3.51 c	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	≈ 90 000 лет	12.11

Спасибо за внимание!

Высоцкая Виктория, v.vysotskaya@kryptonite.ru Чижов Иван, i.chizhov@kryptonite.ru