4. М. Герри, Д. Джонсон, «Вычислительные машины и трудно разрешимые задачи», М.: Мир, 1982., 419 с.

Ключові слова: кінцеві автомати, автомати з магазинною пам'яттю, система шифрування.
Ключевые слова: конечные автоматы, автоматы с магазинною памятью, система шифрования.
Keywords: finite-state machine, pushdown automaton, encryption system.

Онацкий Алексей Витальевич
Национальный университет «Одесская юридическая академия»,
преподаватель кафедры кибербезопасности,
кандидат технических наук, доцент

Поляков Дмитрий Владимирович
Одесская национальная академия связи им. А. С. Попова,
студент 7 курса специальности 125 – Кибербезопасность

Дубовой Ярослав Владимирович
Одесская национальная академия связи им. А. С. Попова,
студент 6 курса специальности 125 – Кибербезопасность

ПРОТОКОЛ АУТЕНТИФИКАЦИИ НА ОСНОВЕ КРИПТОСИСТЕМЫ NTRU

Протоколы аутентификации можно рассматривать как вид интерактивного доказательства знания. Интерактивное доказательство – понятие теории сложности вычислений, составляющее основу понятия доказательства с нулевым разглашением (zero-knowledge proof – ZKP) [1…3]. Широкое распространение получили криптографические протоколы ZKP на базе ассиметричного шифрования, наиболее известными являются: Fiat–Shamir, Schnorr, Okamoto, Guillou–Quisquater, Brickell–McCurley, Feige–Fiat–Shamir [1 … 3].

Целью работы является разработка протокола ZKP на основе криптосистемы NTRU (Nth-degree TRUncated polynomial

ring) [4], которая стойкая к атакам, осуществляемым на квантовых компьютерах (рис. 1). Криптосистема NTRU основана на решетчатой криптосистеме (lattice cryptosystem), в которой используются операции над кольцом усеченных многочленов степени, не превосходящей $n - 1$. В системе шифрования NTRU используем следующие обозначения: n – размерность кольца многочленов; p и q – натуральные взаимно простые числа НОД$(p, q) = 1$.

Пусть числа n, p, q известны участникам информационного процесса; $g(x)$ – многочлен в кольце $Z[X]/(q, X^n - 1)$ предварительно согласован; $f(x)$ – многочлен в кольце $Z[X]/(X^n - 1)$, причем для многочлена $f(x)$ существуют обратные многочлены $F_p(x)$ и $F_q(x)$. Абонент A вычисляет значения открытого ключа $Y_a(x) = F_q(x)g(x)$, который передает абоненту B вместе с заявкой γ. Абонент B выбирает случайный многочлен $r(x)$, сообщение $M(x)$ и вычисляет запрос – $y(x) = pY_a(x)r(x) + M(x)$, который передает абоненту A. Абонент A определяет $M(x) = (F_p(x)(f(x)y(x)(q, x^n - 1))(p, x^n - 1)$ и передает ответ – $X(x) = f(x)M(x)h(x)$ абоненту B. Абонент B проверяет равенство $Y_a(x)X(x) = \gamma M(x)g(x) = h(x)M(x)g(x)$.

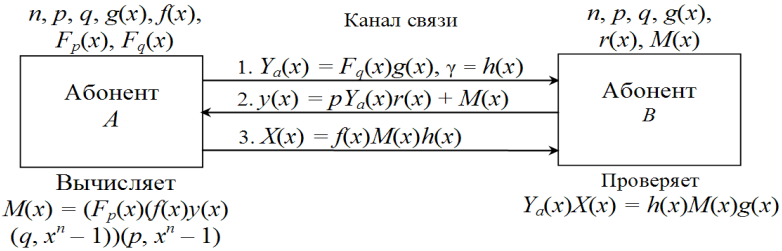

Рис. 1. Протокол аутентификации на основе криптосистемы NTRU

Полнота протокола. Абонент A расшифровывает сообщение $M(x)$, пользуясь своим секретным ключом. Докажем, что абонент A может расшифровать $M(x)$. Абонент A получает

от абонента B запрос $y(x) = (M(x) + pY_a(x)r(x))(q, x^n - 1)$, так как $Y_a(x) = (F_q(x)g(x))(q, x^n - 1)$, то $y(x) = (M(x) + pF_q(x)g(x)r(x))(q, x^n - 1)$.

Умножим левую и правую части равенства $y(x)$ на $f(x)$ по модулю q:

$$(f(x)y(x))(q, x^n - 1) = (f(x)(M(x) + pF_q(x)g(x)r(x)))(q, x^n - 1);$$

$$(f(x)y(x))(q, x^n - 1) = (f(x)M(x) + pg(x)r(x))(q, x^n - 1).$$

Умножим левую и правую части полученного равенства на $F_p(x)$:

$$(F_p(x)(f(x)y(x)(q, x^n - 1))(p, x^n - 1) = (F_p(x)(f(x)M(x) + pg(x)r(x))(q, x^n - 1))(p, x^n - 1) =$$

$$= (F_p(x)(f(x)M(x)(q, x^n - 1))(p, x^n - 1) + (F_p(x)pg(x)r(x))(q, x^n - 1))(p, x^n - 1) = M(x).$$

Абонент A расшифровал $M(x)$. Абонент A знает значения $f(x)$ и $F_p(x)$, поэтому он в состоянии ответить на любые запросы абонента B. При этом проверяющий абонент B убеждается в справедливости соотношения

$$Y_a(x)X(x) = F_q(x)g(x)f(x)M(x)\gamma(x) = h(x)M(x)g(x).$$

В работе приведено математическое обоснование, пример расчета, которые показывают, что предложенный протокол, на основе алгебраической структуры полиномиального кольца, работает корректно и технически реализуем. Стойкость протокола ZKP NTRU обеспечивается трудностью нахождения кратчайшего вектора в заданной числовой решетке, что в свою очередь делает протокол устойчивым к атакам на квантовых компьютерах.

Список использованных источников:

1. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C / B. Schneier. – Wiley, 2015. – 784 p.
2. Молдовян А. А. Протоколы аутентификации с нулевым разглашением секрета / А. А. Молдовян, Д. Н. Молдовян, А. Б. Левина. – СПб: Университет ИТМО, 2016. – 55 с.
3. Menezes A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 1996. – 816 p.
4. NTRU [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/ wiki/ NTRUEncrypt

Ключевые слова: аутентификация, криптографический протокол, решетчатая криптосистема, алгебраическая структура полиномиального кольца, шифрование.

Ключові слова: автентифікація, криптографічний протокол, решітчаста криптосистема, алгебраїчна структура поліноміального кільця, шифрування.

Keywords: authentication, cryptographic protocol, lattice cryptosystem, algebraic structure of a polynomial ring, encryption.

Толокнов Анатолій Арнольдович
Національний університет «Одеська юридична академія»,
асистент кафедри інформаційних технологій

ОГЛЯД І КЛАСИФІКАЦІЯ ОСНОВНИХ ПОГРОЗ WEB-ЗАСТОСУНКІВ

З ростом кількості та значення різних веб-сервісів в суспільному житті, наприклад, таких як банківські послуги, покупка товарів он-лайн та ін., також зростає значення забезпечення їх безпеки. Ефективність забезпечення безпеки може зростати якщо знати звідки чекати загрози. Попереджений – значить озброєний – прислів'я, зміст якого полягає в тому, що будучи попереджений про близьку небезпеку (або можливість такої), людина тепер до неї підготовлена і може з нею впоратися. Це в рівній мірі відноситься і до web-застосунків.

У даному невеликому огляді ми розглянемо основні загрози web-застосунків, а також наведемо приклади їх класифікації.

Повний список загроз безпеки веб-сайтів можна розглянути в розділі «Категорія: атаки» (Open Web Application Security Project) [1]. Також проект OWASP представляє стандартизований список топ 10 основних загроз web-застосунків, які повинні братися до уваги розробниками, перш ніж приступати до створення web-застосунків [2].

Крім цього Консорціум безпеки web-застосунків (WASC), www.webappsec.org, міжнародна організація, що об'єднує професіоналів в області безпеки web-застосунків, випустила