На правах рукописи

Чмора Андрей Львович

Методы теории помехоустойчивого кодирования в некоторых задачах защиты информации

05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва – 2012

Работа выполнена в *Федеральном государственном бюджетном учреждении науки «Институте проблем передачи информации им. А. А. Харкевича Российской академии наук» (ИППИ РАН).*

Научный руководитель : (консультант)	*доктор техническх наук, профессор,* ***Зяблов Виктор Васильевич***
Официальные оппоненты:	***Крук Евгений Аврамович****, доктор технических наук, профессор, ГУАП (Санкт-Петербург), заведующий кафедрой «Комплексная защита информации»*
	Кабатянский Григорий Анатольевич*, доктор физико-математических наук, ИППИ РАН, главный научный сотрудник лаборатории №4*
Ведущая организация:	*Московский физико-технический институт (государственный университет)*

Защита состоится «____» _____ 2012 г. в ____ часов на заседании диссертационного совета *Д 002.077.01* при *ИППИ РАН*, расположенном по адресу: *127994, г. Москва, ГСП-4, Большой Каретный переулок, д. 19, стр. 1.*

С диссертацией можно ознакомиться в библиотеке *ИППИ РАН.*

Автореферат разослан «____» _____ 2012 г.

Ученый секретарь
диссертационного совета Д 002.077.01,
доктор физико-математических наук *Цитович И. И.*

Общая характеристика работы

Актуальность работы. В ближайшие десятилетия следует ожидать появления действующего прототипа квантового компьютера. В 1997 году П. В. Шор[1] (P. W. Shor) продемонстрировал существование эффективных квантовых методов решения сложных вычислительных задач, определяющих криптостойкость известных алгоритмов цифровой подписи и асимметричного шифрования. В первую очередь к ним относятся широко применяемые на практике алгоритмы RSA, DSA, KCDSA, EC-DSA, EC-KCDSA, EC-GDSA (ISO/IEC 14888-3, ISO/IEC 14888-2 и IEEE P1363), а также ГОСТ Р 34.10-2001. Другой известный результат[2] К.-П. Шнорра (C.-P. Schnorr) и М. Якобссона (M. Jakobsson) указывает на то, что криптостойкость перечисленных алгоритмов определяется вычислительной трудоемкостью решения задач целочисленной факторизации и дискретного логарифмирования.

Вопрос об эффективном решении на квантовом компьютере некоторых трудноразрешимых задач в настоящее время остается открытым. В частности, утверждение справедливо для задачи декодирования случайного кода по минимуму расстояния, которая, как известно[3], относится к классу **NP**-трудных.

Аппарат теории кодирования широко применяется для построения протоколов идентификации и цифровой подписи. Следует отметить протокол Ж. Штерна[4] (J. Stern), а также схему цифровой подписи на случайных кодах[5] Г. А. Кабатянского, Е. А. Крука и Б. Дж. М. Смитса (B. J. M. Smeets).

Широко известны криптосистемы Р. МакЭлиса (R. McEliece) и Г. Нидеррайтера (H. Niederreiter) на основе кодов Гоппы[6] и обобщенных кодов Рида—Соломона[7]. В работе В. М. Сидельникова и С. О. Шестакова предложена эффективная атака на криптосистему на основе обобщенных кодов Рида—Соломона[8]. В. М. Сидельников разработал вариант криптосистемы на кодах

---

[1] Shor P. W. Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM J. of Comp. 1997. no. 26. Pp. 1484–1509.

[2] Schnorr C.-P., Jakobsson M. Security of Discrete Log Cryptosystems in the Random Oracle and Generic Model // In The Mathematics of Public-Key Cryptography. The Fields Institute. 1999.

[3] Barg A. Complexity Issues in Coding Theory // Handbook of coding theory. Ed. by V. S. Pless, W. C. Huffman, R. Brualdi. Amsterdam, Holland: Elsevier Science, 1998.

[4] Stern J. A New Identification Scheme Based on Syndrome Decoding // Advances in Cryptology–CRYPTO'93. Lect. Notes in Comp. Sci. Springer-Verlag. 1993. Vol. 773. Pp. 13–21.

[5] Kabatianskii G., Krouk E., Smeets B. J. M. A Digital Signature Scheme Based on Random Error-Correcting Codes // Lect. Notes in Comp. Sci. Springer-Verlag. 1997. Vol. 1355. Pp. 161–167.

[6] McEliece R. A Public-key Cryptosystem Based on Algebraic Coding Theory // Deep Space Network Progress Report / DSN PR 42–44. 1978. – Apr 15. Pp. 114–116.

[7] Niederreiter H. Knapsack-type Cryptosystems and Algebraic Coding Theory // Prob. of Control and Inform. Theory. 1986. Vol. 15, no. 5. Pp. 159–166.

[8] Sidelnikov V. M., Shestakov S. O. On Insecurity of Cryptosystems Based on Generalized Reed-Solomon Codes // Disc. Math. and App. 1992. Vol. 2, no. 4. Pp. 439–444.

Рида—Маллера[9]. Подробное исследование этой криптосистемы завершилось доказательством ее уязвимости[10]. В 1991 году Э. М. Габидулин, А. В. Парамонов, О. В. Третьяков предложили криптосистему, основанную на кодах, исправляющих ошибки в ранговой метрике[11].

В диссертационном исследовании рассматривается задача *организации интерактивного взаимодействия удаленных пользователей с разделяемым сетевым ресурсом при соблюдении гарантий доступности, подлинности, конфиденциальности данных, правил использования цифрового контента в части ограничения его незаконного изготовления, воспроизведения и распространения.*

Для решения задачи применялись методы теории помехоустойчивого кодирования.

В рамках поставленной задачи в качестве технического средства защиты авторских прав (ТСЗАП) разработан метод маскировки ключа с помощью биометрии (метод «биометрической вуали»). Для противодействия поглощающей ресурсы стратегии, так называемой DDoS-атаке, которая на прикладном уровне приводит к отказу в обслуживании, или, по-другому, компрометации такой востребованной услуги безопасности как доступность, разработана эффективная конструкция в рамках метода шарад.

Использование биометрии в качестве секретного ключа в криптографических приложениях представляется логичным. Суть практической привлекательности биометрии как криптографического инструмента заключается в ее естественной *неотторжимости*. Напротив носитель, на который записан секретный ключ, не является неотъемлемой частью владельца ключа и легко может быть отторгнут. Например потерян, украден или уничтожен.

Биометрия подвержена изменчивости и результаты измерений одного и того же объекта варьируются в некотором диапазоне. Как правило, такая изменчивость носит кратковременный характер и зависит от факторов внешней среды, но с течением времени может стать необратимой. По причине изменчивости биометрические данные невозможно использовать в качестве криптографического ключа. Решение проблемы, тем не менее, существует. Обзор способов связывания биометрических данных и криптографического ключа приводится в первой главе диссертации.

Отметим, что известные решения не всегда адекватно согласуются с требованиями практики и часто не обеспечивают достаточного количества эн-

---

[9] Sidelnikov V. M. A Public-key Cryptosystem based on Binary Reed-Muller Codes // Disc. Math. and App. 1994. Vol. 4, no. 3. Pp. 439–444.

[10] Minder L., Shokrollahi A. Cryptanalysis of the Sidelnikov Cryptosystem // Advances in Cryptology–EUROCRYPT'07 / Ed. by M. Naor. Vol. 4515 of Lect. Notes in Comp. Sci. Springer-Verlag, 2007. Pp. 347–360.

[11] Gabidulin E. M., Paramonov A. V., Tretjakov O. V. Ideals Over a Non-Commutative Ring and Their Application in Cryptology // Advances in Cryptology–EUROCRYPT'91 / Ed. by D. W. Davies. Vol. 547 of Lect. Notes in Comp. Sci. Springer-Verlag, 1991. Pp. 482–489.

тропийных разрядов.

Разработка метода маскировки криптографического ключа с помощью биометрии, удовлетворяющего практическим требованиям и гарантирующего адекватный уровень криптостойкости, представляется перспективной и актуальной.

DoS[12]-атаки отличаются от других известных атак. Задача DoS-атаки — создание искусственной ситуации, в которой добросовестному потребителю будет отказано в предоставлении соответствующих услуг.

За последние полтора десятка лет разработаны различные меры противодействия DoS-атаке, в том числе и метод шарад[13]. Обзор существующих решений представлен во второй главе диссертации.

Основная идея метода шарад заключается в создании искусственной вычислительной нагрузки на стороне отправителя — инициатора запроса. Это означает, что для успеха DoS-атаки необходимо инвестировать. Инвестиционные решения могут варьироваться в широком диапазоне: от организации распределенных вычислений до использования высокопроизводительных вычислительных платформ. Понятно, что атакующий способен прибегнуть к той или иной выигрышной стратегии, но неизбежное инвестирование безусловно является сдерживающим фактором. Вычислительный ресурс, задействованный в распределенной DoS-атаке (DDoS[14]), может также использоваться для отыскания решения, например с помощью распараллеливания вычислений, что очевидно снижает эффективность метода шарад. Кроме этого, шарады некоторых типов, например на основе таких трудноразрешимых задач как факторизация и дискретное логарифмирование, уязвимы с точки зрения атаки с применением квантового компьютера. Таким образом, при DDoS-атаке, а также атаке с применением квантового компьютера, адекватное противодействие с использованием известных решений затруднено или даже невозможно.

Конструирование шарад, не поддающихся распараллеливанию, для которых, с одной стороны, не существует эффективного квантового алгоритма, и которые обладают максимально широким диапазоном трудоемкости с возможностью плавной регулировки, а также минимальными объемом памяти и накладными расходами при передаче по каналу связи, с другой, — важнейшая практическая задача, от решения которой зависит качество предоставляемых услуг.

Цель диссертационной работы. Разработка метода «биометрической вуали», а также эффективных конструкций в рамках метода шарад с привле-

[12] *Denial of Service.*

[13] Brainard J., Juels A. Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks // Proc. of the ISOC Network and Distr. Sys. Sec. Sym. 1999. Pp. 151–165.

[14] *Distributed Denial of Service.*

чением аппарата теории помехоустойчивого кодирования.

Задачи исследования. Для достижения поставленной цели необходимо было решить следующие задачи.

1. Построить абстрактную модель маскировки ключа с помощью биометрии на основе фундаментального свойства однородности образов/эталонов, полученных в результате измерений и обработки проекций биометрического объекта, и выполнить ее анализ.
2. Разработать метод маскировки криптографического ключа с помощью биометрии и обосновать его криптостойкость.
3. Разработать конструкции шарад на основе кодов, исправляющих ошибки.

Методы исследования. В качестве научного аппарата диссертационного исследования использовались методы теории помехоустойчивого кодирования, криптографии, линейной алгебры, комбинаторного анализа, теории алгоритмов и вычислительной сложности.

Научная новизна. Научная новизна диссертационной работы заключается в том, что в ней впервые:

- построена абстрактная модель маскировки ключа с помощью биометрии на основе фундаментального свойства однородности образов/эталонов, полученных в результате измерений и обработки проекций биометрического объекта;
- предложена практическая реализация модели маскировки ключа с помощью биометрии с привлечением аппарата теории помехоустойчивого кодирования, — так называемый метод «биометрической вуали», и приведен пример кодовой конструкции;
- выполнен анализ криптостойкости метода «биометрической вуали»;
- выполнен анализ метода шарад и обозначены недостатки известных конструкций;
- введен класс шарад на основе кодов, исправляющих ошибки (кодовые шарады);
- сконструирована итеративная кодовая шарада и выполнен анализ ее устойчивости;
- предложена компактная и устойчивая итеративная кодовая шарада, обладающая широким диапазоном трудоемкости и допускающая плавную настройку.

Практическая значимость работы. Поскольку метод «биометрической вуали» применим к криптографическому ключу, то возможно его использование в различных приложениях, например, как показано в первой главе диссертации, для ограничения незаконного тиражирования мультимедийного контента.

Актуальность разработки эффективных методов противодействия DDoS-атакам невозможно переоценить, с развитием сетевых технологий, а также с появлением на рынке квантовых вычислителей, востребованность таких методов будет только возрастать.

Научные положения, выносимые на защиту. На защиту выносятся следующие основные результаты и положения:

- абстрактная модель маскировки ключа с помощью биометрии на основе фундаментального свойства однородности как универсальная методология, покрывающая широкий спектр решений вне зависимости от типа биометрии;
- метод «биометрической вуали», гарантирующий адекватный уровень практической криптостойкости: при параноидальном подходе трудоемкость раскрытия эталона методом силовой атаки не менее 2^{89} двоичных операций;
- анализ метода шарад; показано, что к недостаткам известных конструкций относятся возможность распараллеливания и существование эффективного квантового алгоритма решения;
- класс шарад на основе кодов, исправляющих ошибки, для которых не известен квантовый алгоритм отыскания решения с полиномиальной трудоемкостью. Показано, что такие шарады позволяют адекватно реагировать на атакующее воздействие за счет полиномиальной функции изменения трудоемкости;
- итеративная кодовая шарада, которая не поддается распараллеливанию;
- компактная итеративная кодовая шарада с плавной настройкой, обладающая устойчивостью, широким диапазоном трудоемкости, минимальным объемом памяти и накладными расходами при передаче по каналу.

Апробация работы. На представленные в первой главе результаты получен патент Российской Федерации, а также патенты Республики Корея и США [1–3]. Кроме этого, материалы диссертационной работы были использованы при подготовке курса лекций по теме «Криптографические методы защиты информации в компьютерных системах и сетях» по направлению 011674 факультета РТК Московского физико-технического института

кафедры «Проблемы передачи и обработки информации», прочитанных в период с 2008 по 2011 гг. Следует также отметить, что результаты, представленные ранее в патентах [1–3] и позднее в публикации [4], были впоследствии воспроизведены группой специалистов Компьютерной лаборатории (Computer Laboratory) Кембриджского университета под руководством известного эксперта в области защиты информации, профессора Р. Андерсона (R. Anderson), и опубликованы в техническом отчете UCAM-CL-TR-640 в июле 2005 г., а затем и в статье[15] 2006 г. Однако, приоритет принадлежит российским авторами, как авторам первой патентной заявки по данной тематике, зарегистрированной в мае 2004 г. Таким образом, можно заключить, что результаты, изложенные в первой главе настоящей диссертации, с успехом прошли международную апробацию.

Публикации. В ходе подготовки диссертации соискателем опубликованы 14 печатных работ [1–14], включая патенты Российской Федерации, США и Республики Корея. Конкретно по теме диссертации опубликованы 5 печатных работ [1–4, 7], из них 2 опубликованы в реферируемых изданиях, включенных в Перечень ВАК [4, 7].

Личный вклад автора. Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованные работы. Подготовка заявок по патентам [1–3] проводилась совместно с соавтором, причем вклад диссертанта не менее 50%. Все представленные в диссертации результаты получены лично автором.

Структура и объем диссертации. Диссертация состоит из введения, трех глав, заключения, библиографии и приложения. Общий объем работы составляет 115 страниц. Диссертация содержит 2 рисунка и одну таблицу по объему не превышающих одну страницу. Список литературы состоит из 101 наименования на 13 страницах.

Содержание работы

Во Введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

В первой главе описан метод маскировки ключа с помощью биометрии. Результаты опубликованы в работе [4], а также в патентах [1–3].

Биометрический эталон T — обобщенная характеристика, полученная в результате измерений и обработки множества проекций одного и того же биометрического объекта. Биометрический эталон формируется на этапе реги-

[15] Hao F., Anderson R., Daugman J. G. Combining Crypto with Biometrics Effectively // IEEE Trans. on Comp. 2006. Vol. 55, no. 9. Pp. 1081–1088.

страции и сохраняется в долговременной памяти. Биометрический образ S — характеристика, полученная в результате текущего, как правило однократного, измерения биометрического объекта. Образ предъявляется для распознавания с помощью эталона.

Определение. Образ и эталон считаются *однородными*, если получены от одного объекта и удовлетворяют критерию однородности, который задается как ограничение расстояния между образом и эталоном.

Для фиксированного биометрического объекта может быть получено множество однородных образов и эталонов. Если образ и эталон однородны, то выдается положительное заключение. Отрицательное заключение указывает на то, что связь образа и эталона с конкретным биометрическим объектом не установлена. Тогда с высокой вероятностью можно предположить, что образ и эталон *неоднородны*, т.е получены от различных биометрических объектов.

Для указания на однородность образа и эталона воспользуемся обозначением «$\leftrightharpoons$» и «$\not\leftrightharpoons$» — для неоднородности.

Пусть задан криптографический ключ K и произвольные S, T. Введем следующую пару преобразований: $\mathcal{M} = f(T, K)$ и $\mathcal{K} = g(\mathcal{M}, S)$. Положим $\gamma = \log_2 \mathcal{M}$ и $\lambda = \log_2 K$.

Рассмотрим ряд условий и предположений, составляющих основу модели.

1. $f(\cdot,\cdot)$ и $g(\cdot,\cdot)$, $\mathcal{M}$ — общедоступны.
2. Если $S \leftrightharpoons T$, то $\mathcal{K} = K$. Если $S \not\leftrightharpoons T$, то $\mathcal{K} \neq K$.
3. При известных T и K, значение $\mathcal{M}$ вычисляется со сложностью $O(\lambda^\alpha)$, $\alpha > 1$.
4. Для заданного S, $S \leftrightharpoons T$, ключ K вычисляется со сложностью $O(\lambda^\beta)$, $\beta \geqslant \alpha$.
5. Для заданного S, $S \not\leftrightharpoons T$, ключ K вычисляется со сложностью $O(\exp(\gamma))$.
6. При известном T, ключ K вычисляется со сложностью $O(1)$.
7. При неизвестном T, ключ K вычисляется со сложностью $O(\exp(\gamma))$.

Согласно 6, ключ K и эталон T должны сохраняться в секрете. Из 4 следует, что образ S также должен сохраняться в секрете.

Предположим, что секретность определяется наличием *зоны относительной неуязвимости*, которая ограничена периметром безопасности. Следовательно, формирование T и S, генерацию ключа K и получение K из $\mathcal{M}$ при заданном S, необходимо выполнять в пределах обозначенной зоны.

В дальнейшем будем исходить из следующих предположений.

- Доверенная сторона отвечает за регистрацию, генерацию ключа K, формирование эталона T, а также $\mathcal{M}$. Операционная активность доверенной стороны ограничена пределами зоны относительной неуязвимости.
- Значение $\mathcal{M}$ заносится в специализированную базу данных для долговременного хранения. База данных размещается вне зоны относительной неуязвимости и соответственно подвержена атакам.
- В ходе формирования образа S может быть предъявлен не тот биометрический объект, который использовался при формировании эталона T. Также может быть предъявлен артефакт.
- Операционная активность на этапе распознавания образа S с помощью эталона T и принятия решения по результатам распознавания осуществляется в пределах зоны относительной неуязвимости.

Пусть криптографический ключ K трактуется как информационные символы линейного k-мерного кода $\mathcal{C}$ с минимальным расстоянием d. Код $\mathcal{C}$ задан $k \times n$ порождающей матрицей G. Тогда существует кодовое слово $\mathbf{c} = KG$, $\mathbf{c} \in \mathsf{ker}(H)$, где $H - (n-k) \times n$ проверочная матрица кода $\mathcal{C}$. Биометрический эталон T рассматривается как вектор ошибки $\mathbf{e}$ для кодового слова $\mathbf{c}$. Сумма $\mathcal{M} = \mathbf{c} + \mathbf{e} = KG \oplus T$ сохраняется в долговременной памяти. Если $T \leftrightharpoons S$, то $\mathsf{wt}(T \oplus S) < \lceil (d-1)/2 \rceil$ и код способен исправить $T \oplus S$ ошибок. Если $T \not\leftrightharpoons S$, то $\mathsf{wt}(T \oplus S) > \lceil (d-1)/2 \rceil$ и код не сможет исправить ошибки. Свойства радужной оболочки глаза человека таковы[16], что при $T \leftrightharpoons S$ получение ключа K не сопряжено с высокими вычислительными трудозатратами, но при $T \not\leftrightharpoons S$ ключ недоступен. Доказано, что декодирование по максимуму правдоподобия случайного кода, эквивалентное в нашем случае декодированию в ближайшее кодовое слово, относится к классу **NP**-трудных проблем[17].

Кроме этого показано, что декодирование по максимуму правдоподобия даже для специфических семейств случайных кодов, например кодов Рида—Соломона, также относится к классу **NP**-трудных проблем[18].

Отметим, что алгоритм декодирования Гурусвами—Судана[19] позволяет исправлять ошибки веса $t > \lceil (d-1)/2 \rceil$. Однако несложно выбрать код так, что декодирование с исправлением ошибок станет невозможным.

---

[16] Daugman J. G. Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons // Proc. of the IEEE. 2006. Vol. 94, no. 11. Pp. 1927–1935.

[17] Berlekamp E. R., McEliece R. J., van Tilborg H. C. A. On the Inherent Intractability of Certain Coding Problems // IEEE Trans. Inform. Theory. 1978. Vol. IT–24, no. 3. Pp. 384–386.

[18] Guruswami V., Vardy A. Maximum-Likelihood Decoding of Reed-Solomon Codes is NP-hard // IEEE Trans. Inform. Theory. 2005. Vol. 51, no. 7. Pp. 2249–2256.

[19] Guruswami V., Sudan M. Improved Decoding of Reed-Solomon Codes and Algebraic Geometry Codes // IEEE Trans. Inform. Theory. 1999. Vol. 45, no. 6. Pp. 1757–1767.

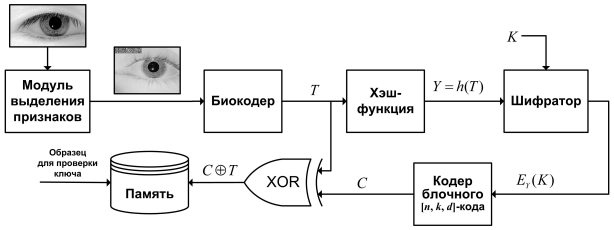

Рис. 1. Представление ключа

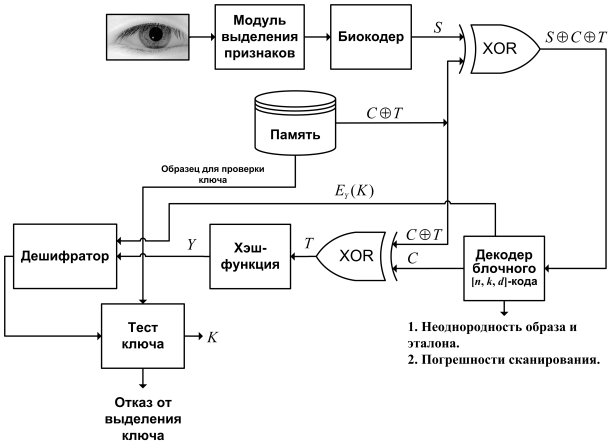

Рис. 2. Получение ключа

Дадим описание метода «биометрической вуали», который в существенной степени использует свойства радужной оболочки глаза.

Для представления криптографического ключа выполняются следующие действия (рис. 1).

1. В результате обработки множества проекций биометрического объекта получают набор данных, на основании которого формируют эталон T.
2. С помощью генератора псевдослучайных чисел генерируют ключ K.
3. Формируют тестовый образец для проверки ключа. Например, $\hat{K} = h(K)$, где $h(\cdot)$ — криптографическая хэш-функция.
4. Вычисляют $Y = h(T)$.
5. Ключ K зашифровывают с помощью Y, $X = E_Y(K)$, где $E_Y(\cdot)$ — функция зашифрования.
6. Выполняют кодирование X блочным (n, k, d)-кодом с целью получения кодового слова C.
7. Вычисляют поразрядную сумму $C \oplus T$ и сохраняют результат в долговременной памяти.

Для получения криптографического ключа выполняется следующая последовательность действий (рис. 2).

1. Получают данные от, по меньшей мере, одного биометрического объекта.
2. Формируют образ S.
3. Извлекают из долговременной памяти сумму $C \oplus T$.
4. Вычисляют поразрядную сумму $C_{\text{ош}} = C \oplus T \oplus S$. Отметим, что после суммирования кодовое слово $C_{\text{ош}}$ все еще может содержать ошибки.

5. Выполняют конструктивное декодирование $C_{\text{ош}}$. Возможны следующие три события.

I. *Вес вектора ошибки не превышает* t. Это означает, что $T \leftrightharpoons S$. Ошибки будут исправлены в декодере блочного кода, информационные символы X восстановлены корректно.

II. *Вес вектора ошибки незначительно превышает* t. Ошибка данного веса не может быть исправлена: на специальном выходе декодера блочного кода формируется признак отказа от декодирования, который указывает на неоднородность или сигнализирует о погрешностях сканирования.

III. *Вес вектора ошибки значительно превышает* t. Это означает, что $T \not\leftrightharpoons S$. Декодер блочного кода исправляет ошибки меньшего веса в другом, отличном от $C_{\text{ош}}$, кодовом слове и вместо X восстанавливает случайную последовательность информационных символов. Событие опосредованно обнаруживается на шаге 10.

6. Предположим, что вес вектора ошибки не превышает t. В результате декодирования получают исправленное кодовое слово $\hat{C}_{\text{ош}}$.
7. Извлекают $C \oplus T$ из долговременной памяти и вычисляют поразрядную сумму $T = \hat{C}_{\text{ош}} \oplus (C \oplus T)$.
8. Вычисляют $Y = h(T)$.
9. Выделяют ключ $K = D_Y(X)$, где $D_Y(\cdot)$ — функция расшифрования.
10. Для верификации ключа извлекают тестовый образец из долговременной памяти и проверяют справедливость равенства $\hat{K} \stackrel{?}{=} h(K)$. Если равенство не подтверждено, то на специальном выходе формируется признак отказа от получения ключа.

Выполним анализ криптостойкости метода «биометрической вуали». При известном $X = E_Y(K)$ несложно вычислить C и T. Отметим, что X присутствует в памяти устройства в течение короткого промежутка времени, тогда как ключ K используется для зашифрования/расшифрования значительных объемов информации и в большей степени подвержен компрометации. Также возможно использование тестового образца для проверки ключа $\hat{K} = h(K)$. Действительно, если автономный носитель доступен на чтение, то злоумышленник может скопировать $C \oplus T$ и $\hat{K}$ без ведома владельца.

Для того, чтобы определить T при известном K необходимо вычислить X, но для этого необходимо знать T. Следовательно, при известном K и неизвестном T невозможно вычислить X.

Предположим, декодер исправляет ошибки веса $t < \lceil (d-1)/2 \rceil$. Обозначим образ-претендент как $\tilde{S}$, отличное от C кодовое слово обозначим через $\check{C}$,

$\tilde{K} = D_{\tilde{Y}}(\tilde{X})$, где $\tilde{Y} = h(\tilde{T})$. Испытание каждого претендента сопровождается проверкой следующих гипотез.

I. $C \oplus T \oplus \tilde{S} = \check{C}$.

II. $C \oplus T \oplus \tilde{S} = C$.

III. $C \oplus T \oplus \tilde{S} = \check{C} + \mathbf{e}$, $t < \lceil (d-1)/2 \rceil$.

IV. $C \oplus T \oplus \tilde{S} = C + \mathbf{e}$, $t < \lceil (d-1)/2 \rceil$.

Подтверждение гипотез II и IV указывает на факт получения эталона T. Причем гипотеза II соответствует случаю $\tilde{S} = T$ и декодированию без исправления ошибок, а гипотеза IV — декодированию с исправлением ошибок, когда $\mathsf{wt}(T \oplus \tilde{S}) < \lceil (d-1)/2 \rceil$. Поскольку вектор ошибки $\mathbf{e} = T \oplus \tilde{S}$ определяется в результате декодирования, то легко вычислить $T = \tilde{S} \oplus \mathbf{e}$. Однако по результатам декодирования невозможно отделить гипотезу II от I, а также гипотезу IV от III. Тогда равенство $K = \tilde{K}$ свидетельствует о подтверждении гипотезы II или IV, а $K \neq \tilde{K}$ — о подтверждении гипотезы I или III.

Отдельное испытание в ходе силовой атаки состоит из следующих шагов.

1. Синтез претендента $\tilde{S}$.
2. Декодирование $C \oplus T \oplus \tilde{S}$. Получение $\check{C}$, $\tilde{X}$, $\mathbf{e}$.
3. Вычисление $\tilde{T} = \tilde{S} \oplus \mathbf{e}$.
4. Вычисление $\tilde{Y} = h(\tilde{T})$.
5. Расшифрование $\tilde{K} = D_{\tilde{Y}}(\tilde{X})$.
6. Сравнение $K \stackrel{?}{=} \tilde{K}$ или $\hat{K} \stackrel{?}{=} h(\tilde{K})$.

Образ состоит из 2^{11} двоичных разрядов. Энтропия образа, так же как эталона, не превышает 249 двоичных разрядов[20]. Предположим, что известны все 249 позиций, на которых располагаются случайные и независимые символы. Предположим также, что этот набор позиций зафиксирован для всевозможных образов. Значения символов на остальных позициях образа могут быть вычислены с приемлемой трудоемкостью. Сделаем упрощающее предположение о расположении на этих позициях символов с нулевыми значениями. Следовательно, если заданы два различных образа S_1 и S_2, то $\mathsf{wt}(S_1 \oplus S_1) \leqslant 249$.

Пусть имеется шаблон из 2^{11} разрядов. Синтез образа заключается в генерации 249 случайных двоичных символов и размещении значений на известных позициях шаблона. При таком подходе силовая атака практически

[20] Daugman J. G. How Iris Recognition Works // IEEE Trans. Circ. Sys. Video Tech. 2004. Vol. 14, no. 1. Pp. 21–30.

неосуществима, так как в среднем для поиска решения необходимо испытать 2^{248} претендентов.

Предположим, что код исправляет все двоичные ошибки веса t и меньше. Пусть задано кодовое слово с ошибками $C_{\text{ош}} = C \oplus T$. Очевидно, что значение, которое принимает символ на каждой из 249 позиций слова $C_{\text{ош}}$, есть результат суммирования случайного и кодового символов. Если код исправляет не более t ошибок, то можно изменить значения символов на произвольных t из известных 249 позиций и затем провести испытание (шаги 2, 3, 4, 5 и 6). Пусть задан список из 249 позиций. Чтобы изменить значения символов достаточно сформировать шаблон $\tilde{S}$ веса t такой, что его разрядность равна 2^{11} и на позициях из списка расположены t единиц, а нули расположены на всех остальных позициях. Затем выполнить суммирование $C_{\text{ош}} \oplus \tilde{S}$. Тогда совокупное число испытаний не превысит $\sum_{i=0}^{t} \binom{249}{i}$ попыток. Следует, однако, отметить, что при $i = 10$ число испытаний не более 2^{56}, но при $i > 100$ число испытаний сравнимо с 2^{248} и атака методом перебора ошибок веса t не имеет никаких преимуществ.

Из свойств радужной оболочки следует, что можно ввести ограничение на t сверху, положив $t = 83$. Но уже при $t = 16$ число испытаний приближается к 2^{80}. Согласно действующим прогнозам[21], криптостойкость гарантируется при разрядности ключа от 75 до 80. Это означает, что в диапазоне $10 < t \leqslant 83$ исчерпывающий перебор невозможен. Следовательно, с помощью перебора ошибок веса t можно проверить не более 9% от общего числа претендентов.

Оценим трудоемкость перебора как совокупное число двоичных операций при $t = 10$. Трудоемкость отдельного испытания определяется вычислительной сложностью шагов 2, 4 и 5. Известно, что вычислительная сложность алгоритма синдромного декодирования алгебраического кода полиномиальна по n и, как правило, не превышает $O(n^3)$. Для приведенного ранее примера кодовой конструкции сложность декодирования порядка 2^{33} двоичных операций. Сложность расшифрования по алгоритму AES порядка 2^{10} двоичных операций на 128-разрядный блок[22]. Для вычисления значения хэш-функции по алгоритму SHA-256 потребуется не более 2^{16} двоичных операций на 512-разрядный блок. Предположим, трудоемкость испытания не превышает 2^{33} двоичных операций. Тогда трудоемкость перебора ошибок веса $t = 10$ составит порядка 2^{89} двоичных операций. Если производительность испытательного устройства 100 Гбит/с, то для поиска решения методом исчерпывающего перебора при $t = 10$ понадобится не менее 10^8 лет.

---

[21] Yearly Report on Algorithms and Key Sizes (2010) // D.SPA.13 Rev. 1.0. ICT-2007-216676 ECRYPT II. 03/2010.

[22] Bertoni G., Breveglieri L., Fragneto P., Macchetti M., Marchesin S. Efficient Software Implementation of AES on 32-bit Platforms // Lect. Notes in Comp. Sci. 2003. Vol. 2523. Pp. 129–142.

Во второй главе приводятся сведения о методе шарад как эффективном способе противодействия DDoS-атаке.

Подойдем к разработке мер противодействия DDoS-атаке с позиций вычислительной трудоемкости. Воспользуемся вычислительными задачами, для которых решение может быть получено исключительно с помощью *силовой атаки*, т.е. методом проб и ошибок с исчерпывающим перебором вариантов. Назовем такие задачи *шарадами*[23].

Сервер предлагает решить шараду в ответ на запрос. Доступ к ресурсу предоставляется по факту решения шарады. При DDoS-атаке число запросов аномально велико. Это значит, что число шарад также велико. Следовательно, искусственно созданная сетевая нагрузка возвращается к атакующему в виде вычислительной нагрузки, и для достижения поставленной цели он вынужден тратить собственные ресурсы (фактор сдерживания).

Назовем *экзаменатором* того, кто создает шараду и знает её решение, а *экзаменуемым* того, кто выполняет поиск решения по заданию экзаменатора.

Сформулируем набор требований к шарадам в контексте DDoS-атаки.

A. Собственно шарады не должны быть инструментом атаки. Вычислительная трудоемкость построения шарады и проверки ее решения не должна быть чрезмерной.

B. Трудоемкость решения шарады должна быть регулируемой. Адекватная реакция на изменение сетевой нагрузки достигается настройкой трудоемкости.

C. Решение шарады возможно при наличии определенного вычислительного потенциала. Алгоритм решения должен быть задан явно. Трудоемкость отыскания решения должна быть ограничена сверху.

Некоторые шарады[24] допускают возможность отыскания решения независимыми вычислителями, причем каждый из таких вычислителей выполняет поиск в пределах некоторого подмножества претендентов, мощность которого меньше мощности исходного множества. Назовем такой подход к поиску решения *распараллеливанием*. Атакующий может воспользоваться методом распределенных вычислений. Для организации таких вычислений необходимо выполнить предварительную подготовку заданий с последующим их распределением с помощью специализированного протокола. Как только решение найдено одним из вычислителей, все остальные должны по команде прекратить обработку заданий.

[23] В англо-язычной литературе используется термин «puzzle».

[24] Brainard J., Juels A. Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks // Proc. of the ISOC Network and Distr. Sys. Sec. Symp. 1999. Pp. 151–165.

Шарады с последовательным алгоритмом решения[25] не допускают распараллеливания, но эффективно решаются при известном $\phi(n) = (q-1)(p-1)$, $n = pq$. Можно получить q и p в результате факторизации n. Алгоритм факторизации с полиномиальной трудоемкостью для квантового компьютера предложен П. В. Шором[26].

Другие шарады[27] не только эффективно решаются с помощью квантового вычислителя, но также допускают распараллеливание.

В третьей главе описаны конструкции шарад на основе кодов, исправляющих ошибки. Результаты опубликованы в работе [7].

Пусть имеется k-мерный линейный код $\mathcal{C}$ с минимальным расстоянием d. Код задан $k \times n$ порождающей матрицей G. Тогда существует кодовое слово $\mathbf{c} = \mathbf{p}G$, $\mathbf{c} \in \mathsf{ker}(\mathbf{H})$, где $\mathbf{H} - (n-k) \times n$ проверочная матрица кода $\mathcal{C}$ и $\mathbf{p}$ — информационная последовательность. Если $\mathbf{c_1}, \mathbf{c_2} \in \mathcal{C}$, то $\mathbf{c_3} = \mathbf{c_1} + \mathbf{c_2} = (\mathbf{p_1} + \mathbf{p_2})G$ и $\mathbf{c_3} \in \mathcal{C}$.

Назовем *кодовыми* шарады, построенные на основе кода $\mathcal{C}$. Код известен как экзаменатору, так и экзаменуемому.

Шарада *устойчива*, если не существует иного, менее трудоемкого способа её решения, кроме заданного по построению. Устойчивость кодовых шарад теоретически обоснована, т.к. альтернативный способ отыскания решения — декодирование по максимуму правдоподобия, а это — **NP**-трудная проблема.

Чем меньше минимальное кодовое расстояние d, тем шире диапазон трудоемкости. Очевидно, что d обратно-пропорционально размерности кода и для конструирования шарад предпочтительнее высокоскоростные коды, для которых отношение $R = k/n$ стремится к 1.

Пусть задан $[n, n-d+1, d]_q$ код Рида—Соломона (код РС) над $\mathbb{F}_q$, $q = p^m$, где p — простое число, m — положительное целое, который имеет максимально возможную размерность при заданных n и d. Тогда $d = n - k + 1$ и код может исправлять $t \leqslant \lceil (n-k)/2 \rceil$ ошибок. Известно[28], что существуют коды РС с блоковой длиной $n = q - 1$, расширенные с $n = q$ и дважды расширенные с $n = q + 1$. Это означает, что всегда можно выбрать код с четным n. Шараду на основе кода РС будем называть $RS_q(n, d)$-шарадой.

$RS_q(n, 1)$-шарада обладает максимально широким диапазоном трудоемкости, поскольку вес ошибки варьируется в интервале $n/2 \geqslant t \geqslant 1$. Шарада безусловно устойчива, т.к. $k > n/2$.

---

[25] Rivest R. L., Shamir A., Wagner D. Time-lock puzzles and timed-release crypto // Tech. Rep. MIT/LCS/TR-684. 1996.

[26] Shor P. W. Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM J. of Comp. 1997. no. 26. Pp. 1484–1509.

[27] Waters B., Juels A., Halderman A., Felten E. New Client Puzzle Outsourcing Techniques for DoS Resistance // ACM CCS. 2004. Pp. 246–256.

[28] МакВильямс Ф. Д., Слоэн Н. Дж. Теория кодов, исправляющих ошибки. Москва: Связь, 1979. 744 с.

Очевидно, что при $k \leqslant n/2$ наблюдается объективное сужение диапазона трудоемкости, т.к. вес ошибки необходимо выбирать из интервала $\lceil (d-1)/2 \rceil + \epsilon \leqslant t < k$. Если указанное ограничение на интервал не выполняется и $k < t \leqslant n/2$, то шарада неустойчива, т.к. справедливо неравенство $q^k < \sum_{i=\lceil (d-1)/2 \rceil + \epsilon}^{t} (q-1)^i \binom{n}{i}$ и трудоемкость отыскания решения будет ниже запланированной. Здесь ϵ — величина, которая обеспечивает маскировку кода с алгоритмом декодирования полиномиальной трудоемкости под код, для которого возможно только корреляционное декодирование. Для $RS_q(n,1)$-шарады $\epsilon = 0$.

Следовательно, для построения устойчивых $RS_q(n,d)$-шарад с широким диапазоном трудоемкости следует использовать коды со скоростями в интервале $0.5 < R \leqslant 1$. $RS_q(n,1)$-шарады представляются наиболее перспективными с практической точки зрения.

Отмечено, что для организации параллельных вычислений необходимо выполнить распределение заданий. Пусть шарада состоит из нескольких подшарад. Распределение заданий усложнится, если скомбинировать подшарады так, что решение каждой последующей будет зависеть от решения предыдущей. Тогда атакующий будет вынужден распределять задания для каждой подшарады (фактор сдерживания). Важно, чтобы подшарады раскрывались последовательно по мере получения промежуточных решений.

Назовем *итеративным хэшированием* преобразование вида $\psi_{l-1} = h(\underbrace{h(\ldots h(h(s))\ldots)}_{l \text{ раз}})$, где l — число итераций. Финальное значение ψ_{l-1} получается из стартового s. Совокупность значений $\psi_{l-1}, \psi_{l-2}, \ldots, \psi_0$ будем называть *хэш-цепочкой*.

Вначале зададим вес ошибки t_j для каждой из ℓ подшарад. Затем для $s \in_R \mathbb{Z}$ методом итеративного хэширования вычислим цепочку $\psi_{\ell-1}, \psi_{\ell-2}, \ldots, \psi_1, \psi_0$. Отобразим каждый ψ_i на линейное пространство размерности n над $\mathbb{F}_q$. Предположим $n = p^m$, $b = \lceil \frac{\lambda}{m \log_2 p} \rceil$, $1 \leqslant b \leqslant n$ и каждый ψ_i состоит из b q-ичных символов. В результате отображения получим $\Psi_i = 0_q^{n-b} \| \psi_i$, где 0_q^{n-b} — последовательность из $n-b$ нулевых символов поля $\mathbb{F}_q$ и $\Psi_i \in \mathbb{F}_q^n$, $0 \leqslant i \leqslant \ell - 1$.

Заданы наборы $\{\Psi_{\ell-1}, \ldots, \Psi_1, \Psi_0\}$ и $\{t_1, \ldots, t_\ell\}$. Для построения $RS_q^\ell(n,1)^*$-шарады экзаменатор выполняет следующие действия.

1. Выбирает информационную последовательность $\mathbf{p} \in_R \mathbb{F}_q^n$.
2. Сохраняет $\varphi = h(\mathbf{p})$ для проверки решения.
3. Устанавливает $j := 1$ и $\check{\mathbf{p}} := \mathbf{p}$.
4. Выбирает ошибку $\mathbf{e} \in_R \mathbb{F}_q^n$ такую, что $1 \leqslant \mathsf{wt}(\mathbf{e}) \leqslant t_j$.
5. Вычисляет $\check{\mathbf{c}} = (\check{\mathbf{p}} + \Psi_{\ell-j})G + \mathbf{e}$.

6. Устанавливает $j := j + 1$ и $\check{\mathbf{p}} := \check{\mathbf{c}}$.
7. Проверяет $j \stackrel{?}{=} \ell + 1$. При равенстве к 8, иначе к 4.
8. Передает $\{\check{\mathbf{c}}, \ell, s, (t_1, \ldots, t_\ell)\}$ экзаменуемому.

Экзаменуемый выполняет следующие действия.

1. Устанавливает $j := \ell$, $\mathbf{p} := \check{\mathbf{c}}$ и $\hbar := h(s)$.
2. Выбирает ошибку $\mathbf{e} \in \mathbb{F}_q^n$ такую, что $1 \leqslant \mathsf{wt}(\mathbf{e}) \leqslant t_j$.
3. Вычисляет сумму $\check{\mathbf{c}} = \mathbf{p} + \mathbf{e}$.
4. В результате декодирования $\check{\mathbf{c}}$ получает $\check{\mathbf{p}}$.
5. Отображает $\Psi_{\ell-j} = 0_q^{n-b} \| \hbar$.
6. Проверяет $(\check{\mathbf{p}} + \Psi_{\ell-j})G \stackrel{?}{=} \check{\mathbf{c}} + \Psi_{\ell-j}G$. При равенстве к 7, иначе к 2.
7. Устанавливает $j := j - 1$, $\mathbf{p} := \check{\mathbf{p}} + \Psi_{\ell-j}$ и $\hbar := h(\hbar)$.
8. Проверяет $j \stackrel{?}{=} 0$. При равенстве к 9, иначе к 2.
9. Предъявляет $\varphi' = h(\mathbf{p})$ в качестве решения.

Предположим, что для представления числа s в памяти достаточно λ двоичных разрядов. Тогда для хранения $RS_q^\ell(n,1)^*$-шарады потребуется зарезервировать не более $O(nm \log_2 p + \frac{\ell n m \log_2 p}{2} + \lambda)$ двоичных разрядов.

Трудоемкость отыскания решения не превышает

$$\sum_{j=1}^{\ell} \sum_{i=1}^{t_j} (q-1)^i \binom{n}{i} \tag{1}$$

испытаний.

Проанализируем $RS_q^\ell(n,1)^*$-шараду на устойчивость. Соответствующее итеративное преобразование можно представить в виде

$$\check{\mathbf{c}} = ((((\ldots((((\mathbf{p}+\Psi_{\ell-1})G+\mathbf{e}_1)+\Psi_{\ell-2})G+\mathbf{e}_2)+\ldots+\Psi_1)G+\mathbf{e}_{\ell-1})+\Psi_0)G+\mathbf{e}_\ell),$$

где $\mathbf{p}, \mathbf{e}_j \in_R \mathbb{F}_q^n$ и $\Psi_j \neq \Psi_i$ для $i \neq j$, $0 \leqslant i, j \leqslant \ell$.

Каждое кодовое слово $[n,n,1]_q$-кода располагается в центре сферы нулевого радиуса и все такие сферы не пересекаются. Число сфер равно числу кодовых слов, которое для $[n,n,1]_q$-кода совпадает с мощностью $\mathbb{F}_q^n$. Тогда произвольная ошибка веса $0 < t \leqslant n$ переводит кодовое слово $[n,n,1]_q$-кода в другое кодовое слово того же кода с единичной вероятностью и каждая подшарада $RS_q^\ell(n,1)^*$-шарады имеет единственное решение.

При заданном s несложно вычислить $\Psi_{\ell-j}$. Если $\mathbf{c} = (\mathbf{p} + \Psi_{\ell-j})G$, то в результате декодирования будет получена информационная последовательность $\mathbf{I} = \mathbf{p} + \Psi_{\ell-j}$ и уравнение вида $(\mathbf{I} + \Psi_{\ell-j})G = \mathbf{c} + \Psi_{\ell-j}G$ следует из линейности кода. По построению кодовое слово $\mathbf{c}$ маскируется ошибкой $\mathbf{e}$, $1 \leqslant \mathsf{wt}(\mathbf{e}) \leqslant t_j$ и $\hat{\mathbf{c}} = \mathbf{c} + \mathbf{e}$. Решение j-ой подшарады заключается в нахождении ошибки $\mathbf{e}$. Пусть заданы $\hat{\mathbf{c}}$, $\Psi_{\ell-j}$ и некоторая ошибка $\check{\mathbf{e}} \neq \mathbf{e}$. Для $\check{\mathbf{c}} = \hat{\mathbf{c}} + \check{\mathbf{e}}$ в результате декодирования будет получена информационная последовательность $\check{\mathbf{I}} \neq \mathbf{I}$. Решение $\check{\mathbf{e}}$ будет отвергнуто, т.к. $(\check{\mathbf{I}} + \Psi_{\ell-j})G \neq \check{\mathbf{c}} + \Psi_{\ell-j}G$.

Поскольку применяется безызбыточный код, то для j-ой подшарады существует q^n кодовых слов. При $1 \leqslant t_j \leqslant n/2$ справедливо неравенство $q^n > \sum_{i=1}^{t_j}(q-1)^i\binom{n}{i}$ и для отыскания решения исчерпывающий перебор по $\mathbf{e}$ выгоднее, чем исчерпывающий перебор по $\mathbf{p}$.

В ряде случаев экспоненциальное изменение трудоемкости не адекватно воздействию и поэтому не оправдано. Из (1) следует, что трудоемкость отыскания решения для $RS_q^{\ell}(n,1)^*$-шарады задается функцией, которая допускает гибкую настройку шага изменения трудоемкости. Очевидно, что $\binom{n}{i+1} = \binom{n}{i}\frac{n-i}{i+1}$, $1 \leqslant i \leqslant n$. Тогда при увеличении/уменьшении на единицу веса t ошибки $\mathbf{e}$ трудоемкость отыскания решения возрастает/убывает в $\frac{n-t}{t+1}$ раз. Поскольку $\binom{n}{1} = n$, то для $RS_q^{\ell}(n,1)^*$-шарады минимальный шаг изменения трудоемкости равен n.

В Заключении обобщены полученные в диссертационной работе результаты и сделаны выводы.

Основные результаты

Сформулируем основные результаты диссертационного исследования.

1. Построена абстрактная модель маскировки ключа с помощью биометрии на основе фундаментального свойства однородности образов/эталонов, полученных в результате измерений и обработки проекций биометрического объекта, учитывающая параметрические зависимости и отражающая специфический набор требований.
2. Показано, что модель отвечает сформулированным требованиям, если биометрия обладает специальными статистическими свойствами. К биометрии такого типа относится радужная оболочка глаза человека. Приведен пример кодовой конструкции.
3. Выполнен анализ криптостойкости метода «биометрической вуали». Показано, что метод гарантирует адекватный уровень практической криптостойкости.

4. Выполнен анализ метода шарад. Обозначены недостатки известных конструкций, к которым относятся возможность распараллеливания и существование эффективного квантового алгоритма решения.
5. Введен класс шарад на основе кодов, исправляющих ошибки, для которых не известен квантовый алгоритм отыскания решения с полиномиальной трудоемкостью. Показано, что такие шарады позволяют адекватно реагировать на атакующее воздействие за счет полиномиальной функции изменения трудоемкости.
6. Сконструирована итеративная кодовая шарада, которая не поддается распараллеливанию.
7. Предложена компактная итеративная кодовая шарада с плавной настройкой, обладающая устойчивостью, минимальным объемом памяти и накладными расходами при передаче по каналу связи, широким диапазоном трудоемкости.

Список публикаций

1. Чмора А. Л., Уривский А. В. Биометрическая система аутентификации / ФГУ ФИПС. Патент на изобретение, 2004. — Май 12. № 2316120.

2. Chmora A., Ourivski A. Method and Apparatus for Generating Cryptographic Key Using Biometric Data / Republic of Korea Patent Office. Republic of Korea Patent, 2005. — Mar 26. No. 10-2005-0025211.

3. Chmora A., Ourivski A. Method and Apparatus for Generating Cryptographic Key Using Biometric Data / United States Patent and Trademark Office. United States Patent, 2010. — Sep 21. No. 7,802,105.

4. Чмора А. Л. Маскировка ключа с помощью биометрии // Проблемы Передачи Информации. 2011. Т. 47, № 2. С. 131–146.

5. Чмора Андрей. Современная прикладная криптография. Москва: Гелиос, 2002. 256 с. ISBN: 5-85438-046-3.

6. Error Control, Cryptology, and Speech Compression // Workshop on Information Protection / Ed. by A. Chmora, S. B. Wicker. Lecture Notes in Computer Science. Moscow, Russia: Springer-Verlag, 1994. — Dec 6–9.

7. Чмора А. Л. Кодовые шарады // Информационно-управляющие системы. 2010. № 6. С. 47–53.

8. Chmora A., Ourivski A. Method and System for Distributed Certificate Management in Ad-hoc Networks / United States Patent and Trademark Office. United States Patent, 2008. — Jun 3. No. 7,382,762.

9. Chmora A., Urivskiy A. Method of Managing a Key of User for Broadcast Encryption / United States Patent and Trademark Office. United States Patent, 2010. — Aug 10. No. 7,774,598.

10. Urivskiy A., Chmora A., Bogachov A. et al. Method for Making Seed Value Used in Pseudo Random Number Generator and Device Thereof / United States Patent and Trademark Office. United States Patent, 2010. — Aug 10. No. 7,773,748.

11. Chmora A., Ourivski A. Light-weight Key Distribution Scheme in Wireless Network / United States Patent and Trademark Office. United States Patent, 2010. — Jun 15. No. 7,738,663.

12. Чмора А. Л., Уривский А. В., Ким В. Схема предварительного распределения ключей для кластерных сетей и способ ее функционирования / ФГУ ФИПС. Патент на изобретение, 2008. — Июль 27. № 2330382.

13. Чмора А. Л., Уривский А. В., Захаров С. В. и др. Способ и устройство формирования стартового значения для генератора псевдослучайных чисел / ФГУ ФИПС. Патент на изобретение, 2007. — Январь 20. № 2292074.

14. Уривский А. В., Чмора А. Л. Система распределения ключей и способ ее функционирования / ФГУ ФИПС. Патент на изобретение, 2008. — Июль 20. № 2329605.