ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Ալավերդյան Եղիսաբեթ Ծերունի

ԲՈՒԼՅԱՆ ՏԵՂԱՓՈԽՈՒՄՆԵՐԻ ՎՐԱ ՀԻՄՆՎԱԾ ԲԱՐՁՐ ԱՐԱԳԱԳՈՐԾՈՒԹՅԱՆ ԱՆՀԱՄԱՉԱՓ ԳԱՂՏՆԱՀԱՄԱԿԱՐԳԻ ՀԵՏԱԶՈՏՈՒՄԸ ևՎ ՄՇԱԿՈՒՄԸ

Ե13.04. ”Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում” մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

Երևան 2012

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК РЕСПУБЛИКИ АРМЕНИЯ

Алавердян Егисабет Церуновна

ИССЛЕДОВАНИЕ И РАЗРАБОТКА АСИММЕТРИЧНОЙ КРИПТОСИСТЕМЫ ВЫСОКОЙ ПРОИЗВОДИТЕЛЬНОСТИ, ОСНОВАННОЙ НА БУЛЕВЫХ ПЕРЕСТАНОВКАХ

АВТОРЕФЕРАТ

Дисертации на соискание ученой степени кандидата технических наук по специальности 05.13.04 –«Математическое и програмное обеспечение математических машин, комплексов, систем и сетей»

Ереван 2012

Ատենախոսության թեման հաստատվել է Հայաստանի Պետական Ճարտարագիտական Համալսարանում (Պոլիտեխնիկ)

Գիտական ղեկավար՝	տ.գ.թ.	Գ. Ի. Մարգարով
Պաշտոնական ընդդիմախոսներ՝	տ.գ.դ.	Գ.Հ. Խաչատրյան
	տ.գ.թ.	Ա.Կ. Ասլանյան

Առաջատար կազմակերպություն՝ Երևանի Կապի միջոցների գիտահետազոտական ինստիտուտ

Պաշտպանությունը կայանալու է 2012 թ. օգոստոսի 28-ին, ժամը 15.00-ին, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացված պրոբլեմների ինստիտուտում գործող 037 "Ինֆորմատիկա և հաշվողական համակարգեր" մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ 0014, Երևան, Պ. Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրն առաքված է 2012 թ. հուլիսի 26-ին:

Մասնագիտական խորհրդի գիտական քարտուղար, ֆ.մ.գ.դ.՝ Հ. Գ. Սարուխանյան

Тема диссертации утверждена в Государственном Инженерном Университете Армении (Политехник)

Научный руководитель:	к.т.н.	Г. И. Маргаров
Официальные оппоненты:	д.т.н.	Г.Г. Хачатрян
	к.т.н.	А.К. Асланян

Ведущая организация: Ереванский научно-исследовательский институт средств связи

Защита состоится 28 августа 2012г. в 15.00 часов на заседании специализированного совета 037 «Информатика и вычислительные системы» Института проблем информатики и автоматизации НАН РА по адресу: 0014, Ереван, ул. П. Севака 1.

С диссертацией можно ознакомиться в библиотеке института.
Автореферат разослан 26 июля 2012г.

Ученый секретарь специализированного совета 037, д.ф.м.н. А. Г. Саруханян

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность. Человечество вступило в эру, когда деловая переписка, финансовые транзакции и оперативный обмен данными все чаще осуществляются с помощью открытых компьютерных систем связи, таких, например, как глобальная сеть. Одним из основных путей обеспечения конфиденциальности передаваемой информации при этом является применение криптографии, обеспечивающей безопасность связи посредством шифрования/дешифрования информации с использованием криптографических ключей. Для преодоления проблемы доверия между сторонами и упразднения предварительного обмена ключами используются асимметричные криптосистемы. Однако существующие асимметричные криптосистемы, обладающие высокой степенью стойкости, имеют низкую производительность процессов шифрования/дешифрования информации, поскольку математическая реализация этих систем основана на сложных вычислениях, требующих огромных затрат машинного времени и ресурсов. В результате асимметричные криптосистемы используются только для обмена криптографических ключей и цифровой подписи.

Возможным решением проблемы низкой производительности процессов шифрования/дешифрования информации может являться создание асимметричных криптосистем, спроектированных на основе математической логики. Данный подход мотивирован тем, что функции этого семейства реализуются легко и быстро за счет применения исключительно логических операций, эффективно реализующихся как на программном, так и на аппаратном уровнях.

Известные асимметричные криптосистемы, спроектированные на основе математической логики, в частности, криптосистемы, основанные на конечных автоматах, обладают большой эффективностью процессов шифрования/дешифрования, однако до настоящего времени не находят практического применения из-за низкого уровня стойкости. Повышение стойкости имеет определенную степень сложности из-за включения нелинейных автоматов в состав шифрующего/дешифрующего автоматов, усложняя при этом аппаратную и программную реализации.

Исходя из вышеизложенного, актуальным является создание быстродействующей асимметричной криптосистемы с требуемым уровнем стойкости, основанной на криптографических свойствах логических функций и операций высшей алгебры, реализующих неассоциативные алгебраические структуры, в частности, квазигруппы. В результате асимметричные криптосистемы могут быть использованы не только для обмена криптографических ключей и цифровой подписи, но и для эффективного шифрования/дешифрования информации.

Цель диссертационной работы – Исследование и разработка асимметричной криптосистемы высокой производительности, основанной на Булевых перестановках.

Для достижения указанной цели в работе ставятся и решаются следующие задачи:

- Определить методы построения быстродействующих асимметричных криптосистем, обладающих требуемым уровнем стойкости на основе анализа существующих асимметричных криптосистем.
- Разработать методы построения односторонних функций с секретом на основе логических операций с целью повышения производительности проектируемых асимметричных криптосистем.

- Разработать модель ключей асимметричной криптосистемы на основе логических операций, позволяющпх упростить их практическую реализацию,
- Спроектировать алгоритм и программные средства, реализующие асимметричную криптосистему на основе Булевых перестановок.

Объект исследования: Объектом исследования является производительность и стойкость асимметричных криптосистем на основе Булевых перестановок.

Методы исследования: Исследования, проводимые в работе, основаны на комплексном использовании методов теории множеств, математической логики, высшей алгебры и комбинаторного анализа.

Научная новизна:

В диссертационной работе получены и выносятся на защиту следующие научные результаты.

- Предложен метод построения односторонней функции с секретом, основанный на комбинировании сбалансированных Булевых функций и квазигрупп, что является необходимым условием для построения асимметричных криптосистем. Высокая производительность подобных криптосистем по сравнению с существующими обусловлена замещением алгебраических операций логическими операциями.
- Разработан метод генерации составляющих функций Булевых перестановок на основе квазигрупп, который позволяет существенно ускорить процедуру построения пары криптографических ключей.
- Разработан метод формального описания криптографических ключей асимметричной криптосистемы на основе Булевых перестановок, который позволяет упростить функциональную структуру криптосистемы и ее практическую реализацию за счет представления ключей в форме положительных целых чисел.
- Получены оценки стойкости асимметричной криптосистемы на основе Булевых перестановок по отношению к типичным видам атак, что позволяет обосновать выбор размера криптографических ключей при заданном уровне стойкости криптосистемы.

Практическая значимость полученных результатов и внедрение:

- Разработаны алгоритмы и программные средства, реализующие асимметричную криптосистему на основе Булевых перестановок. Программное обеспечение предусмотрено как для автономного, так и для удаленного использования.
- Спроектирована асимметричная криптосистема BP Crypto, которая предоставляет удобный пользовательский интерфейс шифрования/дешифрования информации на основе сгенерированных криптографических ключей выбранного размера и распределения их посредством спроектированного сетевого транспорта.
- Программный продукт BP Crypto представляет собой также учебно-исследовательское средство для поведенческого анализа асимметричных алгоритмов RSA, FAPKC3 и BP Crypto, реализованное в виде WEB – приложения, использующего облачные технологии и дистрибутивные вычисления.

Внедрения. Приложение внедрено в организации ЗАО "Инфоком-Ереван", предоставляющей документальную электросвязь на территории республик Армении, Нагорного Карабаха и ближнего зарубежья на основании телеграфных протоколов, установленных Региональным Содружеством Связи стран СНГ. Посредством программного интерфейса BP Crypto обеспечивается шифрование/дешифрование и защищенное хранение информации юридической значимости. Приложение также применяется в учебно-исследовательском процессе кафедры ИБПО ГИУА с целью ознакомления студентов с технологией построения асимметричной криптосистемы на основе Булевых перестановок.

На защиту выносятся следующие основные положения:

- Метод достижения сбалансированных нелинейных Булевых функций в составе Булевых перестановок посредством применения квазигрупп.
- Метод формального описания криптографических ключей асимметричной криптосистемы на основе Булевых перестановок.
- Алгоритмы и программные средства, реализующие функционально независимые модули генерации криптографических ключей, шифрования/дешифрования и построенные на их основе программные средства BP Crypto.

Апробация полученных результатов. Основные результаты работы докладывались и обсуждались на VI международной конференции "Computer Science and Information Technologies" (2007г., г. Ереван), международной конференции "New Challenges in Digital Communications" (2008г., г. Влора, Албания), на научно-практической конференции по вопросам безопасности информационных систем (2008г., г. Ереван), на научных конференциях ГИУА (2009, 2010, 2011) гг, г. Ереван, на II международной конференции IEEE/ACS Int. Conf. on Computer Systems and Applications, Rabat, Morocco, 2009, на II международной конференции по применению цифровой информации и веб-технологий ICADIWT09, (2009, Лондон, Великобритания), на международном конгрессе The 2009 World Congress in Computer Science (2009 Las Vegas, USA), на конференции World Congress in Computer Science, (2010 Las Vegas, USA), а также обсуждались на научных семинарах кафедры ИБПО ГИУА (2008-2011), на международном симпозиуме Совета Безопасности и Сотрудничества в Европе, OSCE, Workshop on Global Issues in Information Security and Cyber Warefare, (2012, Yerevan), на семинаре Американского университета в Армении (2012, Ереван), на общем семинаре Института проблем информатики и автоматизации НАН РА (2012, Ереван).

Публикации. Основные результаты опубликованы в **10** научных трудах, перечисленных в конце автореферата.

Структура и объем работы. Диссертация состоит из введения, трех глав, заключения, списка использованной литературы и двух приложений. Общий объем работы – 106 страниц, включая 10 рисунков, 18 таблиц, 45 наименований в списке исользованной литературы и 9 страниц приложений.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы, сформированы цели работы, научная новизна и основные положения, выносимые на защиту.

В первой главе диссертационной работы рассматривается организация существующих асимметричных криптосистем, в частности, наиболее распространенных криптосистем RSA, Эль Гамаля и Рабина, стойкость которых приравнивается к сложности факторизации целых чисел и сложности вычисления дискретных логарифмов на конечном поле. Исследование стойкости основных асимметричных криптосистем, в том числе и вышеприведенных, неизменно приводят к положительным выводам: каждый отдельный бит исходного текста, скрытый такими функциями, распознать также сложно, как и весь блок.

Следует отметить однако, что наряду с оценками стойкости существующих асимметричных криптосистем на основе теории чисел, другие аспекты этих криптосистем также рассматриваются, в частности - эффективность их построения.

Анализ алгоритмической сложности этих криптосистем указывает на то, что они практикуют трудоемкие математические расчеты над большими числами. При этом, используемые сложные математические преобразования чисел, имеющих сто и больше цифр, требуют огромные затраты машинного времени и ресурсов и неизбежно приводят к снижению быстродействия криптосистемы. В приложениях, особенно связанных с передачей конфиденциальной информации определенных объемов или реализацией динамически реконфигурируемых структур быстрого реагирования теоретико - числовые асимметричные криптосистемы не обеспечивают требуемой производительности и неизбежно включают быстродействующие симметричные алгоритмы. В результате, существующие асимметричные алгоритмы применяются только для выполнения вспомогательных (относительно процесса обеспечения секретности) функций, таких, как цифровая подпись и шифрование ключей, применяемых симметричными алгоритмами.

Тем не менее учитывая превосходство асимметричных криптосистем над симметричными криптосистемами в элегантном решении проблемы согласования и распределения криптографических ключей, обоснована важность исследования асимметричных криптосистем, основанных на других областях математики.

Исследован инвертируемый тип автоматов с точки зрения применения их в криптографии. Асимметричные криптосистемы, основанные на конечных автоматах, отличаются явно высокой производительностью в отличие от всех, без исключения, теоретико – числовых асимметричных криптосистем, так как реализуют только логические, то есть, самые быстрые операции. Производительность этих криптосистем определяется временем перехода конечного автомата из одного состояния в другое и не зависит от числа состояний таблицы переходов. Конечные автоматы также обладают легкой перестройкой оконечного устройства и простотой реализации в виде аппаратного устройства, например, на базе FPGA. Для достижения требуемого уровня стойкости привлекаются нелинейные автоматы, в результате чего шифрующий автомат представляет собой композицию линейных и нелинейных автоматов.

Тем не менее, несмотря на высокую производительность асимметричных криптосистем, спроектированных на конечных автоматах, эти криптосистемы не обладают достаточным уровнем стойкости к атакам и также не находят практического

применения. Криптоанализ этих криптосистем указывает на возможность достижения факторизации композиционного шифрующего конечного автомата в разумный промежуток времени, посредством использования классов эквивалентности конечного автомата. Конечные автоматы с одинаковой задержкой τ фактически относятся к одному и тому же классу эквивалентности, если все они порождены от того же самого исходного автомата. Это свойство позволяет легко построить инверсы автоматов того же класса эквивалентности, если инверс исходного автомата с задержкой τ известен.

Другой способ факторизации нелинейных конечных автоматов является декомпозиция автомата в квазипрямое произведение линейных автоматов. Вычисление нелинейных конечных автоматов может быть достигнута посредством параллельных схем двоичной логики глубиной $O(\log^2 t)$, или же глубиной $O(\log t)$ параллельными компьютерами быстрее чем явным симулированием, даже если автоматы – нелинейные.

В конце главы на основе проведенного анализа принципов построения асимметричных криптосистем сформулирована цель диссертационной работы и поставлены задачи ее достижения.

Применение Булевых перестановок для построения стойкой асимметричной криптосистемы высокой производительности обосновывается тем, что на их основе возможно проектирование односторонней функции с секретом. Привлечение методов неассоциативной алгебры позволяют проектировать структуры данных, обладающих высокой стойкостью к обращениям и предоставляет возможность использования этих алгоритмов для шифрования/дешифрования информации, не снижая при этом производительность асимметричной криптосистемы.

Для реализации быстродействующей асимметричной криптосистемы требуемой стойкости сформулированы основные задачи, способствующие достижения цели диссертационной работы.

Во второй главе приведен сравнительный анализ эффективностей процессов генерации сбалансированных Булевых функций методом их алгебраическиого преобразования и применением квазигрупп. Приведен детальный анализ Булевых функций с целью сочетания необходимых криптографических свойств, среди них – нелинейность, сбалансированность и лавинный эффект. Алгебраическая степень Булевой функции должна быть высокая с целью противостояния дифференциальным атакам для блочных шифров, свойственных асимметричным криптосистемам.

Алгебраическая нормальная форма Булевых функций представляет сумму по модулю 2 положительных монотонных элементарных коньюнкций, приведенная ниже:

$f(x_1, x_2, \dots, x_n) = \alpha_0 \oplus \alpha_1 x_1 \oplus \dots \oplus \alpha_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus a_{23} x_2 x_3 \oplus \dots \oplus a_{1\dots n} x_1 x_2 \dots x_n$, где все коэффициенты равны 0 или 1. Число таких полиномов равно 2^{2^n}, т.е. числу всех Булевых функций от n переменных.

Исследован важный, но криптографически слабый класс Булевых функций, названных аффинными функциями с алгебраической степенью равной единице, определяющимся следующим образом:

$A_f(x_1, x_2, \dots, x_n) = \alpha_0 \oplus \alpha_1 x_1 \oplus \dots \oplus \alpha_n x_n$ для всех $\alpha_i \in F_2, i = 1,2, \dots, n$.

Структура аффинных функций указывает на их статистическую слабость и недостаточность по отношению к общему количеству Булевых функций - поэтому и считаются криптографически нестойкими. Количество аффинных функций над F_2^n равно 2^{n+1}.

В противоположность функциям семейства аффинных, в построении стойких асимметричных криптосистем важную роль играют нелинейные функции, у которых алгебраическая степень больше единицы.

Нелинейностью $N(f)$ Булевой функции f называется также расстояние Хэмминга между f и множеством аффинных функций A_n. Количество Булевых функций алгебраической степени n равно половине всего количества Булевых функций. Более того, количество Булевых функций нечетной степени равно $\binom{2^n}{1} + \binom{2^n}{3} + \cdots + \binom{2^n}{2^n-1}$, что может быть представлено как 2^{2^n-1}. А это, в свою очередь, равно количеству Булевых функций с алгебраической степенью равной n. Для количественной оценки нелинейности и других криптографических показателей приведен ряд характеристик Булевых функций. В первую очередь - это спектры Уолша-Адамара, указывающие на степень корреляции между функцией f и линейными функциями.

Пусть R обозначает поле реальных чисел. Тогда для каждой Булевой функции $f(x)$ над F_2^n имеется функция $W_f(\alpha) : a \in F_2^n$, определяемая преобразованием Уолша-Адамара :

$$W_f(\alpha) = \sum_x (-1)^{f(x)+a\cdot x} .$$

Обратное этой трансформации вычисляется следующим образом:

$$(-1)^{f(x)} = \frac{1}{2^n}\sum_\alpha W_f(\alpha)(-1)^{a\cdot x}.$$

В таком случае имеем:

$$(W_f(\alpha_0), \dots, W_f(\alpha_{2^n-1}))^t = H_n \cdot ((-1)^{f(\alpha_0)}, \dots, (-1)^{f(\alpha_{2^n-1})})^t,$$

где H_n представляет собой матрицу Силвестера – Адамара порядка n, определенная следующим образом:

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{ а } \quad H_n = \overset{n}{\otimes} H_1.$$

Упорядоченный одномерный массив значений Уолша Булевой функции называется спектром Уолша функции f и включает целые числа в диапазоне $[-2^n; 2^n]$.

Сложность вычисления алгебраической нормальной формы, а также трансформация Уолша Булевой функции – порядка $O(2^{2n})$.

Степень нелинейности Булевой функции определяет меру сложности построения ее аффинной аппроксимации, а последняя, в свою очередь, обуславливает стойкость криптографического алгоритма по отношению к линейному криптоанализу. Нелинейность Булевой функции определенной над F_2^n может быть вычислена следующим образом:

$$N_f = 2^{n-1} - \frac{1}{2}\max_{a\in F_2^n}|W_f(a)|.$$

Для того, чтобы определить предельно высокую степень Булевой функции, воспользуемся тождеством Парсерваля, которая также основана на спектре Уолша и состоит в том, что для каждой Булевой функции f над F_2^n имеем:

$$\sum_{a\in F_2^n} W_f(a)^2 = 2^{2n}$$

С целью максимизации меры нелинейности Булевой функции в криптографии выделяют класс максимально нелинейных функций, названных бент функциями, удалённых от множества всех афинных функций на наибольшее возможное расстояние,

где все значения Уолша W_f бент функции f имеют одинаковые абсолютные значения, равных $2^{\frac{n}{2}}$.

Следующий критерий, чему криптографически стойкая Булева функция удовлетворяет – это сбаланасированность, когда таблица истинности Булевой функции содержит одинаковое количество единиц и нулей, т.е. $w(f) = 2^{n-1}$. Отметим, что сбалансированность Булевых функций – также существенное криптографическое свойство в том смысле, что выходные значения Булевой функции не пропускают никакой статистической информации относительно ее структуры.

Используя комбинаторные методы исчисления, выведено количество всех сбалансированных Булевых функций, определенных в F_2^n. Из всевозможных таблиц истинностей, $\binom{2^n}{2^{n-1}}$ количество представляют собой сбалансированные функции. Отмечено также, что любая неконстантная аффинная функция сбалансированная и расстояние Хемминга любой сбалансированной Булевой функции с $\deg(f) > 1$ от семейства аффинных- четное число, а бент Булевы функции не сбалансированные.

Показано, что построение сбалансированных Булевых функций высокого порядка нелинейности осуществляется модификацией нормальных бент функций, в которых изменение $2^{\frac{n}{2}-1}$ битов приводит к балансированию бент Булевой функции за счет некоторой потери ее нелинейности.

Другой критерий, чему криптографически стойкая Булева функция удовлетворяет – это устойчивость к корреляции. Булева функция называется устойчивой к корреляции порядка m, если распределение выходных значений не меняется в результате изменения m битов входных значений функции. Отметим, что оппонент не должен выявить хоть какую-то информацию от распределения выходных значений Булевой функции. Для этого, выходные значения Булевой функции должны быть распределены идентично, а иначе говоря, Булева функция должна быть сбалансированной. Поэтому, любая сбалансированная Булева функция с порядком устойчивости к корреляции равным m, называется устойчивой функцией порядка m. Выявлено, что любая m – устойчивая Булева функция имеет алгебраическую степень меньшую или равную $n - m - 1$ для $0 \leq m < n - 1$ и любая $n - 1$ - устойчивая Булева функция имеет алгебраическую степень равной 1. Показано также, что Булева функция f устойчивая к корреляции порядка m, если

$$W_f(\alpha) = 0 \text{ для всех } \alpha \epsilon F_2^n \text{ так, что } 1 \leq w(\alpha) \leq m.$$

Для Булевой функции над F_2^n автокорреляционная функция данной функции f со смещением α представляет собой функцию $\Delta_f : F_2^n \to R$, определенную следующим образом:

$$\Delta_f(\alpha) = \sum_x (-1)^{f(x)+f(x+\alpha)}.$$

Заметим, что $\Delta_f(\alpha)$ принимает значения в диапазоне $[-2^n; 2^n]$. В частности, $\Delta_f(\alpha_0) = 2^n$.

Выходные значения криптографически стойкой Булевой функции должны меняться с вероятностью 1/2 при изменении некоторых ее входных значений. Эта концепция прямо ассоциирована с автокорреляционной функцией функции f. В этом случае возможно установление глобального лавинного свойства функции f, который представляет собой абсолютный индикатор функции f, определенный посредством

$\Delta_f = \max_{\alpha \in F_2^n} |\Delta_f(\alpha)|$. Фактически, при меньших значениях абсолютного индикатора лавинная характеристика Булевой функция $f -$ высокая.

Сочетание вышеприведенных трех характеристик Булевых функций обеспечивает фильтрацию криптографически слабых структур, усложняя тем самым линейную аппроксимацию нелинейных Булевых фунцкий.

Показано, что для генерации сбалансированной Булевой функции с нелинейностью требуемого порядка, необходимо:

- генерировать произвольную бент Булеву функцию и вычислить алгебраическую нормальную форму. Сложность такого вычисления – порядка $O(2^{2n})$.
- изменить $2^{\frac{n}{2}-1}$ битов бент Булевой функции для сбалансирования ее значений.
- попарно сравнить сгенерированные функции с целью исключения совпадений.

Для m количества функций - это $\binom{m}{2}$ количество сложений по модулю 2.

Один способ достижения вышеуказанной цели – начать с произвольной сбалансированной Булевой функции, а потом уже повысить степень ее нелинейности, сохраняя при этом другие качества. Другой способ – это начать с заранее известной бент Булевой функции, а потом балансировать эту же функцию, пожертвовав некоторую степень ее нелинейности изменением некоторых битов. Обе процедуры – трудоемкие, к тому же применяются последовательно к каждой отдельно взятой Булевой функции..

Другой подход генерации сбалансированных нелинейных Булевых функций – это применение квазигрупп, позволяющего спроектировать стойкие к обращениям неассоциативные алгебраические структуры.

Под неассоциативной алгеброй подразумевается векторное пространство над полем, определяющем операцию умножения, взаимодействующая с операцией сложения посредством обыкновенного закона дистрибутивности. Операция умножения, при этом, не обязательно коммутативна или ассоциативна. Например, квазигруппы, в отличие от конечных групп, не обладают свойством ассоциативности, а также не имеют нейтрального элемента. Очевидно, что обращение таких структур потребует экспоненциальное количество чтений таблиц, описывающих эти структуры, для того, чтобы удостовериться в выполнении заданных условий. Математической основой таких алгебраических структур могут служить обобщенные супертождества.

Другое, и самое важное, свойство квазигрупп – это равномерное распределение их всевозможных элементов, что указывает на возможность посторения саблансированных Булевых функций на их основе. Представляя квазигруппу как коллекцию Булевых функций посредством отображения двумерного пространства элементов квазигруппы в одномерное пространство значений Булевых функций, достигнуто проектирование односторонней функции с секретом на их основе. Последнее обстоятельство позволяет реализовать асимметричную криптосистему блочного типа, обладающей высокой производительностью, обоснованной тем, что квазигруппы, как и Булевы функции, реализуются логическими операциями, которые являются самыми быстрыми в вычислительной технике.

С этой целью определяется квазигруппа $(Q, *)$ конечного порядка, равной 2^d. Используя операцию $*$, возможно задание Булевой функции векторного значения(б. ф. в. з):

$$a * b = c \iff *_{vv}(x_1, x_2, \dots, x_d, y_1, y_2, \dots, y_d) = (z_1, z_2, \dots, z_d),$$

где $(x_1 \dots x_d, y_1 \dots y_d,\ z_1 \dots z_d)$ представляют собой двоичное равномерное кодирование кодирование символов данного алфавита, a, b, c.

Каждый элемент z_i зависит от битов $x_1, x_2, \dots, x_d, y_1, y_2, \dots, y_d$ и однозначно определяется ими. Таким образом, каждый z_i можно интерпретировать как Булеву функцию типа 2d, уже не линейную, $z_i = f_i(x_1, x_2, \dots, x_d, y_1, y_2, \dots, y_d)$, где f_i: $\{0,1\}^{2d} \to \{0,1\}$ представляет собой отображение. однозначно определенное посредством $*$. Для каждой квазигруппы $(Q,*)$ порядка 2^d и каждой биекции $Q \longrightarrow \{0,1,\dots,2^d-1\}$ существуют однозначно определенные б.ф.в.з и однозначно определенные Булевы функции $f_1, f_2, \dots, f_d$ таким образом, что для каждой $a, b, c \in Q$ имеют место следующие соотношения:

$$a * b = c \Leftrightarrow *_{\text{бфвз}} (x_1, \dots, x_d, y_1, \dots, y_d) =$$
$$(f_1(x_1, \dots, x_d, y_1, \dots, y_d), \dots, f_d(x_1, \dots, x_d, y_1, \dots, y_d)) .$$

В свою очередь, каждая k - значная Булева функция $f(x_1, \dots, x_k)$ может быть однозначно представлена в алгебраической нормальной форме, АНФ, с коэффициентами $\alpha_0, \alpha_i, \alpha_{i,j}, \dots, \in \{0,1\}$, реализующие сложение и умножение над полем $GF(2)$.

Очевидно, что АНФ Булевых функций f_i описывает сложность квазигруппы $(Q,*)$ посредством алгебраической степени этих функций. Степени полиномов АНФ(f_i) увеличиваются в зависимости от порядка квазигруппы. В общем случае, для произвольно сгенерированной квазигруппы порядка 2^d , где $d \geq 4$, алгебраическая степень Булевой функции больше двух, что создает предпосылки для построения сбалансированных Булевых структур с высоким порядком нелинейности.

Эффективность применения квазигрупп в построении стойких асимметричных криптосистем основана на том факте, что квазигруппы применяют исключительно логические операции, а количество квазигрупп порядка n равно $n! \cdot (n-1)! \cdot \dots \cdot 2! \cdot 1!$. Обращение таких структур без знания функции, реализующей квазигруппу, приводит к экспоненциальным чтениям таблиц, описывающих квазигруппу. К тому же, сгенерировав квазигруппу порядка 2n, мы получаем сразу n количество сбалансированных Булевых функций желаемого порядка, ускоряя при этом процесс генерации этих функций. Заметим также, что коллекция Булевых функций, полученных на основе данной квазигруппы, коллизии не подлежит согласно определению квазигруппы.

Таким образом, применение квазигруппы позволяет упростить процедуру генерации сбаланцированных нелинейных функций на $2^{2n}/n^2 - \binom{m}{2}$ - $2^{\frac{n}{2}-1}$ порядка при n количестве входных параметров и m количества Булевых функций.

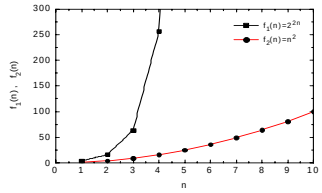

Рис. 1. Сложность генерации сбалансированных Булевых функций на основах алгебраического преобразования и применения квазигруппы.

<u>В третьей главе</u> приведено построение асимметричной криптосистемы на основе Булевых перестановок.

При построении асимметричной криптосистемы, основанной на Булевых перестановках, используется то обстоятельство, что для данной матрицы существует множество других матриц, произведение которых с первоначальной матрицей равно нулю.

С этой целью рассмотрено отображение типа $F_2^n \to F_2^m$, который называется Булевой функцией типа (n, m). Булева функция такого типа всегда может быть представлена как набор m функций в $\mathcal{F}_n$. Для построения асимметричной криптосистемы с использованием криптографических свойств Булевых функций наибольший интерес для нас представляет именно класс функций типа (n, m), когда $m = n$, и когда разным значениям входных параметров соответствуют разные выходные значения функции. В таком случае, рассмотрев каждый из входных комбинаций как двоичное представление некоторого целого числа в диапазоне $S = \{0, 1, , \dots, 2^n - 1\}$, можно утверждать, что вышеописанные функции осуществляют перестановку над множеством S.

Булева перестановка может быть представлена как набор Булевых функций над n переменными :

$$BP = [f_1(x), f_2(x), \dots, f_n(x)],$$

где $f_1(x), f_2(x), \dots, f_n(x)$ – функции – компоненты Булевой перестановки BP, а перестановку множества S можно назвать Булевой перестановкой порядка n.

Теоретические основы построения Булевых перестановок приведены в 14 леммах. Обосновано, что Булева перестановка может служить основой для построения стойкой асимметричной криптосистемы тогда и только тогда, когда следующие условия будут удовлетворены:

- вычисление обратной перестановки заданной Булевой перестановки – легкая задача для обладателей секрета.
- вычисление обратной перестановки заданной Булевой перестановки – неразрешимая задача без обладания секрета.

Булева перестановка, обладающая приведенными двумя свойствами – односторонняя функция с секретом, на основе которой можно проектировать стойкую асимметричную криптосистему с высоким уровнем быстродействия.

В предложенной асимметричной криптосистеме открытый текст и криптотекст – целые числа в диапазоне $[0; 2^n - 1]$. Рассмотрим множество S, представляющее алфавит N символов. Тогда, Булевы функции типа (n, m), задающие взаимно – однозначное отображение $S \leftrightarrow S$ на множестве S, осуществляют перестановку на S.

Начальная Булева перестановка BP принимает множество элементарных коньюнкций n переменных и производит коллекцию $E_S = \{ f_1, f_2, \dots, f_n\}$, где $f_1, f_2, \dots, f_n$ являются функциями – компонентами Булевой перестановки BP. Для данной Булевой перестановки можно сконструировать обратную Булеву перестановку с целью воспроизведения начальных элементарных коньюнкций. В результате, эта пара Булевых перестановок повторяет входную комбинацию параметров.

Шифрование блока открытого текста производится в следующем порядке:

1. Открытый текст, который представляет собой множество целых чисел в диапазоне $[0; 2^n - 1]$, представленных в виде битовых строк, разделяется в блоки длиной k и подвергается начальной перестановке посредством квазигруппы порядка 2^k, $(Q_1, *)$, обратное которой, $(Q_1, /)$ известно только

легитимному пользователю. С целью неразглашения лидирующего элемента квазигруппы, последнее включается в конец первого блока открытого текста и подвергается последующему преобразованию.

2. На основании таблицы истинности начальной Булевой перестановки BP строится бинарная матрица размерностью $n \times k$, где k представляет количество Булевых функций в Булевой перестановке BP, а n - количество входных комбинаций параметров в таблице истинности. Коллекция Булевых функций генерируется на осовании квазигруппы соответствующего порядка.
3. Для вышеприведенной матрицы строится транспонированная матрица размерностью $k \times n$, названной BM_1. Для матрицы BM_1 создаются дополнительные две другие матрицы размерностей $n \times k$ и $(n-k) \times n$ соответсвенно, обладающие следующими свойствами:

$$\mathrm{BM}_1 \times \mathrm{BM}_2 = \mathrm{I}_\mathrm{k},$$
$$\mathrm{BM}_3 \times \mathrm{BM}_2 = 0.$$

Здесь I_k представляет собой идентичную матрицу размерности $\mathrm{k} \times \mathrm{k}$.

Для удобства выбора тройки вышеуказанных матриц BM_1, BM_2 и BM_3, генерируется произвольная несингулярная матрица размерностью $n \times n$. Назовем эту матрицу C. Первые k строки матрицы C формируются значениями матрицы BM_1, остальные $n-k$ строки для BM_3, а BM_2 формируется левыми k столбцами матрицы C^{-1}. Под C^{-1} подразумевается обратная матрицы C.

4. Генерируется вторая квазигруппа, $(Q_2,*)$, и на ее основе создается вторая Булева перестановка, $\mathrm{R} = [\mathrm{r}_1, \mathrm{r}_2, \dots, \mathrm{r}_{\mathrm{n-k}}]$. Вычисляется $PKC = \mathrm{R} \times \mathrm{BM}_3$.
5. Блок открытого текста **шифруется** посредством следующей процедуры:

$$E_{PK} = (\mathrm{BP} \times \mathrm{BM}_1) \oplus PKC$$

6. Генерируется третья квазигруппа, $(Q_3,*)$, на основании которой шифрованный текст подвергается окончательной перестановке.
7. **Открытый ключ** в предложенной асимметричной криптосистеме – пары двух бинарных матриц $[\mathrm{BM}_1; PKC]$ и двух квазигрупп $[(Q_1,*); (Q_3,*)]$.
8. **Секретный ключ** криптосистемы - это Булева матрица BM_2 и пара двух обратных квазигрупп $[(\mathrm{Q}_1,/); (\mathrm{Q}_3,/)]$.

   Дешифрование блока открытого текста производится в следующем порядке:
   1. Криптотекст подвергается обратной перестановке согласно $(\mathrm{Q}_3,/)$,
   2. Начальная Булева перестановка извлекается посредством вычисления:

$$\mathrm{BP} = \mathrm{BP}_{\mathrm{PKC}} \times \mathrm{BM}_2.$$

   3. Результирующий текст подвергается обратной перестановке согласно $(\mathrm{Q}_1,/)$, тем самым извлекая открытый текст.

Вычислительные аспекты построения асимметричной криптосистемы на основе Булевых перестановок. Рассмотрим две самые важные процедуры: генерация пары криптографических ключей; шифрование/дешифрование.

Генерация открытого ключа в предложенной асимметричной криптосистеме выдвигает и решает следующие проблемы:

1. Разъяснение диапазона положительных целых чисел для покрытия символов открытого текста и установление требуемого количества битов для двоичного кодирования этих чисел.

2. Построение пары квазигрупп для первоначальной перестановки открытого текста и генерации коллекции сбалансированных нелинейных Булевых функций, составляющих Булеву перестановку BP.
3. Построение квадратной матрицы C размерностью $\mathrm{n} \times \mathrm{n}$ для генерации Булевых матриц BM_1 ,BM_2 и BM_3,
4. Создание дополнительной Булевой перестановки R порядка $\mathrm{n} - \mathrm{k}$ на основе второй квазигруппы.
5. Вычисление $\mathrm{PKC} = \mathrm{R} \times \mathrm{BM}_3$.

Приступим к оценке сложности генерации тройки матриц BM_1, BM_2 и BM_3. Матрицы BM_1 и BM_3 занимают соответственно k и $n-k$ строки матрицы C и не требуют особой вычислительной техники. Что касается матрицы C, то она – несингулярная и тестирование ее детерминанта на ненулевое значение, а также вычисление ее обратной – процедуры полиномиального времени.

Рассмотрим количество операций, требуемых для вычисления произведения двух матриц. Для общности оценки рассмотрим наихудший случай, когда умножаются матрицы размерностей $n \times n$. Так как имеются n^2 входов в обеих матрицах, то для вычисления их произведения потребуется n количество сложений и n количество умножений. Таким образом, $2n$ операций требуются для вычисления каждого элемента матрицы. Имея n^2 элементов в матрицах, $2\mathrm{n}^3$ операций потребуются для вычисления их произведения в целом. Так как операция сложения двух матриц размерностей $n \times n$ производится в результате n^2 операций, вычисление PKC потребует в целом $2\mathrm{n}^3 + \mathrm{n}^2$ количества операций.

Оценка вычислительной сложности генерации секретного ключа в предложенной асимметричной криптосистеме зависит от сложности извлечения матрицы BM_2, занимающей левые k столбца матрицы C^{-1}. Это производится посредством $k \times n$ операций. Что касается нахождения обратной Булевой перестановки, R^{-1}, то заметим, что это задача оппонента, так как легитимному получателю криптотекста обращение Булевой перестановки R не понадобится.

Алгоритмическая сложность шифрования/дешифрования информации. Шифрование блока включает произведение двух матриц и одну операцию сложения, а это - порядка $2\mathrm{n}^3 + \mathrm{n}^2$ операций. Дешифрование включает обращение второй квазигруппы (Q,/), произведение двух матриц и обращение начальной Булевой перестановки. Таким образом, $2\mathrm{n}^3 + 2\mathrm{n}^2 + \mathrm{n}$ операций потребуется для дешифрации блока криптотекста.

Из вышеизложенного следует, что в предложенной асимметричной криптосистеме генерация криптографических ключей, а также процессы шифрования/дешифрования, представляют вычисления полиномиального времени, что удовлетворяет требованиям, предъявленным односторонним функциям с секретом.

Криптоанализ асимметричной криптосистемы, основанной на Булевых перестановках. Стойкость предложенной асимметричной криптосистемы рассмотрено против классических атак.

1. *Атака на основе вероятностного текста*

Стойкость криптосистемы против этого типа атаки основана на сложности получения открытого текста от криптотекста. В этом случае атакующий пробует все доступные открытые ключи и дешифрует тексты, сопоставив их с переданным криптотекстом. В результате такой атаки может дешифроваться более чем один

смысловой текст, что указывает на не уникальность дешифрования без знания секретных ключей, а более точно, на то, что шифрование не иньективна по отношению к опубликованному методу шифрования.

Очевидно, что мера защищенности криптосистемы против неуполномоченного дешифрования приравнивается к верхней границе требуемых вычислений для осуществления исчерпывающих попыток угадывания коллекции Булевых функций в Булевой перестановке R, что при n количестве параметров равно $(2^n)!$. Для данного натурального числа k перечисление его факториала осуществляется со сложностью $O(k!\,\mathrm{k})$, из чего следует, что атака на основе вероятностного текста имеет сложность порядка $O((2^n)!\,2^n)$.

2 *Алгебраическая атака.*

Алгебраическая атака приводится к проблеме разложения произведения матриц, обращения Булевых перестановок и квазигрупп. Вспомним, что шифрование открытого текста включает матрицу размерности $n \times n$, состоящая из нескольких матриц – компонентов. Заметим, что результирующая шифрующая матрица не несет никакой информации о структуре компонентных матриц, Начальная и дополнительные Булевы перестановки – сложные композиционные структуры, основанные на квазигруппах, обращение которых при немалом количестве элементов - задача неполиномиального времени. Очевидно, что сложность разложения произведения матриц может быть приведена к сложности разложения целого числа на множители. Вспомним, что для b количества битов, представляющих собой двоичное представление произведения двух простых чисел одинакового порядка, сложность разложения на простые множители – порядка $O(\exp\left(\frac{16}{3}(\log b)^{\frac{2}{3}}\right))$. Обращение квазигруппы также является трудноразрешимой задачей, так как отсутствие единичного элемента приводит к экспоненциальному чтению таблицы, описывающей квазигруппу.

3. *Атака на основе исчерпывающего поиска секретного ключа.*

Вспомним, что секретный ключ криптосистемы - это Булева матрица BM_2, обратная Булева перестановка и обратные квазигруппы. Компонент секретного ключа BM_2 математически связана с BM_3 таким образом, что их произведение равно нулю, а это означает, что умножение BM_3 с другими матрицами, в данном случае произвольными неразглашенными матрицами типа R, также обеспечивает нулевое значение вышеуказанного произведения. Выявление BM_3 из структуры $R \times BM_3$ и последующее ее тестирование для выявления BM_2, при немалом количестве параметров - также трудноразрешимая задача. Обращение квазигрупп также известно как NP–полная задача.

4.*Атака вычислением секретного ключа из открытого*.

Вспомним конструкцию открытого ключа. Это пара матриц $[BM_1; PKC]$ и пара квазигрупп $[(Q_1,*); (Q_3,*)]$, Легко заметить, что конструкция секретного ключа, BM_2 и обратных квазигрупп $[(Q_1,/); (Q_3,/)]$, совершенно отличны от конструкции открытого ключа, хотя ключи шифрования/дешифрования математически связаны. Вспомним еще,, что произведение матрицы BM_2 с матрицей BM_3, которая является скрытым компонентом открытого ключа, равно нулю. Это означает, что матрица Булевой перестановки R представляет класс эквивалентных матриц, выявление конкретной из них для извлечения BM_3 приводится к проблеме угадывания случайного числа, что является NP-полной проблемой.

Из вышеизложенного следует, что степень защищенности криптотекста достаточно высока, для того, чтобы задерживать оппонента в дешифровании на такой промежуток времени, по окончании которой оригинальная информация утеряет свою значимость.

Сравнительная оценка производительности предложенной и существующих известных асимметричных криптосистем. Для сравнения рассматриваются криптосистема RSA и FAPKC. Вспомним, что "RSA операции", будь то шифрование или дешифрование, в основном - модулярное возведение в степень. Вычисление производятся сериями модулярных произведений, которые снижают производительность криптосистемы. Отсюда - ограничение существующих асимметричных криптосистем в практическом применении для шифрования/дешифрования информации.

В случае применения конечных автоматов, генерация криптографических ключей, а также шифрования/дешифрования – процедуры полиномиального времени. Однако привлечение нелинейных автоматов с целью повышения стойкости к атакам неизбежно приводит к некоторой потере эффективности функционирования результирующей системы.

В случае построения асимметричной криптосистемы на основе Булевых перестановок применение квазигрупп приближает стойкость криптосистемы к стойкости RSA, сохраняя при этом требуемый уровень эффективности расчетов.

Четвертая глава посвящена программной реализации предложенного алгоритма асимметричной криптосистемы BP Crypto на основе Булевых перестановок.

Раработанное программное средство пригодно как для автономного использования криптографической защиты информации, так и для дистрибутивных расчетов. Система криптографической защиты информации BP Crypto состоит из трех независимых функциональных модулей, которые также могут быть интегрированы в другие программные средства.:

- Модуль генерации пары криптографических ключей,
- Модуль шифрования,
- Модуль дешифрования.

Для активизации модуля генерации криптографических ключей указывается параметр длины блока открытого текста, которая диктует размерность Булевой матрицы BM_1. На основании этой матрицы генерируются Булевы матрицы BM_3 и BM_2. База данных квазигрупп является частью модуля генерации ключей, в которой регистрированы заранее сгенерированные и тестированные квазигруппы и их обратные.

После удостоверения выполнения требований к компонентам пары ключей, последние регистрируются в соответствующем защищенном файловом депозитариуме. Файл с именем public.key предоставляется пользователям.

Программный модуль шифрования предполагает получение открытой информации и соответствующего открытого ключа public.key в качестве входных данных. Выходными данными модуля шифрования является криптотекст с применением открытого ключа.

Программный модуль дешифрования предполагает получение криптотекста и соответствующего секретного ключа private.key в качестве входных данных. Выходными данными модуля дешифрования является открытый текст с применением секретного ключа.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

- Предложен метод построения односторонней функции с секретом, основанный на комбинировании сбалансированных Булевых функций и квазигрупп, что является необходимым условием для построения асимметричных криптосистем. Высокая производительность подобных криптосистем по сравнению с существующими обусловлена замещением алгебраических операций логическими операциями [1,5,9,10].
- Разработан метод генерации составляющих функций Булевых перестановок на основе квазигрупп, который позволяет существенно ускорить процедуру построения пары криптографических ключей [2,3].
- Разработан метод формального описания криптографических ключей асимметричной криптосистемы на основе Булевых перестановок, который позволяет упростить функциональную структуру криптосистемы и ее практическую реализацию за счет представления ключей в форме положительных целых чисел [4,7,8].
- Получены оценки стойкости асимметричной криптосистемы на основе Булевых перестановок по отношению к типичным видам атак, что позволяет обосновать выбор размера криптографических ключей при заданном уровне стойкости криптосистемы [6,7].
- Разработана стойкая асимметричная криптосистема высокой производительности, основанная на Булевых перестановках и программное средство BP Crypto, сочетающих криптографические свойства специального класса Булевых функций и квазигрупп. В результате, обеспечена эффективность процессов шифрования/дешифрования [4,7].
- Показано, что стойкость предложенной асимметричной криптосистемы основана на вычислительной сложности инвертирования Булевых перестановок и квазигрупп [3,6].

ПЕРЕЧЕНЬ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

[1] Е.Ц.Алавердян. “Булева перестановка как математическая основа для построения неассоциативных криптографических структур”, Сборник статей научно-практической конференции *“Вопросы безопасности информационных систем”,* Ереван, 26-27 мая 2011,стр 47-52.

[2] G. Margarov, Y. Alaverdyan, “Non Associative Algebraic Structures embedded Fast Public Key Cryptosystem based on Boolean Product of Matrices”, In Proc. of the Workshop on *Applications of Information Theory, Coding and Security*, Yerevan, Armenia, April, 2010, pp.79-82.

[3] G. Margarov, Y. Alaverdyan, “Quasigroup Equipped Strong Public Key Cryptosystem based on Boolean Product of Matrices”, *The 2010 World Congress in Computer Science*, Las Vegas, Nevada, USA, July, pp. 157-161.

[4] Y. Alaverdyan, “Construction Efficiency of the Public Key Cryptosystem based on Boolean Product of Matrices”, In Proc. of the *7 th International Conference on Computer Science and Information Technologies*, Yerevan, Armenia, September 28-October 2, 2009, pp.105-108.

[5] G. Margarov, S. Chopuryan, Y. Alaverdyan, “Cryptanalysis of Finite Automata Public Key Cryptosystems”, *The 2009 World Congress in Computer Science*, Las Vegas, Nevada, USA, July, pp. 157-161.

[6] G. Margarov, Y. Alaverdyan, “Stability of the Public Key Cryptosystem based on Boolean Product of Matrices”, In Proc. of the *Second int. conf. on the applications of digital info. & web technologies*, London, UK, August, 2009, pp. 592-597.

[7] G. Margarov, Y. Alaverdyan, “Fast asymmetric cryptosystem based on Boolean product of matrices” , In *Proc. of the 7th IEEE/ACS Int. Conf. on Computer Systems and Applications*, Rabat, Morocco, May, 2009, pp. 392-397.

[8] Е.Ц.Алавердян, “Стойкая асимметричная криптосистема основанная на булевом произведении матриц”, Вестник-75 Государственного инженерного университета Армении (Политехник), Сборник научных и методических статей, Часть 1, стр. 306-310, Ереван, 2009.

[9] Г. Маркаров, Е. Алавердян, С. Чопурян, “Теория конечных автоматов как основа для построения ассиметричных систем”, Вестник-75 Государственного инженерного университета Армении (Политехник), Сборник научных и методических статей, Часть 1, стр. 306-310, Ереван, 2008.

[10] G. Margarov, S. Chopuryan, Y. Alaverdyan, ”Fast Public Key Algorithm Based on Finite Automata”, In Proc. of the Int’ Conf. on Computer Science and Information Technologies (CSIT’07), pp. 112-115, September 2007.

Ալավերդյան Եղիսաբեթ Ծերունի

ԲՈՒԼՅԱՆ ՏԵՂԱՓՈԽՈՒՄՆԵՐԻ ՎՐԱ ՀԻՄՆՎԱԾ ԲԱՐՁՐ ԱՐԱԳԱԳՈՐԾՈՒԹՅԱՆ ԱՆՀԱՄԱՉԱՓ ԳԱՂՏՆԱՀԱՄԱԿԱՐԳԻ ՀԵՏԱԶՈՏՈՒՄ ԵՎ ՄՇԱԿՈՒՄ

ԱՄՓՈՓԱԳԻՐ

Մարդկությունը թևակոխել է մի այնպիսի դարաշրջան, երբ գործարար փաստաթղթաշրջանառությունն իրականացվում է համակարգչային այնպիսի բաց համակարգերի միջոցով, ինչպիսին համացանցն է: Փոխանակվող տեղեկույթի պաշտպանության հիմնական միջոցներից մեկը գաղտնագրությունն է, որն ապահովում է հաղորդվող տեղեկույթի անվտանգությունը գաղտնագրման միջոցով՝ գաղտնագրային բանալիների կիրառմամբ: Հաղորդակցվող կողմերի միջև վստահության հաստատման և գաղտնագրային բանալիների վաղօրոք փոխանակման անհրաժեշտության վերացման նպատակով կիրառվում են անհամաչափ գաղտնահամակարգերը: Գոյություն ունեցող անհամաչափ գաղտնահամակարգերը, որոնք կառուցված են թվերի տեսության մեթոդների կիրառմամբ, ապահովում են գաղտնահամակարգի բարձր կայունություն, սակայն, միևնույն ժամանակ, չափազանց դանդաղագործ են բարդ հաշվարկներ կիրարկելու պատճառով: Վերջին հանգամանքը խիստ նեղացնում է անհամաչափ գաղտնահամակարգերի կիրառության տիրույթը՝ սահմանափակելով դրանց օգտագործումը միայն գաղտնագրային բանալիների փոխանակման և թվային ստորագրությունների գեներացման համար:

Հաշվի առնելով բաց բանալինային գաղտնահամակարգերի նկատմամբ օրավուր աճող հետաքրքրությունը և անհրաժեշտությունը դրանք կիրառելու նաև տեղեկութի գաղտնագրման/վերծանման համար, անհամաչափ գաղտնահամակարգերի զարգացումը դառնում է արդիական խնդիր:

Վերոհիշյալ խնդրի հնարավոր լուծումներից մեկը կարող է հանդիսանալ անհամաչափ գաղտնահամակարգերի նախագծումը Բուլյան փոխատեղությունների հիման վրա, որը ներգրավում է արագագործ հանրահաշվական կառուցվածքներ, իսկ համակարգի անվտանգությունը հիմնվում է ոչ տեղափոխական և ոչ զուգորդական գործողությունների օգտագործման վրա: Վերջիններս ապահովվում են Բուլյան ֆունկցիաների և քվազիխմբերի կիրառմամբ:

<u>Հետազոտության հիմնական նպատակը</u>

Աշխատանքի հիմնական նպատակն է՝ հետազոտել և մշակել արագագործ անհամաչափ գաղտնահամակարգերի կառուցման սկզբունքները:

Նշված նպատակին հասնելու համար աշխատանքում անհրաժեշտ է լուծել հետևյալ խնդիրները.

- Սահմանել պահանջվող գաղտնակայունությամբ օժտված արագագործ անհամաչափ գաղտնահամակարգերի կառուցման մեթոդները, հիմնվելով գոյություն ունեցող անհամաչափ գաղտնահամակարգերի վերլուծության վրա:
- Նախագծել գաղտնիքով միակողմանի ֆունկցիա՝ հիմնված տրամաբանական գործողությունների վրա, նպատակ ունենալով բարձրացնել նախագծվող անհամաչափ գաղտնահամակարգի արդյունավետությունը:
- Մշակել անհամաչափ գաղտնահամակարգի բանալիների մոդել՝ հիմնված տրամաբանական գործողությունների վրա, որոնք հնարավորություն կընձեռեն պարզեցնելու բանալիների գործնական իրականացումը:
- Նախագծել Բուլյան փոխատեղությունների վրա հիմնված անհամաչափ գաղտնահամակարգն իրականացնող ալգորիթմներն ու ծրագրային միջոցները:

ՀԻՄՆԱԿԱՆ ԱՐԴՅՈՒՆՔՆԵՐ ԵՎ ԵԶՐԱՀԱՆԳՈՒՄՆԵՐ

- Առաջարկված է գաղտնիքով միակողմանի ֆունկցիայի նախագծման մեթոդ հիմնված հավասարակշռված Բուլյան ֆունկցիաների և քվազիխմբերի վրա, որն անհրաժեշտ պայման է հանդիսանում անհամաչափ գաղտնահամակարգերի կառուցման համար: Նման գաղտնահամակարգերի բարձր արդյունավետությունը համեմատած գոյություն ունեցող համակարգերի հետ պայմանավորված է հանրահաշվական գործողությունները տրամաբանականով փոխարինելու հանգամանքով [1,5,9,10]:.
- Առաջարկված է Բուլյան փոխատեղությունների բաղադրիչ ֆունկցիաների գեներացման մեթոդ հիմնված քվազիխմբերի վրա, որը հնարավորություն է տալիս էապես արագացնել գաղտնագրային բանալիների զույգի կառուցման ընթացակարգը [2,3]:
- Մշակված է Բուլյան փոխատեղությունների վրա հիմնված անհամաչափ գաղտնահամակարգի գաղտնագրային բանալիների ձևայնացված նկարագրության մեթոդ, որը հնարավորություն է տալիս պարզեցնել գաղտնահամակարգի ֆունկցիոնալ կառուցվածքը և գործնական իրագործումը՝ իրականացնելով բանալիների ներկայացումն ամբողջ թվերի տեսքով [4,7,8]:
- Ստացված են Բուլյան փոխատեղությունների վրա հիմնված անհամաչափ գաղտնահամակարգի կայունության գնահատականները տիպական

գրոհների նկատմամբ, որը թույլ է տալիս հիմնավորել գաղտնագրային բանալիների չափերի ընտրությունը գաղտնահամակարգի կայունության առաջադրված մակարդակի համար [6,7]:

- Մշակված է արագագործ անհամաչափ գաղտնահամակարգ հիմնված Բուլյան փոխատեղությունների վրա և BP Crypto ծրագրային փաթեթը, որը համադրում է Բուլյան ֆունկցիաների հատուկ դասը և քվազիխմբերը: Արդյունքում ապահովված է գաղտնագման/վերծանման ընթացակարգերի արդյունավետությունը [4,7]:
- Ցույց է տրված, որ առաջարկվող անհամաչափ գաղտնահամակարգի կայունությունը հիմնված է Բուլյան փոխատեղությունների և քվազիխմբերի հակադարձելիության բարդության վրա [3,6]:

Yeghisabet Alaverdyan

DESIGN OF AN EFFICIENT ASYMMETRIC CRYPTOSYSTEM BASED ON BOOLEAN PERMUTATIONS

RESUME

Nowadays the business workflow mainly runs over wide area computer networks, such as Intermet. Protection of the information content is provided through its cryptographical modification, applied cryptographic keys. In order to establish fair communication and to eliminate the cryptographic keys exchange problem, asymmetric cryptosystems are developed. The existing asymmetric cryptosistems, based on the number theory, provide high level of stability. Meanwhile, the effectivenness of the asymmetric cryptosystems is still low due to complex computations over huge numbers. This keeps the asymmetric cryptosystems currently confined to key management and signature applications, leading to restrictions in their practical applications for data ciphering/deciphering procedures.

Taking into account a great interest in public key infrastructures on wide area networks management, further development of asymmetric crytposystems becomes obvious and topical.

A possible resolution of the given problem may be the design of asymmetric cryptosystems based on Boolean permutations. This approach is motivated by usage of efficient algebraical structures in construction of nesting asymmetric cryptosystems. The stability of the proposed cryptosystem is conditioned by the application of non commutative and non associative operations of high algebra. To obtain the required level of stability, a special class of Boolean functions and quasigoups are applied.

Purpose and objectives

The main purpose and objectives of the presented work are the research and development of principles for constructing efficient asymmetric cryptosystems. To achieve this goal the following issues have to be explored:

- Definition of the methods for constructing efficient asymmetric cryptosystems possessing the required level of stabiity based on the anaysis of the existing asymmetric cryptosystems.
- Design a trapdoor one way function baased on logical operations in order to increase the efficiency of the proposed asymmetric cryptosystem.
- Design a model of the proposed asymmetric cryptosystem cryptographic keys based on logical operations in order to symplify their practical realization.
- Design the algorithms and the software to implement the asymmetric cryptosystem based on Boolean permutations.

Main results.

- A method for designing a trapdoor one way function baased on balanced Boolean functions and quasigroups are proposed, which is a necessary condition in construction of asymmetric cryptosystems. High efficiency of such cryptosystems are conditioned by replacement of algebraic operations with logical ones [1,5,9,10].
- A method for generating component functions of the Boolean permutation is proposed based on quasigroups, which allows to significanty speed up the procedure of the cryptographic key pair generation [2,3].
- A formal method to describe the cryptographic key pair of the asymmetric cryptosystem based on Boolean permutations is developed, which allows to symplify the functional structure and practical implementation of the cryptosystem by representing the keys through integral values [4,7,8].
- Estimation of stability of the asymmetric cryptosystem based on Boolean permutations are obtained against classical types of attacks, which allows to justify the choice of the cryptographic key sizes for the required level of security [6,7].
- An efficient asymmetric cryptosystem and a software BP Crypto, based on quasigroup equipped Boolean permutations, have been obtained. The resolution combines the special class of Boolean functions and quasigroups. As a result, the efficiency of the procedures of encryption/decryption has been provided [4,7].
- It is stated that the stability of the proposed asymmetric cryptosystem is based on the complexity of inverting Boolean permutations and quasigroups [3,6].