На правах рукописи

Дулькейт Владимир Игоревич

КНФ ПРЕДСТАВЛЕНИЯ ДЛЯ ЗАДАЧ ФАКТОРИЗАЦИИ, ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ И ЛОГАРИФМИРОВАНИЯ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

01.01.09 – Дискретная математика и математическая кибернетика

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Екатеринбург, 2010

Работа выполнена в Институте математики и информационных технологий Омского государственного университета им. Ф.М. Достоевского

Научный руководитель:	доктор технических наук, профессор Файзуллин Рашит Тагирович
Официальные оппоненты:	доктор физико-математических наук, доцент Хачай Михаил Юрьевич
	кандидат физико-математических наук Рыбалов Александр Николаевич
Ведущая организация:	Институт систем обработки изображений (ИСОИ) РАН, г. Самара

Защита состоится 14 апреля 2010 года в 14 часов на заседании диссертационного совета Д 004.006.04 по защите докторских и кандидатских диссертаций при Институте математики и механики УрО РАН по адресу: 620219, г. Екатеринбург, ул. С. Ковалевской, 16.

С диссертацией можно ознакомиться в библиотеке Института математики и механики УрО РАН.

Автореферат разослан 12 марта 2010 года.

Ученый секретарь диссертационного совета,
кандидат физико-математических наук, ст.н.с. В.Д. Скарин

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В современной информатике огромную роль играют надежные и гарантированно стойкие алгоритмы шифрования, обеспечивающие безопасность каналов связи в телекоммуникационных, финансовых и многих других информационных системах. Это обуславливает большое практическое значение такой области науки, как криптографический анализ. Прогресс в области криптографического анализа, в свою очередь, сопровождается бурным развитием смежных областей математики: алгебры, теории чисел, дискретной математики.

Одним из основных направлений криптографического анализа является проверка криптографической стойкости алгоритмов асимметричного шифрования, поскольку на базе этих алгоритмов работает подавляющее большинство криптографических протоколов обмена ключами, цифровой подписи и других. В настоящее время для проверки криптографической стойкости асимметричных шифров применяются в основном методы решета в поле чисел общего вида[1] и различные модификации ρ- и λ-методов Полларда, базирующиеся на псевдослучайном блуждании по группе[2],[3]. Последние достижения в этой области свидетельствуют о стойкости известных алгоритмов, поскольку для решения задач «рабочих» размерностей (т.е. регламентированных требованиями безопасности) требуется на несколько месяцев задействовать вычислительные системы, относящиеся к верхним позициям списка «Top-500». Таким образом, увеличение длины ключа в полтора или два раза принципиально решает вопрос криптографической стойкости шифров.

Однако, относительно недавно возникло и получило развитие совершено новое, альтернативное алгебраическому подходу, направление криптоанализа – логический криптоанализ. Суть подхода заключается в рассмотрении криптографического алгоритма как программы для машины Тьюринга. Подстановка открытого и шифрованного текстов в эту программу естественным образом приводит к задаче «ВЫПОЛНИМОСТЬ» для конъюнктивной нормальной формы, часть выполняющего набора которой является ключом шифра. Идея такого подхода была впервые предложена Куком С. в 1997 году при поиске сложных задач для тестирования решателей КНФ[4].

В последующих работах по логическому криптоанализу (Massacci F.,

[1]Lenstra A. K., Lenstra H. W. The development of the number field sieve // Lect. Notes in Math. – 1993. – Vol. 1554.

[2]Pollard J. M. Monte-carlo method for factorization // BIT. – 1974. – Vol. 15.

[3]Pollard J. M. Monte carlo methods for index computation (mod p) // Math. Comp. – 1978. – Vol. 32.

[4]Cook S. A., Mitchel D. G. Finding hard instances for the satisfiability problem // A survey. DIMACS series in discrete mathematics and theoretical computer science. – 1997. – Vol. 5. – P. 151.

Marraro L.[5], Srebrny M.[6], Семенова А.А., Беспалова Д.В.[7] и др.) основное внимание исследователей было сосредоточено на криптоанализе блочных и потоковых шифров, генераторов двоичных последовательностей, а так же некоторых аспектах криптоанализа RSA (криптостойкость основана на сложности задачи факторизации). При этом за границами исследований остались такие важные задачи как дискретное логарифмирование и логарифмирование в группе точек эллиптической кривой, на основе которых строятся современные системы шифрования, протоколы обмена ключами и цифровой подписи (DSA, ECDSA и другие). В вопросе применения логического криптоанализа для задачи факторизации недостаточно полно освещены такие аспекты, как использование параллельных алгоритмов для поиска выполняющего набора КНФ, кодирующей исходную задачу, и адаптация алгоритмов кодирования под требования современных алгоритмов поиска выполняющего набора КНФ.

Таким образом, актуальность данной диссертационной работы определяется необходимостью разработки подхода для сведения задач дискретного логарифмирования и логарифмирования в группе точек эллиптической кривой к задаче «ВЫПОЛНИМОСТЬ», что предоставит возможность качественного анализа стойкости этих задач против методов логического криптоанализа.

Сведение к задаче «ВЫПОЛНИМОСТЬ» позволяет не только применять для решения изначально алгебраических задач алгоритмы решения задачи «ВЫПОЛНИМОСТЬ», но и получать качественно новые результаты, недоступные для алгебраических методов. Так, например, выделять наиболее вероятные биты ключа, распознавать определенные последовательности бит и полностью восстанавливать ключ по некоторым известным его фрагментам.

Целью работы является построение и исследование свойств алгоритмов консервативного сведения задач факторизации, дискретного логарифмирования и логарифмирования на эллиптических кривых к задаче «ВЫПОЛНИМОСТЬ»; анализ работы современных алгоритмов решения задачи «ВЫПОЛНИМОСТЬ» (SAT-решателей) на полученных КНФ; разработка алгоритма построения КНФ, пригодных для решателей, использующих параллельную модель вычислений; адаптация алгоритмов кодирования в соответствии с требованиями современных алгоритмов поиска выполняющего набора КНФ (построение 3-КНФ, проекции вещественного вектора приближений на пространство булевых переменных, построение КНФ с учетом нало-

[5]Massacci F., Marraro L. Towards the formal verification of ciphers: Logical cryptanalysis of des // Proc. Third LICS Workshop on Formal Methods and Security Protocols, Federated Logic Conferences. – 1999.

[6]Srebrny M. Factorization with sat – classical propositional calculus as a programming environment // Faculty of Mathematics Informatics and Mechanics at the University of Warsaw. 2004. URL: http://www.mimuw.edu.pl/mati/fsat-20040420.pdf (дата обращения: 06.07.2009).

[7]Беспалов Д. В., Семенов А. А. О логических выражениях для задачи 2-ФАКТОРИЗАЦИЯ // Вычислительные технологии. – 2002. – Т.7.

жения дополнительных условий – требований SAT-решателей); исследование стойкости рассматриваемых задач к восстановлению полного ключа по его известным фрагментам.

Научная новизна работы заключается в том, что в ней впервые получены приведенные ниже результаты.

1. Предложены алгоритмы полиномиального консервативного сведения задач дискретного логарифмирования и логарифмирования на эллиптической кривой к задаче «ВЫПОЛНИМОСТЬ».
2. Предложены алгоритмы полиномиального консервативного сведения задачи факторизации к задаче «3-ВЫПОЛНИМОСТЬ» и к набору различных экземпляров задачи «ВЫПОЛНИМОСТЬ».
3. Разработана система тестов для выделения наиболее вероятных значений битов сомножителей в задаче факторизации.
4. С помощью ассоциированных КНФ исследована стойкость рассматриваемых задач к восстановлению полного ключа по его известным фрагментам.

Теоретическая и практическая ценность. Диссертационная работа имеет теоретическую и практическую значимость. В работе построены и обоснованы новые алгоритмы сведения задач асимметричной криптографии к задаче «ВЫПОЛНИМОСТЬ». Практическая значимость работы обусловлена тем, что предложенные в ней алгоритмы могут быть использованы как при решении задач факторизации, дискретного логарифмирования и логарифмирования на эллиптической кривой, так и для построения тестовых примеров задачи «ВЫПОЛНИМОСТЬ».

Апробация результатов работы. Основные результаты диссертационной работы докладывались на международной научной конференции «Параллельные Вычислительные Технологии» (ПаВТ'2007) (Челябинск, 29 января – 2 февраля 2007 г.); 38-ой Региональной молодежной конференции «Проблемы теоретической и прикладной математики» (Екатеринбург, 29 января – 2 февраля 2007 г.); 13-ой Всероссийской конференции «Математические методы распознавания образов» (Санкт-Петербург, 31 сентября – 4 октября 2007 г.); 39-ой Региональной молодежной конференции «Проблемы теоретической и прикладной математики» (Екатеринбург, 28 января – 1 февраля 2008 г.); международной научной конференции «Параллельные Вычислительные Технологии» (ПаВТ'2009) (Нижний Новгород, 30 марта – 3 апреля 2009 г.); научном семинаре кафедры математической логики и логического программирования Омского государственного университета им. Ф.М. Достоевского; научном семинаре отдела математического программирования Института математики и механики УрО РАН.

Публикации. Основные результаты диссертации опубликованы в 15 работах (см. список в конце автореферата), из которых 3 работы – в журналах, входящих в перечень ВАК. В совместных работах научному руководителю Р.Т. Файзуллину принадлежат постановка задач и общее руководство исследованиями по теме диссертации, И.Г. Хныкину – разработка и реализация алгоритмов поиска выполняющих наборов КНФ, а диссертанту разработка и реализация алгоритмов представления задач асимметричной криптографии в виде КНФ, а также ряд усовершенствований алгоритмов поиска выполняющих наборов КНФ. В ходе выполнения научного исследования диссертантом была разработана программа для ЭВМ, зарегистрированная в Отраслевом Фонде Алгоритмов и Программ (Рег. № 9396, 2007 г.).

Структура и объем диссертации. Диссертация состоит из введения, трех глав и списка литературы. Объем диссертации составляет 131 страницу. Библиографический список содержит 72 наименования.

КРАТКОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

Во введении обосновывается актуальность темы исследований, обсуждается история вопроса, обозначено место проведенных исследований среди других подобных исследований, формулируется цель диссертационной работы и пути ее достижения, кратко описывается содержание диссертации, отмечены новизна и практическое значение работы.

В первой главе диссертации приводятся основные понятия и обзор известных результатов для задач факторизации, дискретного логарифмирования и логарифмирования на эллиптической кривой. Рассматриваются наиболее известные алгоритмы и общие схемы методов решения. Далее в отдельном параграфе рассматривается общий подход к решению некоторых задач дискретной математики, основанный на сведении к задаче «ВЫПОЛНИМОСТЬ» и связанному с ним направлению криптоанализа – «логический криптоанализ». Приводятся основные результаты, известные в рамках данного направления. В заключительной части главы формулируется ключевая идея данной работы о целесообразности применения методов логического криптоанализа для решения рассматриваемых задач.

Во второй главе приводится описание разработанных алгоритмов консервативного сведения рассматриваемых задач к задаче «ВЫПОЛНИМОСТЬ», а так же предлагается ряд улучшений для гибридного метода последовательных приближений с «инерцией» разработанного Р.Т. Файзулли-

ным и И.Г. Хныкиным[8].

Первый параграф посвящен вопросам сведения задачи факторизации к задаче «ВЫПОЛНИМОСТЬ». В начале параграфа вводится понятие о примитиве КНФ, с помощью которого формализуется процесс генерации КНФ. Основной операцией для всех построенных в работе алгоритмов генерации КНФ является операция применения примитива, включающая в себя следующую последовательность действий:

1) выбор примитива КНФ для кодирования конкретной вычислительной операции;
2) подстановка в выбранный примитив литералов, отвечающих контексту использования операции;
3) упрощение полученных дизъюнктов и вставка в итоговую КНФ.

Для алгоритмов, использующих примитив КНФ, справедлива следующая лемма:

Л е м м а 2.1.1. *Нижней оценкой для трудоемкости построения КНФ и количества полученных дизъюнктов является количество операций применения примитива КНФ.*

Для построения примитивов КНФ используются следующие равенства, полученные из свойств совершенных КНФ:

$$\bigoplus_{i=1}^{N} x_i = \bigwedge_{\{\sigma_i\}\in M_N} \left(\bigvee_{i=1}^{N} x_i^{\sigma_i} \right), \tag{1}$$

где в левой части сумма по модулю 2, M_N – множество двоичных векторов длины N, содержащих четное число нулей.

$$\bigvee_{i=1}^{N} x_i^{\delta_i} \vee \bigwedge_{i=1}^{L} y_i^{\sigma_i} = \bigwedge_{\{\pi_k\}\in 2^L/\{0,0,\ldots,0\}} \left(\bigvee_{i=1}^{N} x_i^{\delta_i} \vee \bigvee_{j=1}^{L} (y_i^{\sigma_i})^{\pi_i} \right). \tag{2}$$

Для перехода от задачи факторизации к задаче «ВЫПОЛНИМОСТЬ» основной операцией, которую необходимо закодировать в виде КНФ, является операция умножения двух чисел. Для построения соответствующих примитивов КНФ в работе представлен алгоритм перехода от суммы по модулю два к КНФ. Данный алгоритм базируется на равенствах (1) и (2), а так же правиле де Моргана. С помощью этого же алгоритма осуществляется кодирование в виде КНФ операции переноса в старший разряд, которая представляется как сумма по модулю 2 в следующем виде:

$$c = \overline{s \oplus x \wedge y \wedge z \oplus \bar{x} \wedge \bar{y} \wedge \bar{z}}, \tag{3}$$

[8]Дулькейт В. И., Файзуллин Р. Т., Хныкин И. Г. Непрерывные аппроксимации решения задачи ВЫПОЛНИМОСТЬ применительно к криптографическому анализу асимметричных шифров // Компьютерная оптика. – 2009. – Т.33. – № 1. – С. 86–91.

где s – литерал равный сумме $x \oplus y \oplus z$, а c – бит переноса от этой суммы.

В работе предложено три различных алгоритма кодирования операции умножения чисел в виде КНФ:

1) **алгоритм на основе схемы умножения «столбиком»**;
2) **алгоритм, использующий датчик псевдослучайных чисел для генерации нескольких КНФ, представляющих одну задачу факторизации**;
3) **алгоритм генерации 3-КНФ**.

Первый алгоритм фактически является записью обычного алгоритма умножения «столбиком», в котором на каждом шаге вместо вычисления промежуточной суммы или переноса происходит генерация соответствующего фрагмента КНФ.

Второй алгоритм строит несколько КНФ, представляющих одну задачу факторизации, что позволяет использовать параллельные схемы решателей задачи «ВЫПОЛНИМОСТЬ»[9]. В таких схемах параллельно работает несколько независимых решателей, каждый из которых ищет выполняющий набор своей индивидуальной КНФ. По окончании каждой итерации происходит циклический обмен решениями между решателями и начинается следующая итерация, в которой полученные решения являются начальными приближениями.

Генерация КНФ происходит в два этапа:

1) Попарное сложение промежуточных векторов, составленных из произведений битов сомножителей:

$$\sum_{j=1}^{N+1} 2^{j-1} u_{i\,j} = y_i \sum_{j=1}^{N} 2^{j-1} x_j + 2y_{i+1} \sum_{j=1}^{N} 2^{j-1} x_j, \tag{4}$$

   где x_i, y_i – биты первого и второго сомножителя соответственно,
   $\overline{u_i}$ – вектор, содержащий промежуточную сумму.
2) Сложение двух произвольно выбранных векторов $\overline{u_i}, \overline{u_k}$.

Представление операции умножения в виде 3-КНФ также базируется на алгоритме умножения «столбиком», при этом для кодирования сложения в одном разряде используется следующая система уравнений, каждое уравнение которой представляется в виде фрагмента 3-КНФ:

$$\begin{aligned} s_1 &= x \oplus c, & c_1 &= x \wedge c, \\ s &= s_1 \oplus y, & c_2 &= s_1 \wedge y, \\ c' &= c_1 \oplus c_2. \end{aligned}$$

[9]Салаев Е. В., Файзуллин Р. Т. Применение метода последовательных приближений с инерцией к решению задачи Выполнимость // Вестник Томского Государственного Университета. – 2006. – Т.17.

Достоинством представленных схем кодирования является отсутствие дополнительных, не имеющих смысла с точки зрения исходной задачи, литералов в построенных КНФ.

Консервативность сведения задачи факторизации к задаче «ВЫПОЛНИМОСТЬ» обеспечивается путем включения в итоговую КНФ фрагментов, фиксирующих порядок сомножителей (условие $q \geq p$) и устраняющих тривиальные решения ($1 \times n$).

Все рассмотренные алгоритмы являются консервативным сведением задачи факторизации к задаче «ВЫПОЛНИМОСТЬ» и обладают следующими свойствами (см. ниже теоремы 2.1.2, 2.1.3, 2.1.4):

1) трудоемкость есть $O(N^2)$;
2) количество литералов в КНФ есть $O(N^2)$;
3) количество дизъюнктов в КНФ есть $O(N^2)$;
4) количество различных КНФ представлений одной задачи факторизации, которые могут быть построены алгоритмом генерации нескольких КНФ, представляющих одну задачу факторизации, есть $\left(\frac{N}{2}\right)!\left(\frac{N}{2}-1\right)!$.

Во втором параграфе строится алгоритм консервативного сведения задачи дискретного логарифмирования к задаче «ВЫПОЛНИМОСТЬ». Исходная задача формулируется следующим образом:

$$A^X \equiv B \pmod{P}, \tag{5}$$

где P – большое простое число; A – такое, что $(A, P) = 1$.

Требуется найти число X, удовлетворяющее сравнению (5).

Представим левую часть сравнения (5) в следующем виде:

$$A^X \pmod{P} = \left(\cdots \left((A_1^{x_1} \times A_2^{x_2}) \times A_3^{x_3} \right) \cdots \right) \times A_N^{x_N}, \tag{6}$$

где $A_i \stackrel{\text{def}}{\equiv} A^{2^{i-1}} \pmod{P}$, а операция $\times$ – умножение в поле $GF(P)$:

$$U \times V \stackrel{\text{def}}{\equiv} UV \pmod{P}$$

При кодировании выражения (6) в виде КНФ определяются численные значения A_i и соответствующие биты подставляются в КНФ. Следовательно, требуется закодировать $N-1$ (N – разрядность числа P) операций умножения в поле $GF(P)$.

Итак, требуется реализовать кодирование следующих операций:

1) возведения числа в степень, показатель которой может принимать только значения 0 или 1 (возведением в «однобитовую» степень);
2) умножения в поле $GF(P)$:

$$UV \equiv R \pmod{P}. \tag{7}$$

Для кодирования первой операции предлагается следующий алгоритм, принимающий на вход число A, содержащее N двоичных разрядов, литерал b, отвечающий показателю экспоненты, и вектор c_i $(i = 1, \ldots, N)$ литералов, соответствующих битам результата.

1. Если младший бит A равен 0, то добавить в КНФ два дизъюнкта:
$$(\overline{c_1} \vee b) \wedge \left(c_1 \vee \overline{b}\right),$$
иначе добавить в КНФ дизъюнкт (c_1).
2. Для $i = 2, \ldots, N$. Если i-ый бит A (биты нумеруются с единицы, начиная с младшего) равен 1, то положить $c_i = b$, иначе добавить в КНФ дизъюнкт $(\overline{c_i})$.

Умножение в поле $GF(P)$ представляется в виде следующей системы:
$$\begin{cases} UV = QP + R \\ P > R, \end{cases} \tag{8}$$
где U и V – сомножители, P – модуль поля $GF(P)$, R – результат умножения, Q – целая часть от деления UV/P. Без ограничения общности используется нестрогое неравенство, т.к. с одной стороны его проще закодировать в виде КНФ, с другой – в рассматриваемой задаче $UV \neq 0 \pmod{P}$.

Перепишем систему (8) так, чтобы в каждом уравнении содержалось не более одной бинарной операции:
$$\begin{aligned} UV &= T, & QP &= Y, \\ T &= Y + R, & P &\geq R, \end{aligned} \tag{9}$$
где T и Y – дополнительные переменные связи между уравнениями.

Кодирование операции умножения в поле $GF(P)$ осуществляется на основе системы (9) с использованием генераторов КНФ для операций умножения, сложения и отношения «больше или равно».

Сведение задачи дискретного логарифмирования к задаче «ВЫПОЛНИМОСТЬ» осуществляется следующим алгоритмом, принимающим на вход 3 числа A, B и P, имеющих N двоичных разрядов и связанных соотношением (5), и вектор литералов x_i $(i = 1, \ldots, N)$, отвечающий искомой экспоненте.

1. Вычислить $A_i \equiv A^{2^{i-1}} \pmod{P}$, при $i = 1, \ldots, N$.
2. При $i = 1, \ldots, N-1$ и $S_1 = A_1^{x_1}$ генерировать КНФ представления для выражений вида:
$$S_{i+1} \equiv S_i \times A_i^{x_i} \pmod{P}.$$
3. В полученную КНФ подставить биты P, а также биты B в качестве значений S_N.

Т е о р е м а 2.2.1. *Приведенный выше алгоритм является консервативным сведением задачи дискретного логарифмирования в простом поле по модулю, содержащему N двоичных разрядов, к задаче «ВЫПОЛНИМОСТЬ» и обладает следующими свойствами:*

1) время работы алгоритма есть $O\left(N^3\right)$;

2) количество литералов в построенной КНФ есть $O\left(N^3\right)$;

3) количество скобок в построенной КНФ есть $O\left(N^3\right)$.

В третьем параграфе главы приводится алгоритм сведения задачи логарифмирования на эллиптической кривой к задаче «ВЫПОЛНИМОСТЬ». Исходная задача формулируется следующим образом: дано две точки $\mathcal{R}$, $\mathcal{Q}$ некоторой эллиптической кривой $E(A, B, P)$. Необходимо найти число K такое, что при умножении на него точки $\mathcal{Q}$ получим заданную точку $\mathcal{R}$.

$$\mathcal{R} = K\mathcal{Q}, \quad \mathcal{R}, \mathcal{Q} \in E(A, B, P)$$

В теории эллиптических групп применяются следующие правила вычисления суммы двух точек[10]:

1. $(X, Y) + \mathcal{O} = (X, Y)$,
2. $(X, Y) + (X, -Y) = \mathcal{O}$,
3. $(X_1, Y_1) + (X_2, Y_2) = (X_3, Y_3)$,

где

$$X_3 \equiv \lambda^2 - X_1 - X_2 \pmod{P}, \tag{10}$$

$$Y_3 \equiv \lambda(X_1 - X_3) - Y_1 \pmod{P}, \tag{11}$$

$$\lambda \equiv \begin{cases} \dfrac{Y_2 - Y_1}{X_2 - X_1} \pmod{P}, \text{ при } (X_1, Y_1) \neq (X_2, Y_2), \\ \dfrac{3X_1^2 + A}{2Y_1} \pmod{P}, \text{ при } (X_1, Y_1) = (X_2, Y_2). \end{cases} \tag{12}$$

Точка $\mathcal{O}$ – нулевой элемент группы точек эллиптической кривой.

Для сведения данной задачи к задаче «ВЫПОЛНИМОСТЬ» воспользуемся следующим разложением:

$$\mathcal{R} = K\mathcal{Q} = \left(\cdots\left(k_1\mathcal{Q} + k_2\left\{2\mathcal{Q}\right\}\right) + \cdots\right) + k_N\left\{2^{N-1}\mathcal{Q}\right\}, \tag{13}$$

где k_i $(i = 1, \ldots, N)$ – биты искомой экспоненты.

Выражения, заключенные в фигурные скобки, не зависят от неизвестных величин, поэтому нет необходимости кодировать алгоритм их вычисления в виде КНФ. Без ограничения общности можно считать, что точки $2^i\mathcal{Q}$ отличны от точки $\mathcal{O}$. Если бы это было не так, то, начиная с некоторого номера m $(0 < m < N)$, все слагаемые в левой части (13) были бы равны $\mathcal{O}$, что

[10]Jurisic A., Menezes A. Elliptic curves and cryptography. // Dr. Dobb's Journal. – April 1997. – Vol. 22. – no. 4.

существенно упрощало бы решаемую задачу. Однако, в сумме (13) возможно появление $\mathcal{O}$ за счет того, что отдельные k_i обращаются в нуль.

Итак, для представления правой части (13) в виде КНФ необходимо закодировать следующие операции:

1) суммирование двух точек эллиптической группы;
2) деление в поле $GF(P)$ (12);
3) линейная комбинация точек кривой: $a\mathcal{U}+b\mathcal{V}=c\mathcal{R}$, где a, b и c переменные, принимающие значения 0 и 1, а $\mathcal{U}, \mathcal{V}$ и $\mathcal{R}$ – точки эллиптической кривой.

Кодирование первой операции осуществляется на основе следующей системы уравнений, эквивалентных равенствам (10), (11), (12):

$$
\begin{aligned}
&W \equiv X_{\mathcal{V}} - X_{\mathcal{U}} \pmod P, && T \equiv Y_{\mathcal{V}} - Y_{\mathcal{U}} \pmod P,\\
&L \equiv T/W \pmod P, && S \equiv X_{\mathcal{U}} + X_{\mathcal{V}} \pmod P,\\
&K \equiv L^2 \pmod P, && X_{\mathcal{R}} \equiv K - S \pmod P,\\
&D \equiv X_{\mathcal{U}} - X_{\mathcal{R}} \pmod P, && M \equiv DL \pmod P,\\
&Y_{\mathcal{R}} \equiv M - Y_{\mathcal{U}} \pmod P,
\end{aligned}
$$

где $X_{\mathcal{U}}, Y_{\mathcal{U}}, X_{\mathcal{V}}, Y_{\mathcal{V}}, X_{\mathcal{R}}, Y_{\mathcal{R}}$ – координаты точек, W, T, L, S, K, D, M – вспомогательные числовые переменные.

При этом для кодирования операции деления в поле $GF(P)$ предлагается следующий подход: строится КНФ представление операции умножения в поле $GF(P)$ (7). Далее в построенную КНФ подставляются значения битов U, R и P. Полученная КНФ, очевидно, является КНФ представлением для операции деления.

Для кодирования в виде КНФ линейной комбинации двух точек используется примитив КНФ, представимый в следующем виде:

$$r = (t \wedge c) \vee (f \wedge \overline{c}). \tag{14}$$

Данный примитив обладает следующими свойствами:

1) если литерал c имеет значение «истина», то литерал r принимает значение t;
2) если литерал c имеет значение «ложь», то литерал r принимает значение f.

Далее в работе приводится один из возможных способов представления выражения (14) в виде КНФ, основанный на использовании равенства (2) и правила де Моргана.

Алгоритм сведения задачи логарифмирования на эллиптической кривой к задаче «ВЫПОЛНИМОСТЬ» принимает на вход параметры эллиптической кривой: числа A, B и P, имеющие N двоичных разрядов, точки данной кривой $\mathcal{Q}$ и $\mathcal{R}$, а также литералы $k_1, k_2, \ldots, k_N$, соответ-

ствующие битам искомой экспоненты. Алгоритм состоит из описанных ниже этапов.

1. Вычислить точки $2^{i-1}\mathcal{Q}$ при $i = 1, \ldots, N$.
2. При $i = 1, \ldots, N-1$, $\mathcal{S}_1 = \mathcal{Q}$ и $c_1 = k_1$ генерировать КНФ представления для выражений вида $c_{i+1}\mathcal{S}_{i+1} = c_i\mathcal{S}_i + k_i 2^{i-1}\mathcal{Q}$.
3. В полученную КНФ подставить биты P и $2^{i-1}\mathcal{Q}$ при $i = 1, \ldots, N$. В качестве значений литералов, отвечающих $\mathcal{S}_N$, подставить биты $\mathcal{R}$.

Теорема 2.3.1. *Приведенный алгоритм является консервативным сведением задачи логарифмирования на эллиптической кривой к задаче «ВЫПОЛНИМОСТЬ», обладающим следующими свойствами:*

1) время работы алгоритма есть $O\left(N^4\right)$, при этом основной вклад вносит вычисление точек $2^{i-1}\mathcal{Q}$, сама генерация КНФ за счет эффективного кодирования деления в поле $GF(P)$ имеет трудоемкость $O\left(N^3\right)$;

2) количество литералов в построенной КНФ есть $O\left(N^3\right)$;

3) количество дизъюнктов в построенной КНФ есть $O\left(N^3\right)$.

В четвертом параграфе приводится описание разработанной для задачи факторизации системы тестов, позволяющей осуществлять переход от вещественного вектора, полученного на выходе алгоритма минимизации функционала, ассоциированного с задачей «ВЫПОЛНИМОСТЬ», к булевому вектору – приближению выполняющего набора КНФ. Данные тесты предполагается использовать как дополнение к простой пороговой схеме по значению вещественных переменных, которая не позволяет учитывать связи между литералами, проистекающие из сути исходной задачи.

В основе теста лежит схема формирования промежуточных сумм $u_{i\,j}$, используемая в рамках первого этапа алгоритма генерации нескольких КНФ для задачи факторизации (4). Обратим внимание на тот факт, что если во втором сомножителе (биты y_i) встречаются подряд два единичных бита, то большая часть битов промежуточной суммы $u_{i\,j}$ и переносов $c_{i\,j}$ будут также единичными. Если предположить, что нулевые и единичные биты в сомножителях распределены равномерно, то алгебраическая сумма вещественных приближений для литералов, отвечающих битам переноса и компонентам вектора промежуточной суммы, будет сравнима с размерностью сомножителей N. Аналогично можно выделять два подряд встречающихся нуля во втором сомножителе – соответствующая алгебраическая сумма будет существенно меньше N. Таким образом, получаем **тест «по строкам»** для выделения двух подряд идущих одинаковых битов второго сомножителя, основанный на выделении максимальных и минимальных значений суммы:

$$S_{1\,i} = \sum_{j=1}^{N-1} \widetilde{c}_{i\,j} + \sum_{j=-1}^{N} \widetilde{u}_{i\,2i+j},$$

где $\widetilde{u}_{i\,j}$ и $\widetilde{c}_{i\,j}$ – вещественные переменные, отвечающие битам промежуточной суммы и переносам соответственно.

Далее, рассуждая аналогично, можно построить **тест «по столбцам»** для выделения двух подряд идущих одинаковых битов первого сомножителя:

$$S_{2\,j} = \sum_{i=1}^{N/2} \left(2\widetilde{c}_{i\,j+1} + \widetilde{u}_{i\,2i+j} - \widetilde{c}_{i\,j}\right),$$

где $\widetilde{u}_{i\,j}$ и $\widetilde{c}_{i\,j}$ – вещественные переменные, отвечающие битам промежуточной суммы и переносам соответственно.

В последнем параграфе главы приводится алгоритм генерации КНФ, кодирующей условие неделимости на малые простые числа, что позволяет сократить время поиска выполняющего набора за счет увеличения частоты вхождения в КНФ литералов, отвечающих битам сомножителей.

В третьей главе приводятся результаты вычислительных экспериментов, выполненных для исследования разработанных алгоритмов. Ниже описаны проведенные эксперименты и полученные результаты.

1. Генерация КНФ для задач практически значимых размерностей (т.е. используемых в действующих криптосистемах). Полученные результаты представлены в таблице 1. Полученные данные позволили уточнить теоретические оценки параметров построенных алгоритмов (определить коэффициенты при старших степенях) и сравнить алгоритмы сведения задачи факторизации с известным аналогом – алгоритмом, предложенным Srebrny[11]. Было установлено, что алгоритм сведения к задаче «3-ВЫПОЛНИМОСТЬ» дает трехкратный выигрыш по количеству дизъюнктов и литералов относительно алгоритма Srebrny, а алгоритм сведения к набору экземпляров задачи «ВЫПОЛНИМОСТЬ» дает выигрыш в 2 раза по количеству литералов, но уступает в 3 раза по количеству дизъюнктов.
2. Решение полученных экземпляров задачи «ВЫПОЛНИМОСТЬ» небольших размерностей с помощью современных SAT-решателей (победителей конкурса SAT-Competition 2007[12]). Полученные результаты представлены в таблице 2.
3. Определение наиболее вероятных значений битов сомножителей для задачи факторизации с помощью разработанного эвристического метода проекций вещественного вектора приближений на пространство булевых векторов. В результате, в серии из 31 эксперимента по фактори-

[11]Srebrny M. Factorization with sat – classical propositional calculus as a programming environment // Faculty of Mathematics Informatics and Mechanics at the University of Warsaw. 2004. URL: http://www.mimuw.edu.pl/mati/fsat-20040420.pdf (дата обращения: 06.07.2009).

[12]Sat competition [Сайт]. URL: http://www.satcompetition.org (дата обращения: 10.08.2009)

Таблица 1

Результаты генерации КНФ

Размерность задачи	**Количество литералов**	**Количество дизъюнктов**	**Время генерации** (час : мин : сек)
Задача факторизации			
2048	6,5E5	1,6E7	00:08:05
8192	1,0E7	2,6E8	05:59:50
Задача факторизации (3-КНФ)			
2048	1,5E6	6,3E6	0:01:01
3072	3,5E6	1,4E7	0:04:27
Задача дискретного логарифмирования			
128	1,0E7	1,8E8	02:18:08
152	1,7E7	3,0E8	07:12:06
Задача логарифмирования на эллиптической кривой			
70	5,3E6	8,9E7	03:06:16
100	1,5E7	2,6E8	10:24:00

зации числа размером 512 битов с частотой совпадения не ниже 61% удалось определить значения 161 бита сомножителей (31,45%), а биты с номерами 1, 13, 46, 73, 86, 101, 142, 217, 255 были верно определены в более 80% экспериментов.

4. Исследование стойкости рассматриваемых задач к восстановлению полного ключа по его известным фрагментам. Было установлено, что для задачи факторизации сложность решения соответствующей задачи «ВЫПОЛНИМОСТЬ» существенно уменьшается при подстановке фрагментов ключа. Например, факторизация числа размером 512 битов осуществляется за 8 минут после подстановки в ассоциированную КНФ значений 47% случайно выбранных битов сомножителей. Для задач дискретного логарифмирования и логарифмирования на эллиптической кривой такой закономерности обнаружено не было. Например, для задачи дискретного логарифмирования размерности 24 бита после подстановки 50% случайно выбранных битов ключа не удалось получить решение за отведанные 4 часа. При этом задача размерности 12 битов решается менее, чем за 10 минут (см. таблицу 2).

Таблица 2

Решение полученных экземпляров задачи «ВЫПОЛНИМОСТЬ»

Алгоритм решателя	**Время решения КНФ** (час : мин : сек)		
Сведение задачи факторизации к задаче «ВЫПОЛНИМОСТЬ»			
Размерность задачи	*80*	*96*	*112*
march_ks	0:01:45	0:03:26	0:36:20
Сведение задачи факторизации к задаче «3-ВЫПОЛНИМОСТЬ»			
Размерность задачи	*88*	*96*	*104*
vallst	0:57:28	1:51:50	4:26:34
Сведение задачи дискретного логарифмирования			
Размерность задачи	*10*	*12*	*14*
SatElite	0:00:14	0:09:00	1:16:46
rsat	0:00:33	0:07:56	1:23:23
Сведение задачи логарифмирования на эллиптической кривой			
Размерность задачи	*8*	*10*	*12*
rsat	0:06:51	0:49:42	>5:00:00
minisat	0:00:33	0:07:56	>5:00:00

Основные результаты диссертации

1. Разработаны полиномиальные алгоритмы консервативного сведения задач факторизации, дискретного логарифмирования и логарифмирования на эллиптической кривой к задаче «ВЫПОЛНИМОСТЬ».
2. Сформулирован и доказан ряд теорем относительно корректности построенных алгоритмов, оценок их трудоемкости и параметров генерируемых КНФ.
3. Экспериментально исследована трудоемкость поиска выполняющего набора построенных КНФ с использованием современных алгоритмов решения задачи «ВЫПОЛНИМОСТЬ».
4. Разработан алгоритм сведения одного экземпляра задачи факторизации к набору различных экземпляров задачи «ВЫПОЛНИМОСТЬ», позволяющий распараллеливать процесс решения.
5. Для задачи факторизации разработаны алгоритмы: сведения к задаче «3-ВЫПОЛНИМОСТЬ»; проектирования вещественного вектора при-

ближений на пространство булевых переменных; генерации КНФ, кодирующей условие неделимости на малые простые числа; генерации КНФ, кодирующей упорядочение сомножителей.

6. На основе КНФ, полученных с помощью разработанных алгоритмов, исследована стойкость задач факторизации, дискретного логарифмирования и логарифмирования на эллиптической кривой к восстановлению полного ключа по его известным фрагментам.

ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи, опубликованные в ведущих рецензируемых научных журналах, определенных ВАК

1. Дулькейт В. И., Файзуллин Р. Т., Хныкин И. Г. Алгоритм минимизации функционала, ассоциированного с задачей 3-sat и его практические применения // Компьютерная оптика. — 2008. — Т. 32, № 1. — С. 68–73.
2. Дулькейт В. И., Файзуллин Р. Т., Хныкин И. Г. Минимизация функционалов, ассоциированных с задачами криптографического анализа // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2008. — № 2(18). — С. 54–56.
3. Дулькейт В. И., Файзуллин Р. Т., Хныкин И. Г. Непрерывные аппроксимации решения задачи «ВЫПОЛНИМОСТЬ» применительно к криптографическому анализу асимметричных шифров // Компьютерная оптика. — 2009. — Т. 33, № 1. — С. 86–91.

Другие публикации

4. Faizullin R., Khnykin I., Dulkeit V. Polynomial approximation for sat as applied to crypto ciphers // Polynomial Computer Algebra (April 8-12, 2009). — St. Petersburg, Russia: 2009. — Pp. 100–104.
5. Алгоритм минимизации функционала, ассоциированного с задачей 3-SAT, и его практические применения / В. И. Дулькейт, Р. Т. Файзуллин, И. Г. Хныкин, Е. Салаев // Параллельные вычислительные технологии (ПаВТ'2007): Труды международной научной конференции (Челябинск, 29 января – 2 февраля 2007 г.) / Изд. ЮУрГУ. — Т. 2. — Челябинск: 2007. — С. 156–167.
6. Дулькейт В. Учебно-исследовательская программа Factor-Sat 1.0 для генерации логических формул эквивалентных задаче факторизации (ОФАП Рег.№ 9396, Информационный Фонд РФ Рег. № 50200702415) // Компьютерные учебные программы и инновации. — 2008. — № 3. — С. 131.

7. Дулькейт В., Файзуллин Р. Т., Хныкин И. Г. Минимизация функционалов, ассоциированных с задачами криптографического анализа асимметричных шифров // Таврический вестник информатики и математики. — 2008. — № 1. — С. 178–188.
8. Дулькейт В. И. Построение эквивалентных КНФ для задач факторизации и дискретного логарифмирования // Труды VII всероссийской конференции молодых ученых по математическому моделированию и информационным технологиям (с участием иностранных ученых). — Красноярск: 2006. — С. 85.
9. Дулькейт В. И. КНФ представления для задач факторизации и дискретного логарифмирования // Проблемы теоретической и прикладной математики: Труды 38-й Региональной молодежной конференции / УрО РАН. — Екатеринбург: 2007. — С. 350–355.
10. Дулькейт В. И. КНФ представления для задачи логарифмирования на эллиптической кривой // ПРОБЛЕМЫ ТЕОРЕТИЧЕСКОЙ И ПРИКЛАДНОЙ МАТЕМАТИКИ: Труды 39-й Всероссийской молодежной конференции. — Екатеринбург: УрО РАН: 2008. — С. 360–364.
11. Дулькейт В. И., Файзуллин Р. Т. Алгоритм построения эквивалентных КНФ для задачи факторизации // Труды III всероссийской конференции: Проблемы оптимизации и экономические приложения. — Омск: 2006. — С. 89.
12. Дулькейт В. И., Файзуллин Р. Т., Хныкин И. Г. Сведение задач криптоанализа асимметричных шифров к решению ассоциированных задач ВЫПОЛНИМОСТЬ. — М.: МАКС Пресс, 2007. — С. 249–251.
13. Дулькейт В. И., Файзуллин Р. Т., Хныкин И. Г. Минимизация функционалов, ассоциированных с задачами криптографического анализа. — Новосибирск: Институт математики СО РАН: 2008. — С. 484–485.
14. Дулькейт В. И., Файзуллин Р. Т., Хныкин И. Г. Минимизация функционалов, ассоциированных с задачами криптографического анализа асимметричных шифров // Прикладная дискретная математика. — 2008. — № 2. — С. 113–119.
15. Дулькейт В. И., Файзуллин Р. Т., Хныкин И. Г. Параллельные алгоритмы минимизации функционалов, ассоциированных с задачами криптографического анализа // Параллельные вычислительные технологии (ПаВТ'2009): Труды международной научной конференции (Нижний Новгород, 30 марта – 3 апреля 2009 г.) / Изд. ЮУрГУ. — Челябинск: 2009. — С. 463–473.

Отпечатано с оригинал-макета, предоставленного автором

Подписано в печать 04.03.2010 г. Формат 60 × 84/16.
Бумага офсетная. Усл. печ. л. 1,5.
Заказ № 115. Тираж 100.

Отпечатано в типографии ФГУП «ОНИИП».
г. Омск, ул. Масленников, 231.
тел. (3812)-51-49-25