УДК 681.3

АЛГОРИТМ ВЫЧИСЛЕНИЯ ОРТОГОНАЛЬНЫХ БАЗИСОВ ДЛЯ СИСТЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА С ДИНАМИЧЕСКИ ИЗМЕНЯЕМОЙ ГРУППОЙ АБОНЕНТОВ

Зюзякин Г.И., Калмыков М.И., Степанова Е.П.

Федеральное государственное автономное образовательное учреждение высшего профессионального образования «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ», Ставрополь, Россия, e-mail: kia762@yandex.ru

Чтобы повысить степень защиты данных от несанкционированного доступа в системе, в которой постоянно динамически происходит изменение числа абонентов, необходимо использовать схемы разделения секрета. Такие схемы позволяет только определенному числу пользователей группы восстановить секретный ключ из его образов при работе в многопользовательской информационной системе. Рассмотрен алгоритм модулярной схемы разделения секрета, функционирующий в полиномиальной системе классов вычетов. Представлен алгоритм пересчета ортогональных базисов и его схемная реализация, применение которой позволяет в динамике осуществлять вычисление секрета в постоянно изменяющейся группе пользователей.

Ключевые слова: разделение секрета, остатки, полиномиальная система классов вычетов, китайская теорема об остатках, ортогональные базисы, вес ортогонального базиса

ALGORITHM FOR COMPUTING AN ORTHOGONAL BASIS SYSTEM FOR SECRET SHARING WITH DYNAMIC STATION GROUPS

Zyuzyakin G.I, Kalmykov M.I., Stepanova E.P.

Federal state Autonomous educational institution higher professional education «NORTH-CAUCASIAN FEDERAL UNIVERSITY», Stavropol, Russia, e-mail: kia762@yandex.ru

To increase the degree of protection against unauthorized access to the system, which is constantly dynamically changes the number of subscribers , it is necessary to use the secret sharing schemes . Such schemes allow only a certain number of users in the group to recover the secret key of his images in a multi-user information system. An algorithm for modular secret sharing schemes operating in polynomial system of residue classes . An algorithm for the conversion of orthogonal bases and the circuit implementation , the use of which allows to carry out the calculation of secretion dynamics in a constantly changing group of users.

Keywords: separation secret residues polynomial system of residue classes, the Chinese remainder theorem , orthogonal bases , orthogonal basis weight

Введение

Применение современных IT-технологий практически во всех сферах человеческой деятельности привело к ситуации, когда вопросы обеспечения защиты данных от несанкционированного доступа (НСД) становятся обязательными при построении информационных систем. При этом очевидно, что дальнейшее увеличение объемов хранимой и передаваемой информации приводит к наращиванию потенциальных возможностей злоумышленника по НСД к информационной сфере. Решить данную задачу можно только на основе комплексного подхода.

Одним из направлений обеспечения требуемого уровня защиты информации от НСД является использование схем разделения секрета. Применение таких схемы позволяет определенной группе пользователей восстановить секретный ключ из его образов при работе в многопользовательской информационной системе.

Решение задачи

Несмотря на многообразие схем разделения секретного ключа на секретные доли, все они решают задачу сохранения ключевых данных от НСД, которые при определенных условиях будут восстановлены и использованы в системеобработки и передачи данных. При этом схемы построены таким образом, что ни один абонент группы не сможет вычислить пароль без помощи других абонентов группы.

Рассматривая различные схемы разделения секрета можно отметить, что они состоят из двух взаимосвязанных протоколов:

- протокола формирования и распределения долей секрета между абонентами;
- протокола восстановления секрета группой пользователей с помощью их секретных долей.

В основу первого протокола положен алгоритм действий системы и пользователей, в результате которых каждый авторизованный абонент получает свою долю секретно-

го ключа. Второй протокол применяется для того, чтобы законные пользователи, собравшись вместе и объединив свои секретные доли, могли восстановить секретный ключ.

Рассмотрим модулярную схему разделения секрета и проведем ее реализациюв полиномиальной системе классов вычетов (ПСКВ). В данной алгебраической системе в качестве модулей используются неприводимые полиномы $p_i(z)$. Благодаря своим особенностям полиномиальная система классов вычетов в настоящее время может быть использована в системах цифровой обработки сигналов, при построении систем криптографической защиты данных [1-6], а также для реализации процедур поиска и коррекции ошибок [8,9]. Следует отметить, что полиномиальная система классов вычетов может быть положена в основуалгоритма работы пороговой схемы*(t, N)* разделения секрета. Для реализации *(t, N)*-пороговой схемы разделения секрета выбирается неприводимые полиномы удовлетворяющие условию

$$\deg p_1(z) \le \deg p_2(z) \le ... \le \deg p_n(z) . \quad (1)$$

Затем определяется полином $p_x(z)$, такой что

$$\deg p_i(z) \le \deg p_x(z) , \quad (2)$$

где$i=1, 2, ..., n$.

Данный полином определяет максимальное количество разрядов секретного ключа*M(z)* согласно

$$\deg p_x(z) > \deg M(z) , \quad (3)$$

где *M(z)* - полиномиальную форму секретного ключа.

С целью обеспечения правильной работы схемы разделения секрета, использующего *(t, N)*-пороговую схему, представленную в ПСКВ,осуществляется проверка

$$\deg(p_1(z)p_2(z)...p_t(z)) > \deg(p_x(z)p_{n-t+2}(z)p_{n-t+3}(z)...p_n(z)) . \quad (4)$$

Так как делить секретный ключ на отдельные части и распределять его пользователям нельзя, то в алгоритме предлагается провести «затемнение секрета», используя выражение

$$M^*(z) = M(z) + r(z)p_x(z) . \quad (5)$$

где *r(z)* – полном, выбираемый для затемнения секрета.

Затем затемненный образ секрета делится на части согласно

$$M_i^*(z) \equiv M(z) \bmod p_i(z) . \quad (6)$$

и в виде долейраспределяется между абонентами группы.Кроме долей образа *M*(z)* пользователям по закрытому каналу рассылаются значение полиномов $p_i(z)$,*r(z)* и$p_x(z)$.Таким образом, каждый член группы получает свои данные, с помощью которых группа сможет восстановить секрет.

Для восстановления зашумленного образа секрета *M*(z)* необходимо наличие, как минимум, *t*пользователей, которые применяют китайскую теорему об остатках, в соответствии

$$M^*(z) = \sum_{i \in t} M_i^*(z) B_i^t(z) \bmod P_t(z) , \quad (7)$$

где $B_i^t(z)$ - *i*-й ортогональный базис в системе, состоящей из *t* пользователей; $P_t(z)$ - полный диапазон, определяемый основаниями *t* пользователей.

При этом данный диапазон задается набором оснований согласно

$$P_t(z) = \prod_{i \in t} p_i(z) . \quad (8)$$

Используя выражения (7) и (8), *t* и более пользователей способны восстановить *M*(z)*, а затем, зная *r(z)* и $p_x(z)$, определить секрет *M(z)*.

Однако, как показывает анализ работ [1,7,10], вычисление значения ортогонального базиса для динамически меняющегося набора пользователей группы является довольно сложной задачей. Решить данную задачу можно только на основе алгоритма, позволяющего эффективно осуществить процедуру пересчета ортогональных базисов.Для получения ортогонального базиса необходимо знать $P_t(z)$ - полный диапазон, определяемый основаниями *t* пользователей. Тогда

$$B_j(z) = m_j(z) P_t(z) / p_j(z) , \quad (9)$$

где $m_j(z)$ –вес ортогонального базиса *j* – го основания

Именно вычисление значения веса ортогонального базиса является наиболее сложно операцией. Известно [7], что использова-

ние $m_j(z)$ позволяет обеспечить выполнение условия

$$B_j(z) \equiv 1 \bmod p_j(z). \quad (10)$$

Подставим равенства (8) и (10) в выражение (9). Тогда получаем

$$B_j(z) \equiv m_j(z)\prod_{\substack{i=1\\ i\neq j}}^{t} p_j(z). \quad (11)$$

Воспользуемся равенством (11) и выражением (10). В этом случаеимеем

$$m_j(z)\prod_{\substack{i=1\\ i\neq j}}^{t} p_j(z) \equiv 1 \bmod p_j(z). \quad (12)$$

Разделив обе части равенства (5.6) на величину

$$P_j(z) = \prod_{\substack{i=1\\ i\neq j}}^{t} p_j(z)$$

получаем

$$m_j(z) = (\prod_{\substack{i=1\\ i\neq j}}^{t} p_j(z))^{-1} \bmod p_j(z). \quad (13)$$

Принимая во внимание попарную простоту модулей ПСКВ, имеем

$$m_j^i(z) = p_i(z)^{-1} \bmod p_j(z). \quad (14)$$

Тогда значение веса ортогонального базиса будет определяться

$$m_j(z) = (\prod_{\substack{i=1\\ i\neq j}}^{t} m_j^i(z)) \bmod p_j(z). \quad (15)$$

Таким образом, очевидно, что величина веса ортогонального базиса определяется произведением величин обратных основаниям $p_i(z)$ по модулю $p_j(z)$. Рассмотренный выше алгоритм вычисления значений ортогонального базиса ПСКВ представлен в работе[7]. В таблице 1 представлены значения $m^i_j(z)$ для модулей ПСКВ $p_1(z)=z+1$; $p_2(z)=z^2+z+1$;$p_3(z)=z^4+z^3+z^2+z^1+1$; $p_4(z)=z^4+z^3+1$; $p_5(z)=z^4+z+1$.

Таблица 1

Величины $m^i_j(z)$ для поля $GF(2^4)$.

	Значение $p_i(z)$ основания ПСКВ				
	$p_1(z)$	$p_2(z)$	$p_3(z)$	$p_4(z)$	$p_5(z)$
$m^i_1(z)$	-	1	1	1	1
$m^i_2(z)$	z	-	z	$z+1$	1
$m^i_3(z)$	z^3+z	z^3+1	-	z^2+1	z^3+z^2+1
$m^i_4(z)$	z^3	z^3+z^2+z	z^2	-	z^3+z+1
$m^i_5(z)$	z^3+z^2+z	z^2+z	z^3+z	z^3+z^2	-

На рисунке 1 показана структура устройства вычисления ортогонального базиса для схемы разделения секрета, функционирующего в ПСКВ.

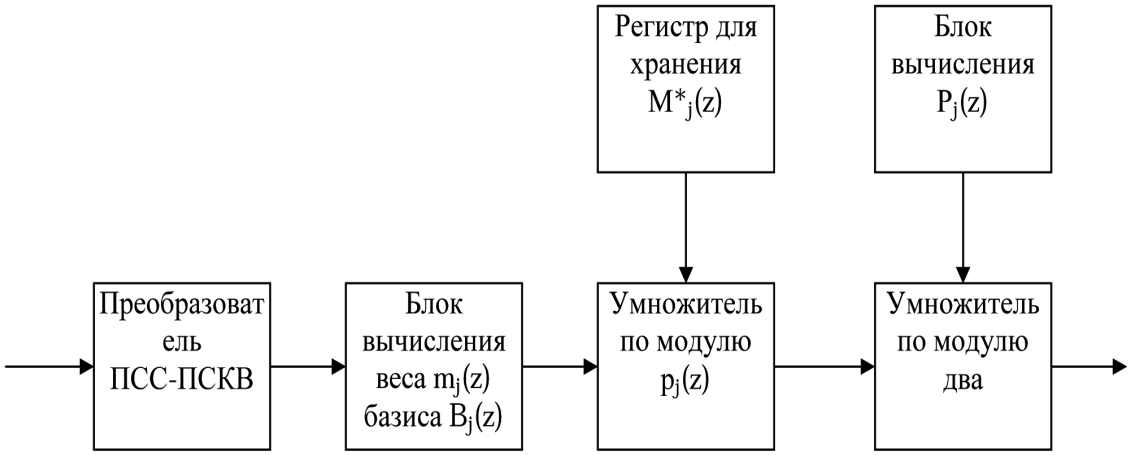

Рисунок 1 - Устройства вычисления ортогонального базиса для схемы разделения секрета, функционирующего в ПСКВ

Устройство работает следующим образом. На вход устройства подается значение модуля $p_i(z)$, где $i \in t$. Данный полином поступает от другого пользователя, входящего в состав группы из t пользователей, желающих получить значение секретного ключа. Значение основания поступает на вход преобразователь из позиционной системы в полиномиальную систему класса вычетов. С выхода данного преобразователя ПСС-ПСКВ снимается значение $p_i(z)$ mod$p_j(z)$. Полученный остаток поступает на вход блока вычисления веса $m_j(z)$ для ортогонального базиса $B_j(z)$.

Затем вычисленное значение веса $m_j(z)$ ортогонального базиса $B_j(z)$, как наглядно видно на рисунке 1, подается на первый вход умножителя по модулю $p_j(z)$, на второй вход которого поступает с регистра хранения значение затемненного секрета$M^*_j(z)$. Полученный результат поступает на первый вход умножителя по модулю два. Данное устройство реализует вычисление

$$M_j^*(z)B_j(z) = M_j^*(z)m_j(z)P_j(z) = M_j^*(z)m_j(z)\prod_{\substack{i=1\\ i\neq j}}^{t} p_i(z) \qquad (16)$$

Пользователя группы обмениваются вычисленными значениями $M^*_j(z)B_j(z)$, а затем, используя выражение (7), вычисляют зашумленный образ секретного ключа M*(z). После этого, зная значения полиномов $r(z)$ и $p_x(z)$, пользователи способны определить и сам секретный ключ$M(z)$.

Рассмотрим алгоритм работы блока вычисления веса ортогонального базиса. Структура этого блока показана на рисунке 2.

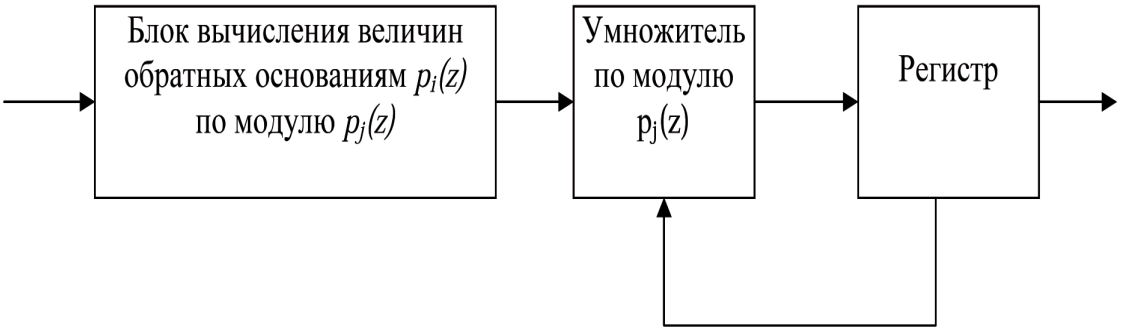

Рисунок 2 – Структура блока вычисления веса ортогонального базиса

Вычисленное значение $p_i(z)$mod$p_j(z)$ подается на вход блока вычисления величин обратных основаниям $p_i(z)$по модулю $p_j(z)$.С выхода последнего снимается полученное значение $m^i_i(z)=p_j(z)^{-1}$mod$p_j(z)$. Это значение подается на первый вход умножителя по модулю $p_j(z)$. Второй вход этого умножителя подключен к выходу регистра. В данный регистр записываются промежуточные результаты вычисления выражения (15). Таким образом, за t тактов будет получено значение веса ортогонального базиса $B_j(z)$.

Выводы

Таким образом, применение полиномиальной системы классов вычетов позволяет реализовать эффективную систему разделения секрета, позволяющей группе авторизованных пользователей восстанавливать общий секретный ключ по его образам. Применение разработанного алгоритма пересчета ортогональных базисов обеспечивает осуществление в реальном масштабе времени процесса восстановление секрета даже при динамически изменяющейся группе пользователей.

Список литературы

1. Дагаева О.И., Калмыков И.А., Кихтенко О. А., Барильская А.В. Криптографическая система на базе непозиционных полиномиальных алгебраических структур// Вестник Северо-Кавказского федерального университета. 2010. № 2. С. 51-57

2. Дагаева О.И., Калмыков И.А. Разработка псевдослучайной функции повышенной эффективности// Известия Южного федерального университета. Технические науки. 2011. Т.125. № 12. С.160-169.

3. Калмыков И.А. Чипига А.А. Алгоритм обеспечения информационной скрытности для адаптивных средств передачи информации// Инфокоммуникационные технологии. Самара. – 2007. - Т.5. №2. - С. 159-162.

4. Калмыков И.А., Барильская А.В., Кихтенко О. А. Разработка математической модели криптографической защиты информации, функционирующей в полиномиальной системы классов вычетов// Информационные системы и технологии. 2010. № 4. С.138-145.

5. Калмыков И.А., Стрекалов Ю.А., Щелкунова Ю.О., Кихтенко О. А., Барильская А.В. Технология нелинейного шифрования данных в высокоскоростных сетях связи // Инфокоммуникационные технологии. 2010. Т.8. № 2. С. 14-22

6. Калмыков И.А., Чипига А.Ф., Барильская А.В., Кихтенко О. А. Криптографическая защита данных в информационных технологиях на базе непозиционных полиномиальных систем// Известия Южного федерального университета. Технические науки. 2009. Т.100. № 11. С.210-220.

7.Калмыков И.А., Сагдеев А.К., Петлеванный С.В., Лисицын А.В. Устройство для преобразования из полиномиальной системы классов вычетов в позиционный код с пересчетом ортогональных базисов//Патент России № 2298873. 24.11.2005.

8. Чипига А.А., Калмыков И.А., Лободин М.В. Устройство спектрального обнаружения и коррекции в кодах полиномиальной системы классов вычетов// Патент России № 2301441. 01.08.2005.

9. Хайватов А.Б., Калмыков И.А. Математическая модель отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов// Инфокоммуникационные технологии. - 2007. - Т.5. - №3. - С.39-42.

10. Чипига А.Ф., Калмыков И.А., Яковлева Е.М., Калмыков М.И. Применение полиномиальной системе классов вычетов в схеме разделения секрета// Информационное противодействие угрозам терроризма. - 2012. - №19. - С.45-49.