УДК 004.056.55

студентка О.В.Червоная, к.ф.-м.н., проф. С.А. Сушко
ГВУЗ «Национальный горный университет»

ПРО КРИПТОАЛГОРИТМ NTRU

Рассмотрена идея и структура асимметричного криптоалгоритма NTRU, указаны его достоинства и недостатки. Проведено сравнение с широко применяемым алгоритмом RSA. Описаны алгоритмы действий для шифрования и дешифрования сообщений.

Асимметричный криптоалгоритм NTRU (Nth-degree TRUncated polynomial ring или просто Number Theorists aRe Us) разработан в середине 1990-х годов и впервые представлен на конференции CRYPTO'96. В этом алгоритме все операции производятся в кольце усечённых многочленов. Криптосистема NTRU основана на алгебраической структуре кольца усеченных многочленов. Трудноразрешимой задачей является поиск кратчайшего вектора в заданной решетке. Процедуры шифрования/дешифрования основаны на смешанных операциях: алгебре многочленов и приведении по модулю двух чисел. NTRU работает быстрее, чем используемые в настоящее время криптосистемы с открытым ключом. Так исследования, проведенные криптологами из Лёвенского католического университета (Бельгия), показали, что при тестировании с максимальными настройками безопасности NTRU на четыре порядка быстрее RSA и на три порядка быстрее ECC [1].

Для шифрования и дешифрования сообщения из N символов необходимо $O(N^2)$ операций для алгоритма NTRU, в то время как для RSA требуется $O(N^3)$ операций. Хотя в NTRU зашифрованное сообщение больше открытого текста примерно в 4,5 раза, криптостойкость NTRU-167 (с параметром n = 167) примерно соответствует RSA-512. Стойкость NTRU-263 и NTRU-503 сопоставима со стойкостью RSA-1024 и RSA-2048 соответственно. При этом при использовании NTRU-263 длина открытого ключа равняется 1841 биту, а секретного — 834 бита. Кроме того, решетчатая конструкция NTRU позволяет этой криптосистеме потенциально лучше противостоять компьютерным атакам «квантового типа» (атакам с использованием квантовых компьютеров).

Различные реализации NTRU характеризуются тремя целыми числами – n, p и q. Числа p и q не обязательно должны быть простыми, но обязательно взаимно простыми. Если Боб хочет создать пару «закрытый - открытый ключ»,

он случайно выбирает многочлены $f, g \in R$, где R – кольцо усечённых многочленов. Многочлен f должен иметь обратный многочлен по модулю p и q, в противном случае выбирается другой многочлен. Далее Боб должен вычислить обратные многочлены f_p^{-1} и f_q^{-1} по модулю p и q. Секретным ключом будет пара f, f_p^{-1}, а открытым ключом $h = p \cdot f_q^{-1} \otimes g \pmod{q}$

Если Алиса хочет отправить сообщение Бобу, используя его открытый ключ h, ей необходимо преобразовать сообщение к виду многочлена m, коэффициенты которого взяты по модулю p [2]. Далее дополнительно произвольно выбрать многочлен r. Используя эти параметры, зашифровать сообщение: $e = r \otimes h + m \pmod{q}$ и отправить Бобу.

Для дешифровки Боб вычисляет $a = f \otimes e \pmod{q}$, используя известный только ему многочлен f, и восстанавливает открытый текст, вычислив $m = f_p^{-1} \otimes a \pmod{p}$.

Рассмотрим, почему при дешифровании получается исходное сообщение:

$$a = f \otimes e \pmod{q} = f \otimes r \otimes h + f \otimes m \pmod{q} = f \otimes r \otimes pf_q^{-1} \otimes g + f \otimes m \pmod{q} =$$

$$= pr \otimes g + f \otimes m \pmod{q}$$

$$m = f_p^{-1} \otimes a \pmod{p} = f_p^{-1} \otimes pr \otimes g + f_p^{-1} \otimes f \otimes m \pmod{p}$$

Из процедуры дешифрования видно, что криптосистема NTRU является вероятностной, поэтому из шифрованного текста открытый текст не всегда восстанавливается правильно. Корректный выбор многочленов f, g, r позволяет снизить вероятность такой ошибки до 2^{-100}.

Какие же преимущества и недостатки можно увидеть от перехода на NTRU уже сейчас? Преимуществ несколько: большая скорость работы и небольшое, но увеличение стойкости при фактически той же длине ключа, что и в RSA. Минус пока один – необходимость использования только рекомендованных параметров. Именно такое же требование вызывало всеобщее недовольство во время перехода на эллиптические кривые и способствовало всяческим подозрениям о наличии тайных лазеек, облегчающих в дальнейшем конструкторам шифра криптоанализ.

Таблица 1. Рекомендуемые параметры для NTRU [3]

	n	p	q	кол-во единиц в многочленах		
				f	g	r
NTRU 167:3	167	3	128	61	20	18
NTRU 251:3	251	3	128	50	24	16
NTRU 503:3	503	3	256	216	72	55
NTRU 167:2	167	2	127	45	35	18
NTRU 251:2	251	2	127	35	35	22
NTRU 503:2	503	2	253	155	100	65

Перечень литературы:

1. http://en.wikipedia.org/wiki/NTRUEncrypt
2. http://habrahabr.ru/blogs/crypto/118458/
3. http://habrahabr.ru/blogs/crypto/127878/