РЕАЛИЗАЦИЯ ПРОТОКОЛА АУТЕНТИФИКАЦИИ ШНОРРА В КОДЕ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Бесланеева Татьяна Юрьевна

студент, Северо-Кавказский федеральный университет, РФ, г. Ставрополь

В отличии от парольных методов аутентификации, методы аутентификации, использующие протоколы доказательства с нулевым разглашением знаний, имеют существенное отличие. В них используется схема типа «запрос-ответ», но при этом проверяющий не владеет секретом. Сам секрет знает только претендент. Для проведения аутентификации проверяющий задает «вопрос», который периодически изменяется. Претендент в процессе аутентификации должен так ответить на «вопрос», чтобы проверяющий смог убедиться, что у него есть секрет. При этом при проверке ответов проверяющая сторона не должна узнать этот секрет [1].

Первым среди протоколов доказательства с нулевым разглашением знаний был протокол аутентификации Фиата-Шамира. Протокол имеет две части. В первой части рассматривается вопрос получения ключей. Секретный ключ используется претендентом. Открытый ключ – нужен проверяющему для проведения проверки ответов. Вторая часть протокола – это многораундовый процесс доказательства того, что у претендента есть секрет.

В качестве недостатка данного протокола можно отметить, что вторую часть протокола Фиата-Шамира надо повторять многократно, например до 50 раз. Это связано с тем, что разрядность вопроса равна единице. В этом случае вероятность имитации ответа составляет $P_{ИО} = \frac{1}{2}$. Это очень высокая вероятность. Чтобы понизить ее предлагается выполнять вторую часть протокола многократно. Если число раундов протокола будет равно W=50, то вероятность имитации ответа составит $P_{ИО} = \frac{1}{2^W} = \frac{1}{2^{50}} = 8{,}881 \cdot 10^{-16}$. В качестве недостатка протокола Фиата-Шамира можно выделить низкую скорость процесса аутентификации. Устранить данный недостаток позволяет протокол аутентификации Шнорра с нулевым разглашением знаний [2].

В отличие от протокола Фиат-Шамира данный протокол проводит аутентификацию претендента за один раунд. Протокол также имеет две части. В первой части рассматривается вопрос получения ключей. Секретный ключ используется претендентом. Открытый ключ – нужен проверяющему для проведения проверки ответов.

Однако данный протокол имеет недостаток. Согласно [2] к данному протоколу были выдвинуты следующие требования. Чтобы обеспечить высокую криптографическую стойкость к подбору правильного ответа на поставленный вопрос разработчики предложили, чтобы модуль А имел не менее 512 разрядов. Размерность второго модуля В, который является делителем числа А, должна составлять не менее 140 двоичных разрядов. При этом параметр С, который используется во второй части протокола должен находиться в пределах от 52 до 72 двоичных разрядов.

Использование таких больших чисел приводит к снижению скорости аутентификации. Так как в основе протокола лежат операции умножения и возведение в степень по модулю, то такие операции требуют значительных временных затрат на сове выполнение. В результате этого увеличивается временной интервал, в течение которого происходит аутентификации

Бесланеева Т.Ю. РЕАЛИЗАЦИЯ ПРОТОКОЛА АУТЕНТИФИКАЦИИ ШНОРРА В КОДЕ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ // Студенческий форум: электрон. научн. журн. 2024. № 23(290). URL: https://nauchforum.ru/journal/stud/290/151302 (дата обращения: 09.09.2025).

претендента. Значит, у нарушителя появляется больше времени на подбор правильного ответа на заданный проверяющей стороной вопрос.

Устранить данный недостаток, то есть повысить скорость выполнения процедуры аутентификации, можно, если использовать коды системы остаточных классов. Это параллельные арифметические коды, в которых вычисления выполняются параллельно по основаниям. При этом аргументы выступают остатки, которые получаются при делении целых числе на числа, которые выбраны в качестве оснований СОК. Рассмотрим реализацию протокола аутентификации Шнорра в коде СОК.

Как отмечалось ранее, протокол Шнорра проводит аутентификацию претендента за один раунд. Протокол также имеет две части. В первой части рассматривается вопрос получения ключей. Секретный ключ используется претендентом. Открытый ключ – нужен проверяющему для проведения проверки ответов. Рассмотрим первую часть протокола.

Как отмечалось ранее, протокол Шнорра проводит аутентификацию претендента за один раунд. Протокол также имеет две части. В первой части рассматривается вопрос получения ключей. Секретный ключ используется претендентом. Открытый ключ – нужен проверяющему для проведения проверки ответов. Рассмотрим первую часть протокола, которая состоит из этапов.

1 этап. Претендент находит основания $m_1, \dots, m_n$ кода СОК, в качестве которых выступают простые числа. Чтобы не снижать стойкость протокола аутентификации к имитации правильного ответа необходимо выбрать основания кода СОК так, чтобы выполнялось условие

$$P_{раб} > A, \tag{1}$$

где А – большое простое число, по которому реализуется протокол Шнорра;

$P_{раб} = \prod_{i=1}^{n} m_i$ – рабочий диапазон кода.

Затем вычисляются функции Эйлера для каждого основания

$$\varphi(m_1) = m_1 - 1, \dots, \varphi(m_n) = m_n - 1. \tag{2}$$

После этого претендент находит простые числа $b_1, \dots, b_n$, которые являются делителями соответствующих функций Эйлера

$$b_1 | \varphi(m_1), b_2 | \varphi(m_2), \ \dots, b_n | \varphi(m_n). \tag{3}$$

2 этап. Претендент находит такие числа N_i, где $i = 1, 2, \dots, n$, для которого справедливо сравнение

$$N_i^{b_i} \equiv 1 \bmod m_i. \tag{4}$$

3этап. Претендент производит выбор чисел K_i, где $i = 1, 2, \dots, n$, которые является секретным ключом. Данное число должно удовлетворять

$$K_i < b_i - 1. \quad (5)$$

4 этап. Претендент производит вычисление открытого ключа протокола аутентификации

$$L_i = N_i^{-K_i} \bmod m_i, \quad (6)$$

где $i = 1, 2, \ldots, n$.

Вторая часть протокола включает в себя этапы аутентификации претендента.

1 этап. Претендент находит набор случайных чисел X_i, где $i = 1, 2, \ldots, n$. Данное число должно удовлетворять

$$X_i < b_i - 1. \quad (7)$$

2 этап. Претендент приступает к вычислению

$$Q_i = N_i^{X_i} \bmod m_i, \quad (8)$$

где $i = 1, 2, \ldots, n$.

Полученный результат претендент по радиоканалу передает на проверяющую сторону V.

3 этап. Проверяющий готовит вопрос. Для этого он находит случайные числа S_i. Данное число выбирается из условия

$$1 \le S_i \le 2^{c_i} - 1, \quad (9)$$

где $C_i = C \bmod m_i$; $i = 1, 2, \ldots, n$.

Сгенерированный вопрос $S = (S_1, S_2, \ldots, S_{n-1}, S_n)$ передается на сторону претендента.

4 этап. Претендент, получив вопрос $S = (S_1, S_2, \ldots, S_{n-1}, S_n)$, должен вычислить ответ

$$Z_i = (X_i + K_i \cdot S_i) \bmod b_i, \quad (10)$$

где $i = 1, 2, \ldots, n$.

Вычисленный ответ $Z = (Z_1, Z_2, \ldots, Z_{n-1}, Z_n)$ на вопрос передается по радиоканалу на сторону проверяющего.

5 этап. Проверяющий осуществляет проверку полученного от претендента ответа $Z = (Z_1, Z_2, \dots, Z_{n-1}, Z_n)$. Для этого используется выражение

$$R_i = N_i^{Z_i} L_i^{S_i} \bmod m_i. \quad (11)$$

где $i = 1, 2, \dots, n$.

Затем проверяющий сравнивает полученный результат с полученным числом $Q = (Q_1, Q_2, \dots, Q_{n-1}, Q_n)$. Если результат совпадает с данным числом, то проверяющая сторона считает претендента легитимным. Если вычисленный результат не совпадает с данным числом, то проверяющая сторона считает претендента нарушителем.

Рассмотрим пример работы данного протокола аутентификации с использованием кодов системы остаточных классов.

1 этап. Пусть задано простое число A = 10369. Претендент находит основания $m_1 = 23, m_2 = 47, m_3 = 83$ кода СОК. Данные основания обеспечивают рабочий диапазон равный $P_{раб} = \prod_{i=1}^{3} m_i = 10373$. Таким образом, выполняется условие (1), то есть $P_{раб} > A$. В этом случае не будет снижение стойкости протокола аутентификации к имитации правильного ответа.

Затем претендент вычисляет функции Эйлера для каждого основания

$$\varphi(m_1) = m_1 - 1 = 22, \varphi(m_2) = m_2 - 1 = 46, \varphi(m_3) = m_3 - 1 = 82.$$

После претендент находит простые числа $b_1 = 11, b_2 = 23, b_3 = 41$, которые являются делителями соответствующих функций Эйлера

$$11|22, 23|46, 41|82.$$

2 этап. Претендент находит такие числа N_i, которые удовлетворяют условию (4). Он выбрал числа N_1=3, N_2=3, N_3=3, так как для них справедливо

$$N_1^{b_1} \equiv 3^{11} \equiv 1 \bmod 23, N_2^{b_2} \equiv 3^{22} \equiv 1 \bmod 47,$$
$$N_3^{b_3} \equiv 3^{41} \equiv 1 \bmod 83.$$

3 этап. Претендент производит выбор чисел K_i, который является секретным ключом. Данное число должно удовлетворять (5). Претендент выбрал числа $(K_1, K_2, K_3) = (7, 2, 35)$.

4 этап. Претендент производит вычисление открытого ключа протокола аутентификации, используя выражение (6)

$$L_1 = N_1^{-K_1} \bmod m_1 = 3^{-7} \bmod 23 = 3^{11-7} \bmod 23 = 3^4 \bmod 23 = 12$$

.

$$L_2 = N_2^{-K_2} \bmod m_2 = 3^{-2} \bmod 47 = 3^{23-2} \bmod 47 = 3^{21} \bmod 47 = 21$$

.

$$L_3 = N_3^{-K_3} \bmod m_3 = 3^{-35} \bmod 83 = 3^{41-35} \bmod 83 = 3^6 \bmod 83 = 65$$

.

Вторая часть протокола включает в себя этапы аутентификации претендента.

1 этап. Претендент находит набор случайных чисел

$(X_1, X_2, X_3) = (7, 3, 11)$. Данное число должно удовлетворять (7).

2 этап. Претендент приступает к вычислению

$$Q_1 = N_1^{X_1} \bmod m_1 = 3^7 \bmod 23 = 2$$

.

$$Q_2 = N_2^{X_2} \bmod m_2 = 3^3 \bmod 47 = 27$$

.

$$Q_3 = N_3^{X_3} \bmod m_3 = 3^{11} \bmod 83 = 25$$

.

Полученный результат $(Q_1, Q_2, Q_3) = (2, 27, 25)$ претендент по радиоканалу передает на проверяющую сторону V.

3 этап. Проверяющий готовит вопрос. Для этого он находит случайные числа $(S_1, S_2, S_3) = (8, 4, 4)$. Сгенерированный вопрос передается на сторону претендента.

4 этап. Претендент, получив вопрос $(S_1, S_2, S_3) = (8, 4, 4)$, приступает к вычислению ответа, используя равенство (10)

$$Z_1 = (X_1 + K_1 \cdot S_1) \bmod b_1 = (7 + 8 \cdot 7) \bmod 11 = 8$$

.

$$Z_2 = (X_2 + K_2 \cdot S_2) \bmod b_2 = (3 + 4 \cdot 2) \bmod 23 = 11$$

.

$$Z_3 = (X_3 + K_3 \cdot S_3) \bmod b_3 = (11 + 4 \cdot 35) \bmod 41 = 28$$

.

Вычисленный ответ $(Z_1, Z_2, Z_3) = (8, 11, 28)$ на вопрос передается по радиоканалу на сторону проверяющего.

5 этап. Проверяющий осуществляет проверку полученного от претендента ответа $(Z_1, Z_2, Z_3) = (8, 11, 28)$ с помощью (11)

$$R_1 = N_1^{Z_1} L_1^{S_1} \bmod m_1 = (3^8 \cdot 12^8) \bmod 23 = 2.$$

$$R_2 = N_2^{Z_2} L_2^{S_2} \bmod m_2 = (3^{11} \cdot 21^4) \bmod 47 = 27.$$

$$R_3 = N_3^{Z_3} L_3^{S_3} \bmod m_3 = (3^{23} \cdot 65^4) \bmod 83 = 25.$$

Затем проверяющий сравнивает полученный результат с полученным числом $Q = (Q_1, Q_2, Q_3)$. Так результат совпал с данным числом

$$(R_1, R_2, R_3) = (Q_1, Q_2, Q_3) = (2, 27, 25),$$

то проверяющая сторона считает претендента легитимным.

Переход к вычислениям по основаниям кода СОК позволяет повысить скорость проведения аутентификации. В рассмотренном примере было выбрано простое число А, которое представляется в виде 14-разрядного двоичного кода. При использовании кода СОК самым большим основанием было число 83. Данное число представляется с помощью 7-разрядного двоичного кода. Так как временные затраты на реализацию операций умножения и возведения в степень по модулю прямо пропорционально разрядности операндов, то применение кодов СОК повысило скорость аутентификации в 2 раза без учета немодульных операций прямого и обратного преобразований.

Список литературы:

1. Запечников, С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности / С. В. Запечников. – М. : Горячая линия-Телеком, 2011. – 256 с.

2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / Б. Шнайер. – М. : Издательство ТРИУМФ, 2003. – 816 с

3. Обработка информации в системе остаточных классов (СОК) : учеб. пособие : [по направлению подготовки 01.04.01 «Математика» (параллельные компьютерные технологии), квалификация «магистр»] / Н. И. Червяков, П. А. Ляхов, Л. Б. Копыткова [и др.] ; Министерство образования и науки Российской Федерации, Северо-Кавказский федеральный университет. – Ставрополь: Изд-во СКФУ, 2016. – 225 с.

4. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Н. И. Червяков, А. А. Коляда, П. А. Ляхов [и др.] ; Научное издание, Издательская фирма «Физико-математическая литература» – Москва : ФИЗМАТЛИТ, 2017. – 400 с

5. Omondi A. Advances in Computer Science and Engineering: Texts. Residue Number Systems. Theory and Implementation в 2 частях / Omondi A., Premkumar B. ; Imperial College Press. – London : World Scientific Publishing Co. Pte. Ltd., 2007 – 311 с.

6. Mohan, P.V. Residue Number Systems. Algorithms and Architectures / P.V. Mohan. – New York: Springer New York, 2002. – 253 с.

7. Mohan, A. Residue Number Systems. Theory and Applications / A. Mohan // Springer International Publishing Switzerland. – 2016. – 351 c.