СРАВНИТЕЛЬНЫЙ АНАЛИЗ АСИММЕТРИЧНЫХ АЛГОРИТМОВ NTRU, RSA И ECC

Бубырь А.П., Заросилова М.Г.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, 14, каф. Безопасности информационных технологий,
тел. (057) 702-14-25
E-mail: bubir@datasvit.net

This work is devoted to a comparative analysis of lattice-based public key algorithm NTRU and systems based on integer factorization (RSA) and the elliptic curve discrete log problem (ECC). Durability and speed of encryption/decryption operations were assessed. Conclusions about the advantages and disadvantages of the discussed cryptographic algorithms are given.

Большинство наиболее значимой информации на сегодняшний день передается с помощью глобальной сети Интернет, например: электронные письма, сообщения чатов, видеоконференции, данные электронной коммерции и онлайн-банкинга.

Использование криптосистем с открытым ключом — основной способ защиты таких данных. Наиболее широкое применение получили криптосистема RSA, основанная на сложности факторизации больших чисел, схема Диффи-Хеллмана, DSA, стойкость которых базируется на сложности решения задачи дискретного логарифмирования в поле, семейство алгоритмов на основе эллиптических кривых. Но все они имеют определенные недостатки, основные из которых — это либо сравнительно невысокая скорость работы (напр., алгоритмы на базе ЭК), либо сравнительно низкая стойкость при сопоставимых размерах ключей и параметров (схема Диффи-Хеллмана и другие алгоритмы, основанные на дискретном логарифме в поле), либо и то, и другое одновременно (RSA).

Решить проблему низкой скорости шифрования при сохранении высокого уровня стойкости призван алгоритм NTRU, который был разработан в середине 1990-х годов и впервые представлен на конференции CRYPTO'96. В 2008 году он был включен в стандарт IEEE 1363.1 «Lattice-based public-key cryptography», а модифицированная версия данного алгоритма была взята за основу стандарта ANSI X9.98-2010 «Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry». В этом алгоритме все операции производятся в кольце усечённых многочленов. Криптографическая стойкость NTRU основана на сложности задачи нахождения короткого вектора в заданной решётке.

Цель данной работы — сравнить скорость и стойкость NTRU и криптосистем на основе дискретного логарифма в группе точек ЭК и факторизации целых чисел (RSA).

Для упрощения сравнения стойкости различных алгоритмов стандартом X9.98 введены 4 обширных класса стойкости: «112 бит», «128 бит», «192 бита», «256 бит». Данные уровни стойкости отображают минимальную сложность атаки «грубая сила» - от 2^{112} до 2^{256} операций. Для различных алгоритмов с каждым из этих уровней связаны соответствующая минимальная длина ключа и размеры параметров.

Следующая таблица сравнивает размеры ключей для NTRU с эквивалентными размерами ключей для систем, основанных на проблемах факторизации целых чисел и дискретного логарифма в группе точек эллиптических кривых. Используются следующие обозначения:

- *IPub* - длина открытого ключа в битах
- *IPri* — длина личного ключа в битах

Для NTRU и систем, основанных на проблеме факторизации целых чисел (IF) размер шифротекста равен размеру открытого ключа.

Для систем, основанных на проблеме дискретного логарифма в группе точек эллиптических кривых (ECDL) размер шифротекста отличается в зависимости от схемы шифрования. Например, онлайновый 1-проходный протокол MQV из X9.63-2001 требует три передачи сообщений, при этом каждое сообщение имеет длину, равную длине откры-

того ключа. Оффлайновая 1-проходная схема транспортировки ключа из X9.63 требует одной передачи сообщения размером примерно в *IPub + 2k* бит.

Таблица 1. Сравнение размеров ключей для NTRU и других алгоритмов с открытым ключом

Уровень стойкости *k*, бит	NTRU		RSA	Эллиптические кривые
	IPub	*IPri*	*IPub, IPri*	*IPub, IPri*
112	4411	802	2048	224
	5951	980		
	7249	760		
128	4939	898	3072	256
	6743	1100		
	8371	840		
192	7183	1306	7680	384
	9757	1620		
	11957	1386		
256	9383	1706	15360	512
	12881	2332		
	16489	1738		

Таким образом, NTRU имеет все необходимые условия для обеспечения наивысшего уровня стойкости и по этому показателю не отстает от конкурентов.

Все криптографические системы, основанные на проблемах факторизации целых чисел, дискретного логарифма и дискретного логарифма в группе точек эллиптических кривых потенциально уязвимы к разработке квантового компьютера соответствующего размера, так как для такого компьютера известны алгоритмы, которые могут решить эти проблемы за полиномиальное время, зависящее от размера входных данных. Для NTRU на данный момент квантовых алгоритмов с полиномиальной сложностью не существует. В [2] предлагается квантовый алгоритм редукции в решетках, который может улучшить скорости редукции, но он остается экспоненциальным по сложности, а в [3] рассматриваются алгоритмы для некоторых проблем, связанных с решетками, которые, возможно, будут иметь субэкспоненциальную сложность. Следовательно, только криптосистемы, основанные на алгебраических решетках, остаются практически неуязвимыми для квантового криптоанализа.

Одним из главных преимуществ алгоритма NTRU также является очень высокая скорость выполнения операций зашифрования/расшифрования. По заявлениям компании Security Innovation, занимающейся разработкой NTRU, данный алгоритм до двухсот раз быстрее, чем алгоритмы на эллиптических кривых и RSA и при этом его реализация гораздо меньше (около 8 Кб). В таблице 2 приводятся сравнительные результаты измерений скорости NTRU, ЭК и RSA, полученные этой компанией (использовался процессор с тактовой частотой 2 ГГц).

Таблица 2. Сравнение скорости NTRU, RSA и ЭК, предложенное компанией-разработчиком

Уровень стойкости	Операций/секунда		
	NTRU	ЭК	RSA
112	10638	951	156
128	9901	650	12
192	6849	285	8
256	5000	116	1

В результате собственных измерений быстродействия реализации NTRU на платформе Java было установлено, что для набора параметров ees1499ep1 из X9.98 средняя скорость зашифрования составила 5,4 Мбайт/с, а расшифрования — 5,1 Мбайт/с.

Группой бельгийских ученых [4] были изучены возможности распараллеливания алгоритмов NTRU, RSA и ECC-NIST-224. Скорость работы данных алгоритмов была замерена как на ЦПУ, так и на графических процессорах с использованием технологии распараллеливания CUDA от Nvidia.

Таблица 3. Сравнение скорости реализаций NTRU, RSA и ЭК для ЦПУ и ГПУ

Алгоритм	Язык и платформа	Параметры алгоритма	Зашифр/с	Расшифр/с	Бит/опер.
NTRU	C , Intel Core2 Extreme @ 3.00GHz	(N, q, p) = (1171, 2048, 3) (k = 256)	95	95	1756
	CUDA , GTX280 (1 операция)		571	546	
	CUDA , GTX280 (20000 операций параллельно)		$24*10^3$	$24*10^3$	
RSA	CUDA, Nvidia 8800GTS	2048 bit (k = 112)	-	104	2048
	C++, Intel Core2 @ 1.83GHz		$(6,66*10^3)$	168	
ЭК	CUDA, Nvidia 8800GTS	ECC-NIST-224 (k = 112)	-	$1,41*10^3$	
	C, Intel Core2 @ 1.83 GHz (ECDSA)		-	$1,86*10^3$	

В таблице 3 приведено сравнение реализаций NTRU с использованием ЦПУ и ГПУ и некоторых реализаций RSA и EC. Следует заметить, что количество данных, шифруемых за одну операцию, различно. Для приложений, которым необходима высокая пропускная способность, реализация с помощью CUDA превосходит все остальные реализа-

ции (принимая параметры более высокого уровня безопасности и большее число данных). Данная реализация способна выполнять более 200 тыс. операций зашифрования в секунду или 41,8 Мбайт/с. Для приложений, которым требуется небольшое число шифрований с малой задержкой, распараллеливание с помощью CUDA работает не так быстро по сравнению с реализацией на ЦПУ.

Скорость работы NTRU гораздо выше, чем RSA и EC: он в 1300 раз быстрее 2048-битного RSA и в 117 раз быстрее ECC NIST-224 (если сравнивать количество операций в секунду), или в 1113 раз быстрее, чем 2048-битный RSA (если сравнивать пропускную способность).

Исходя из данных, имеющихся на текущий момент, можно сделать промежуточные выводы о высоком уровне стойкости NTRU, который не уступает стойкости алгоритмов на базе эллиптических кривых, а в некоторых аспектах и превосходит его (устойчивость NTRU к квантовому криптоанализу). Но в связи с относительной новизной и малой распространенностью асимметричных алгоритмов такого класса необходимо проводить дополнительные исследования на предмет возможных закладок и критических уязвимостей, которые могут быть использованы для разработки эффективных атак.

В результате анализа быстродействия NTRU было установлено, что его скорость работы гораздо выше, чем у RSA и ЭК. Наилучшие результаты производительности NTRU показал при его реализации на платформе CUDA, так как он очень хорошо поддается распараллеливанию, в отличие от RSA, попытки распараллелить который практически не дают прироста скорости. При сравнений скоростей NTRU, RSA и ECC с параметрами, соответствующими уровню стойкости k = 256 бит NTRU на 4 порядка быстрее RSA и на 3 порядка быстрее ECC. Также следует отметить меньший размер реализации NTRU (порядка 8 Кб), что очень важно для мобильных и встраиваемых систем, поэтому NTRU относят к алгоритмам «легковесной криптографии».

Класс асимметричных алгоритмов, основанных на проблемах в алгебраических решетках, по совокупности всех показателей значительно превосходит другие алгоритмы с открытым ключом. Поэтому именно NTRU во многих сферах должен прийти на смену RSA и ECC и стать таким же общепринятым стандартом асимметричной криптографии, каким стал AES в сфере блочного шифрования.

Литература:

1. American National Standard for Financial Services ANSI X9.98-2010 Lattice Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry .

2. C. Ludwig: A Faster Lattice Reduction Method Using Quantum Search, TU-Darmstadt Cryptography and Computeralgebra Technical Report No. TI-3/03, revised version published in Proc. of ISAAC 2003

3. Tsukiji Tatsuie, Kamiyama Hiroaki, "Efficient algorithm for the unique shortest lattice vector problem using quantum oracle?", IEIC Technical Report (Institute of Electronics, Information and Communication Engineers), VOL.101;NO.44(COMP2001 5-12);PAGE.9-16(2001).

4. Jens Hermans, Frederik Vercauteren, Bart Preneel. Speed records for NTRU. Department of Electrical Engineering, University of Leuven Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium