ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

ՉՈՓՈՒՐՅԱՆ ՍԻՐԱՆՈՒՇ ՀՐԱՅՐԻ

ՎԵՐՋԱՎՈՐ ԱՎՏՈՄԱՏՆԵՐԻ ՎՐԱ ՀԻՄՆՎԱԾ ԱՆՀԱՄԱՉԱՓ ԳԱՂՏՆԱԳՐԱՅԻՆ ՀԱՄԱԿԱՐԳԻ ԳԱՂՏՆԱԿԱՅՈՒՆՈՒԹՅԱՆ ԲԱՐՁՐԱՑՄԱՆ ՄԻՋՈՑՆԵՐԻ ՀԵՏԱԶՈՏՈՒՄ ԵՎ ՄՇԱԿՈՒՄ

Ե.13.04-<<Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում>> մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

Ս Ե Ղ Մ Ա Գ Ի Ր

ԵՐԵՎԱՆ 2011

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК РА

ЧОПУРЯН СИРАНУШ ГРАЙРОВНА

ИССЛЕДОВАНИЕ И РАЗРАБОТКА ПРИНЦИПОВ ПОВЫШЕНИЯ СТОЙКОСТИ АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ НА ОСНОВЕ КОНЕЧНЫХ АВТОМАТОВ

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени кандидата технических наук по специальности 05.13.04 – «Математическое и программное обеспечение вычислительных машин, комплексов и сетей»

ЕРЕВАН 2011

Ատենախոսության թեման հաստատվել է Հայաստանի Պետական Ճարտարագիտական Համալսարանում (Պոլիտեխնիկ)

Գիտական ղեկավար՝	տ.գ.թ., դոց.	Գ.Ի. Մարգարով
Պաշտոնական ընդդիմախոսներ՝	ՀՀ ԳԱԱ ակադ., տ.գ.դ., պրոֆ.	Գ. Հ. Խաչատրյան
	տ.գ.թ., դոց.	Վ.Ս. Հակոբյան

Առաջատար կազմակերպություն՝ Հայ-Ռուսական (Սլավոնական) Համալսարան

Պաշտպանությունը կայանալու է՝ հունիսի 17-ին 2011թ. ժ. 16:00-ին, 037 <<Ինֆորմատիկա և հաշվողական համակարգեր>> մասնագիտական խորհրդի նիստում, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացված պրոբլեմների ինստիտուտում (հասցեն՝ 0014, Երևան, Պ. Սևակ փ. 1)

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրն առաքված է մայիսի 17-ին 2011թ.

037 Մասնագիտական խորհրդի գիտական
քարտուղար, ֆ.-մ.գ. դ., պրոֆ. Մ.Ե. Հարությունյան

Тема диссертации утверждена в Государственном Инженерном Университете Армении (Политехник)

Научный руководитель:	к.т.н., доц.	Г.И. Маргаров
Официальные оппоненты:	акад. НАН РА д.т.н., проф.	Г.Г. Хачатрян
	к.т.н., доц.	В.С. Акопян

Ведущая организация: Российско-Армянский (Славянский) университет

Защита диссертации состоится 17 июня 2011г. в $16^{\underline{00}}$ 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 17 мая 2011г.

Ученый секретарь специализированного совета 037,
д.ф-м.н., проф. М.Е. Арутюнян

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. С развитием информационного общества в последние годы возросла необходимость обеспечения защиты информации. Одним из способов достижения этой цели служит использование криптографических средств защиты, выполняющих преобразование информации ее шифрованием и дешифрованием с помощью криптографических ключей. С совершенствованием криптографических средств защиты для решения проблем доверия между сторонами защищенного обмена и распределения криптографических ключей развивались асимметричные криптосистемы, основанные на предоставление каждой стороне обмена информации своего собственного ключа. В основе применяемых на практике асимметричных криптосистем в целях обеспечения высокого уровня стойкости лежат математические трудноразрешимые задачи, в частности, задача факторизации большого числа на простые сомножители и трудноразрешимая дискретно-логарифмическая задача. Однако существующие до настоящего времени асимметричные криптосистемы обладают низким уровнем быстродействия и выполняют шифрование и дешифрование информации намного медленнее, чем симметричные криптосистемы. Это обусловлено использованием сложных арифметических операций для шифрования и дешифрования, таких как умножение и возведение в степень чисел размером от сотни и более цифр, требующих значительных затрат времени и вычислительных ресурсов, что и приводит к понижению быстродействия асимметричных криптосистем. Этим объясняется тот факт, что существующие асимметричные криптосистемы не нашли эффективного применения для шифрования/дешифрования большого объема информации из-за малого быстродействия и в основном используются для распределения ключей и цифровой подписи.

В последние годы проводятся интенсивные исследования по созданию быстродействующих асимметричных криптосистем с применением других областей математики, в частности, теории автоматов. Проектирование быстродействующих асимметричных криптосистем на основе конечных автоматов обусловлено использованием логических операций, применяемых в конечных автоматах. Также быстродействующие криптосистемы могут быть пригодны не только для цифровой подписи, но и могут быть весьма продуктивны для шифрования/дешифрования большого объема данных. Существующие до настоящего времени асимметричные криптосистемы на основе конечных автоматов, обладая высоким быстродействием, в то же время не обладают достаточной стойкостью. Кроме того отсутствуют конкретные алгоритмы реализации криптосистем на основе конечных автоматов, и, следовательно, отсутствуют соответствующие программные средства. Из вышеизложенного следует, что создание быстродействующей и стойкой асимметричной криптосистемы на основе конечных автоматов является актуальной задачей.

Цель и задачи работы – исследование и разработка принципов построения быстродействующих и стойких асимметричных криптосистем на основе конечных автоматов. Для достижения указанной цели в работе ставятся и решаются следующие основные задачи:

- Анализировать существующие асимметричные криптосистемы и определить методы повышения быстродействия процессов шифрования и дешифрования.
- Провести криптоанализ существующих асимметричных криптосистем на основе конечных автоматов и, базируясь на результатах проведенного криптоанализа, разработать методы, повышающие стойкость криптосистем, для противостояния типичным видам атак.
- Создать алгоритмы и программные средства, реализующие асимметричные криптосистемы на основе разработанных методов.

Объект исследования. Объектом исследования является быстродействие и стойкость асимметричных криптосистем на основе конечных автоматов.

Методы исследования. В работе использованы методы теории чисел, линейной алгебры, дискретной математики, криптографии, теории сложности.

Научная новизна:

- Базируясь на результатах криптоанализа существующих асимметричных криптосистем на основе конечных автоматов, предложены подходы к повышению их степени стойкости по отношению к типичным видам атак, в частности, к атакам на основе только шифротекста и на основе выбранного открытого текста.
- Определены инвертируемые нелинейные автоматы и предложены модификации линейных и нелинейных автоматов, повышающие стойкость асимметричной криптосистемы по отношению к типичным видам атак.
- Обоснована возможность построения односторонней функции с секретом на основе конечных автоматов, которая является основой для построения асимметричной криптосистемы с применением конечных автоматов.
- Предложен способ построения криптографического алгоритма с применением нелинейных конечных автоматов, который, в отличие от существующих алгоритмов, позволяет повысить стойкость проектируемой асимметричной криптосистемы на основе конечных автоматов.
- Разработан метод формального описания криптографических ключей асимметричной криптосистемы на основе конечных автоматов, который позволяет генерировать пары открытых и секретных ключей в цифровом виде.

Практическая значимость полученных результатов:

- Разработаны алгоритмы и созданы функционально независимые программные модули генерации ключей, шифрования и дешифрования информации, которые позволяют построить асимметричную криптосистему на основе конечных автоматов.
- Спроектирована стойкая асимметричная криптосистема на основе конечных автоматов FAPKC Crypto, которая по сравнению с существующими асимметричными криптосистемами на основе теории чисел обеспечивает повышение быстродействия процессов шифрования/дешифрования в 10 раз уже при объеме шифруемой информации 10Кб и почти в 2^8 раз при объеме 50Мб.
- Разработана учебно-исследовательская система PK CrypTool, предоставляющая эффективные ресурсы исследований и сравнительного анализа различных асимметричных криптосистем.

Внедрения. Результаты диссертационной работы использованы в представительстве международной фармацевтической организации World Medicine в Армении и фармацевтической организации Тонус-Лес. Посредством программного интерфейса FAPKC Crypto обеспечивается защищенная передача необходимого пакета документов лекарственных препаратов фармацевтической организации World Medicine организации Тонус-Лес для осуществления процесса их регистрации в Армении. Внедрение результатов диссертационной работы в данных организациях гарантирует защищенность пакета документаций лекарственных препаратов в течение 15 лет, что и является необходимым временем их секретности. Кроме того, основные результаты работы применяются в учебно-исследовательском программном приложении PK CrypTool во время учебного процесса кафедры ИБПО ГИУА. Акты о внедрении результатов работы приводятся в Приложении D.

На защиту выносятся следующие положения:

- Методы модификации линейных и нелинейных автоматов, повышающие стойкость асимметричных криптосистем на основе конечных автоматов.
- Метод формального описания криптографических ключей асимметричной криптосистемы на основе конечных автоматов.
- Алгоритмы и программные средства, реализующие функционально независимые модули генерации ключей, шифрования и дешифрования, и построенные на их основе программные средства FAPKC Crypto и PK CrypTool.

Апробация полученных результатов. Основные результаты работы докладывались и обсуждались на VI и VII международных конференциях "Computer Science and Information Technologies (CSIT)" (2007г., 2009г., г. Ереван), на 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 (2007г., 2008г., 2009г. Ереван), на научно-практической конференции по вопросам безопасности информационных систем, (2008г., г. Ереван), на VI международной конференции "Исследование, разработка и применение высоких технологий в промышленности", (2008г., г. Санкт-Петербург), на XXXV международной молодежной научной конференции "Гагаринские чтения", (2009г., г. Москва), на международной конференции по вопросам безопасности и менеджмента SAM'09 (2009г., г. Лас Вегас, США), на II международной конференции по применению цифровой информации и веб-технологий ICADIWT'09 (2009 г., г. Лондон, Великобритания), на семинаре Applications of Information Theory, Coding and Security WAITS2010 (2010г., г. Ереван), а также обсуждались на научных семинарах кафедры ИБПО ГИУА (2007-2010гг., г. Ереван) и на научном семинаре ИПИА НАН РА (2011г., г. Ереван).

Публикации. Основные результаты опубликованы в 14 научных трудах, перечисленных в конце автореферата.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и четырех приложений. Общий объем работы – 114 страниц, включая 60 рисунка, 79 наименований в списке использованной литературы и 21 страниц приложений.

СОДЕРЖАНИЕ РАБОТЫ

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

В первой главе диссертационной работы рассматривается организация существующих асимметричных криптосистем, в частности, наиболее распространенные криптосистемы RSA, Эль Гамаля и Рабина, анализируются особенности и недостатки их практического применения при шифровании/дешифровании большого объема информации.

Представлена тенденция создания быстродействующих асимметричных криптосистем с применением других областей математики, в частности, теории конечных автоматов. Применение конечных автоматов для построения асимметричных криптосистем обусловлено тем, что на их основе можно построить одностороннюю функцию с секретом. Более того, потенциальное быстродействие автоматов за счет использования в них логических операций дает возможность создать стойкую асимметричную криптосистему с высоким быстродействием.

Рассмотрены существующие асимметричные криптосистемы на основе конечных автоматов FAPKC0, FAPKC1, FAPKC2 и FAPKC3. Представлен основной принцип построения асимметричных криптосистем на основе конечных автоматов и рассмотрены функционирования этих криптосистем.

В конце главы на основе проведенного анализа принципов построения асимметричных криптосистем сформулирована цель диссертационной работы и поставлены задачи ее достижения. Для построения стойкой и быстродействующей асимметричной криптосистемы на основе конечных автоматов представляется целесообразным проводить криптоанализ существующей асимметричной криптосистемы FAPKC3. Нахождение и устранение недостатков криптосистемы FAPKC3 по отношению к возможным видам атак приводит к необходимости усовершенствования алгоритма реализации. Для создания стойкой и быстродействующей асимметричной криптосистемы сформулированы основные задачи, способствующие достижению цели диссертационной работы

Во второй главе в рамках криптоанализа асимметричной криптосистемы FAPKC3 рассмотрены следующие криптоаналитические атаки:

- прямое вычисление секретного ключа из открытого ключа;
- атака на основе выбранного открытого текста;
- атака на основе только шифротекста.

Проведены работы по выявлению уязвимых мест асимметричной криптосистемы FAPKC3 по отношению к вышеперечисленным трем видам атак. Рассматриваются пути, по которым криптоаналитик попытается выявить секретный ключ из использованного открытого ключа криптосистемы, и пути получения открытого текста из шифротекста. Вычислены временные сложности алгоритмов, осуществляющие указанные атаки для оценки времени, требуемого противнику для их проведения.

Рассмотрена криптоаналитическая атака прямого вычисления секретного ключа из открытого ключа на асимметричную криптосистему FAPKC3 двумя способами:

1. непосредственное инвертирование композиционного автомата;
2. инвертирование композиционного автомата методом его декомпозиции.

Временная сложность непосредственного инвертирования конечного автомата вычисляется в результате анализа дерева данного конечного автомата. Анализ дерева конечного автомата производится по значению тактовой задержки τ_k , которое и определяет глубину проведенного анализа. Входными данными, необходимыми для решения задачи непосредственного инвертирования композиционного конечного автомата, являются число

состояний и задержка τ_k данного автомата. Показано, что временная сложность задачи непосредственного инвертирования композиционного автомата для входного слова длиной k равна:

$$T(k) = \sum_{j=0}^{k-1} |S|^{k-j}, \quad (1)$$

где k – число тактов, определяющее задержку композиционного конечного автомата; S - множество состояний композиционного конечного автомата M_1.

Суть инвертирования композиционного автомата методом его декомпозиции в отличие от предыдущего метода заключается в декомпозиции композиционного автомата для построения его инверсного автомата. Показано, что в асимметричной криптосистеме FAPKC3, где композиционный автомат шифрования состоит из двух линейных автоматов, соединенных последовательно, задача декомпозиции автомата $M = \langle M_1, M_2 \rangle$ приводится к задаче факторизации матричного полинома. Для определения стойкости асимметричной криптосистемы FAPKC3 по отношению к атаке прямого вычисления секретного ключа из открытого ключа оценивается временная сложность алгоритма инвертирования композиционного автомата методом его декомпозиции. Показано, что временная сложность задачи определения секретного ключа противником, владеющим знанием о компонентных автоматах, которые составляют открытый ключ, оценивается выражением вида:

$$T(k) = \sum_{i=0}^{n} T(k_i) = \sum_{i=0}^{n} \sum_{j=0}^{k_i - j} |S_i|^{k_i - j} = n \times \sum_{j=0}^{k/n-j} \left(|S|/n\right)^{k/n-j} \quad (2)$$

Таким образом, выявляется, что стойкость асимметричной криптосистемы FAPKC3 по отношению к атаке прямого вычисления секретного ключа из открытого ключа двумя методами зависит от значения тактовой задержки τ_k композиционного автомата, являющегося открытым ключом. Также выявлено, что криптосистема FAPKC3 уязвима по отношению к атаке прямого вычисления секретного ключа из открытого ключа, так как задержки τ_k использованных конечных автоматов не являются достаточно большими.

Рассмотрена криптоаналитическая атака на основе только шифротекста на асимметричную криптосистему FAPKC3, которая приводится к задаче решения системы k линейных уравнений с k неизвестными. Посредством численного анализа показано, что время, требуемое противнику для проведения атаки на основе только шифротекста на асимметричную криптосистему FAPKC3, оценивается временной сложностью задачи решения системы линейных уравнений (3), которая равна:

$$T(k) = O(k^3) \quad (3)$$

Выявлено, что недостатки криптосистемы FAPKC3 при атаках на основе только шифротекста обусловлены использованием линейных конечных автоматов с низкой тактовой задержкой τ_k, которая становится причиной малого количества аргументов системы линейных уравнений над полем $GF(2)$, что и упрощает ее решение.

Рассмотрена криптоаналитическая атака на основе выбранного открытого текста на асимметричную криптосистему FAPKC3, которая заключается в том, что противник может выбрать необходимое число открытых текстов и получить соответствующие им шифротексты при неизменном ключе шифрования. Показано, что задача случайного подбора текстов, их шифрование и сравнение с наличествующим шифротекстом упрощается в асимметричной криптосистеме FAPKC3. Это обусловлено тем, что асимметричная криптосистема на основе конечных автоматов является последовательной, т.е. каждый символ, зашифрованный с

помощью этой криптосистемы, включает в себя информацию о предыдущих зашифрованных символах, что позволяет свести определение открытого текста к определению его части. Показано, что последовательное восстановление открытого текста приводится к последовательному поиску, позволяющему найти выходную последовательность конечного автомата из его входной последовательности определенной длины k. Допускается, что противнику известно начальное состояние конечного автомата шифрования и его выходная последовательность длиной k, которые являются входными данными для алгоритма последовательного поиска. Показано, что атака на основе выбранного открытого текста в асимметричной криптосистеме FAPKC3 приводится к задаче поиска в дереве глубиной k. При этом временная сложность данной атаки оценивается временной сложностью алгоритма поиска в дереве и равна:

$$T(k) = O(k) \tag{4}$$

В целях анализа полученных результатов проведенных криптоаналитических атак на асимметричную криптосистему FAPKC3 проведено сравнение временных сложностей этих атак (рис. 1). Показано, что атака прямого вычисления секретного ключа из открытого ключа обеими методами инвертирования конечного автомата шифрования осуществляется экспоненциальными алгоритмами, поэтому не столь существенно увеличение стойкости FAPKC3 по отношению к этой атаке. Стойкость асимметричной криптосистемы FAPKC3 целесообразно увеличить по отношению к атакам на основе только шифротекста и на основе выбранного открытого текста, поскольку алгоритмы их осуществления являются полиномиальными.

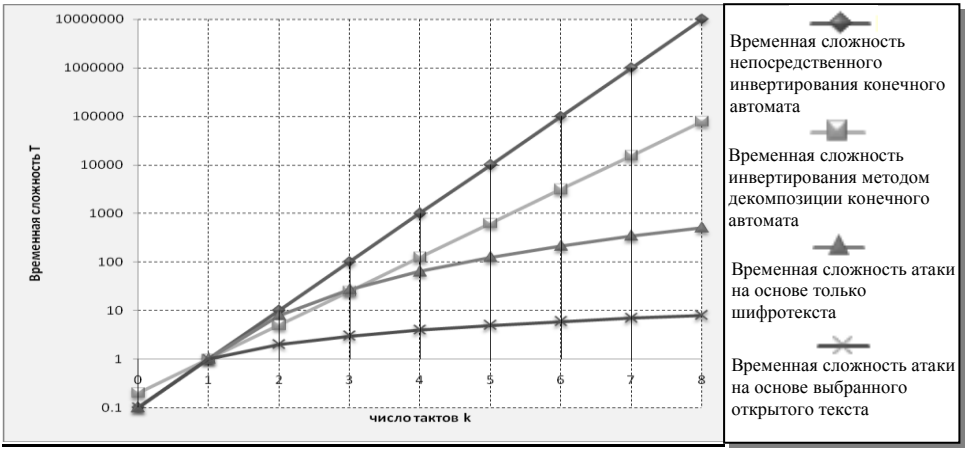

Рис 1. Сравнение временных сложностей различных атак на FAPKC3

Третья глава посвящена разработке принципов построения стойких асимметричных криптосистем на основе конечных автоматов в целях усовершенствования алгоритма реализации данных асимметричных криптосистем по отношению к атакам на основе только шифротекста и выбранного открытого текста. Криптоанализ асимметричной криптосистемы FAPKC3 показывает, что основными направлениями построения эффективного алгоритма реализации криптосистемы на основе конечных автоматов являются: использование нелинейных инвертируемых конечных автоматов вместо линейных легко инвертируемых автоматов и увеличение их тактовых задержек τ_k. Определены инвертируемые нелинейные автоматы и представлена схема их стандартной реализации (рис.2).

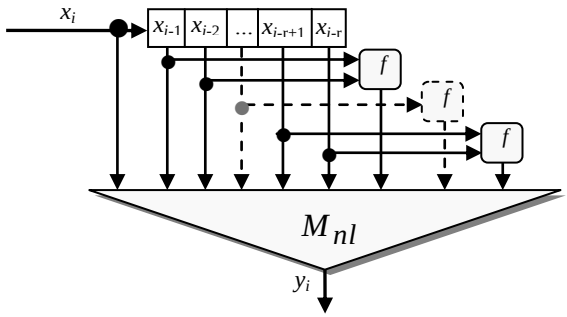

Рис. 2. Стандартная реализация автомата M_{nl}

Автомат M_{nl}, показанный на рис. 2, является конечным автоматом с памятью, исходное состояние которого можно выявить из знания, по крайней мере, r количества входных элементов. Инверсный автомат M_{nl}^{-1} представленного автомата, зависящий от r числа выходных элементов, представляет собой инвертированный автомат с задержкой τ_0, т.е. автомат с нулевой тактовой задержкой.

Стойкость асимметричной криптосистемы FAPKC3 по отношению к рассмотренным видам криптоаналитических атак зависит от значения k, определяющего тактовую задержку τ_k конечного автомата шифрования. Заменив в композиционном автомате один из компонентных линейных автоматов нелинейным автоматом с нулевой тактовой задержкой, в целом, уменьшаем его тактовую задержку τ_k. Предложена модификация линейных и нелинейных автоматов, которая позволяет повысить стойкость асимметричной криптосистемы FAPKC3 по отношению к возможным видам атак, в частности, к атакам на основе только шифротекста и на основе выбранного открытого текста, посредством увеличения тактовой задержки τ_k автомата шифрования. Последняя становится возможным при замене легко инвертируемого нелинейного конечного автомата с задержкой τ_0 легко инвертируемым нелинейным конечным автоматом с задержкой τ_{k_1} и увеличением тактовой задержки линейного конечного автомата.

Описана модификация легко инвертируемого нелинейного автомата с задержкой τ_0 в легко инвертируемый нелинейный автомат с задержкой τ_{k_1}, являющаяся результатом переопределения функции f над полем GF(2).

Схематическое представление функционирования нелинейного автомата M_{nl} с переопределенной нелинейной функцией f приведено на рис. 3.

Предложен способ модификации линейных конечных автоматов с целью увеличения задержки линейного автомата добавлением новых состояний между двумя состояниями автомата. Полученный при этом новый линейный конечный автомат является эквивалентным начальному автомату, но имеет большую тактовую задержку, поскольку с увеличением мощности множества состояний конечного автомата при добавлении новых состояний к этому множеству значение тактовой задержки квадратично увеличивается. Для усложнения взлома улучшенной криптосистемы FAPKC осуществляется также дополнительная модификация линейного автомата, посредством определения нелинейной операции для его двух последовательных входных элементов. Тем самым линейный автомат в композиционном

автомате шифрования заменяется нелинейным автоматом, что приводит к построению автомата шифрования только из композиции нелинейных автоматов.

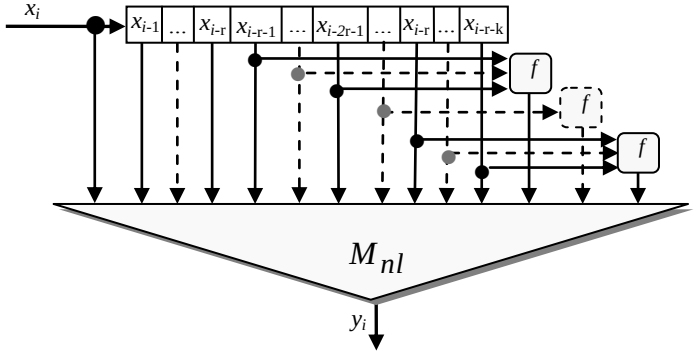

Рис. 3. Модифицирование автомата M_{nl}

Дана оценка временных сложностей рассмотренных в предыдущей главе криптоаналитических атак для спроектированной криптосистемы FAPKC_adv (рис. 4).

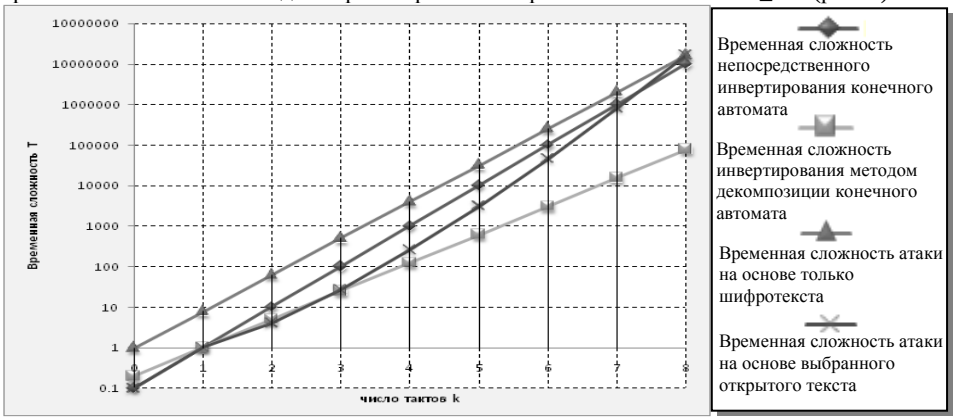

Рис 4. Сравнение временных сложностей различных атак на FAPKC_adv

На основе реализованных модификаций автоматов предложен и спроектирован криптографический алгоритм с применением нелинейных конечных автоматов и показана его стойкость к разного рода атакам. Разработанный алгоритм представляет собой криптографический алгоритм, на основе которого можно построить стойкую асимметричную криптосистему, так как он соответствует всем классическим требованиям криптографических систем защиты информации.

В данной главе предложен принцип генерации целых чисел, однозначно определяющих соответствующие конечные автоматы и являющихся ключами данной криптосистемы. В зависимости от того, является ли конечный автомат линейным или нелинейным, различаются принципы генерирования соответствующих чисел. Представлены разработки процедур шифрования и дешифрования информации с применением генерируемых криптографических ключей.

С целью оценки криптостойкости асимметричной криптосистемы на основе конечных автоматов показано, что математическая функция, лежащая в основе криптосистемы, является односторонней, обладающей секретом. Показано, что секрет односторонней

функции заключается в том, что обладатель информации о компонентных автоматах и о композиционном автомате, получает возможность упростить задачу его инвертирования.

Для реального использования асимметричной криптосистемы на основе конечных автоматов определено количество пар криптографических ключей, которые генерируются на основе конечных автоматов. Доказана достаточность количества конечных автоматов с памятью для построения на их основе однозначнообратимой асимметричной криптосистемы.

Четвертая глава посвящена программной реализации предложенных алгоритмов асимметричной криптосистемы FAPKC на основе конечных автоматов.

Разработано программное средство FAPKC_adv, предназначенное для автономного использования криптографической защиты информации. Система криптографической защиты информации FAPKC_adv состоит из независимых трех функциональных модулей с возможностью их раздельного использования, а также включения в другие программные средства:

- Модуль генерации ключей, обеспечивающий генерацию пар открытых и секретных ключей до начала обмена информации.
- Модуль шифрования, обеспечивающий шифрование информации с использованием открытого ключа.
- Модуль дешифрования, обеспечивающий дешифрование полученной информации с использованием соответствующего секретного ключа.

Для активизации модуля генерации ключей указывается степень защищенности информации в качестве входных данных модуля. На основе входной информации генерируется пара открытого и секретного ключей, которые обеспечат заданную степень защищенности. База данных конечных автоматов является частью модуля генерации ключей, в которой записаны прежде сгенерированные конечные автоматы и их соответствующие инверсные автоматы. Разработаны тесты для выявления необходимых конечных автоматов, удовлетворяющих требуемым условиям их использования в криптографической системе, в частности, условию обладания автомата конечной памятью.

Разработанный модуль шифрования предполагает получение открытой информации и соответствующего открытого ключа public.key в качестве входных данных. Выходным результатом модуля шифрования является шифрованная информация указанной открытой информации с использованием ключа public.key. Для модуля дешифрования криптографической системы FAPKC_adv входными данными являются зашифрованная информация и соответствующий секретный ключ private.key, с использованием которого возможно дешифрование данной информации.

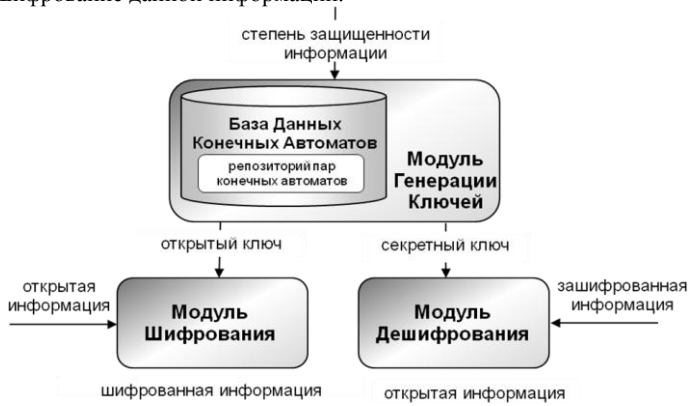

Рис. 5. Принцип работы программного средства FAPKC Crypto.

Реализовано программное средство FAPKC Crypto, которое, основываясь на модулях системы FAPKC_adv, использует модель шифрования/дешифрования информации с применением конечных автоматов. Программный пакет FAPKC Crypto предоставляет пользователю возможность генерировать криптографические ключи, шифровать и дешифровать информацию.

В учебно-исследовательских целях была создана программная среда, поддерживающая исследования свойств и особенностей функционирования различных асимметричных криптосистем и анализа их сравнительных характеристик. Для практической оценки асимметричных криптосистем в учебно-исследовательскую систему PK Crypto Tool включены программные реализации асимметричных криптосистем RSA, FAPKC3 и FAPKC_adv. Программный пакет PK Crypto Tool реализован на основе модульного подхода с учетом ресурсного расширения и имеет возможность аккумуляции новых криптосистем. Созданы программные средства на основе алгоритмов FAPKC3, так как отсутствуют программные средства ее реализации и, следовательно, соответствующие открытые исходные коды.

В рамках экспериментального исследования использовалось программное средство PK Crypto Tool. Для сравнения результатов перечисленных криптосистем приведены в соответствие их ключи, так как данные асимметричные криптосистемы основаны на разных теориях, в частности теории чисел и теории автоматов. Получена функциональная зависимость времени вычисления значения ключа, интерполированного на работу одного процессора AMD Opteron 2.2ГГц с 2Гб памяти, от длины ключа для асимметричных криптосистем RSA и FAPKC. Также выявлена обратная функциональная зависимость, позволяющая выявить длину ключей данных криптосистем, обеспечивающих одинаковую степень стойкости. Например, вычислено, что ключ криптосистемы FAPKC длиной 2^{25} бит требует 2^{80} процессорного времени, которое обеспечивается ключом длиной 2048 бит криптосистемы RSA.

На рис. 6 приведена оценка времени, требуемого для генерации ключей разной длины с одинаковой степенью стойкости для рассматриваемых асимметричных криптосистем. Из полученных характеристик видно, что время генерации ключей криптосистемы RSA, экспоненциально увеличивается. При этом заметим, что время генерации 2048-битного RSA ключа превышает время генерации FAPKC_adv ключа, обеспечивающего ту же степень стойкости, приблизительно в 16 раз.

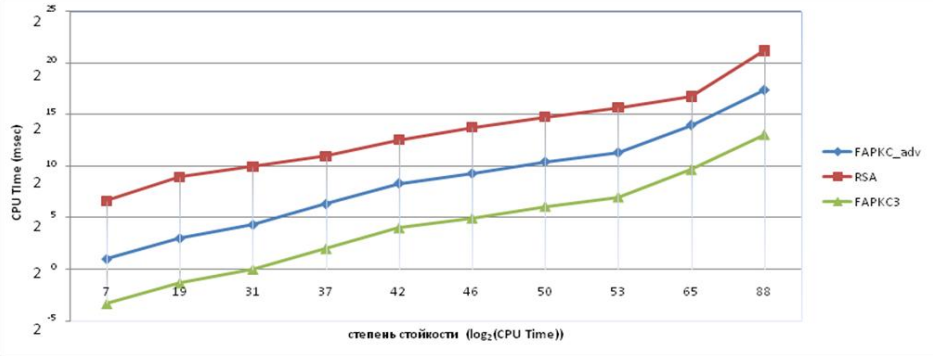

Рис. 6. Сравнение процессорного времени генерации ключей

Для оценки времени шифрования и дешифрования асимметричных криптосистем FAPKC_adv, FAPKC3, RSA с помощью программного средства PK CrypTool рассмотрены данные разного объема. На рис. 7 приведены характеристики процессорного времени,

которое необходимо для шифрования и дешифрования данных в зависимости от увеличения их объема. Получены графики, показывающие, что процессорное время как шифрования, так и дешифрования информации объемом до 200Кб криптосистем FAPKC_adv, FAPKC3, RSA сопоставимо. Однако с увеличением объема информации время для ее шифрования в криптоситеме RSA резко увеличивается, и, например, время для шифрования информации объемом 50Мб превышает время шифрования в криптоситеме FAPKC_adv в 2^8 раз.

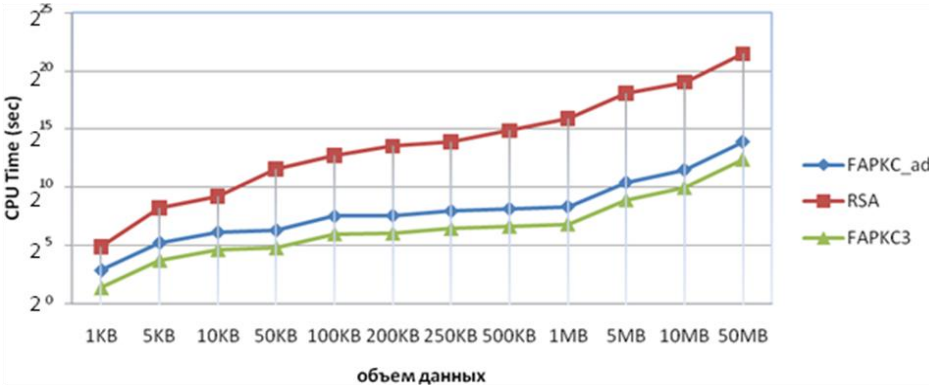

Рис. 7. Сравнение процессорного времени шифрования информации

Также заметим, что с увеличением объема шифрируемой информации увеличивается время, необходимое для шифрования в криптосистеме FAPKC_adv по сравнению с криптосистемой FAPKC3. Это означает, что модификации, направленные на повышение стойкости асимметричных криптосистем, основанных на конечных автоматах, привели к понижению быстродействия шифрования/дешифрования. Например, время шифрования информации объемом 50Мб снизилось на 60%.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

- Проведен криптоанализ существующей асимметричной криптосистемы на основе конечных автоматов и определены ее недостатки по отношению к типичным видам атак, в частности, к атакам на основе только шифротекста и на основе выбранного открытого текста.
- Определены инвертируемые нелинейные автоматы и предложена возможная модификация линейных и нелинейных автоматов, повышающая стойкость асимметричной криптосистемы по отношению к типичным видам атак.
- Доказано существование односторонней функции с секретом на основе конечных автоматов, позволяющей создать асимметричную криптосистему с применением конечных автоматов.
- Предложен подход к проектированию криптографического алгоритма с применением нелинейных конечных автоматов, который, в отличие от существующих алгоритмов, позволяет повысить стойкость проектируемой асимметричной криптосистемы на основе конечных автоматов.
- Разработана стойкая асимметричная криптосистема на основе конечных автоматов, которая по сравнению с существующими асимметричными криптосистемами на основе теории чисел обеспечивает повышение быстродействия процессов шифрования/дешифрования 10 раз уже при объеме шифруемой информации 10Кб и почти в 2^8 раз при объеме 50Мб.
- Разработаны метод и соответствующий программный модуль генерации пар криптографических ключей асимметричной криптосистемы на основе конечных автоматов, которые положены в основу созданных программных средств реализации асимметричной криптосистемы.
- Спроектировано программное средство криптографической защиты информации FAPKC Crypto, обеспечивающее обмен защищенной информацией по модели шифрования/дешифрования с применением конечных автоматов.
- Разработана учебно-исследовательская система PK CrypTool, поддерживающая эффективные исследования и сравнительный анализ с использованием различных асимметричных криптосистем.

ПЕРЕЧЕНЬ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

[1] 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), September 2007, pp. 112-115.

[2] 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, Ереван, 2008, стр. 306-310.

[3] С. Х. Согомонян, С. Г. Чопурян, "Односторонняя функция с секретом на базе конечных автоматов", Доклады международной научно-практической конференции по вопросам безопасности информационных систем, Ер.: Арм. "АТА".,2008, стр. 45-49.

[4] С. Г. Чопурян, "Криптоанализ асимметричных криптосистем на базе конечных автоматов", Сборник трудов шесрой международной конференции "Исследование, разработка и применение высоких технологий в промышленности", Санкт-Петербург, 2008, стр. 108-109.

[5] С. Г. Чопурян, “Метод генерации криптографических ключей в асимметричных криптосистемах на основе конечных автоматов”, XXXV ГАГАРИНСКИЕ ЧТЕНИЯ. Научные труды Международной молодежной научной конференции в 8 томах. Москва, 7-10 апреля 2009 г.-М.: МАТИ, 2009. Т.4.- стр. 171-172.

[6] С. Чопурян, “Метод генерации простых конечных автоматов”, Вестник-76 Государственного инженерного университета Армении (Политехник), Сборник научных и методических статей, Часть 1, Ереван, 2009, стр. 449-453.

[7] Chopuryan S., “The stability of trapdoor one-way function based on finite automata”, In Proc. of the 2009 Int’ Conf. on Security & Management (WORLDCOMP’09), vol.1, CSREA Press, Las Vegas, Nevada, USA, July 2009, pp. 157-161.

[8] Margarov G., Chopuryan S., Alaverdyan Y., “Cryptanalysis of finite automata public key cryptosystems”, In Proc. of the 2009 Int’ Conf. on Security & Management (WORLDCOMP’09), vol.2, CSREA Press, Las Vegas, Nevada, USA, July 2009, pp. 429-433.

[9] Margarov G., Chopuryan S., “Strong finite automata public key cryptosystem”, In Proc. of the Second International Conference on the Applications of Digital Information and Web Technologies (ICADIWT’09), London, United Kingdom August 2009, pp. 625-628.

[10] С. Г. Чопурян, “Построение стойкой асимметричной криптосистемы на основе конечных автоматов”, In Proc. of the Int’ Conf. on Computer Science and Information Technologies (CSIT’09), Armenia, Yerevan, September 2009, pp. 73-76.

[11] С. Г. Чопурян, “Разработка принципов функционирования асимметричной криптосистемы на основе конечных автоматов”, Вестник Государственного инженерного университета Армении (Политехник), Сборник научных и методических статей, Часть 2, Ереван, 2010, стр. 245-249.

[12] Chopuryan S., “Constructiv analysis of cryptanalytic attacks on FAPKC”, Applications of Information Theory, Coding and Security Workshop (WAITS2010), Yerevan, Armenia, April 14-16, 2010, pp. 43-46.

[13] Margarov G. and Chopuryan S., “Public key cryptosystem based on finite automata for multilateral antiterrorist activity support”, NATO Science for Peace and Security Series E: Human and Societal Dynamics–Vol.67, IOS Press, Amsterdam.Berlin.Tokyo.Washington.DCJune 2010, pp. 183-188.

[14] Margarov G. and Chopuryan S., “Modification of Finite Automata Public Key Cryptosystem”, Journal of Information Security Research, Vol. 1 N2, Digital Information Research Foundation, June 2010, pp. 39-54.

Չոփուրյան Սիրանուշ Հրայրի

ՎԵՐՋԱՎՈՐ ԱՎՏՈՄԱՏՆԵՐԻ ՎՐԱ ՀԻՄՆՎԱԾ ԱՆՀԱՄԱՉԱՓ ԳԱՂՏՆԱԳՐԱՅԻՆ ՀԱՄԱԿԱՐԳԻ ԳԱՂՏՆԱԿԱՅՈՒՆՈՒԹՅԱՆ ԲԱՐՁՐԱՑՄԱՆ ՄԻՋՈՑՆԵՐԻ ՀԵՏԱԶՈՏՈՒՄ ԵՎ ՄՇԱԿՈՒՄ

ԱՄՓՈՓԱԳԻՐ

Վերջին տարիների ընթացքում ինֆորմացիոն հասարակության զարգացումը խթանեց ինֆորմացիայի պաշտպանության անհրաժեշտության աճին: Վերոհիշյանլ նպատակին ծառայող եղանակներից են հանդիսանում պաշտպանության գաղտնագրման միջոցները, որոնք իրականացնում են ինֆորմացիայի պաշտպանությունը բանալիների միջոցով նրա գաղտնագրմամբ և վերծանմամբ: Պաշտպանության գաղտնագրման միջոցների կատարելագործումը հանգեցրեց անհամաչափ գաղտնագրային համակարգերի ստեղծմանը, ուղղված ինֆորմացիա փոխանակող կողմերի միմյանց վստահելու և բանալիների բաշխման խնդրի լուծմանը, որի հիմքում ընկած է ինֆորմացիա փոխանակող կողմերից յուրաքանչյուրին իր սեփական բանալին տրամադրելը: Սակայն մինչ այժմ գոյություն ունեցող անհամաչափ գաղտնագրային համակագերը ունեն ցածր արագագործություն և իրականացնում են ինֆորմացիայի գաղտնագրումն ու վերծանումը շատ ավելի դանդաղ քան համաչափ գաղտնագրային համակարգերը: Այս հանգամանքը պայմանավորված է գաղտնագրման և վերծանման ժամանակ բարդ թվաբանական գործողությունների օգտագործմամբ, որոնք պահանջում են ժամանակային և հաշվողական մեծ ռեսուրսներ: Դրանով է պայմանավորված այն հանգամանքը, որ գոյություն ունեցող անհամաչափ գաղտնագրային համակարգերը չեն գտել արդյունավետ կիրառություն մեծ ծավալի ինֆորմացիայի գաղտնագրման և վերծանման համար, և հիմնականում օգտագործվում են բանալիների բաշխման և թվային ստորագրության համար:

Վերջին տարիներին կատարվել են հետազոտություններ արագագործ անհամաչափ գաղտնագրային համակարգեր ստեղծելու ուղղությամբ՝ կիրառելով մաթեմատիկայի այլ ճյուղեր, մասնավորապես՝ ավտոմատների տեսություն: Վերջավոր ավտոմատների վրա հիմնված արագագործ անհամաչափ գաղտնագրային համակարգերի նախագծումը պայմանավորված է ավտոմատների հիմքում ընկած տրամաբանական գործողություններով: Ներկայումս գոյություն ունեցող վերջավոր ավտոմատների վրա հիմնված անհամաչափ գաղտնագրային համակարգերը, օժտված լինելով բարձր արագագործությամբ, միևնույն ժամանակ չեն ապահովում բավականաչափ գաղտնակայունություն: Բացի այդ, բացակայում են վերջավոր ավտոմատների վրա հիմնված անհամաչափ գաղտնագրային համակարգերի իրականացման հստակ ալգորիթմներ, և, հետևաբար, համապատասխան ծրագրային միջոցներ:

<u>Հետազոտության հիմնական նպատակը</u>

Հետազոտել և մշակել վերջավոր ավտոմատների վրա հիմնված արագագործ և գաղտնակայուն անհամաչափ գաղտնագրային համակարգերի կառուցման սկզբունքներ:

Նշված նպատակին հասնելու համար աշխատանքում լուծվել են հետևյալ խնդիրները՝

1) Հետազոտվել են գոյություն ունեցող անհամաչափ գաղտնագրային համակարգերը և որոշվել գաղտնագրման և վերծանման արագագործությունների բարձրացման մեթոդներ:
2) Կատարվել է վերջավոր ավտոմատների վրա հիմնված գոյություն ունեցող անհամաչափ գաղտնագրային համակարգերի գաղտնավերլուծություն և, հիմնվելով ստացված արդյունքների վրա, մշակվել են տվյալ գաղտնագրային համակարգերի գաղտնակայունության բարձրացման մեթոդներ, որոնք թույլ են տալիս դիմակայել հիմնական տիպի գրոհներին:
3) Ստեղծվել են ալգորիթմներ և նախագծվել ծրագրային միջոցներ՝ իրագործող ստեղծված անհամաչափ գաղտնագրային համակարգերը:

<u>Աշխատանքի հիմնական արդյունքները հետևյալն են՝</u>

- Իրականացված է վերջավոր ավտոմատների հիման վրա կառուցված գոյություն ունեցող անհամաչափ գաղտնագրային համակարգի գաղտնավերլուծություն և որոշված են վերջինիս թերությունները տիպային գրոհների նկատմամբ, մասնավորապես, միայն գաղտնագրված տեքստի գրոհի նկատմամբ և ընտրված բաց տեքստի գրոհի նկատմամբ:
- Սահմանված են հակադարձելի ոչ գծային ավտոմատները, և, տիպային գրոհների նկատմամբ անհամաչափ գաղտնագրային համակարգի գաղտնակայունության բարձացման նպատակով, առաջարկված են գծային և ոչ գծային ավտոմատների հնարավոր ձևափոխությունները:
- Ապացուցված է վերջավոր ավտոմատների հիման վրա կառուցված գաղտնիքով միակողմանի ֆունկցիայի գոյությունը, որը հնարավորություն է տալիս վերջավոր ավտոմատների կիրառմամբ ստեղծել անհամաչափ գաղտնագրային համակարգ:
- Առաջարկված է ոչ գծային վերջավոր ավտոմատների կիրառմամբ գաղտնագրային ալգորիթմ նախագծելու սկզբունք, որը, ի տարբերություն գոյություն ունեցող ալգորիթմների, թույլ է տալիս բարձրացնել վերջավոր ավտոմատների հիման վրա նախագծվող անհամաչափ գաղտնագրային համակարգի գաղտնակայունությունը:
- Մշակված է վերջավոր ավտոմատների վրա հիմնված գաղտնակայուն անհամաչափ գաղտնագրային համակարգ, որն, ի տարբերություն թվերի տեսության վրա հիմնված գոյություն ունեցող անհամաչափ գաղտնագրային համակարգերի, ապահովում է գաղտնագրման/վերծանման գործընթացների արագագործության աճ մոտավորապես 2^8 անգամ:
- Մշակված է վերջավոր ավտոմատների վրա հիմնված անհամաչափ գաղտնագրային համակարգի բանալիների զույգ գեներացնելու մեթոդ և համապատասխան ծրագրային մոդուլ:
- Նախագծված է ինֆորմացիայի գաղտնագրային պաշտպանության FAPKC Crypto ծրագրային միջոցը, որն ապահովում է ինֆորմացիայի պաշտպանված փոխանակում ըստ վերջավոր ավտոմատների կիրառմամբ գաղտնագրման/վերծանման մոդելի:
- Մշակված է PK CrypTool ուսումնահետազոտական համակարգը, որը հնարավորություն է տալիս օգտագործել տարբեր անհամաչափ գաղտնագրային համակարգեր, վերջիններիս հետազոտության և համեմատական վերլուծության նպատակներով:

Siranush Chopuryan

RESEARCH AND DEVELOPMENT OF PRINCIPLES FOR INCREASING THE PERFORMANCE AND SECRECY OF FINITE AUTOMATA PUBLIC KEY CRYPTOSYSTEM

RESUME

The necessity to protect information has increased in recent years due to information society progress. One main way for secure communications is the usage of cryptography. The existing public key cryptosystems possess high level of secrecy, but at the same time not quite all are suitable for practical realization due to the usage of too long keys or sizeable differences between plaintext and ciphertext. Only few public key cryptosystems are practical for realization and secure against attack. Some of them suit only for key exchange, others suit for encryption or usable only for digital signature. The most widespread public key cryptosystems are RSA, ElGamal encryption system and Rabin. Those are eligible for encryption as well as for digital signature, but they still do not find their effective usage for encryption/decryption of large amount of data. It is conditioned by the use of algorithms that are based on complex arithmetic operations within cryptosystems, such as multiplication and exponentiation of large numbers. These kinds of operations require considerable expenditure of time and computational resources.

The creation of high-performance public key cryptosystems is an actual problem now days. There is a widespread interest in cryptosystems based on problems of the other areas of mathematics, in particular, the theory of automata. The approach of application of finite automata for construction of public key algorithms is motivated by the use of logic operations in automata which are the fastest. This allows to create public key algorithms with high level of performance. Existing finite automata public key cryptosystems possess high level of performance. At the same time they don't possess sufficient level of secrecy. In addition there are no specific algorithms for implementing finite automata public key cryptosystems, and hence there are no corresponding software tools. From the foregoing follows the importance of finite automata public key cryptosystem creation with high level of performance and security.

The purpose and objectives

The main purpose and objectives of the work is the research and development of principles for increasing the performance and secrecy of finite automata public key cryptosystems. To achieve this goal it is necessary to solve the following tasks:

1) Analyze the existing public key cryptosystems and identify methods to improve the performance of the encryption and decryption processes

2) Perform a cryptanalysis of the existing finite automata public key cryptosystems, and then based on the results develop methods that increase the resistance of cryptosystems to withstand the typical types of attacks
3) Construct new algorithms and corresponding software tools that implement the finite automata public key cryptosystem based on develo

The main results are:

- The cryptanalysis of the existing finite automata public key cryptosystems is performed and its imperfections against typical types of attacks are identified, particularly its imperfection against ciphertext-only and chosen plaintext attacks
- Invertible nonlinear automata are determined and possible modification of the linear and nonlinear automata are proposed, which increases the resistance of a finite automata public key cryptosystem against typical types of attacks
- The existence of trapdoor one-way function based on finite automata is proved, which allows to create finite automata public key cryptosystem
- An approach to design a cryptographic algorithm with the usage of nonlinear finite automata is suggested. Unlike the existing algorithms it allows to improve secrecy of designed finite automata public key cryptosystem
- The finite automata public key cryptosystem with high level of secrecy is designed, which in comparison with the existing public key cryptosystems based on number theory has an advantage already for 50MB data encryption in almost 2^8 times.
- The methods and corresponding software modules are developed intended for cryptographic key pair generation in finite automata public key cryptosystem
- The cryptosystem FAPKC Crypto is designed that provides a secure exchange of information by the encryption/decryption model with the usage of finite automata
- The software tool PK CrypTool is developed for trainings and research works that supports effective research and comparative analysis for various public key cryptosystems