УДК 004.052.2

ПРИМЕНЕНИЕ МОДУЛЯРНЫХ ТЕХНОЛОГИЙ ПРИ РАЗРАБОТКЕ ПСЕВДОСЛУЧАЙНЫХ ФУНКЦИЙ

[1]Харечкина Ю.О., [2]Навальнева Р.С., [2]Бажин В.О., [2]Калмыков И.А., [2]Попов А.И., [3]Ряднов С.А.

[1]ФГБОУ ВО «Ставропольский государственный аграрный университет» Ставрополь, e-mail: kia762@yandex.ru;

[2]ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru;

[3]Филиал Московского государственного университета приборостроения и информатики, Ставрополь, e-mail: kia762@yandex.ru

Стремление обеспечить обработку информации с требуемым уровнем защиты от несанкционированного доступа способствовало разработке псевдослучайных функций. Для построения псевдослучайных функций широко используются модулярные технологии, которые базируются на алгебраических системах, обладающих свойство кольца и поля. Благодаря использованию модулярных кодов можно обеспечить более высокую производительность при вычислении псевдослучайной функции. Это связано с тем, что в модулярных кодах обработка данных осуществляется параллельно по основаниям кода и независимо, при этом данные представляют собой малоразрядные остатки. При этом реализация псевдослучайной функции в системе остаточных классов позволит обеспечить требуемый уровень стойкости к атакующим алгоритмам при меньшей размерности секретного ключа. В работе рассмотрены вопросы применения модулярных технологий для повышения скорости синтеза псевдослучайной функции.

Ключевые слова: псевдослучайная функция, расширенный каскад, модулярные коды, система остаточных классов, основания модулярного кода

THE USE OF MODULAR TECHNOLOGY IN THE DEVELOPMENT PSEUDORANDOM FUNCTIONS

[1]Kharechkina Y.O., [2]Navalneva R.S., [2]Bazhin V.O., [2]Kalmykov I.A., [2]Popov A.I., [3]Ryadnov S.A.

[1]Stavropol State Agrarian University, Stavropol, e-mail: kia762@yandex.ru;

[2]North-Caucasian Federal University, Stavropol, e-mail: kia762@yandex.ru;

[3]Filial Moscow state University of instrument engineering and informatics in the city of Stavropol, e-mail: kia762@yandex.ru

The desire to provide processing information with the required level of protection from unauthorized access has contributed to the development of pseudorandom functions. For building pseudo-random functions are widely used modular technologies, which are based on algebraic systems having the property of rings and fields. Through the use of modular codes can provide a higher productivity when computing pseudo-random functions. This is due to the fact that modular codes data processing is performed in parallel on the grounds of code independently, and the data represent maloletnye residues. The realization of the pseudorandom function in the system of residual classes will allow to provide the required level of resistance to the attacking algorithms for lower-dimensional h-rechnogo key. In the article the questions of application of modular technology to increase the rate of synthesis of pseudorandom functions.

Keywords: pseudorandom function, advanced cascade, modular code system of residual classes, foundation of the modular code

Псевдослучайные функции (ПСФ) постоянно расширяют сферу своего применения, занимая прочные позиции, начиная от имитационного моделирования до криптографии. При этом к таким функциям предъявляются довольно высокие требования, как с точки зрения их устойчивости к атакующим алгоритмам, так и к скорости вычисления конечного результата. Поэтому вопросам разработки алгоритмов быстрого вычисления псевдослучайных функций повышенной эффективности в настоящее время уделяется значительное внимание.

Цель исследования. Эффективность применения псевдослучайных функций зависит не только от их криптографической стойкости, но и от скорости их вычислений. Для обеспечения высокой степени защиты от несанкционированного доступа (НСД) требуется использование больших модулей, с помощью которых происходит синтез ПСФ. Однако это приводит к снижению скорости вычисления ПСФ. Решить данную проблему можно за счет использования модулярных кодов, которые обладают свойством кольца и поля. Поэтому целью работы является повышение скорости синтеза псевдослучайной функции, обладающей требуемым уровнем криптостойкости, за счет использования модулярной техноло-

гии, в частности кодов системы остаточных классов.

Материалы и методы исследования

Для разработки псевдослучайных функций, как правило, используют генераторы псевдослучайных последовательностей (ПСП) [7]. Благодаря довольно простой структуре классических генераторов ПСП на основе линейных регистров сдвига с обратной связью, двоичные псевдослучайные последовательности используются для решения задач, среди которых можно выделить: помехоустойчивое кодирование; защита информации; встроенное техническое диагностирование компонентов компьютерных систем (КС); системы электронных платежей; обеспечение целостности передаваемого сообщения; генерация ключей из некоторого секретного значения (например, мастер-ключа); аутентификация пользователей.

Во всех вышеперечисленных случаях ПСФ используются либо непосредственно, либо на их основе строятся алгоритмы хеширования информации. В последних двух случаях качество операций генерации псевдослучайных функций и хеширования определяется в первую очередь эффективностью ПСФ. Таким образом, именно от свойств псевдослучайных функций, особенно в тех случаях, когда необходимо обеспечить устойчивую работу КС при наличии случайных и умышленных деструктивных воздействий, в значительной степени зависит надежность процессов сбора, обработки, хранения и передачи информации. Кроме того, к техническим реализациям алгоритмов вычисления ПСФ предъявляются высокие требования с точки зрения обеспечения высоких скоростных показателей. Поэтому получение высокоэффективных ПСФ в реальном масштабе времени является актуальной задачей.

Анализ работ [3–6] показал, что в настоящее время известно несколько алгоритмов, позволяющих получать довольно хорошие псевдослучайные функции. Так, в работе [6] была представлена ПСФ Наора-Рейнголда, стойкость которой была выведена из сложности решения проблемы принятия решения Диффи-Хеллмана (DDH). Алгоритм вычисления такой ПСФ определяется следующим образом: на ее вход поступают *m*-битная строка $b = b_1,..,b_m \in \{0,1\}^m$ и секретный ключ $(h, x_1,..., x_m)$, результатом работы является

$$F_{NR}((h, x_1,..., x_m),(b_1,..., b_m)) := h^w, \qquad (1)$$

где $w = \prod_{i=1}^{m} x_i^{b_1}$.

Вычислительная сложность этой функции составляет m-1 модулярных умножений для вычисления w и одно заключительное возведение в степень.

Однако алгебраическая конструкция ПСФ Наора-Рейнголда, несмотря на то, что она лежит в основе многих криптографических схем и даже таких алгебраических конструкций, как верифицируемые случайные функции рассеянные и распределенные ПСФ, обладает недостатками, среди которых можно выделить – большой размер секретного ключа и довольно низкое быстродействие ее технической реализации [3,4].

С целью устранения данных недостатков в работе [1] была разработана алгебраическая ПСФ, имеющая точно такой же размер области определения, как ПСФ Наора-Рейнголда и Бонеха-Монтгомери-Рагунатана (БМР ПСФ), но использующая более короткий секретный ключ по сравнению с ПСФ Наора-Рейнголда. Рассмотрим особенности построения такой псевдослучайной функции. Данная ПСФ на вход принимает входную последовательность вместе с ключом $(h, s_1,..., s_n)$ и на выход выдает

$$F((h, s_1,..., s_n),(x_1,..., x_n)) := h^W, \qquad (2)$$

где $W = \prod_{i=1}^{n} \left(s_i^{x_1}\right)^{-1}$.

Для области определения размером 2^m значение $n = m/\log_2 L$, вследствие чего при вычислении данной функции требуется в $\log_2 L$ раз меньше умножений, но на $m/\log_2 L$ больше возведений в степень по сравнению с (1) для вычисления значения *w*. В общей сумме нам необходимо $2m-1-\left(m/\log_2 L\right)$ умножений для вычисления значения w. Основным преимуществом данной ПСФ является использование меньшего объема памяти для вычисления значения функция, так как она использует ключ в $\log_2 L$ раз меньший размером по сравнения с ПСФ Наора-Рейнголда. Стойкость ПСФ основывается на предположении о сложности решения λ-DDH проблемы. Применение разработанной ПСФ в системах электронных платежей показано в работе [1].

Применение каскадной реализации позволяет повысить производительность вычисления псевдослучайной функции, однако для дальнейшего повышения скоростных характеристик генератора ПСФ целесообразно использовать систему остаточных классов. В данном случае система остаточных классов задается набором простых чисел $p_1, p_2, \ldots, p_n$, называемых модулями. Тогда динамический диапазон такой системы будет определяться

$$P = \prod_{i-1}^{n} p_i . \qquad (3)$$

Для любого целого числа $0 \le A < P$ задается единственным образом через n–кортеж остатков

$$A = (\alpha_1, \alpha_2, \ldots, \alpha_n), \qquad (4)$$

где $\alpha_i = A \bmod p_i (i = 1,2,\ldots,n)$.

Модулярное число со знаком определяется в диапазоне $\frac{P}{2} \le A < P-1$. Вычисления над n-кортежем независимы от целого числа. Таким образом, существует изоморфизм между кольцом целых чисел по модулю $P(Z(P))$ и прямой суммой колец $Z(p_i),(i = 1,2,\ldots,n)$, а арифметические операции в *Z*(*P*) отражены на соответствующих операциях с остатками. Для $0 \le A, B, Z < P$ справедливо

$$Z = (A \circ B) \bmod P = (z_1, z_2, \ldots, z_n);$$
$$Z_i = (a_i \circ b_i) \bmod p_i \quad (i = 1,2,\ldots,n) \qquad (5)$$

где ∘ представляет сложение, вычитание или умножение по модулю.

Выражение (5) отражает основные характеристики модулярной арифметики: любая система, состоящая из большого числа сложений, вычитаний

и умножений может быть представлена несколькими независимыми каналами, работающими параллельно. При этом разрядность обрабатываемых данных будет определяться выбранным модулем p_i, характеризующегося относительно небольшой разрядностью. В результате этого увеличивается производительность системы. Необходимо отметить, что каждая цифра модулярной арифметики независима и равнозначна, поэтому нет необходимости распространения сигнала переноса между кольцами. Таким образом, арифметические операции сложения, вычитания и умножения выполняются без переносов в отличие от обычного позиционного представления чисел и для каждого значения модуля p_i арифметические операции выполняются с парой соответствующих вычетов параллельно, при этом вычеты имеют гораздо меньшую разрядность, чем исходные операнды A и B. Введение метрики в кольце по модулю p позволяет рассматривать его как метрическое конечномерное пространство векторов конечной размерности.

Восстановление числа A по его модулярному коду основано на фундаментальном положении, лежащем в основе модулярного представления числа – Китайской теореме об остатках (КТО) [8]. На основании известного представления числа в СОК $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ КТО делает возможным определение числа в ПСС $|A|_p$, если наибольший общий делитель любой пары модулей равен 1. Тогда

$$|A|_p = \left| \sum_{i=1}^{n} P_i \left| \frac{\alpha_i}{p_i} \right|_{p_i} \right|_P, \qquad (6)$$

где $P_i = \frac{P}{p_i}$, $P = \prod_{i=1}^{n} p_i$; $(p_i, p_j) = 1, i \neq j$

Из (6) видно, что из КТО получаем $|A|_p$, а не само A. Если известно, что A находится между 0 и $P-1$, то можно записать

$$A = \left| \sum_{i=1}^{n} P_i \left| \frac{\alpha_i}{p_i} \right|_{p_i} \right|_P, \text{ для } 0 \le A < P \qquad (7)$$

В некоторых случаях желательно иметь вид КТО, где сумма появляется без оператора по модулю P. Это можно сделать путем определения вспомогательной функции $R(A)$, так, чтобы

$$A = \sum_{i=1}^{n} P_i \left| \frac{\alpha_i}{p_i} \right|_{p_i} - P \cdot R(A) \qquad (8)$$

где $R(A) = \frac{1}{P}\left(\sum_{i=1}^{n} P_i \left| \frac{\alpha_i}{p_i} \right|_{p_i} - A \right)$, $R(A)$ – ранг числа A.

Тогда вычисление ПСФ с использованием модулярной технологии будет определяться выражением

$$f_i = F((h, s_1, \ldots, s_n), (x_1, \ldots, x_n)) \bmod p_i = h^{W_i} \bmod p_i, \qquad (9)$$

где $w_i = W \bmod p_i = \prod_{i=1}^{n} \left(s_i^{x_i} \right)^{-1} \bmod p_i$.

Результаты исследования и их обсуждение

Рассмотрим пример вычисления псевдослучайной функции повышенной эффективности в кодах СОК. Пусть заданы модули $p_1 = 11$ и $p_2 = 13$. В этом случае диапазон СОК равен

$$P = \prod_{i=1}^{2} p_i = 11 \cdot 13 = 143 \cdot$$

Для восстановления числа вычисляем ортогональные базисы:

$$B_1 = m_1 p_2 = 6 \cdot 13 = 78,$$

где m_1 – вес первого ортогонального базиса, удовлетворяющий условию

$$B_1 = m_1 p_2 \equiv 1 \bmod p_1;$$

$$B_2 = m_2 p_1 = 6 \cdot 11 = 66,$$

где m_2 – вес второго ортогонального базиса, удовлетворяющий условию

$$B_2 = m_2 p_1 \equiv 1 \bmod p_2.$$

В качестве первообразного элемента выбираем $h = 2$. Предположим, что в качестве секретного ключа выбирается число $X = 8_{10}$, которое принадлежит мультипликативной группе. В качестве входного значения выбираем число $U = 10_{10}$. Представим эти значения в двоичном коде. В результате преобразований имеем следующие значения^

$$U = 10_{10} = 1010_2;$$

$$X = 8_{10} = 1000_2.$$

Полученные значения, представленные 4-битовым блоком. Разобьем эти значения на m = 2 блока, по 2 бит каждый. В результате этого имеем

$$u_1 = 10_2 = 2_{10}; u_2 = 10_2 = 2_{10}; x_1 = 10_2 = 2_{10}; x_2 = 00_2 = 0_{10}.$$

Для вычисления ПСФ повышенной эффективности по модулю p_1 =11 используем (9). Тогда

$$f_1 = F\left((h, x_1, x_2)(u_1, u_2) \right) \bmod p_1 =$$

$$= h^{\prod_{i=1}^{2} \frac{1}{(x_i + u_i)}} \bmod p_1 = 2^{\frac{1}{(2+2)} \cdot \frac{1}{(2+0)}} \bmod 11 =$$

$$= 2^{\frac{1}{4} \cdot \frac{1}{2}} \bmod 11 =$$

$$= 2^{\frac{1}{8}} \bmod 11 = 2^7 \bmod 11 = 7.$$

Для вычисления ПСФ повышенной эффективности по модулю p_2 =13 используем (9). Тогда

$$f_2 = F\left(\left(h, x_1, x_2\right)\left(u_1, u_2\right)\right) \bmod p_2 =$$

$$= h^{\prod_{i=1}^{2} \frac{1}{(x_i + u_i)}} \bmod p_2 = 2^{\frac{1}{(2+2)} \cdot \frac{1}{(2+0)}} \bmod 13 =$$

$$= 2^{\frac{1}{4} \cdot \frac{1}{2}} \bmod 13 =$$

$$= 2^{\frac{1}{8}} \bmod 13 = 2^5 \bmod 13 = 6.$$

Тогда, согласно китайской теореме об остатках, получаем значение ПСФ

$$F_{\text{ПСФ}} = \sum_{i=1}^{2} f_{it} B \bmod P =$$

$$= \left(7 \cdot 78 + 6 \cdot 66\right) \bmod P = 84.$$

Проведем сравнительную оценку времени вычисления ПСФ согласно алгоритма, задаваемого выражением (2) и алгоритма, реализованного в кодах системы остаточных классов вычетов (9). Анализ этих выражений показывает, что основным фактором, от которого будет зависеть время вычисления ПСФ, будет вычисления показателя степени. Из выражения (1) наглядно видно, чтобы реализовать эту процедуру необходимо выполнить m умножений данных размером $\lceil \log_2 P \rceil$. При использовании выражения (9) число умножений остается таким же, но разрядность обрабатываемых операндов сокращается до значений $\lceil \log_2 p_i \rceil < \lceil \log_2 P \rceil$. Таким образом, очевидно, что применение модулярных кодов, в частности кодов СОК, позволяет повысить быстродействие вычисления псевдослучайной функции повышенной эффективности.

Заключение

В статье проведена разработка нового подхода, позволяющего за счет использования модулярных технологий повысить скорость вычисления ПСФ. Применение кодов системы остаточных классов позволяет перейти к параллельным вычислениям псевдослучайной функции. При этом скорость синтеза значений ПСФ обуславливается тем, что при выполнении m умножений в алгоритме (2) используются операнды размером $\lceil \log_2 P \rceil$. При переходе к кодам СОК, согласно (9), разрядность обрабатываемых операндов сокращается до значений $\lceil \log_2 p_i \rceil < \lceil \log_2 P \rceil$. Очевидно, что при увеличении размерности позиционной ПСФ, эффективность применения модулряных технлогий возрастает при сохранеии требуемого уроня защиты от НСД.

Список литературы

1. Калмыков И.А., Дагаева О.И. Науменко Д.О., Вельц О.В. Системный подход к применению псевдослучайных функций в системах защиты информации // Известия ЮФУ. Технические науки. – 2013. – №12. – С. 228–234.

2. Червяков Н.И. Элементы компьютерной математики и нейроноинформатики / Н.И. Червяков, И.А. Калмыков. – М.: ФИЗМАТЛИТ, – 2003. – 288 с.

3. Dan Boneh, Shai Halevi Circular-secure encryption from decision Diffie-Hellman. In CRYPTO'08, pages 108–125, 2008. http://crypto.stanford.edu/~dabo/abstracts/circular.html

4. Dan Boneh, Hart Montgomery Algebraic pseudorandom functions with improved efficiency from the augmented cascade. In ACM Conference on Computer and Communications Security – CCS 2010 (to appear), 2010. http://crypto.stanford.edu/~dabo/pubs/abstracts/algebprf.html.

5. Mihir Bellare, Ran Canetti Pseudorandom functions revisited: The cascade construction and its concrete security. In FOCS'96. http://cseweb.ucsd.edu/~mihir/papers/cascade.html.

6. Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. In FOCS'97, PP. 458–67. http://www.wisdom.weizmann.ac.il/~naor/PAPERS/gdh_abs.html.

7. Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. JACM, Vol. 33, №. 4, October 1986. http://www.wisdom.weizmann.ac.il/~oded/ggm.html.