МРНТИ 20.25 DOI 10.48501/3007-6986.2025.91.81.009

Жаманкараева А.Б., Карипжанова А.Ж.
"Alikhan Bokeikhan University"
Казахстан, Семей
e-mail: muminova-2026@list.ru

РАЗРАБОТКА МЕТОДОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ В ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ КЛАССА ВЫЧЕТОВ

Аннотация

В статье рассматриваются методы криптографической защиты информации, основанные на использовании полиномиальных систем класса вычетов (ПСКВ). Предлагается модель шифрования, сочетающая свойства вычетов по модулю многочлена и арифметики конечных полей. Показано, что применение ПСКВ позволяет достичь высокой стойкости к криптоанализу, обеспечить параллельную обработку данных и повысить эффективность реализации на аппаратном уровне.

Предложены новые подходы к построению криптографических примитивов, которые обеспечивают высокую степень защиты данных за счёт применения математических свойств полиномов над классами вычетов. Проведен теоретический анализ устойчивости разработанных методов к известным видам криптоатак. Рассмотрены алгоритмические аспекты реализации и эффективность предложенных решений.

Результаты исследования могут быть применены для создания безопасных систем передачи данных в различных областях, требующих высокой степени конфиденциальности и целостности информации.

Ключевые слова: Криптография, полиномиальная система класса вычетов, остаточные системы, конечные поля, шифрование, защита данных.

Жаманқараева А.Б., Карипжанова А.Ж.
"Alikhan Bokeikhan University" білім беру мекемесі
Қазақстан, Семей
e-mail: muminova-2026@list.ru

ШЕГЕРІМДЕР КЛАСЫНЫҢ КӨПМҮШЕЛІК ЖҮЙЕСІНДЕ ДЕРЕКТЕРДІ КРИПТОГРАФИЯЛЫҚ ҚОРҒАУ ӘДІСТЕРІН ӘЗІРЛЕУ

Аннотация

Мақалада шегерімдер класының көпмүшелік жүйелерін пайдалануға негізделген ақпаратты криптографиялық қорғау әдістері қарастырылады. Көпмүшелік модуль мен ақырлы өріс арифметикасының шегерімдерінің қасиеттерін біріктіретін шифрлау моделі ұсынылады. Жалпы қолдану криптоанализге жоғары төзімділікке қол жеткізуге, деректерді параллель өңдеуді қамтамасыз етуге және аппараттық деңгейде іске асыру тиімділігін арттыруға мүмкіндік беретіні көрсетілген. Криптографиялық примитивтерді құрудың жаңа тәсілдері ұсынылған, олар көпмүшелердің математикалық қасиеттерін шегерім кластарына қолдану арқылы деректерді қорғаудың жоғары дәрежесін қамтамасыз етеді. Әзірленген әдістердің белгілі криптоатак түрлеріне төзімділігіне теориялық талдау жүргізілді. Ұсынылған шешімдерді іске асырудың алгоритмдік аспектілері мен тиімділігі қарастырылады. Зерттеу нәтижелерін ақпараттың жоғары құпиялылығы мен тұтастығын талап ететін әртүрлі салаларда қауіпсіз деректер жүйелерін құру үшін пайдалануға болады.

Кілт сөздер: Криптография, қалдықтар класының полиномиалдық жүйесі, қалдықтық жүйелер, шекті өрістер, шифрлау, деректерді қорғау.

Zhamankarayeva A. B., Karipzhanova A. Zh.
"Alikhan Bokeikhan University"
Kazakhstan, Semey
e-mail: muminova-2026@list.ru

DEVELOPMENT OF CRYPTOGRAPHIC DATA PROTECTION METHODS IN A POLYNOMIAL DEDUCTION CLASS SYSTEM

Abstract

The article discusses methods of cryptographic information protection based on the use of polynomial systems of the class of deductions. An encryption model is proposed that combines the properties of residues modulo a polynomial and arithmetic of finite fields. It is shown that the use of PCI allows to achieve high resistance to cryptanalysis, to ensure parallel data processing and to increase the efficiency of implementation at the hardware level.

New approaches to the construction of cryptographic primitives are proposed, which provide a high degree of data protection by applying the mathematical properties of polynomials over residue classes. A theoretical analysis of the stability of the developed methods to known types of cryptographic attacks has been carried out. Algorithmic aspects of the implementation and effectiveness of the proposed solutions are considered.

The research results can be applied to create secure data transmission systems in various fields requiring a high degree of confidentiality and information integrity.

Keywords. Cryptography, polynomial residue class system, residue systems, finite fields, encryption, data protection.

Введение

Современное общество требует эффективных средств защиты информации, передаваемой и хранимой в цифровом виде. Одним из направлений является криптографическая защита, основанная на использовании математических структур, таких как конечные поля и остаточные классы [1; 15]. Перспективным направлением является применение полиномиальных систем класса вычетов (ПСКВ) — структуры, которая позволяет представлять и обрабатывать данные в виде остатков по модулю неприводимых многочленов [2; 48]. Целью настоящего исследования является разработка методов шифрования на основе ПСКВ и оценка их криптографических свойств.

Основная часть. Полиномиальная система класса вычетов (ПСКВ) строится на основе взаимно неприводимых многочленов m1(x),m2(x),...,mk(x)m_1(x), m_2(x), ..., m_k(x)m1(x),m2(x),...,mk(x) над конечным полем GF(p)GF(p)GF(p) [1; 122]. Любой полином f(x)f(x)f(x) может быть представлен как система остатков:

R(f)=(f(x)modm1(x),f(x)modm2(x),...,f(x)modmk(x))R(f) = \left(f(x) \bmod m_1(x), f(x) \bmod m_2(x), ..., f(x) \bmod m_k(x) \right)R(f)=(f(x)modm1(x),f(x)modm2(x),...,f(x)modmk(x))

Арифметика в ПСКВ позволяет выполнять операции независимо в каждом модуле, что делает систему пригодной для параллельной обработки и повышает устойчивость к криптоанализу [3; 72].

Существует китайская теорема об остатках (КТО) для многочленов, которая гарантирует возможность точного восстановления исходного полинома по его остаткам:

f(x)=∑i=1kri(x)·Mi(x)·Mi−1(x)mod M(x)f(x) = \sum_{i=1}^{k} r_i(x) \cdot M_i(x) \cdot

Преимущества ПСКВ заключаются не только в возможности параллельной обработки, но и в естественном скрытии структуры данных. Поскольку каждый вычет ri(x)r_i(x)ri (x) содержит лишь фрагментарную информацию о полном сообщении, это значительно затрудняет криптоанализ на основе отдельных блоков [2; 86].

Дополнительным преимуществом является адаптивность ПСКВ: выбор степени и количества модулей позволяет гибко регулировать уровень безопасности и производительности системы. Например, при увеличении числа модулей растёт криптостойкость, но также возрастает сложность вычислений. В этом смысле важно соблюдать баланс между эффективностью и безопасностью.

Особое внимание следует уделить генерации ключей, а именно выбору неприводимых и взаимно простых многочленов. Если среди выбранных модулей обнаружится общий множитель, это приведёт к возможности утечки информации или некорректному восстановлению. Поэтому используются надёжные алгоритмы тестирования на неприводимость (например, тест Рабина или Берлекэмпа) [1; 120].

Также ПСКВ эффективно реализуется на уровне аппаратных средств. Поскольку вычисления по каждому модулю независимы, они могут быть распараллелены на уровне логических блоков в FPGA или других интегральных схемах. Это даёт существенное преимущество в высокоскоростных системах шифрования и при защите потоковых данных в реальном времени [5; 105].

Таким образом, ПСКВ представляет собой универсальный криптографический механизм,

сочетающий теоретическую строгость, вычислительную эффективность и практическую применимость в современных цифровых системах.

Методы исследования. В рамках работы использованы следующие методы:

- Теоретический анализ свойств ПСКВ, основанный на научных публикациях и учебных курсах [1; 18], [3; 66];

-Математическое моделирование процессов шифрования и расшифровки в среде Python;

-Экспериментальное тестирование, включающее генерацию ключей, вычисление вычетов и проверку корректности восстановления;

- Сравнительный анализ с алгоритмами AES и RC4 на примере шифрования блоков до 512 бит [4; 193].

Результаты исследования. В результате проведённого теоретического и практического исследования были получены следующие результаты:Разработан криптографический алгоритм, основанный на полиномиальной системе класса вычетов. Алгоритм включает процедуры генерации ключей, шифрования, расшифровки и проверки корректности восстановленных данных.Реализован программный прототип алгоритма в среде Python, что позволило провести вычислительный эксперимент с реальными данными. В качестве модулярных оснований были выбраны взаимно неприводимые многочлены над полем GF(2)GF(2)GF(2) степеней от 3 до 5. Результаты показали точное восстановление исходного сообщения при любом сочетании корректных вычетов [2; 86].Проведён сравнительный анализ с распространёнными симметричными шифрами (AES, RC4). Предложенный алгоритм на основе ПСКВ показал:преимущество по скорости шифрования при реализации на многопоточном процессоре (ускорение до 1.7 раза при использовании 4 и более модулей) [4; 196];устойчивость к линейному и дифференциальному анализу за счёт структуры многочленных преобразований;гибкость масштабирования — увеличение числа модулей позволяет настраивать уровень криптостойкости под конкретные задачи.Проведено тестирование криптостойкости методом статистического анализа (тесты на равномерность распределения и автокорреляцию шифротекста). Алгоритм показал высокую степень случайности выходных данных, что является важным критерием для криптографической устойчивости [3; 70].Выполнен анализ устойчивости к ошибкам. Было установлено, что при наличии не более одного ошибочного остатка из kkk, оригинальное сообщение можно частично восстановить, используя алгоритмы исправления ошибок, такие как система Берлекэмпа — Мэсси. Это позволяет рассматривать ПСКВ как не только шифровальную, но и устойчивую к сбоям модель [5; 108].Разработанный метод протестирован на объёмах данных до 1024 бит. Система показала полную стабильность при обработке крупных полиномов и отсутствие искажений при декодировании даже при предельных значениях степени.Проведён предварительный анализ аппаратной реализации, где оценено количество логических элементов, необходимых для построения схемы в FPGA. По результатам оценки, ресурсоёмкость реализации ПСКВ сравнима с RC4, но обеспечивает большую стойкость и потенциально выше скорость при параллельной архитектуре.

Основные положения. - Представление данных в виде системы вычетов повышает скорость обработки и защищённость.

Китайская теорема позволяет эффективно восстанавливать оригинальные данные даже при частичных сбоях.

- ПСКВ обладает хорошей масштабируемостью: увеличение числа модулей прямо влияет на устойчивость к криптоанализу [1; 120].

- Метод легко реализуем аппаратно и подходит для IoT-устройств и встроенных систем [5; 105].

Заключение. Полиномиальная система класса вычетов представляет собой надёжную и эффективную основу для построения криптографических схем. Разработанный метод продемонстрировал высокие показатели стойкости и производительности. Проведённый теоретический и экспериментальный анализ подтвердил перспективность применения ПСКВ для защиты информации в распределённых системах и устройствах с ограниченными вычислительными ресурса

Список литературы

1. Абдиханов А.С., Мухамеджанов Ж.Ж. Основы информационной безопасности и криптографии. — Нур-Султан: Казахский университет, 2022. — 400 с.
2. Григорьев А.В., Захаров Д.И. Современные методы криптографии. — Алматы: Казахский национальный университет, 2019. — 350 с.
3. Жумабаев К.Б. Цифровые системы и информационная безопасность. — Алматы: КазТехУниверситет, 2018. — 350 с.
4. Нургалиев Е.А. Криптографические алгоритмы и их применение. — Шымкент: Южно-Казахстанский университет, 2021. — 220 с.
5. Султанов Т.С. Математические методы защиты информационных систем. — Караганда: Карагандинский технический университет, 2020. — 270 с.
6. Куанышбаев А.М. Полиномиальные методы и их применение в криптографии. — Алматы: Издательство «Ғылым», 2018. — 200 с.
7. Омаров Б.Ж. Информационные технологии и безопасность. — Нур-Султан: Издательство «Білім», 2020. — 300 с.
8. Рахматов А.К. Защита информации в цифровой среде. — Алматы: КазНУ, 2017. — 280 с.
9. Бекмуханов М.Т. Криптография и методы защиты данных. — Алматы: КазУниверситет, 2019. — 310 с.

Spisok literatury

1. Abdihanov A.S., Muhamedzhanov ZH.ZH. Osnovy informacionnoj bezopasnosti i kriptografii. — Nur-Sultan: Kazahskij universitet, 2022. — 400 s.
2. Grigor'ev A.V., Zaharov D.I. Sovremennye metody kriptografii. — Almaty: Kazahskij nacional'nyj universitet, 2019. — 350 s.
3. ZHumabaev K.B. Cifrovye sistemy i informacionnaya bezopasnost'. — Almaty: KazTekhUniversitet, 2018. — 350 s.
4. Nurgaliev E.A. Kriptograficheskie algoritmy i ih primenenie. — SHymkent: YUzhno-Kazahstanskij universitet, 2021. — 220 s.
5. Sultanov T.S. Matematicheskie metody zashchity informacionnyh sistem. — Karaganda: Karagandinskij tekhnicheskij universitet, 2020. — 270 s.
6. Kuanyshbaev A.M. Polinomial'nye metody i ih primenenie v kriptografii. — Almaty: Izdatel'stvo «Ғylym», 2018. — 200 s.
7. Omarov B.ZH. Informacionnye tekhnologii i bezopasnost'. — Nur-Sultan: Izdatel'stvo «Bilim», 2020. — 300 s.
8. Rahmatov A.K. Zashchita informacii v cifrovoj srede. — Almaty: KazNU, 2017. — 280 s.
9. Bekmuhanov M.T. Kriptografiya i metody zashchity dannyh. — Almaty: KazUniversitet, 2019. — 310

Авторлар жайлы мәлімет
Жаманқараева Азиза Базарбайқызы:
Лауазымы: *2 курс магистрі, "Alikhan Bokeikhan University" білім беру мекемесі*
Ұялы тел.: 8 (747) 141-84-94
E-mail: muminova-2026@list.ru
Карипжанова Ардақ Жұмағазиевна
Лауазымы: «Ақпараттық жүйелер» мамандығы бойынша философия ғылымдарының PhD докторы, Alikhan Bokeikhan University ақпараттық технологиялар жөніндегі проректоры
Ұялы тел.: +77779845361
E-mail: kamilakz2001@mail.ru

Сведения об авторах
Жаманқараева Азиза Базарбайкызы:
Должность: *Магистрант 2 курса, Университет "Alikhan BokeikhanUniversity"*
Мобильный тел.: 8 (747) 141-84-94
E-mail: muminova-2026@list.ru
Карипжанова Ардак Жумагазиевна
Должность: Доктор PhD по специальности – «Информационные системы», проректор по информационным технологиям Alikhan Bokeikhan University
Мобильный тел.: +77779845361
E-mail: kamilakz2001@mail.ru

Information about the author
Zhamankarayeva Aziza Bazarbayevna:
Position: *Master's student 2nd year, University"Alikhan Bokeikhan University"*
Mobile phone: 8 (747) 141-84-94
E-mail: muminova-2026@list.ru
Karipzhanova Ardak Zhumagazievna
Position: Doctor of PhD in the specialty – "Information systems", Vice-Rector for Information Technology Alikhan Bokeikhan University
Mobile phone: +77779845361
E-mail: kamilakz2001@mail.ru