ИСПОЛЬЗОВАНИЕ NTRUENCRYPT КРИПТОСИСТЕМЫ В КАЧЕСТВЕ АЛЬТЕРНАТИВЫ RSA

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Разумов Е.В.

Ярмолик В. Н. – д-р. техн. наук, профессор

При передаче конфиденциальной информации по сети следует особое внимание уделять защите этой информации от злоумышленников. Одним из возможных способов защиты информации является ее шифрование асимметричным алгоритмом. В настоящее время наиболее распространенным алгоритмом, применяемым для данных целей, является алгоритм RSA. Однако в последнее время все чаще начинает подыматься вопрос о его замене.

Рассмотрим криптосистему NTRUEncrypt и ее преимущества и недостатки перед криптосистемой RSA.

NTRUEncrypt был разработан в 1996 году. Он основан на решетчатой криптосистеме, в которой используются операции над кольцом усеченных многочленов степени, не превосходящей N-1. Стойкость алгоритма обеспечивается трудностью нахождения кратчайшего вектора в заданной числовой решетке, что в свою очередь делает этот алгоритм также более устойчивым к атакам на квантовых компьютерах. При этом данная криптосистема может использоваться в устройствах с ограниченными ресурсами, что делает ее еще более привлекательной для использования в будущем.

NTRU использует три постоянных параметра: N, p, q. Числом N характеризуется размер выбираемых в качестве ключей многочленов. Числа p и q не обязательно должны быть простыми, но НОД(p,q) должен равняться 1. После выбора этих трех основных параметров нужно будет выбрать еще три дополнительных, которые принято обозначать d_f, d_g, d. Эти три параметра служат для определения набора следующих многочленов: $L_f=L(d_f, d_f-1)$, $L_g=L(d_g, d_g)$, $L_r=L(d, d)$.

Для процессов шифрования/расшифровки необходимо сгенерировать пару секретный/открытый ключ. Открытый ключ будет использоваться для шифрования, а секретный в свою очередь – для расшифровки. Алгоритм генерация пары ключей следующий:

1. Из набора L_f выбирается произвольный многочлен f(x);
2. Из набора Lg выбирается многочлен g(x);
3. Вычисляются многочлены $f_q(x)$ и $f_p(x)$ такие что $f_p(x)*f(x)=1 \bmod p$ и $f_q(x)*f(x)=1 \bmod q$;
4. Открытый ключ определяется как $h(x)=f_q(x)*g(x) \bmod q$;
5. Секретный ключ это пара $(f(x),f_p(x))$.

Шифрование происходит по следующему алгоритму: $C(x)=p*r(x)*h(x)+M(x) \bmod q$.

Алгоритм расшифровки:

1. Вычисляется $a(x)=f(x)*C(x) \bmod q$;
2. Вычисляется $b(x)=a(x) \bmod p$;
3. Вычисляется $M= b(x)* f_p(x) \bmod p$ – это и есть исходное сообщение.

Если сравнивать NTRUEncrypt и RSA, то можно выделить несколько преимуществ рассматриваемой криптосистемы:

1. NTRU имеет большую скорость работы. Выполнение операций шифрования/расшифровки требует $O(n^2)$ операций, в отличие от $O(n^3)$ у RSA.
2. Небольшое, но увеличение стойкости при фактически такой же длине ключа, что отображено в следующей таблице:

RSA-1024	1012 MIPS-years
NTRUEncrypt N=263	1014 MIPS-years
RSA 2048	1021 MIPS-years
RSA 4096	1033 MIPS-years
NTRUEncrypt N=503	1035 MIPS-years

Приблизительная оценка времени взлома криптосистем RSA и NTRU

Стоит также отметить, что самой затратной операцией данного алгоритма является операция умножения элементов кольца. Возможным решением этой проблемы может стать использование Chinese Remainder Theorem для замены операций умножения на операции сложения при небольших значениях параметра p.

Список использованных источников:

1. Е. А. Киршанова Анализ структуру и стойкости криптосистемы NTRU. - М.: СОЛОН-Пресс, 2002. - 272с.
2. J. Hoffstein, J. Pipper, and J. H. Silverman, “NTRU: A Ring Based Public Key Cryptosystem”, in Proc. of Algorithmic Number Theory: Third International Symposium (ANTS 3) (J. P. Buhler, ed.), vol. LNCS 1423, Springer-Verlag, June 21-25 1998, pp. 267-288.
3. J. Hoffstein, J. Pipper, and J. H. Silverman, “NTRU: A New High Speed Public Key Cryptosystem”, Preprint, presented at the rump session of Crypto 1996. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Claredon, 1892, pp. 68-73