УДК 519.7

П.С. Стафийчук, О.Н. Товма

Харьковский национальный университет радиоэлектроники, Харьков

АНАЛИЗ И СРАВНЕНИЕ СВОЙСТВ КЛЮЧЕВЫХ ДАННЫХ СИСТЕМЫ NTRUSIGN

В статье рассматривается алгоритм цифровой подписи, основанный на теории решеток, анализируются и сравниваются параметры и ключевые данные криптоалгоритма NTRUSign, рассматриваются математические свойства ключевых и общесистемных параметров алгоритма. Выполнено сравнение свойств ключевых и общесистемных параметров системы NTRUSign и популярной криптографической системы с открытым ключом RSA с точки зрения производительности и надежности. Приведены результаты сравнения быстродействия генерации ключей для NTRUSign и RSA.

Ключевые слова: *NTRUSign, RSA, алгоритм, генерация, свойства.*

Введение

В последнее время активно разрабатываются алгоритмы и стандарты криптосистем, основанных на математических задачах теории решеток, которые отличаются от предыдущих стандартов тем, что обеспечивают более высокий уровень стойкости при меньшей вычислительной сложности криптографических преобразований.

При реализации криптографических систем одним из наиболее критических моментов является увеличение уровня стойкости. Этот вопрос напрямую связан со свойствами методов и алгоритмов, которые используются для формирования криптографических параметров и ключевых данных.

Формирование криптографически стойких ключевых параметров и ключей обычно требует значительных вычислительных ресурсов, поэтому важными вопросами являются теоретические и экспериментальные исследования методов и алгоритмов их генерации.

Основная часть

В этом разделе рассматривается алгоритм NTRUSign: примитивы генерации случайного базиса и ключевой пары.

1. Алгоритм NTRUSign

Алгоритм был впервые представлен в 2001 году Хофстейном(Hoffstein), Пифер(Pipher) и Сильверманом (Silverman). Полная спецификация была опубликована в 2003 году в работе [2].

NTRUsign – это первая эффективная реализация алгоритма цифровой подписи, основанная на сложности задач теории решеток [3].

Алгоритм NTRUSign использует следующие параметры, описанные ниже.

1.1 Степень NTRUSign

Степень *N* определяет размерность сверточного кольца многочленов. Поскольку параметр N определен как степень NTRUSign, элементы кольца представлены как полиномы степени N–1.

1.2 Большой модуль NTRUSign

Большой модуль q определяет кольцо многочленов, которое используется в NTRUSign – коэффициенты полиномов приводятся по модулю q. Для увеличения производительности рекомендуется выбирать q как степень 2.

1.3 Пространство секретного ключа NTRUSign

Секретный ключ NTRUSign состоит из четырех полиномов (f,g,F,G). Полиномы f и g уникальным образом определяют секретный ключ. В общем случае, из четырех полиномов (f,g,F,G), только два необходимы для генерации подписи сообщения. Обозначим эти два полинома как (f, $f^{|}$). В зависимости от типа базиса, $f^{|}$ может равняться F (в случае со стандартным базисом) или g (в случае с транспонированным базисом).

Остальные два полинома (компонента секретного ключа), которые не используются в генерации подписи, могут быть уничтожены после генерации ключевых параметров.

В общем случае, полином f может быть выбран как небольшой полином такой, что f имеет обратный в $(Z/qZ)[X](X^N–1)$. Однако, для увеличения производительности, f должен выбираться из D_f – пространства всех полиномов степени N–1, которые имеют d_f коэффициентов, равных 1, и остальные коэффициенты равны 0 [1].

В общем случае, компонент секретного ключа g может быть выбран как любой небольшой полином. Однако, для увеличения производительности, g стоит выбирать из пространства D_g всех полиномов степени N–1, которые имеют d_g коэффициентов равных 1 и остальные коэффициенты равны 0.

Как только параметры f и g были выбраны, формирующая базис пара (F,G) вычисляется так, что (f,g) и (F,G) формируют небольшой базис для NTRUSign модуля. Другими словами f*G – F*g = q

и (F,G) небольшой (обычно размера $\sqrt{N/12}$). Пара (F,G) не уникальна для заданных (f,g), но только одна такая пара необходима.

В общем случае, пара (F,G) может быть любой парой, которая формирует базис. Однако, для того чтобы максимизировать вероятность генерации «хорошей» подписи, (F,G) должны быть ограничены пространством D_{FG}, которое состоит из всех векторов, у которых центрированная норма меньше чем параметр безопасности KeyNormBound. Если в процессе генерации пара (F,G) не может быть найдена с центрированной нормой меньше чем KeyNormBound, секретный ключ должен быть отброшен и выбран заново.

1.4 MaxAdjustment

При генерации пары (F,G) возможно уменьшить уменьшить ее центрированную норму путем добавления или вычитания небольших кратных пары секретного ключа (f,g). После нескольких итераций, потери в скорости генерации ключей могут перевесить преимущества, которые дает уменьшение центрированной нормы (F,G). Параметр безопасности MaxAdjustment может быть выбран для ограничения количества итераций алгоритма.

1.5 Тип секретного ключа

Базис NTRUSign – это набор полиномов (f,g,F,G) таких, что f*G – F*g = q. В стандартной NTRU решетке базис состоит из двух векторов (f,g) и (F,G) и всех их покомпонентных вращений. Каждый базис такого типа определяет транспонированный базис (f, F) и (g, G) с детерминантами q. При генерации подписи, использование транспонированного базиса в качестве секретного ключа может значительно повысить производительность в сравнении со стандартным базисом. Однако, если транспонированный базис используется, один компонент подписи будет значительно меньше чем другой, это приведет к раскрытию информации о секретном ключе быстрее, чем в случае со стандартным базисом. По этой причине использование транспонированного базиса рекомендуется только тогда, когда, по крайней мере, был использован один базис пертурбации (искажения).

1.6 Пространство отрытого ключа NTRUSign

Пространство открытого ключа NTRUSign однозначно определяется пространством секретного ключа, поэтому нет необходимости явно описывать как его как параметр. В стандартной решетке пространство открытого ключа D_h состоит из всех полиномов h степени N–1 таких, что $h=f^{-1}*g$ с коэффициентами по модулю q, где f и g выбраны из D_f и D_g, соответственно, и f^{-1} – полином с коэффициентами по модулю q такой, что $f^{-1}*f = f*f^{-1}=1$ в $(Z/qZ)[X](X^N–1)$. В транспонированном базисе, пространство открытого ключа состоит из всех полиномов h степени N–1 таких, что $h=f^{-1}*F \bmod q$.

1.7 Базис пертурбации

Схема цифровой подписи NTRUSign не является схемой с нулевым разглашением, это значит, что информация о секретном ключе может быть получена из подписи сообщения. В некоторых случаях злоумышленник может восстановить секретный ключ, используя некоторое количество подписей сообщений.

Каждое использованное искажение значительно увеличивает количество подписей, которые нужно получить злоумышленнику для успешной атаки на секретный ключ. Количество базисов искажений определяется параметром perturbationBases.

1.8 Устойчивость к ошибкам NTRUSign

В зависимости от размера границы нормы для подписи, примитив подписи иногда может генерировать недопустимые значения подписей с данными параметрами m и r, где m – сообщение, а r – значение рандомизации сообщения. В процессе генерации подписи сообщения может быть выбрано другое значение r для получения другого представления сообщения и другого значения подписи.

2. Опции схемы NTRUSign

Опции схемы состоят из параметров и примитивов, которые не зависят от ключевого пространства, но должны быть согласованны при реализации NTRUSign.

2.1 NTRUSign NormBound

Параметр NormBound определяет, насколько подпись должна быть близка к представлению сообщения для того, чтобы проверка подписи была возможна. Параметр выбирается достаточно малым для предотвращения атак подделки подписи и достаточно большим для того, чтоб подпись лежала ниже границы NormBound.

2.2 Параметр рандомизации сообщения

Алгоритм NTRUSign детерминировано находит достаточно близкую к сообщению точку в решетке. В связи с непредсказуемой природой близких точек в решетке, алгоритм генерации может давать недопустимые значения, не удовлетворяющие значению NormBound. Параметр рандомизации сообщения r используется для генерации другого представления сообщения, которое не удовлетворяет значению NormBound.

2.3 Константа генерации случайных полиномов

В процессе генерации полиномов с помощью генератора псевдослучайных чисел, например, в методе генерации представления сообщения, необходимо выбрать количество выходных бит, которое будет использовано для вычисления следующего полинома. Константа c – это значение, которое выбирается для генерации полинома с помощью генератора псевдослучайных чисел и представляет количество бит, которое используется для генерации вводного значения mod N.

3. Генерация ключевой пары

В процессе генерации ключевой пары для NTRUSign необходимо генерировать случайные базисы. Ниже представлен алгоритм генерации случайного базиса и на его основе алгоритм генерации ключей.

3.1 Алгоритм генерации случайного базиса

Вход: параметры домена N, q, безопасности df, dg, MaxAdjustment.

Выход: базис (f, g, F, G).

1. Случайно выбирается полином f степени N – 1 с коэффициентами df = 1, остальные равны 0.

2. Случайно выбираются полином g степени N – 1 коэффициентами dg = 1, остальные равны 0.

3. Если 2N + 1 простое:

a. Установить resf1 та resg1 равными результанту f и g (mod 2N + 1)

b. Если resf1 и resg1 равняются 0, перейти к шагу 1.

4. Установить целые числа resf равные результанту f и установить полином rhof, который удовлетворяет уравнению rhof*f = resf в $Z[X]/(X^N – 1)$.

5. Установить целое resg, равное результанту g и установить полином rhog, которые удовлетворяет уравнению rhog*g := resg в $Z[X]/(X^N – 1)$.

6. Вычислить целые alpha, beta и gcd =gcd(resf,resg) такие, что alpha*resf + beta*resg=gcd.

7. Если gcd ≠1, перейти к шагу 1.

8. Вычислить полином f^{-1} такой, что $f^{-1}*f = f*f^{-1}=1$ в $(Z/qZ)[X]/(X^N – 1)$. Если не существует f^{-1} перейти к шагу 1.

9. Установить полином F:= –rhog*beta*q в $Z[X]/(X^N – 1)$.

10. Установить полином G:= rhof*alpha*q в $Z[X]/(X^N – 1)$.

11. Пусть frev полином степени N – 1 такой, что $frev_0 = f_0$ and $frev_i = f_{N-i}$ для $1 \le i \le N – 1$.

12. Пусть grev полином степени N – 1 такой, $grev_0$ = что g_0 и $grev_i = g_{N-i}$ для $1 \le i \le N – 1$.

13. Установить полином t := f*frev + g*grev в $Z[X]/(X^N – 1)$.

14. Установить целое число rest, равное результанту t и восстановить полином rhot в соответствии с rhot*t:= rest in $Z[X]/(X^N – 1)$.

15. Установить полином c := rhot*(frev*F + + grev*G) в $Z[X]/(X^N – 1)$.

16. Установить целые числа i := 0, j := 0, k := 0.

17. While j < N do

a. Установить c_j := floor[c_j/rest + .5].

b. Установить j := j + 1.

18. Установить F := F – c*f в $Z[X]/(X^N – 1)$.

19. Установить G := G – c*g в $Z[X]/(X^N – 1)$.

20. (необязательно) Установить целые D := 0, E:= 0.

21. (необязательно) Установить полиномы u := f, v:=g.

22. (необязательно) Установить j := 0.

23. (необязательно) While j < N do

a. Установить E := E + 2*N*($f_j^2 + g_j^2$)

b. Установить j := j + 1.

24. (необязательно) Установить E := E – (f(1) + g(1))^2.

25. (необязательно) Установить j := 0.

26. (необязательно) While k < MaxAdjustment and j < N do:

a. Установить D := 0

b. While i < N do

i. Установить D := D + 4*N*($F_i*f_i + G_i*g_i$)

ii. Установить i := i + 1

c. Установить D := D – 2*(F(1) + G(1))*(f(1) + g(1))

d. If D > E

i. Установить F := F – u в $Z[X]/(X^N – 1)$

ii. Установить G := G – v в $Z[X]/(X^N – 1)$

iii. Установить k := k + 1

iv. Установить j := 0

e. Else, if D < –E

i. Установить F := F + u в $Z[X]/(X^N – 1)$

ii. Установить G := G + v в $Z[X]/(X^N – 1)$

iii. Установить k := k + 1

iv. Установить j := 0

f. Установить j := j + 1

g. Установить u := u*X в $Z[X]/(X^N – 1)$

h. Установить v := v*X в $Z[X]/(X^N – 1)$

27. Выход f, g, F, G.

3.2 Алгоритм генерации ключевой пары

Вход: N, q, Df, Dg, DFG, perturbationBases, basisType, KeyNormBound, MaxAdjustment.

Выход**:** Секретный ключ (f, f'i) и базис искривления (fi, f'i, hi), открытый ключ h.

1. Установить i = perturbationBases.

2. While i≥0:

a. Сгенерировать базис (f_i, g_i, F_i, G_i)

b. Если basisType = "standard", установить $f'_i = F_i$.

Если basisType = "transpose", установить $f'_i = g_i$. Установить $h_i = f_{i-1}*f'_i$ mod q.

c. Установить i = i–1.

3. Открытый ключ h_0. Секретный ключ – набор из (f_i, f'_i, h_i) для $0 \le i \le$ perturbationBases.

4. Сравнение характеристик ключевых параметров

Поскольку система RSA является наиболее популярной и широко используемой среди криптографических систем с открытым ключом, сравнение выполнено именно с этой криптографической системой. Результаты сравнения приведены в табл. 1.

Стойкость схемы с данной длиной ключа приведена в MIPS – лет, необходимых для взлома.

На рис. 1 изображен график отношения времени генерации ключевых параметров и длины секретного ключа для NTRUSign и RSA.

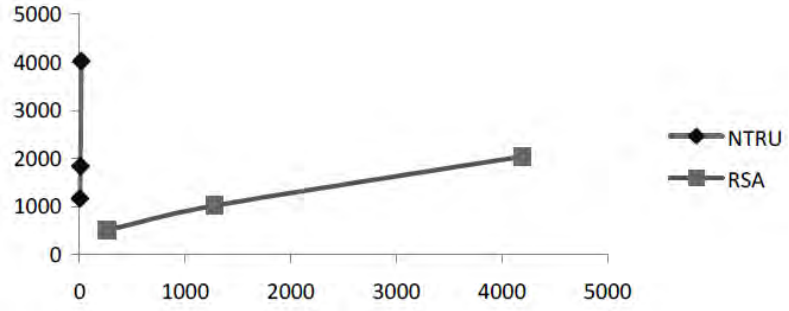

Рис. 1. График зависимости длины ключа от времени генерации

Таблица 1

Сравнение времени, затраченного на генерацию ключевых данных систем NTRUSign и RSA

Алгоритм	MIPS-лет	Длина ключа, бит	Время генерации ключей, мс
RSA signature	$4*10^5$	512	260
	$3*10^{12}$	1024	1280
	$3*10^{21}$	2048	4195
NTRUSign	$2*10^6$	1169	4
	$4{,}6*10^{14}$	1841	7.5
	$3.4*10^{35}$	4024	17.3

Выводы

Все существующие криптографические системы, основанные на проблемах факторизации, дискретного логарифма или дискретного логарифма в группе точек эллиптической кривой, потенциально уязвимы к криптоанализу с помощью квантовых алгоритмов, например, алгоритма Шора.

Из приведенных результатов можно сделать вывод, что система NTRUSign обладает такими преимуществами как быстродействие и криптографическая стойкость по сравнению с существующими криптографическими системами с открытым ключом. Главным отличием данной криптографической системы является отсутствие успешных попыток криптоанализа с помощью квантового компьютера. Таким образом, можно утверждать, что система NTRUSign является перспективной для предоставления услуг информационной безопасности.

Список литературы

1. Silverman J.H. Dimension-Reduced Lattices, Zero-Forced Lattices, and the NTRU Public Key Cryptosystem, NTRU Cryptosystems Technical Report 13 / Joseph H. Silverman. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ntru.com.

2. Silverman J.H. Estimating Decryption Failure Probabilities for NTRUEncrypt / J.H. Silverman, W. Whyte // Technical Report #18.

3. Hoffstein J. NTRU: A new high speed public key cryptosystem / J. Hoffstein, J. Pipher, J.H. Silverman // Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, Lecture Notes in Computer Science 1423 (J.P. Buhler, ed.), Springer-Verlag, Berlin, 1998. – P. 267-288.

4. Lidl R. Applied Abstract Algebra / R. Lidl, G.Pilz. – Spring-Verlag,Berlin, 1984.

Поступила в редколлегию 18.05.2012

Рецензент: д-р техн. наук, проф. Е.П. Путятин, Харьковский национальный университет радиоэлектроники, Харьков.

АНАЛІЗ ТА ПОРІВНЯННЯ ВЛАСТИВОСТЕЙ КЛЮЧОВИХ ДАНИХ СИСТЕМИ NTRUSIGN

П.С. Стафійчук, О.М. Товма

У статті розглядається алгоритм цифрового підпису, заснований на теорії решіток, аналізуються та порівнюються параметри та ключові дані криптоалгоритму NTRUSign, розглядаються математичні властивості ключових та загальносистемних параметрів алгоритму. Виконано порівняння властивостей ключових та загальносистемних параметрів системи NTRUSign та відомої криптографічної системи з відкритим ключем RSA. Надані результати порівняння швидкодії генерування ключів для NTRUSign і RSA.

Ключові слова: *NTRUSign, RSA, алгоритм, генерація, властивості.*

ANALYSIS AND COMPARISON OF NTRUSIGN CRYPTOGRAPHIC ALGORITHM PROPERTIES

P.S. Stafiychuk, O.N. Tovma

The given work deals with new family digital signature schemes based on solving approximate closest vector problem in NTRU-type lattices. The paper considers the cryptographic algorithm parameters and their properties, discusses the mathematical properties of the keys and algorithm parameters. The comparison of the properties of key parameters and system parameters NTRUSign and popular cryptographic system with public key RSA. Results of comparing the speed of key generation for NTRUSign and RSA is given.

Keywords: *NTRUSign, RSA, generation, properties.*