УДК 004.056.55

О.В. Бочаров

Харківський національний університет радіоелектроніки, Харків

ДОСЛІДЖЕННЯ АЛГОРИТМУ ШИФРУВАННЯ NTRU

Об'єктом дослідження є алгоритм шифрування із відкритим ключем NTRU (Nth-degree TRUncated polynomial ring). Наводиться коротка історія розвитку алгоритму, опис його реалізації з точки зору виконуваних математичних операцій. Велика увага приділяється значимості алгоритму у сучасному комп'ютерному світі. Розглянуті найбільш відомі методи криптографічних атак. Сформульовані переваги алгоритму, що роблять його фаворитом серед асиметричних алгоритмів.

Ключові слова: *шифрування, алгоритм NTRU, публічний ключ, факторизація, продуктивність.*

Вступ

Постановка проблеми та аналіз останніх досліджень. Проблема захисту інформації шляхом перетворень, що виключають її прочитання сторонньою особою, хвилювала людство з давніх часів. Криптографія історично зародилася з потреби передачі секретної інформації. В даний час у зв'язку з бурхливим розвитком міжнародної глобальної мережі Internet і масовим застосуванням комп'ютерних інформаційних технологій, криптографія вирішує важливі завдання по збереженню конфіденційності даних, захисту від зловмисницьких повідомлень, контролю цілісності інформації.

Поряд із розвитком криптографічних систем удосконалювалися і методи, що дозволяють відновлювати початкове повідомлення, виходячи з шифротексту та іншої відомої інформації, тобто методи злому.

Стійким вважається той алгоритм, який для свого розкриття вимагає від противника практично недосяжних обчислювальних ресурсів, або недосяжного обсягу перехоплених зашифрованих повідомлень, або часу розкриття, який перевищує час життя.

Але оскільки методики злому шифрів безперервно удосконалюються, потрібно бути готовим до адекватної відповіді зловмисникам. Збільшення довжини ключа є одним з найбільш радикальних методів протистояння спробам злому. Чим довше ключ, чим більша кількість комбінацій випадкових значень в ньому, тим більше часу знадобиться зловмисникові на перебір варіантів. Співвідношення між довжиною ключа і кількістю можливих комбінацій носить експоненціальний характер (подовження ключа на один біт подвоює кількість можливих комбінацій значень ключа і таким чином, в середньому подвоює час на відшукання потрібного значення перебором). Подвоєння ж довжини ключа значно збільшує ступінь захисту повідомлення.

Проте постійне збільшення довжини ключа призводить до збільшення часу, необхідного для шифрування і дешифрування повідомлень. А даний критерій також є безсумнівно важливим. Наприклад, щоб досягти досить високої криптостійкости, алгоритму RSA знадобиться виповняти перемножування між числами з бітністю, рівною 1024. Це величезні числа і подібні операції є надзвичайно витратними за часом та необхідними для виконання ресурсами. Ця проблема особливо актуальна у наш час розвитку мобільних технологій, коли мобільні пристрої хоч і мають потужну апаратну складову, але все ж обмежені у потужностях.

Однією з останніх розробок в області алгоритмів шифрування даних є алгоритм NTRU. На відміну від RSA він не отримав широкого розповсюдження, тому що з самого початку потрібно було підвищити стійкість і продуктивність цього шифру. Зараз всі недоліки виправлені і на практиці NTRU вже вважається набагато швидшим, ніж RSA. Алгоритм заснований на операціях множення поліномів, на відміну від множення величезних чисел. Менша обчислювальна складність у купі з більшою стійкістю при однаковій довжині ключа робить алгоритм NTRU кандидатом на застосовування в майбутньому в будь-яких сферах, що вимагають шифрування даних – від звичайних користувацьких до банківських та урядових.

Метою статті є опис алгоритму NTRU, його переваг у порівнянні до інших алгоритмів асиметричного шифрування.

Виклад основного матеріалу

Криптосистема NTRU, що заснована на решітчастій криптосистемі, була створена як альтернатива RSA та криптосистемам на еліптичних кривих

(ECC). Стійкість алгоритму забезпечується складністю пошуку найкоротшого вектора решітки, котра є більш стійкою до атак, що здійснюються на квантових комп'ютерах. На відміну від своїх конкурентів RSA, ECC, Elgamal, алгоритм використовує операції над кільцем $\frac{Z|X|}{\left(X^N-1\right)}$ усічених многочленів степені, що не перевищує N – 1

$$a(X) = a = a_0 + a_1X + a_2X^2 + \\ +... + A_{N-2}X^{N-2} + a_{N-1}X^{N-1}.$$

Алгоритм NTRU є відносно новою криптосистемою. Перша версія була розроблена приблизно у 1996 році трьома математиками – Хоффшейном, Пифером та Сильверманом. У 1996 році ці математики разом із Девидом Лиманом заснували корпорацію «NTRU Cryptosystems» та отримали патент на криптосистеми. На перших порах криптосистема інколи давала збій при розшифруванні повідомлення назад у оригінальне навіть коли повідомлення було зашифроване правильно. Але протягом останніх десяти років люди працювали над вдосконаленням криптосистеми. Після першої презентації системи деякі зміни були зроблені для покращення продуктивності системи та її безпеки. Більшість покращень продуктивності були зосереджені на прискоренні процесу, аніж на вирішенні проблеми із неправильною дешифровкою. У літературі до 2005 року можна знайти приклади, де описуються невдачі при розшифруванні повідомлень за допомогою NTRU. Що стосується безпеки, починаючи с першої версії NTRU, нові параметри були введені, що забезпечують безпеку для усіх відомих на сьогоднішній день атак і непогане збільшення обчислювальної потужності.

Завдяки швидкості роботи та низькому споживанню пам'яті NTRU може використовуватися у мобільних пристроях чи смарт-картах. Криптологи із Бельгійського університету встановили, що при тестуванні із максимальними налаштуваннями безпеки NTRU на 4 порядки швидше RSA та на 3 порядки швидше ECC. У квітні 2011 року американський комітет «Accredited Standarts Committee X9» затвердив використання алгоритму NTRU у фінансових додатках. Виконавчий директор компанії «Security Innovation» Ед Адамс говорить, що в майбутньому правильно спроектований квантовий комп'ютер буде мати змогу зламати і RSA і системи на еліптичних кривих. Доки ще невідомо, чи можливо зібрати такий комп'ютер на практиці, але фінансові установи можуть перелякатися і вже зараз почати міграцію на новий стандарт.

Розглянемо принципи роботи алгоритму. Для передачі повідомленні від сторони А стороні В необхідні відкритий та закритий ключі. Відкритий знає і сторона В і сторона А, закритий знає тільки сторона В і використовує його для генерації відкритого ключа. Для цього сторона В вибирає два «маленьких» полінома f та g із R. «Малість» поліномів мається на увазі в тому сенсі, що він маленький відносно довільного поліному по модулю q – у довільному поліномі коефіцієнти повинні бути приблизно рівномірно розподілені по модулю q, а в малому поліномі вони набагато менші q. Малість поліномів визначається за допомогою чисел df і dg:

– поліном f має df коефіцієнтів, що дорівнюють 1, і df–1 коефіцієнтів, що дорівнюють -1, інші дорівнюють 0. У цьому випадку кажуть, що $f \in A_f$;

– поліном g має dg коефіцієнтів, що дорівнюють 1, і стільки же, що дорівнюють -1, інші дорівнюють 0. У цьому випадку кажуть, що $g \in A_g$.

Причина, по якій поліноми вибираються саме таким чином полягає в тому, що f, можливо, буде мати зворотній, а g – однозначно ні (g(1) = 0, а нульовий елемент не має зворотнього).

Сторона В повинна зберігати ці поліноми у секреті. Далі сторона В рахує зворотні поліноми F_p і F_q, тобто такі, що $f * f_p \equiv 1 (\mathrm{mod}\, p)$ і $f * f_q \equiv 1 (\mathrm{mod}\, q)$.

Якщо f не має зворотнього поліному, то сторона В обирає інший поліном f.

Секретний ключ – це пара (f, f_p), а відкритий ключ h обчислюється за формулою $h = (pf_q * g) \bmod q$.

Тепер, коли у сторони А є відкритий ключ, вона може відправити зашифроване повідомлення стороні В. Для цього потрібно представити повідомлення у вигляді поліному m з коефіцієнтами по модулю p, вибраними з діапазону $\left(-\frac{p}{2}, \frac{p}{2}\right]$. Тобто m є «малим» поліномом по модулю q. Далі стороні А необхідно обрати інший «малий» поліном r, що визначається за допомогою числа dr. Поліном r має dr коефіцієнтів, що дорівнюють 1, і стільки ж, рівних -1, інші дорівнюють 0. У цьому випадку кажуть, що $r \in A_r$.

Використовуючи ці поліноми, зашифроване повідомлення отримуємо по формулі $e = (r * h + m) \bmod q$. При цьому кожен, хто знає чи може обчислити поліном r, матиме змогу прочитати повідомлення m.

Тепер, отримавши зашифроване повідомлення e, сторона В може його розшифрувати, використовуючи свій секретний ключ. Спочатку треба отримати проміжний поліном $a = (f * e) \bmod q$. Якщо розписати шифротекст, то отримаємо наступний ланцюг

$$a = (f*e) \bmod q = (f*(r*h+m)) \bmod q =$$
$$= (f*(r*pf_q*g+m)) \bmod q,$$

і в результаті $a = (pr*g+f*m) \bmod q$.

Після того, як сторона B обчислила поліном a по модулю q, потрібно вибрати його коефіцієнти із діапазону $\left(-\frac{q}{2}, \frac{q}{2}\right]$ і далі обчислити поліном b, що отримуємо із поліному a приведенням по модулю p: $b = a \bmod p = (f*m) \bmod p$, так як $(pr*g) \bmod p = 0$.

Тепер, використовуючи другу частину секретного ключа і отриманий поліном b, сторона B може розшифрувати повідомлення: $c - (f_p * b) \bmod p$.

Нескладно побачити, що $c \equiv f_p * f * m \equiv m (\bmod p)$. Таким чином, отриманий поліном c дійсно є вихідним повідомленням m.

Говорячи про методи атак на алгоритм NTRU, треба відмітити наступні найбільш розповсюджені:

– атака повним перебором. Можливо декілька варіантів перебору: або перебирати усі $f \in A_f$ і перевіряти на малість коефіцієнти отриманих результатів $f*h(\bmod q) = g(\bmod q)$, які повинні бути малими, або перебирати усі $g \in A_g$, також перевіряючи на малість коефіцієнти результату $f(\bmod q) = f*h*h^{-1}(\bmod q) =$ $= f*f_q*g*h^{-1}(\bmod q) = g*h^{-1}(\bmod q)$. На практиці простір A_g менше простору A_f, тому стійкість визначається простором A_g. А стійкість окремого повідомлення визначається простором Ar.

– зустріч посередині. Цей метод був запропонований Андрю Одлижко. Він зменшує кількість варіантів до квадратного кореню.

Стійкість закритого ключа дорівнює

$$\sqrt{A_g} = \frac{1}{d_g!}\sqrt{\frac{N!}{(N-2d_g)}},$$

стійкість окремого повідомлення –

$$\sqrt{A_r} = \frac{1}{d!}\sqrt{\frac{N!}{(N-2d)!}}.$$

Атака потребує більше пам'яті для зберігання проміжних результатів.

Таким чином, якщо ми хочемо забезпечити стійкість системи 2^n, треба вибрати ключ розміром 2^{2n}.

Висновки

Таким чином, алгоритм NTRU є дуже обіцяючим алгоритмом асиметричного шифрування. Він має достатню стійкість від злому за допомогою квантового комп'ютеру та більш велику швидкість операцій, аніж у інших алгоритмах асиметричного шифрування. Ці переваги роблять алгоритм актуальним для використання як у мобільних пристроях, так і у фінансовій сфері.

Список літератури

1. Петров А. Компьютерная безопасность. Криптографические методы защиты [Текст] / А. Петров. – М.: ДМК, 2000. – 448 с.

2. NTRU Cryptography [Електронний ресурс] / Security Innovation. – Режим доступу до ресурсу: www/ URL: http://www.securityinnovation.com/products/encryption-libraries/ntru-cryptography.html - 15.01.2012 р. – Загол. з екрану.

3. NTRUEncrypt криптосистема будущего? [Електронний ресурс] / Хабрахабр. – Режим доступу до ресурсу: www/ URL: http://habrahabr.ru/blogs/crypto/127878/ - 14.01.2012 р. – Загол. з екрану.

Надійшла до редколегії 8.05.2012

Рецензент: канд. техн. наук, проф. О.Г. Качко, Харківський національний університет радіоелектроніки, Харків.

ИССЛЕДОВАНИЕ АЛГОРИТМА ШИФРОВАНИЯ NTRU

А.В. Бочаров

Объектом исследования является алгоритм шифрования с открытым ключом NTRU (Nth-degree TRUncated polynomial ring). Приводится короткая история развития алгоритма, описание его реализации с точки зрения используемых математических операций. Большое внимание уделяется значимости алгоритма в современном компьютерном мире. Рассмотрены наиболее известные методы криптографических атак. Сформированы преимущества алгоритма, которые делают его фаворитом среди ассиметричных алгоритмов.

Ключевые слова: *шифрование, алгоритм NTRU, публичный ключ, факторизация, производительность.*

RESEARCH OF NTRU ENCRYPTION ALGORITHM

A.V. Bocharov

The object of research is encryption algorithm with the public key called NTRU (Nth-degree TRUncated polynomial ring). Contains the briefly history of algorithm, description of implementation from the point of used mathematical operations. Big attention is dedicated to significance of the algorithm in the modern computer world. Possible methods of cryptographic attacks were reviewed. Benefits of the algorithm that make it better than the others were described.

Keywords: *encryption, NTRU algorithm, public key, factorization, performance.*