УДК 004.056.55

Кузнецов О.О., Горбенко Юрій, Шевцов О.В., Кузнецова Т.Ю.
Харківський національний університет ім. В.Н. Каразіна

Дослідження криптографічних атак на схеми електронного цифрового підпису в фактор-кільцях зрізаних поліномів

Вступ. Застосування електронних цифрових підписів (ЕЦП) в фактор-кільцях зрізаних поліномів (ФКЗП) дозволить будувати криптопримітиви, які є стійкими до квантового криптоаналізу [1-5]. Однак всі попередні версії ЕЦП в ФКЗП виявилися вразливими до атак, коли атакуючий може нав'язати підроблене повідомлення [1-3]. Тому дослідження умов та можливостей застосування атак підробки підписів є актуальним науковим завданням.

Підпис в фактор-кільцях поліномів NTRUSign є доказово стійким від повного розкриття за умови, що криптоаналітик перехопив тільки одну пару підпис-повідомлення [0]. Проте, у відомій літературі не проаналізовано можливості атаки типу maleability [0] на підпис із пертурбаціями та на схеми із посиленими параметрами, в тому числі, із гаусовським зашумленням [0]. Підписи в ФКЗП потребують більшого обґрунтування захищеності від підробки даного типу.

Математична модель підпису в фактор-кільцях зрізаних поліномів NTRUSign. В алгоритмі NTRUSign [0] базові операції відбуваються в фактор-кільці зрізаних поліномів $K = Z[X]/(X^N - 1)$, де поліном $a(x) \subset K$ може бути представлений вектором його коефіцієнтів наступним чином:

$$a = \sum_{i=0}^{N-1} a_i x^i = (a_0, a_1, ..., a_{N-1}).$$

Визначення 1. Алгебраїчна решітка - дискретна адитивна підгрупа, задана на множині R^N. Решітку L можна представити як множину цілочисельних лінійних комбінацій

$$L(b_1, ...b_N) = \sum_{i=1}^{N} x_i b_i : x_1, ..., x_N \in Z,$$

де N - лінійно незалежних базисних векторів $(\bar{b}_1, ..., \bar{b}_N) \subset R^N$ в N - вимірному просторі, R - множина дійсних чисел.

Ненульовий вектор решітки мінімальної довжини називається її *найкоротшим вектором*.

Визначення 2. Під найкоротшим вектором решітки L будемо розуміти вектор, довжина якого для решітки розмірністю N буде $i-$й послідовний мінімум $\lambda_i(L)$ - найменший радіус кулі, яка містить i лінійно незалежних векторів

$$\lambda_i(L) = r, r \in R : \exists v_i \in L, \max_i \|v_i\| \le r,$$

де v_i - це лінійно незалежні вектори.

Безпека підпису NTRU заснована на важкості вирішення задачі знаходження найкоротших чи найближчих векторів (відповідно, SVP, CVP) в спеціальних NTRU решітках. Іншими словами, нехай U - це базис решітки L. Задача знаходження найкоротшого вектору (задача SVP) полягає в тому, щоб знайти такий вектор $u \in L$, $u \neq 0$, що $\forall v \in L$, $\| u \| \le \| v \|$.

Зауваження 1. Наскільки короткою може бути довжина ненульового вектору в довільній решітці, залежить від таких

властивостей, як розмірність решітки та її детермінант. Так, N-розмірна решітка L має експоненційно багато векторів з нормою $d = \sqrt{N}\det(L)^{1/N}$.

Задача CVP (знаходження найближчого вектору) полягає в знаходженні вектору $v \in L$, який є *найближчим до вектору* w, де $w \in R^N$ та w не знаходиться в L. Треба знайти такий вектор $v \in L$, який мінімізував би Евклідову норму $\| w - v \|$. Вираз $\| w - v \|$ визначає найменшу відстань між векторами w та v, яка обчислюється як Евклідова норма вектору $\| \cdot \|$. Зокрема, Евклідова норма вектору $a = (a_0, a_1, ..., a_{N-1})$ визначає його довжину та обчислюється за формулою:

$$\| a \| = \sqrt{(a_0)^2 + (a_1)^2 + ... + (a_{N-1})^2}.$$

Далі будемо застосовувати поняття *базису мінімальної довжини*.

Визначення 3. *Базис мінімальної довжини* - це базис U решітки L який складається із найкоротших векторів $u_i \in L$, тобто $U = (u_0, u_1, ..., u_{N-1})$ і $\forall v \in L, \forall u_i \in U : \| u_i \| \leq \| v \|$.

Для зручності оцінки довжини векторів будемо розрізняти *великі вектори* $a = (a_0, a_1, ..., a_{N-1})$, коли їх довжина набагато більша за довжину найкоротшого вектору решітки $\forall u_i \in U : \| u_i \| \models \| a \|$.

Аналогічно будемо використовувати поняття *коротких векторів* $a = (a_0, a_1, ..., a_{N-1})$, коли їх норма приблизно дорівнює $\| a \| \approx \sqrt{(N-1)/12}$ [0].

Надалі під *довжиною полінома* $a = \sum_{i=0}^{N-1} a_i x_i$ будемо розуміти довжину відповідного вектору $a = (a_0, a_1, ..., a_{N-1})$, тобто під коротким (великим) поліномом будемо розуміти відповідний короткий (великий) вектор у введених вище позначеннях.

Базис, складений із великих векторів, будемо називати великим базисом.

Визначення 4 [0]. Секретний ключ NTRUSign визначається кортежом поліномів (f, g, F, G), де g, f - це поліноми з коефіцієнтами, вибраними з діапазону {-1,0,1}, f має інверсію в $(Z/qZ)[X]/(X^N - 1)$, q - ціле число та степінь двійки, F, G - короткі поліноми з нормою приблизно $\| F \| = \sqrt{(N-1)/12}$ та $fG - Fg = q$.

Матричне подання називають секретним базисом решітки, який є базисом мінімальної довжини.

Визначення 5 [0]. Відкритий ключ NTRUSign визначається поліномом $h = f^{-1} \cdot g$ з коефіцієнтами з діапазону $[-q/2, q/2]$.

Зауваження 2. Поліном h, що формує *відкритий базис решітки*:

$$\begin{pmatrix} e & h \\ 0 & q \end{pmatrix},$$

де e - одинична матриця.

Підпис можна представити двома визначеннями.

Визначення 6 [0]. Нехай $m = (m_1, m_2)$ - хеш-значення повідомлення (далі просто повідомлення) та $m = m_1 \| m_2$ - дві рівні половини полінома m. Підпис визначається вектором $(s, t) \in L$, котрий знаходиться близько до повідомлення. Підпис обчислюється за правилом:

$$\begin{aligned} s &\equiv f \cdot B + F \cdot b (mod\ q), \\ t &\equiv g \cdot B + G \cdot b (mod\ q), \end{aligned} \qquad (1)$$

де B та b обчислюють із співвідношень

$$\begin{aligned} G \cdot m_1 - F \cdot m_2 &= A + q \cdot B \\ g \cdot m_1 - f \cdot m_2 &= a + q \cdot b \end{aligned} \quad (2)$$

Поліноми a, A мають коефіцієнти із діапазону [-1/2, 1/2] та b, $B \in Z[X]/(X^N - 1)$.

Наведені формули (1), (2) вирішують задачу знаходження найближчого вектору за допомогою секретного ключа. Можна обчислити t іншим способом $t = s \cdot h \; mod(q)$, в такому випадку не треба застосовувати при підписанні g [0].

Для зручності рівняння (1), (2) можна подати в матричному вигляді.

Визначення 7 [0]. Підпис - це вектор $(s,t) \in L$, який задовольняє рівнянню:

$$(s,t) = (B,b)\begin{pmatrix} f & g \\ F & G \end{pmatrix} = \left[(m_1, m_2)\begin{pmatrix} G/q & -g/q \\ -F/q & f/q \end{pmatrix}\right]\begin{pmatrix} f & g \\ F & G \end{pmatrix} = \left[(m_1, m_2)\begin{pmatrix} f & g \\ F & G \end{pmatrix}^{-1}\right]\begin{pmatrix} f & g \\ F & G \end{pmatrix}, \quad (3)$$

де квадратні дужки [ ] є операцією округлення коефіцієнтів полінома до найближчого цілого. Вектор (s,t) у формулі (3) - це вираз вектору (m_1, m_2), в секретному базисі решітки із округленням, причому власне значення (m_1, m_2) подано в ортонормованому базисі.

Модель атаки підробки підпису NTRUSign за допомогою анулюючих поліномів з посиленими параметрами. NTRUSign не завжди може знайти застосування на практиці, наприклад, в системах електронних платежів, адже цьому підписові властива наступна слабкість - наявність кількох підписів для одного повідомлення [0]. Автори роботи називають цю особливість malleability (англ. *гнучкість*). Ця особливість пов'язана з явищем анулюючих поліномів.

Визначення 8. Поліном α називається анулюючим, якщо в нього одинакові коефіцієнти та, відповідно, центрована норма анулюючого полінома $\| \vec{\alpha}(x) \| = 0$.

Властивості 1[0]. В кільці $R = Zq[X]/(X^N - 1)$ існує q анулюючих поліномів. Для випадкового $r \in R$ анулюючого $\alpha \in Z$:

1) різниця $\| \vec{r} + \alpha \| - \| \vec{r} \|$ близька до 0;

2) добуток $\| \vec{r} \cdot \alpha \| = 0$.

Визначення 9 [0]. Центрована норма полінома $s(x) = x^0 c_0 + \ldots x^m c_m$ знаходиться за формулою

$$\| \vec{s}(x) \|^2 = \sum_{i=0}^{N-1} (c_i - \mu_c)^2 \approx \approx \sum_{i=0}^{N-1} c^2 - \frac{1}{N}\left(\sum_{i=0}^{N-1} c\right)^2,$$

де μ_c є середнє арифметичне $\frac{1}{N}\sum_{i=0}^{N-1} c_i$ від коефіцієнтів полінома $s(x) = x^0 c_0 + \ldots x^{N-1} c_{N-1}$

При проведенні численних експериментів вдалося показати, наскільки на практиці ефективна розглянута атака на підписи, які згенеровано на різних наборах загальносистемних параметрів NTRUSign. Також експериментально визначено, що техніка пертурбації не суттєво захищає від даної загрози. Практична цінність отриманих результатів полягає в експериментальному доведенні того, що ефективність атаки не суттєво зменшується від збільшення раундів пертурбацій. Дійсно, кількість підроблений підписів зменшується від кількості пертурбацій, але це зменшення *не є*

критичним (приблизно на 10-30% при збільшенні на один раунд пертурбацій). Навіть після 3-х раундів пертурбацій кількість вдало підроблених підписів зменшилася лише у 2-3 рази, що дозволяє фактично порівняти оцінки стійкості ЕЦП NTRUSign із пертурбацією та без пертурбації. Наприклад, для довжини поліному N= 743 з q= 2048 підроблених підписів 1180 проходять перевірку при застосуванні NTRUSign без посиленої схеми, тобто половина всіх підробок вважається справжніми підписами. Якщо застосувати посилену схему із 3-ма раунди пертурбації із 2048 підроблених підписів 515 вважаються справжніми, тобто кількість підробок, які пройшли перевірку, зменшується удвічі, але це замало, щоб стверджувати про істотне покращення захисту. Практично це означає, що застосовувані досі методи посилення стійкості ЕЦП NTRUSign, які були засновані на техніці пертурбації і які, як вважалося, є ефективними, насправді не дають суттєвого виграшу, їх практичне використання втрачає сенс.

Висновки. Вперше запропоновано модель атаки підробки на підпис в ФКЗП із посиленими параметрами та із застосуванням техніки пертурбації, що дозволило отримати меншу складність підробки в порівнянні з повним перебором. Дана модель атаки відрізняється від відомих раніше врахуванням особливостей реалізації ЕЦП NTRUSign із посиленими параметрами та додатковим захистом за допомогою техніки пертурбації. Це дозволило отримати нові оцінки стійкісті ЕЦП NTRUSign, які показують, що використання техніки пертурбацій не покращує захист від досліджуваного виду підробки. Вперше проаналізовано та показано, що ефективність атаки не суттєво зменшується від збільшення раундів пертурбацій. Отримано експериментальні підтвердження у вигляді кількісних показників ефективності атаки (кількість вдалих спроб підробки підпису) для великих розмірів вхідних параметрів підпису. Важливою та актуальною задачею є подальший аналіз можливості поширення запропонованої моделі атаки для інших підписів на решітках.

Список використаних джерел

1. *Min Sung Jun. Weak property of malleability in NTRUSign [Електронний ресурс] / Sung Jun Min, Go Yamamoto, and Kwangjo Kim. Режим доступу: http://www.academy.ualiberty.com/ru/ goodsquality/details/174, свободный.*
2. *Hoffstein Jeffrey. NSS: The NTRU Signature SchemeNTRU Cryptosystems [Електронний ресурс] / Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. Режим доступу: http://www/citeseerx.ist.psu.edu, свободный.*
3. *Nguyen P. Q. Learning a Zonotope and More: Cryptanalysis of NTRUSign countermeasures [Електронний ресурс] / L. Ducas, P. Q. Nguyen. Режим доступу: http://www.di.ens.fr/ducas/NTRUSignCryptanalysis/ DucasNguyen/Learning.pdf, свободный.*
4. *Carlos Aguilar Melchor. Sealing the Leak on Classical NTRU Signatures [Електронний ресурс] / Carlos Aguilar Melchor , Xavier Boyen, Jean-Christophe Deneuville, Philippe Gaborit. Cryptology ePrint Archive, 2014. Режим доступу: url: http://eprint.iacr.org/2014/48*
5. *Gentry Craig. Cryptanalysis of the Revised NTRU Signature Scheme [Електронний ресурс] / Craig Gentry, Mike Szydlo. Режим доступу: http://www.szydlo.com/ntru-revised-short02.pdf, свободный.*
6. *Meskanen Tommi. On the NTRU Cryptosystem [Електронний ресурс] / Tommi Meskanen. Режим доступу: http://www/tucs./publications/attachment.php?fname=DISS63.pdf, свободный.*
7. *Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. 2003. NTRUSign: digital signatures using the NTRU lattice. In Proceedings of the 2003 RSA conference on The cryptographers' track (CT-RSA'03), Marc Joye (Ed.). Springer-Verlag, Berlin, Heidelberg, 122-140.*
8. *sourceforge. Ntru sourceforgenet, The source code repository. 2012. URL: http: //sourceforge.net/projects/ntru/?source.*