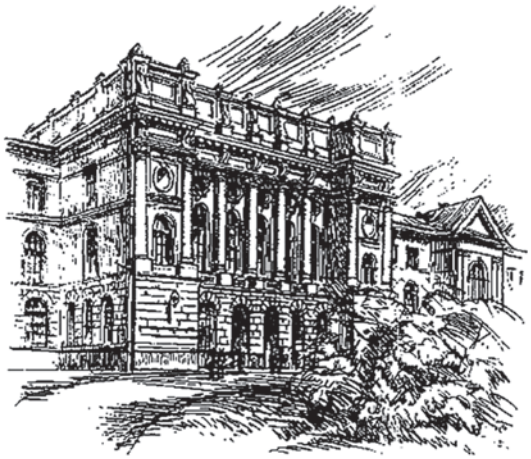
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ



НАУЧНО-ТЕХНИЧЕСКИЕ ВЕДОМОСТИ

САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО ПОЛИТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

Информатика. Телекоммуникации. Управление

4(176) 2013

Издательство Политехнического университета
Санкт-Петербург
2013

ИНФОРМАТИКА. ТЕЛЕКОММУНИКАЦИИ. УПРАВЛЕНИЕ

Журнал с 1995 года издается под научно-методическим руководством Российской академии наук. С 2008 года выпускается в составе сериального периодического издания «Научно-технические ведомости СПбГПУ» ISSN 1994-2354.

Журнал с 2002 года входит в Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени доктора и кандидата наук.

Сведения о публикациях представлены в Реферативном журнале ВИНИТИ РАН, в международной справочной системе «Ulrich`s Periodical Directory».

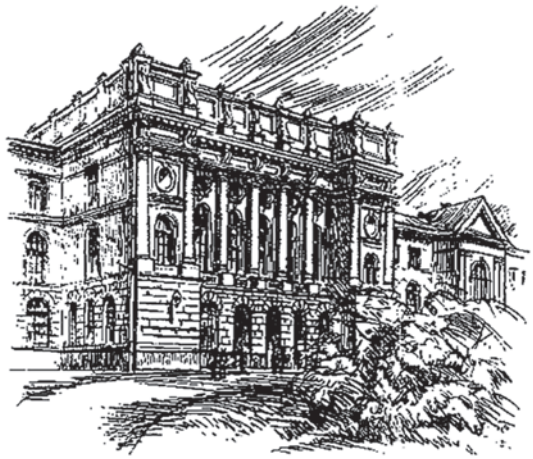
Журнал зарегистрирован Федеральной службой по надзору в сфере информационных технологий и массовых коммуникаций (Роскомнадзор). Свидетельство о регистрации ПИ № ФС77-51457 от 19.10.2012 г.

Подписной индекс **47517** в каталоге «Газеты. Журналы» Агентства «Роспечать».

Журнал включен в базу данных «Российский индекс научного цитирования» (РИНЦ), размещенную на платформе Национальной электронной библиотеки на сайте http://www.elibrary.ru

Адрес редакции и издательства: Россия, 195251, Санкт-Петербург, ул. Политехническая, д. 29.
Тел. редакции (812) 552-62-16.

THE MINISTRY OF EDUCATION AND SCIENCE OF THE RUSSIAN FEDERATION



ST. PETERSBURG STATE POLYTECHNICAL UNIVERSITY JOURNAL

Computer Science. Telecommunications and Control Systems

4(176) 2013

Polytechnical University Publishing House
Saint Petersburg
2013

The journal is published under scientific and methodical guidance of the Russian Academy of Sciences since 1995. The journal is published since 2008 as part of the periodical edition «Nauchno-tekhnicheskie vedomosti SPbGPU» (ISSN 1994-2354).

The journal is included in the List of Leading Peer-Reviewed Scientific Journals and other editions to publish major findings of PhD theses for the research degrees of Doctor of Sciences and Candidate of Sciences.

The publications are presented in the VINITI RAS Abstract Journal and Ulrich's Periodical Directory International Database.

The journal is registered with the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR). Certificate ПИ № ФС77-51457 issued Oct. 19, 2012.

Subscription index **47517** in the «Journals and Magazines» catalogue, Rospechat agency.

The journal is on the Russian Science Citation Index (RSCI) database

The address: 195251 Polytekhnicheskaya Str. 29, St. Petersburg, Russia.

Содержание

Высокопроизводительные вычисления

Contents

УДК 519.7

С.А. Диченко, Н.И. Елисеев, О.А. Финько

КОНТРОЛЬ ОШИБОК ФУНКЦИОНИРОВАНИЯ ГЕНЕРАТОРОВ ДВОИЧНЫХ ПСП, РЕАЛИЗОВАННЫХ НА АРИФМЕТИЧЕСКИХ ПОЛИНОМАХ

S.A. Dichenko, N.I. Eliseev, O.A. Finko

ERROR FUNCTION GENERATOR BINARY PRS CONTROL IMPLEMENTED ON ARITHMETIC POLYNOMIALS

Предложена методика повышения безопасности функционирования средств криптографической защиты информации (СКЗИ), в частности, узлов формирования двоичных псевдослучайных последовательностей (ПСП), действующих в условиях помех, генерируемых злоумышленником. Системы булевых характеристических уравнений реализуются линейными арифметическими полиномами, позволяющими распараллелить процесс вычисления элементов ПСП. «Арифметизация» логического счета, в свою очередь, позволила применить аппарат избыточных модулярных кодов для контроля ошибок функционирования узлов генерации ПСП и обеспечить тем самым, необходимую безопасность их функционирования в составе СКЗИ.

ДВОИЧНАЯ ПСЕВДОСЛУЧАЙНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ. ПАРАЛЛЕЛЬНЫЕ ЛОГИЧЕСКИЕ ВЫЧИСЛЕНИЯ ПОСРЕДСТВОМ АРИФМЕТИЧЕСКИХ ПОЛИНОМОВ. МОДУЛЯРНАЯ АРИФМЕТИКА. КОНТРОЛЬ ОШИБОК ФУНКЦИОНИРОВАНИЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ. ГЕНЕРАЦИЯ АППАРАТНЫХ ОШИБОК. КРИПТОГРАФИЯ. ШИФРУЮЩАЯ ГАММА.

A method of improving safety of the cryptographic protection of information (CPS), in particular the formation of binary nodes pseudorandom sequence (PRS), operating in a noise generated by an attacker. System of Boolean equations realize linear characteristic polynomial arithmetic, allowing parallelize the process of calculating the elements of the PRS. «Arithmetization» logical accounts, in turn, allowed the use of redundant modular device codes for error control operation of generating units and to provide bandwidth, thus the necessary security of their operation in the CPS.

BINARY PSEUDORANDOM SEQUENCE. PARALLEL LOGICAL CALCULATIONS BY POLYNOMIALS ARITHMETIC. MODULAR ARITHMETIC. THE ERROR CONTROL OPERATION OF THE CRYPTOGRAPHIC PROTECTION OF INFORMATION. GENERATION OF HARDWARE ERRORS. CRYPTOGRAPHY. CIPHER SCHEME.

Из перечня известных атак на СКЗИ важным является новый малоизученный вид атак, основанный на генерации аппаратных ошибок функционирования узлов СКЗИ [1]. Выработка мер защиты от данного вида атак необходима для решения задач обеспечения безопасности функционирования СКЗИ. Безопасность функционирования СКЗИ обеспечивается в т. ч. и за счет повышения достоверности их функционирования. В настоящее время необходимый уровень достоверности функционирования СКЗИ достигается и с помощью привлечения избыточного оборудования (резервирования), и с привлечением временной избыточности за счет различного рода повтора вычислений (реализации прямых и обратных преобразований с последующим сравнением результатов) [2].

Известно, что хорошие результаты для повышения достоверности функционирования цифровых устройств дают различные методы избыточного кодирования. Однако для логических типов данных, подверженных криптопреобразованиям, обеспечение кодового контроля вызывает множество за-

труднений [3]. В то же время известно, что контроль ошибок арифметических вычислений может эффективно обеспечиваться за счет использования методов избыточного модулярного кодирования, применение которых для осуществления контроля логических типов данных стало возможным, благодаря полученной в [4, 5] возможности представления логических операций арифметическими выражениями, в частности, арифметическими полиномами.

Цель статьи – повышение безопасности функционирования узлов СКЗИ методами модулярной арифметики.

Алгоритм генерации двоичных ПСП, реализованный на арифметических полиномах

Одним из основных узлов СКЗИ, как известно [1], наиболее подверженных атакам, основанных на генерации аппаратных ошибок, являются генераторы двоичных ПСП, т. к. от качества их функционирования напрямую зависит качество функционирования СКЗИ.

Генератор ПСП имеет важнейшее значение для различных криптоалгоритмов и систем генерации ключевого материала [6–8]. Наиболее распространенными и проверенными практикой являются алгоритмы генерации ПСП, основанные на использовании рекуррентных логических выражений и неприводимых полиномов [6–8].

В частности, наиболее простым по структуре является рекуррентный регистр сдвига с обратной связью, реализуемой некоторой функцией f (см. рисунок).

Из [9–14] известно, что большинство криптографических функций можно реализовать посредством арифметических полиномов. В частности, в [9, 13, 14] рассмотрены параллельные генераторы ПСП, основанные на линейных числовых полиномах (ЛЧП), где w-й блок участка двоичной ПСП можно представить посредством одного ЛЧП. Благодаря этому методу на выходе генератора может быть получен не один, а блок новых элементов ПСП необходимой длины.

Суть метода состоит в следующем. Пусть имеется характеристическое уравнение:

$$x_q = x_{q+\varphi-\tau} \oplus x_{q-\tau},$$

где $x_q, x_{q+\varphi-\tau}, x_{q-\tau} \in \{0,1\}$; $q \geq t$; $q \in N$, полученное на основе тринома (частный случай):

$$D(\chi) = \chi^{\tau} + \chi^{\varphi} + 1,$$

где τ – степень тринома, $\tau \in N$, $1 < \varphi < \tau - 1$, $\varphi \in N$.

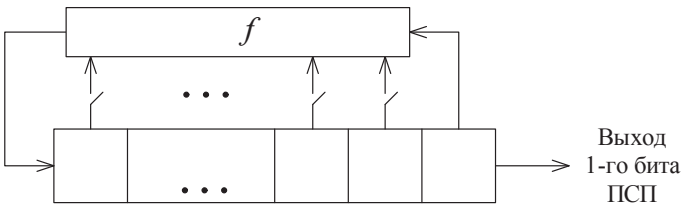
В соответствии с [13, 14] получим систему характеристических уравнений для участка ПСП длины τ:

$$\begin{cases} x_q = x_{q+\varphi-\tau} \oplus x_{q-\tau}, \\ x_{q+1} = x_{q+\varphi-\tau+1} \oplus x_{q-\tau+1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_{q+\tau-1} = x_{q+\varphi-1} \oplus x_{q-1}, \end{cases}$$

где $[x_{q-\tau}\ x_{q-\tau+1}\ \ldots\ x_{q-1}]$ – вектор начальных условий; $[x_q\ x_{q+1}\ \ldots\ x_{q+\tau-1}]$ – вектор участка ПСП; $x_\varphi \in \{0,1\}$; $\varphi = q - \tau + 1, \ldots, q + \tau - 1$.

Систему характеристических уравнений представим как систему булевых функций (БФ), которую в свою очередь, в соответствии с правилами, приведенными в [4, 5, 15], преобразуем в систему ЛЧП:

$$\begin{cases} L_q(x_{q-\tau}, x_{q-\tau+1}, \ldots, x_{q-1}) = \sum_{i=q-\tau}^{q-1} g_{q,i} x_i, \\ L_{q+1}(x_{q-\tau}, x_{q-\tau+1}, \ldots, x_{q-1}) = \sum_{i=q-\tau}^{q-1} g_{q+1,i} x_i, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_{q+\tau-1}(x_{q-\tau}, x_{q-\tau+1}, \ldots, x_{q-1}) = \sum_{i=q-\tau}^{q-1} g_{q+\tau-1,i} x_i, \end{cases}$$



Общий вид рекуррентного регистра сдвига с обратной связью

где $g_{\varepsilon,i}$ (здесь и далее) принимает значение ноль или единица в зависимости от вхождения в ε-й ЛЧП x_i; $\varepsilon = q, q+1, ..., q+\tau-1$. Результат вычисления ε-го ЛЧП системы представим двоичным машинным словом длины $l_\varepsilon = \left\lfloor \log\left(\sum_{i=q-\tau}^{q-1} g_{\varepsilon,i} \right) \right\rfloor + 1$.

Полученную систему ЛЧП представим посредством одного ЛЧП:

$$\begin{aligned} U &= L(x_{q-\tau}, x_{q-\tau+1}, ..., x_{q-1}) = \\ &= L_q(x_{q-\tau}, x_{q-\tau+1}, ..., x_{q-1}) + \\ &+ \sum_{j=q+1}^{q+\tau-1} 2^{\gamma_j} L_j(x_{q-\tau}, x_{q-\tau+1}, ..., x_{q-1}) = \\ &= g_{q,q-\tau}x_{q-\tau} + ... + g_{q,q-1}x_{q-1} + ... \\ &... + 2^{\gamma_{q+d-1}} g_{q+d-1,q-\tau}x_{q-\tau} + ... \\ &... + 2^{\gamma_{q+d-1}} g_{q+d-1,q-1}a_{q-1} = h_{q-\tau}x_{q-\tau} + \\ &+ h_{q-\tau+1}x_{q-\tau+1} + ... + h_{q-1}x_{q-1}, \end{aligned}$$

где $\gamma_j = \sum_{\varepsilon=q}^{j-1}(l_\varepsilon + 1)$; $h_i \in Z$;

$i = q-\tau, q-\tau+1, ..., q-1$.

Запишем ЛЧП следующим образом:

$$\begin{aligned} U &= L(\mathrm{X}) = h_0 + \sum_{i=1}^{r} h_i x_i = \\ &= h_0 + h_1x_1 + ... + h_rx_r, \end{aligned} \qquad (1)$$

где коэффициенты $h_0, h_1, ..., h_r$ – целые числа.

Первый способ контроля функционирования генераторов ПСП

В модулярной арифметике (МА) целый неотрицательный коэффициент ЛЧП (1) h_t $(t = 0, 1, ..., r)$ может быть однозначно представлен набором остатков по основаниям МА ($m_1, m_2, \ldots, m_n < m_{n+1} < \ldots < m_k$ – попарно простые, $M_n = m_1m_2 \ldots m_n > h_t$):

$$h_t = (\alpha_1, \alpha_2, ..., \alpha_n, \alpha_{n+1}, ..., \alpha_k)_{\mathrm{MA}}, \qquad (2)$$

где $\alpha_j = \left| h_t \right|_{m_j}$; $j = 1, 2, ..., n, n+1, ..., k$; $\left|\bullet\right|_m$ – наименьший неотрицательный остаток числа $\bullet$ по модулю m.

При этом остатки $\alpha_1, \alpha_2, ..., \alpha_n$ являются информационными, а $\alpha_{n+1}, ..., \alpha_k$ – контрольными (избыточными). МА в этом случае называется расширенной, где $M_k = m_1m_2 \ldots m_nm_{n+1} \ldots m_k$, и охватывает полное множество состояний, представляемых всеми k вычетами. Эта область будет являться полным диапазоном МА $[0, M_k)$ и состоять из рабочего диапазона $[0, M_n)$, где $M_n = m_1m_2 \ldots m_n$, и диапазона, определяемого избыточными основаниями $[M_n, M_k)$, представляющего недопустимую область. Это означает, что операции над числами h_t выполняются в диапазоне $[0, M_k)$. Поэтому если результат операции МА выходит за пределы M_n, то делается вывод о возникновении ошибки вычислений.

Для осуществления контроля ошибок при реализации ЛЧП рассмотрим МА, заданную основаниями $m_1, m_2, ..., m_n, m_{n+1}$. Представим каждый коэффициент ЛЧП h_t в виде (2), получим избыточный код МА, представленный системой ЛЧП:

$$\begin{cases} U^{(1)} = L^{(1)}(\mathbf{X}) = \\ = \alpha_0^{(1)} + \alpha_1^{(1)}x_1 + \ldots + \alpha_r^{(1)}x_r, \\ U^{(2)} = L^{(2)}(\mathbf{X}) = \\ = \alpha_0^{(2)} + \alpha_1^{(2)}x_1 + \ldots + \alpha_r^{(2)}x_r, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ U^{(n)} = L^{(n)}(\mathbf{X}) = \\ = \alpha_0^{(n)} + \alpha_1^{(n)}x_1 + \ldots + \alpha_r^{(n)}x_r, \\ U^{(n+1)} = L^{(n+1)}(\mathbf{X}) = \\ = \alpha_0^{(n+1)} + \alpha_1^{(n+1)}x_1 + \ldots + \alpha_r^{(n+1)}x_r, \end{cases} \qquad (3)$$

где вектор $\mathbf{X} = [x_1 \quad x_2 \quad \ldots \quad x_r]$.

Подставив в (3) значения остатков МА по соответствующим основаниям для каждого коэффициента (1), а также значения переменных $x_1, ..., x_r$, получим значения ЛЧП системы (3), где $U^{(1)}, U^{(2)}, ..., U^{(n)}, U^{(n+1)}$ – целые числа. В соответствии с Китайской теоремой об остатках (КТО) решим систему уравнений:

$$\begin{cases} U^* = \left|U^{(1)}\right|_{m_1}, \\ U^* = \left|U^{(2)}\right|_{m_2}, \\ \ldots\ldots\ldots\ldots \\ U^* = \left|U^{(n)}\right|_{m_n}, \\ U^* = \left|U^{(n+1)}\right|_{m_{n+1}}. \end{cases} \qquad (4)$$

Так как основания $m_1, m_2, ..., m_n, m_{n+1}$ попарно просты, то решением системы (4) является остаток по модулю $M_{n+1} = m_1m_2 \ldots m_{n+1}$:

$$U^* = \left| \sum_{s=1}^{n+1} M_{s,n+1} \mu_{s,n+1} U^{(s)} \right|_{M_{n+1}}, \qquad (5)$$

где $M_{s,n+1} = \dfrac{M_{n+1}}{m_s}$, $\mu_{s,n+1} = \left| M_{s,n+1}^{-1} \right|_{m_s}$.

Вхождение результата вычисления (5) в диапазон (контрольное выражение)

$$0 \le U^* < M_n \qquad (6)$$

означает отсутствие обнаруживаемых ошибок вычислений.

Пример 1. Пусть w-й блок участка двоичной ПСП представлен одним ЛЧП вида:

$$U = L(\mathbf{X}) = x_1 + 5x_2 + 20x_3 + 80x_4 + 64x_5.$$

Выберем основания МА: $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $m_4 = 7$, $m_5 = 11$ (m_5 – контрольное основание). Рабочий и полный диапазоны МА в этом случае соответственно равны: $M_4 = m_1 m_2 m_3 m_4 = 210$ и $M_5 = M_4 m_5 = 2310$. Представим каждый коэффициент ЛЧП с помощью кода МА:

$$h_1 = 1 = (1, 1, 1, 1, 1),$$
$$h_2 = 5 = (1, 2, 0, 5, 5),$$
$$h_3 = 20 = (0, 2, 0, 6, 9),$$
$$h_4 = 80 = (0, 2, 0, 3, 3),$$
$$h_5 = 64 = (0, 1, 4, 1, 9).$$

Получим систему (3):

$$\begin{cases} U^{(1)} = L^{(1)}(\mathbf{X}) = x_1 + x_2, \\ U^{(2)} = L^{(2)}(\mathbf{X}) = x_1 + 2x_2 + 2x_3 + 2x_4 + x_5, \\ U^{(3)} = L^{(3)}(\mathbf{X}) = x_1 + 4x_5, \\ U^{(4)} = L^{(4)}(\mathbf{X}) = x_1 + 5x_2 + 6x_3 + 3x_4 + x_5, \\ U^{(5)} = L^{(5)}(\mathbf{X}) = x_1 + 5x_2 + 9x_3 + 3x_4 + 9x_5. \end{cases}$$

Пусть $x_1 = 1$, $x_2 = 0$, $x_3 = 1$, $x_4 = 0$, $x_5 = 1$.

Тогда $U^{(1)} = 1$, $U^{(2)} = 4$, $U^{(3)} = 5$, $U^{(4)} = 8$, $U^{(5)} = 19$.

Решая систему (4):

$$\begin{cases} U^* = \left| 1 \right|_2, \\ U^* = \left| 4 \right|_3, \\ U^* = \left| 5 \right|_5, \\ U^* = \left| 8 \right|_7, \\ U^* = \left| 19 \right|_{11}, \end{cases}$$

в соответствии с (5) получим $U^* = 85$.

Так как полученный результат U^* удовлетворяет $0 \le U^* < 210$, то согласно (6) делается заключение об отсутствии ошибок.

Второй способ контроля функционирования генераторов ПСП

Из [9, 13, 14] известно, что w-й блок участка двоичной ПСП можно разбить на v-е подблоки и представить каждый из них одним ЛЧП, который определяется выражением:

$$U^{(v)} = L^{(v)}(X) = h_0^{(v)} + \sum_{i=1}^{r} h_i^{(v)} x_i^{(v)} =$$
$$= h_0^{(v)} + h_1^{(v)} x_1^{(v)} + \ldots + h_r^{(v)} x_r^{(v)},$$

где $v = 1, \ldots, z$.

Таким образом, для w-го блока участка двоичной ПСП можно получить систему ЛЧП:

$$\begin{cases} U^{(1)} = L^{(1)}(\mathbf{X}) = h_0^{(1)} + \sum_{i=1}^{r} h_i^{(1)} x_i, \\ U^{(2)} = L^{(2)}(\mathbf{X}) = h_0^{(2)} + \sum_{i=1}^{r} h_i^{(2)} x_i, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ U^{(z)} = L^{(z)}(\mathbf{X}) = h_0^{(z)} + \sum_{i=1}^{r} h_i^{(z)} x_i, \end{cases} \qquad (7)$$

где совокупность коэффициентов $h_0^{(v)}$, а также совокупность слагаемых $h_1^{(v)} x_1, \ldots, h_r^{(v)} x_r$ являются остатками МА:

$$\begin{cases} b_0 = (h_0^{(1)}, h_0^{(2)}, \ldots, h_0^{(z)})_{\text{МА}}, \\ b_1 = (h_1^{(1)} x_1, h_1^{(2)} x_1, \ldots, h_1^{(z)} x_1)_{\text{МА}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_r = (h_r^{(1)} x_r, h_r^{(2)} x_r, \ldots, h_r^{(z)} x_r)_{\text{МА}} \end{cases} \qquad (8)$$

по основаниям $m^{(1)}, m^{(2)}, \ldots, m^{(z)}$, выбранных по правилам:

1) $m^{(v)} \ge 2^{\rho}$, где ρ – максимальное количество двоичных разрядов, требуемых для представления результата вычисления v-го ЛЧП системы (7);

2) $m^{(1)}, m^{(2)}, \ldots, m^{(z)}$ – попарно простые.

Запишем систему (8) следующим образом:

$$\begin{cases} b_0 = (\beta_0^{(1)}, \beta_0^{(2)}, \ldots, \beta_0^{(z)})_{\text{МА}}, \\ b_1 = (\beta_1^{(1)}, \beta_1^{(2)}, \ldots, \beta_1^{(z)})_{\text{МА}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_r = (\beta_r^{(1)}, \beta_r^{(2)}, \ldots, \beta_r^{(z)})_{\text{МА}}, \end{cases}$$

где $\beta_0^{(v)} = h_0^{(v)}$, $\beta_i^{(v)} = h_i^{(v)} x_i$.

Из [16] известно, что при отсутствии ошибок вычислений каждое значение $b_0, b_1, ..., b_r$, полученное при решении систем сравнений, будет лежать в диапазоне $[0, M^{(z)})$, где $M^{(z)} = m^{(1)}m^{(2)}\dots m^{(z)}$. Например, для b_0 система уравнений имеет вид:

$$\begin{cases} b_0 = \left|\beta_0^{(1)}\right|_{m^{(1)}}, \\ b_0 = \left|\beta_0^{2)}\right|_{m^{(2)}}, \\ \dots\dots\dots\dots \\ b_0 = \left|\beta_0^{(z)}\right|_{m^{(z)}}. \end{cases}$$

Для корректного применения к системе (7) методов избыточного модулярного кодирования необходимо выполнить масштабирование системы путем введения дополнительного (попарно простого по отношению к другим основаниям) основания $m^{(0)}$ МА, где $m^{(0)} \geq r+1$ (r — наибольшая длина (количество слагаемых) ЛЧП из системы (7).

Ввод общего дополнительного основания $m^{(0)}$ в рамках операции масштабирования позволит выполнять операции над числами $b_0, b_1, ..., b_r$, лежащими в рабочем диапазоне $[0, M^{(z)})$, в более широком рабочем диапазоне $[0, r(M^{(z)}-1))$. Поэтому если в результате операции МА полученное число выходит за пределы $r(M^{(z)}-1)$, то делается вывод об ошибке вычислений.

Система ЛЧП (7) примет вид:

$$\begin{cases} U^{(0)} = L^{(0)}(\mathbf{X}) = h_0^{(0)} + \sum\limits_{i=1}^{r} h_i^{(0)} x_i, \\ U^{(1)} = L^{(1)}(\mathbf{X}) = h_0^{(1)} + \sum\limits_{i=1}^{r} h_i^{(1)} x_i, \\ U^{(2)} = L^{(2)}(\mathbf{X}) = h_0^{(2)} + \sum\limits_{i=1}^{r} h_i^{(2)} x_i, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ U^{(z)} = L^{(z)}(\mathbf{X}) = h_0^{(z)} + \sum\limits_{i=1}^{r} h_i^{(z)} x_i. \end{cases}$$

Вычислим значения элементов β_0, β_i ЛЧП $L^{(0)}(\mathbf{X})$, где $\beta_0 = h_0^{(0)}$, $\beta_i = h_i^{(0)} x_i$, решив КТО для отдельных групп остатков по основаниям МА:

$$\begin{cases} b_0 = (h_0^{(1)}, h_0^{(2)}, ..., h_0^{(z)})_{\text{МА}}, \\ b_1 = (h_1^{(1)} x_1, h_1^{(2)} x_1, ..., h_1^{(z)} x_1)_{\text{МА}}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ b_r = (h_r^{(1)} x_r, h_r^{(2)} x_r, ..., h_r^{(z)} x_r)_{\text{МА}}. \end{cases}$$

В случае неполного состава элементов ЛЧП (отсутствие некоторых переменных), необходимо выполнить выравнивание имеющихся элементов справа налево, оставшиеся свободные места заполнить нулями.

Полученные значения $b_0, b_1, ..., b_r$ необходимо взять по введенному модулю $m^{(0)}$, получим:

$$\begin{cases} \beta_0 = \left|b_0\right|_{m^{(0)}}, \\ \beta_1 = \left|b_1\right|_{m^{(0)}}, \\ \dots\dots\dots\dots \\ \beta_r = \left|b_r\right|_{m^{(0)}}. \end{cases}$$

Для осуществления контроля ошибок арифметических вычислений при реализации z-х ЛЧП рассмотрим МА, заданную основаниями $m^{(0)}, m^{(1)}, m^{(2)}, \dots, m^{(z)}, m^{(z+1)}$. Получим избыточный код МА, представленный системой ЛЧП вида:

$$\begin{cases} U^{(0)} = L^{(0)}(\mathbf{X}) = h_0^{(0)} + \sum\limits_{i=1}^{r} h_i^{(0)} x_i, \\ U^{(1)} = L^{(1)}(\mathbf{X}) = h_0^{(1)} + \sum\limits_{i=1}^{r} h_i^{(1)} x_i, \\ U^{(2)} = L^{(2)}(\mathbf{X}) = h_0^{(2)} + \sum\limits_{i=1}^{r} h_i^{(2)} x_i, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ U^{(z)} = L^{(z)}(\mathbf{X}) = h_0^{(z)} + \sum\limits_{i=1}^{r} h_i^{(z)} x_i, \\ U^{(z+1)} = L^{(z+1)}(\mathbf{X}) = h_0^{(z+1)} + \sum\limits_{i=1}^{r} h_i^{(z+1)} x_i. \end{cases} \quad (9)$$

Подставив в (9) известные значения остатков МА по соответствующим основаниям, а также вычислив аналогично с вычислениями для $L^{(0)}(\mathbf{X})$ значения элементов для ЛЧП $L^{(z+1)}(\mathbf{X})$, получим значения ЛЧП системы (9), где $U^{(0)}, U^{(1)}, U^{(2)}, ..., U^{(z)}, U^{(z+1)}$ — целые числа.

Решим систему:

$$\begin{cases} U^* \equiv \left|U^{(0)}\right|_{m^{(0)}}, \\ U^* \equiv \left|U^{(1)}\right|_{m^{(1)}}, \\ U^* \equiv \left|U^{(2)}\right|_{m^{(2)}}, \\ \dots\dots\dots\dots \\ U^* \equiv \left|U^{(z)}\right|_{m^{(z)}}, \\ U^* \equiv \left|U^{(z+1)}\right|_{m^{(z+1)}}. \end{cases} \quad (10)$$

Так как основания $m^{(0)}, m^{(1)}, m^{(2)}, ..., m^{(z)}, m^{(z+1)}$ попарно просты, то решением (10) является наименьший неотрицательный вычет по модулю $M^{(z+1)} = m^{(1)}m^{(2)} \dots m^{(z+1)}$:

$$U^* = \left| \sum_{s=0}^{z+1} M^{(s,z+1)} \mu^{(s,z+1)} U^{(s)} \right|_{M^{(z+1)}}, \qquad (11)$$

где $M^{(s,z+1)} = \dfrac{M^{(z+1)}}{m^{(s)}}$, $\mu^{(s,z+1)} = \left| M^{(s,z+1)-1} \right|_{m^{(s)}}$.

Вхождение результата вычисления (11) в диапазон (контрольное выражение)

$$0 \le U^* < r(M^{(z)} - 1) \qquad (12)$$

означает отсутствие обнаруживаемых ошибок вычислений.

Пример 2. Пусть *w*-й блок участка двоичной ПСП разбит на *v*-е подблоки, каждый из которых представлен одним ЛЧП. Система (7) имеет вид:

$$\begin{cases} U^{(1)} = L^{(1)}(\mathbf{X}) = x_1 + 5x_2 + 4x_3, \\ U^{(2)} = L^{(2)}(\mathbf{X}) = x_3 + 5x_4 + 4x_5, \\ U^{(3)} = L^{(3)}(\mathbf{X}) = 5x_1 + x_2 + 4x_3 + x_5. \end{cases}$$

Выберем основания системы: $m^{(1)} = 16$, $m^{(2)} = 17$, $m^{(3)} = 19$.

Вычислим значение рабочего диапазона: $M^{(3)} = m^{(1)}m^{(2)}m^{(3)} = 5168$.

Выполним выравнивание имеющихся элементов ЛЧП справа налево, оставшиеся свободные места заполним нулями. Для наглядности запишем систему ЛЧП следующим образом:

$$\begin{cases} U^{(1)} = L^{(1)}(\mathbf{X}) = 0 + x_1 + 5x_2 + 4x_3, \\ U^{(2)} = L^{(2)}(\mathbf{X}) = 0 + x_3 + 5x_4 + 4x_5, \\ U^{(3)} = L^{(3)}(\mathbf{X}) = 5x_1 + x_2 + 4x_3 + x_5. \end{cases}$$

Выполним операцию масштабирования (введем дополнительное основание $m^{(0)} = 5$) и получим:

$$\begin{cases} U^{(0)} = L^{(0)}(\mathbf{X}) = h_1^{(0)}x_1 + h_2^{(0)}(x_1, x_2, x_3) + \\ + h_3^{(0)}(x_2, x_3, x_4) + h_4^{(0)}(x_3, x_5), \\ U^{(1)} = L^{(1)}(\mathbf{X}) = 0 + x_1 + 5x_2 + 4x_3, \\ U^{(2)} = L^{(2)}(\mathbf{X}) = 0 + x_3 + 5x_4 + 4x_5, \\ U^{(3)} = L^{(3)}(\mathbf{X}) = 5x_1 + x_2 + 4x_3 + x_5. \end{cases}$$

В соответствии с КТО вычислим значения элементов $\beta_1, \beta_2, \beta_3, \beta_4$ ЛЧП $L^{(0)}(\mathbf{X})$ для отдельных групп остатков по основаниям МА:

$$\begin{cases} b_1 = (0, 0, 5x_1)_{\text{МА}}, \\ b_2 = (x_1, x_3, x_2)_{\text{МА}}, \\ b_3 = (5x_2, 5x_4, 4x_3)_{\text{МА}}, \\ b_4 = (4x_3, 4x_5, x_5)_{\text{МА}}. \end{cases}$$

Получим:

0	0	$h_1^{(3)}x_1$	β_1
0	0	0	0
0	0	5	3

$h_2^{(1)}x_1$	$h_2^{(2)}x_3$	$h_2^{(3)}x_2$	β_2
0	0	0	0
0	0	1	2
0	1	0	2
0	1	1	1
1	0	0	3
1	0	1	2
1	1	0	2
1	1	1	1

$h_3^{(1)}x_2$	$h_3^{(2)}x_4$	$h_3^{(3)}x_3$	β_3
0	0	0	0
0	0	4	4
0	5	0	4
0	5	4	3
5	0	0	1
5	0	4	0
5	5	0	0
5	5	4	1

$h_4^{(1)}x_3$	$h_4^{(2)}x_5$	$h_4^{(3)}x_5$	β_4
0	0	0	0
0	0	1	2
0	4	0	0
0	4	1	4
4	0	0	1
4	0	1	0
4	4	0	3
4	4	1	2

Пусть $x_1 = x_2 = x_3 = x_4 = x_5 = 1$, тогда система ЛЧП примет вид:

$$\begin{cases} U^{(0)} = L^{(0)}(\mathbf{X}) = 3 + 1 + 1 + 2 = 7, \\ U^{(1)} = L^{(1)}(\mathbf{X}) = 0 + 1 + 5 + 4 = 10, \\ U^{(2)} = L^{(2)}(\mathbf{X}) = 0 + 1 + 5 + 4 = 10, \\ U^{(3)} = L^{(3)}(\mathbf{X}) = 5 + 1 + 4 + 1 = 11. \end{cases}$$

Рабочий диапазон после масштабирования равен $r(M^{(z)} - 1) = 20668$.

Для осуществления контроля ошибок при реализации *z*-х ЛЧП введем избыточное основание $m^{(4)} = 21$. Получим избыточный код МА, представленный системой ЛЧП вида:

$$\begin{cases} U^{(0)} = L^{(0)}(\mathbf{X}) = 3+1+1+2 = 7, \\ U^{(1)} = L^{(1)}(\mathbf{X}) = 0+1+5+4 = 10, \\ U^{(2)} = L^{(2)}(\mathbf{X}) = 0+1+5+4 = 10, \\ U^{(3)} = L^{(3)}(\mathbf{X}) = 5+1+4+1 = 11, \\ U^{(4)} = L^{(4)}(\mathbf{X}) = 17+1+2+16 = 36. \end{cases}$$

В соответствии с КТО решим систему:

$$\begin{cases} U^* \equiv |7|_5, \\ U^* \equiv |10|_{16}, \\ U^* \equiv |10|_{17}, \\ U^* \equiv |11|_{19}, \\ U^* \equiv |36|_{21}. \end{cases}$$

В соответствии с (11) получим $U^* = 4362$. Так как $0 \le U^* < 20668$, то согласно (12) делается заключение об отсутствии ошибок.

Таким образом, использование методов МА для реализации логических операций, в частности, при формировании ПСП и ключевых последовательностей, помимо повышения производительности СКЗИ позволяет получить важные преимущества по повышению безопасности их функционирования.

СПИСОК ЛИТЕРАТУРЫ

1. **Yang, B.** Scan Based Side Channel Attack on Data Encryption Standard [Электронный ресурс] / B. Yang, K. Wu, R. Karri// Report. −2004/083. −Режим доступа http://eprint.iacr.org (Дата обращения 2004).

2. **Щербаков, Н.С.** Достоверность работы цифровых устройств [Текст] / Н.С. Щербаков. − М.: Машиностроение, 1989. − 224 с.

3. **Савельев, А.Я.** Прикладная теория цифровых автоматов [Текст] / А.Я. Савельев. − М.: Высш. школа, 1987. − 272 с.

4. **Малюгин, В.Д.** Параллельные логические вычисления посредством арифметических полиномов [Текст] / В.Д. Малюгин. − М.: Физматлит, 1997. − 192 с.

5. **Финько, О.А.** Реализация систем булевых функций большой размерности методами модулярной арифметики [Текст] / О.А. Финько // Автоматика и телемеханика. − 2004. − № 6. − С. 37−60.

6. **Бабаш, А.В.** Криптография [Текст] / А.В. Бабаш, Г.П. Шанкин; под ред. В.П. Шерстюка, Э.А. Применко. −М.: СОЛОН-П Gutmann ПРЕСС, 2007. − 512 с.

7. **Шнайер, Б.** Практическая криптография [Текст] / Б. Шнайер. − М.: ИД «Вильямс», 2005. − 424 с.

8. **Фороузан, Б.А.** Криптография и безопасность сетей: Учеб. пособие [Текст] / Б.А. Фороузан ; пер. с англ. под ред. А.Н. Берлина. − М.: Интернет-Университет информационных технологий: БИНОМ. Лаборатория знаний, 2010. − 784 с.

9. **Финько, О.А.** Самопроверяемый специализированный вычислитель систем булевых функций [Текст] / О.А. Финько, С.А. Диченко, А.К. Вишневский // Патент России № 2485575, 20.06.2013.

10. **Финько, О.А.** Арифметический вычислитель систем булевых функций [Текст] / О.А. Финько, А.К. Вишневский, С.А. Диченко, Д.В. Самойленко [и др.] // Патент России № 2461868, 20.09.2012.

11. **Финько, О.А.** Самопроверяемый модулярный вычислитель систем логических функций [Текст] / О.А. Финько, С.М. Сульгин, А.В. Щербаков [и др.] // Патент России № 2417405, 27.04.2011.

12. **Финько, О.А.** Модулярный вычислитель систем логических функций [Текст] / О.А. Финько, А.В. Щербаков // Патент России № 2417303, 16.11.2009.

13. **Диченко, С.А.** Реализация двоичных псевдослучайных последовательностей линейными числовыми полиномами [Текст] / С.А. Диченко, А.К. Вишневский, О.А. Финько // Изв. Южного федерального ун-та. Технические науки. − 2011. −№ 12. − С. 130−140.

14. **Диченко, С.А.** Алгоритм генерации блочной ПСП, основанный на применении логико-числовых форм [Текст] / С.А. Диченко, О.А. Финько // Изв. Южного федерального ун-та. Технические науки. − 2012. −№ 12. − С. 158−166.

15. **Yanushkevich, L.** Logic design of nano-ICs [Text] / S. Yanushkevich, V. Shmerko, S. Lyshevski. −CRC Press, 2005.

16. **Акушский, И.Я.** Машинная арифметика в остаточных классах [Текст] / И.Я. Акушский, Д.И. Юдицкий. − М.: Сов. радио, 1968. − 440 с.

REFERENCES

1. **Yang B., Wu K., Karri R.** Scan Based Side Channel Attack on Data Encryption Standard / Report. – 2004/083, http://eprint.iacr.org, 2004.

2. **Shcherbakov N.S.** Dostovernost' raboty tsifrovykh ustroistv. – Moscow: Mashinostroenie, 1989. – 224 s. (rus)

3. **Savel'ev A.Ia.** Prikladnaia teoriia tsifrovykh avtomatov. – Moscow: Vyssh. shkola, 1987. – 272 s. (rus).

4. **Maliugin V.D.** Parallel'nye logicheskie vychisleniia posredstvom arifmeticheskikh polinomov. – Moscow: Fizmatlit, 1997. – 192 s. (rus)

5. **Fin'ko O.A.** Realizatsiia sistem bulevykh funktsii bol'shoi razmernosti metodami moduliarnoi arifmetiki / Avtomatika i telemekhanika. – 2004. – № 6. – S. 37–60. (rus)

6. **Babash A.V., Shankin G.P.** Kriptografiia; pod red. V.P. Sherstiuka, E.A. Primenko. – Moscow: SOLON-P Gutmann PRESS. – 512 s. (rus)

7. **Shnaier B.** Prakticheskaia kriptografiia. – Moscow: ID «Vil'iams», 2005. – 424 s. (rus)

8. **Forouzan B.A.** Kriptografiia i bezopasnost' setei: Ucheb. posobie; per. s angl.; pod red. A.N. Berlina. – Moscow: Internet-Universitet Informatsionnykh Tekhnologii: BINOM. Laboratoriia znanii, 2010. – 784 s. (rus)

9. **Fin'ko O.A., Dichenko S.A., Vishnevskii A.K.** Samoproveriaemyi spetsializirovannyi vychislitel' sistem bulevykh funktsii / Patent Rossii № 2485575, 20.06.2013. (rus)

10. **Fin'ko O.A., Vishnevskii A.K., Dichenko S.A., Samoilenko D.V. i dr.** Arifmeticheskii vychislitel' sistem bulevykh funktsii / Patent Rossii № 2461868, 20.09.2012. (rus)

11. **Fin'ko O.A., Sul'gin S.M., Shcherbakov A.V. i dr.** Samoproveriaemyi moduliarnyi vychislitel' sistem logicheskikh funktsii / Patent Rossii № 2417405, 27.04.2011. (rus)

12. **Fin'ko O.A., Shcherbakov A.V.** Moduliarnyi vychislitel' sistem logicheskikh funktsii / Patent Rossii № 2417303, 16.11.2009. (rus)

13. **Dichenko S.A., Vishnevskii A.K., Fin'ko O.A.** Realizatsiia dvoichnykh psevdosluchainykh posledovatel'nostei lineinymi chislovymi polinomami / Izv. Iuzhnogo federal'nogo un-ta. Tekhnicheskie nauki. –2011. – № 12 – S. 130–140. (rus)

14. **Dichenko S.A.**, **Fin'ko O.A.** Algoritm generatsii blochnoi PSP, osnovannyi na primenenii logiko-chislovykh form / Izv. Iuzhnogo federal'nogo un-ta. Tekhnicheskie nauki. –2012. –№ 12. – S. 158–166. (rus)

15. **Yanushkevich L., Shmerko V., Lyshevski S.** Logic design of nanoICs. – CRC Press, 2005.

16. **Akushskiy I.Ya., Yuditskiy D.I.** Mashinnaya arifmetika v ostatochnykh klassakh. – Moscow: Sov. radio, 1968. – 440 s. (rus)

ДИЧЕНКО Сергей Александрович – *адъюнкт филиала Военной академии связи (г. Краснодар).*
350035, Россия, г. Краснодар, ул. Красина, д. 4.

DICHENKO, Sergey A. *Military Academy of Communications (Krasnodar).*
350035, Krasin Str. 4, Krasnodar, Russia

ЕЛИСЕЕВ Николай Иванович – *доцент кафедры специальной техники филиала Военной академии связи (г. Краснодар), кандидат технических наук.*
350035, Россия, г. Краснодар, ул. Красина, д. 4.

ELISSEEV, Nikolai I. *Military Academy of Communications (Krasnodar).*
350035, Krasin Str. 4, Krasnodar, Russia

ФИНЬКО Олег Анатольевич – *профессор кафедры обеспечения безопасности информации в автоматизированных системах филиала Военной академии связи (г. Краснодар), доктор технических наук, профессор.*
350035, Россия, г. Краснодар, ул. Красина, д. 4.
E-mail: ofinko@yandex.ru; URL: http://финько.рф

FINKO, Oleg A. *Military Academy of Communications (Krasnodar).*
350035, Krasin Str. 4, Krasnodar, Russia
E-mail: ofinko@yandex.ru; URL: http://ofinko.ru

НАУЧНОЕ ИЗДАНИЕ

«НАУЧНО-ТЕХНИЧЕСКИЕ ВЕДОМОСТИ САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО ПОЛИТЕХНИЧЕСКОГО УНИВЕРСИТЕТА. ИНФОРМАТИКА. ТЕЛЕКОММУНИКАЦИИ. УПРАВЛЕНИЕ»

«ST. PETERSBURG STATE POLYTECHNICAL UNIVERSITY JOURNAL. COMPUTER SCIENCE. TELECOMMUNICATIONS AND CONTROL SYSTEMS»

№ 4 (176) 2013

Учредитель – Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный политехнический университет»

Журнал зарегистрирован Федеральной службой по надзору в сфере информационных технологий и массовых коммуникаций (Роскомнадзор). Свидетельство о регистрации ПИ № ФС77-51457 от 19.10.2012 г.

Телефон редакции (812)552-62-16, 297-18-21

E-mail: infocom@spbstu.ru

Компьютерная верстка *А.Н. Смирнов*

Директор Издательства Политехнического университета *А.В. Иванов*

Лицензия ЛР № 020593 от 07.08.97

Подписано в печать 29.08.2013. Формат 60×84 1/8. Бум. тип. № 1.
Печать офсетная. Усл. печ. л. 18,83. Уч.-изд. л. 18,83. Тираж 1000. Заказ

Санкт-Петербургский государственный политехнический университет
Издательство Политехнического университета
член Издательско-полиграфической ассоциации университетов России
Адрес университета и издательства: 195251, Санкт-Петербург, ул. Политехническая, д. 29.