БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Matsui M.* Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology – EUROCRYPT'93, Springer-Verlag, 1998. – 386 p.
2. *Popov V., Kurepkin I., Leontiev S.* Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms. – January 2006. - http://www.ietf.org/rfc/rfc4357.
3. *Saarien M.-J.* A Chosen Key Attack Against the Secret S-boxes of GOST // http://www.m.-js.com – Helsinki University of Technology, Finland.
4. *Schneier B.* Applied Cryptography, Protocols, Algorithms and Source Code in C (Second Edition). John Wiley and Sons, Inc. 1996.
5. *Oreku G.S., Li J., Pazynyuk T., Mtenzi F.J.* Modified S-box to Archive Accelerated GOST // http://paper.ijcsns.org, International Journal of Computer Science and Network Security. – June 2007. – Vol. 7, № 6.
6. *Biham E., Shamir A.* Differential Cryptanalysis of DES-like Cryptosystems, Extended Abstract, Crypto'90, Springer-Velgar, 1998. – P. 2.
7. *Birukov A., Wagner D.* Advanced Slide Attacks // http://citeseer.ist.psu.edu.
8. *Babenko L.K., Ishchukova E.A., Maro E.A.* Theory and Practice of Cryptography Solutions for Secure Information Sysmems. GOST Encryption Algorithm and Approaches to its Analysis. IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) Book Series, USA, 2013. – P. 34-62.
9. *Babenko L.K., Ishchukova E.A., Maro E.A.* Research about Strength of GOST 28147-89 Encryption Algorithm. – Proceedings of the 5th international conference on Security of information and networks (SIN 2012). – ACM, New York, NY, USA, 2012. – P. 138-142.
10. *Babenko L.K., Ishchukova E.A.* Differential Analysis of GOST Encryption Algorithm. – Proceedings of the 3rd International Conference of Security of Information and Networks (SIN 2010). – ACM, New York, NY, USA, 2010. – P. 149-157.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@fib.tsure.ru; 347928, г. Таганрог, ул. Чехова, 2, корпус "И"; тел.: 88634312018; кафедра безопасности информационных технологий; профессор.

Ищукова Евгения Александровна – e-mail: jekky82@mail.ru; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Babenko Lyudmila Klimentevna – Southern Federal University; e-mail: blk@fib.tsure.ru; Block "I", 2, Chehov street, Taganrog, 347928, Russia; phone: +78634312018; the department of security of information technologies; professor.

Ischukova Evgeniya Aleksandrovna – e-mail: jekky82@mail.ru; phone: +78634371905; the department of security of information technologies; associate professor.

УДК 681.03.245

Л.К. Бабенко, Е.А. Ищукова

ИСПОЛЬЗОВАНИЕ СЛАБЫХ БЛОКОВ ЗАМЕНЫ ДЛЯ ЛИНЕЙНОГО КРИПТОАНАЛИЗА БЛОЧНЫХ ШИФРОВ*

Работа является продолжением исследований влияния используемых слабых S-блоков на возможность проведения атаки с помощью метода линейного криптоанализа для алгоритма шифрования ГОСТ 28147-89. Ранее авторами статьи разработан универсальный алгоритм поиска блоков замены, ослабленных по отношению к методу линейного криптоа-

* Работа выполнена при поддержке грантов РФФИ №12-07-31120_мол_а, №12-07-33007_мол_а_вед, № 12-07-00037-а.

нализа. В настоящей работе рассматриваются основные подходы, которые позволяют получать наиболее эффективные линейные аналоги для алгоритма шифрования ГОСТ 28147-89. Показано, что построение аналогов осуществляется достаточно просто и может иметь различные варианты построения, которые зависят от структуры анализируемого шифра, используемого блока замены и числа раундов шифрования. Дальнейшее исследование в данной области будет направлено на решение проблемы быстрого построения линейных аналога при использовании различных наборов S-блоков. А так же на комплексную оценку устойчивости алгоритма шифрования ГОСТ и других блочных шифров, малоизученных по отношению к методу линейного криптоанализа.

Симметричные алгоритмы шифрования; анализ стойкости; сеть Фейстеля; ГОСТ 28147-89; раундовые ключи шифрования; блок замены; линейный криптоанализ.

L.K. Babenko, E.A. Ischukova

USING OF WEAK BLOCKS OF REPLACEMENT FOR LINEAR CRYPTOANALYSIS OF BLOCK CIPHERS

This work is further work on research of influence of used weak S-blocks on possibility of carrying out attack by means of a method of linear cryptoanalysis for algorithm of enciphering of GOST 28147-89. Earlier authors of article developed universal algorithm of search of replacement blocks weakened in relation to a method of linear cryptoanalysis. In the given work the main approaches which allow to receive the most effective linear analogs for algorithm of enciphering of GOST 28147-89 are considered. It is shown that, creation of analogs is carried out rather simply and can have various options of construction. Further research in this field will be directed on a solution of the problem of fast construction of linear analog using various sets of S-blocks. And also on a complex assessment of strength of GOST enciphering algorithm and other block codes low-studied in relation to a method of linear cryptoanalysis.

GOST; S-Box; secret key; linear cryptanalysis; probability.

Метод линейного криптоанализа, впервые был предложен М. Матсуи для анализа алгоритма DES [1], базируется на составлении линейных аналогов, которые с некоторой вероятностью описывают работу криптоалгоритма. Исследование направлено на изучение стойкости к методу линейного криптоанализа алгоритма ГОСТ, определенного в качестве государственного стандарта в Российской Федерации. Его использование обязательно для шифрования данных в государственных организациях РФ. Алгоритм ГОСТ является симметричным блочным шифром, построенным по схеме Фейстеля (Feistel). На вход алгоритма поступает 64-битовый блок данных, который под воздействием 256-битового ключа преобразуется в 64-битовый блок шифрованных данных. В каждом раунде правая часть шифруемого сообщения поступает на вход функции F, где преобразуется с использованием трех криптографических операций: сложения данных с раундовым подключом по модулю 2^{32}, замена данных с использованием S-блоков, циклический сдвиг влево на 11 позиций. Выход функции F складывается по модулю 2 с левой частью шифруемого сообщения, после чего правая и левая части меняются местами. Алгоритм содержит 32 раунда, в последнем раунде шифрования правая и левая части местами не меняются. В [2] был предложен, реализован и опробован алгоритм, позволяющий получать для алгоритма ГОСТ слабые блоки в отношении линейного криптоанализа. В результате проведенного эксперимента получены различные варианты заполнения для блоков замены, один из которых представлен в [2]. Для данного блока замены была получена таблица анализа, отражающая возможность построения линейных аналогов для линейного криптоанализа [2].

Нахождение эффективных уравнений для анализа алгоритма с использованием метода линейного криптоанализа. Следующим шагом после получения слабых блоков замены, является проверка того факта, будет ли алгоритм ГОСТ уязвим, если в его составе будет присутствовать подобный S-блок. Для того,

чтобы ответить на данный вопрос, будем рассматривать возможность проведения анализа поэтапно, двигаясь от простого к сложному. Введем несколько упрощений. Будем рассматривать алгоритм ГОСТ, в котором все восемь S-блоков будут работать в соответствии с найденным нами слабым блоком заметы [2]. В алгоритме ГОСТ присутствует операция целочисленного сложения по модулю 2^{32}, которая накладывает свои ограничения на определение вероятности при построении линейного аналога. В рассматриваемой нами версии заменим данную операцию на операцию сложения по модулю 2.

Для начала рассмотрим три раунда шифрования. Рассмотрим восьмой S-блок. Для построения аналога будем использовать пару векторов (1, 8), что следует из таблицы анализа в [2]. В данном случае на вход блока замены поступит 32 бит сообщения, сложенный с 32 битом первого подключа. После прохождения через S-блок, мы ожидаем получить на выходе бит 29, который, после смещения на 11 позиций влево, окажется в позиции номер 18 (рис. 1). Для трех раундов шифрования воспользуемся приемом, предложенным М. Матсуи [1] (рис. 2). Пусть на вход функции F i-го раунда шифрования поступает значение XRi, на выходе функции F i-го раунда шифрования образуется значение XLi. Используемый бит для значений XRi и XLi будем заключать в квадратные скобки. Составим уравнения для первого и третьего раунда шифрования на основе выбранной пары векторов

$$XR1[32] \oplus YL1[18] = K1[32]; \quad (1)$$

$$XR3[32] \oplus YL3[18] = K3[32]. \quad (2)$$

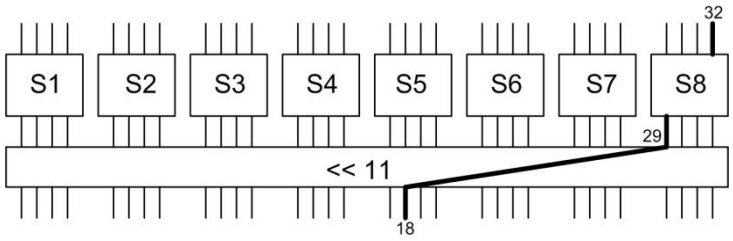

Рис. 1. Преобразование входного бита

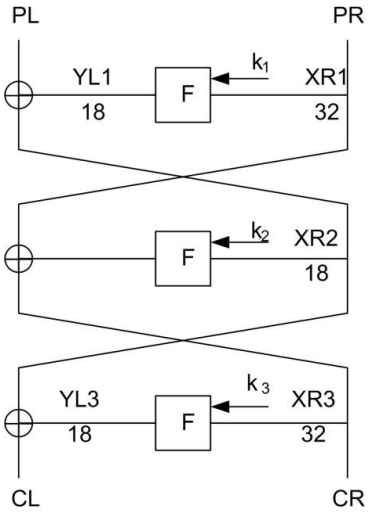

Рис. 2. Анализ раундов

Заменим в уравнениях (1) и (2) значения XR1 и XR3 соответственно на известные значения входного сообщения PR и выходного сообщения CL. Также представим YL1 как сумму значений PL и XR2: YL1[18] = PL[18] ⊕ XR2[18]. Аналогичным образом представим YL3 как сумму значений CL и XR2: YL3[18] = CL[18] ⊕ XR2[18]. Тогда вместо уравнений (1) и (2) получим уравнения:

$$PR[32] \oplus PL[18] \oplus XR2[18] = K1[32]; \quad (3)$$

$$CL[32] \oplus CL[18] \oplus XR2[18] = K3[32]. \quad (4)$$

Сложив между собой уравнения (3) и (4) получим итоговое уравнение для 3-раундового алгоритма ГОСТ:

$$PR[32]\oplus PL[18]\oplus CL[32]\oplus CL[18] = K1[32]\oplus K3[32]. \quad (5)$$

В уравнении (5) для 3-раундового алгоритма ГОСТ известны все составляющие в левой части уравнения Определим вероятность, с которой будет выполняться данный аналог. Рассмотрим определение вероятности для объединенного линейного аналога в общем виде. Пусть имеется два линейных аналога: Q1 и Q2. Для первого линейного аналога вероятность того, что значение Q1 равно нулю, равна p1 = p(Q1=0). Для второго линейного аналога вероятность того, что значение Q2 равно нулю, равна p2 =p(Q2=0). Тогда для первого аналога вероятность того, что значение Q1 равно единице, равна:

$$p3=p(Q1=1) = 1 – p(Q1=0)= 1 – p1.$$

Для второго аналога вероятность того, что значение Q2 равно единице, равна:

$$p4 = p(Q2=1) = 1 – p(Q2=0) = 1 – p2.$$

При объединении двух аналогов получаем третий аналог Q3 = Q1 ⊕ Q2. Необходимо определить какова вероятность того, что Q3 = 0. Значение Q3 может быть равно нулю в двух случаях: когда Q1 и Q2 равны нулю, либо когда Q1 и Q2 равны единице. Таким образом, получаем:

$$p(Q3 = 0) = p(Q1=0)*p(Q2=0) + p(Q1=1)* p(Q2=1) = p1p2 + p3p4 = p1p2 +$$
$$+(1– p1)(1 – p2) =p1p2 + 1 – p1 – p2 + p1p2 =1 – p1 – p2 + 2p1p2. \quad (6)$$

Если же аналоги Q1 и Q2 выполняются с одинаковой вероятностью, то есть если p1 = p2 = p, то выражение (6) принимает вид:

$$p(Q3 = 0) = 1 – 2p + 2p^2. \quad (7)$$

В рассмотренном случае для трех раундов алгоритма ГОСТ оба аналога в соответствии с [2] имели вероятность p=0 (напомним, что в данном случае мы пока рассматриваем сложение данных с ключом по модулю 2, которое не оказывает влияния на определение вероятности, таким образом вероятность аналога определяется только исходя из таблицы анализа [2]. В результате итоговая вероятность аналога в соответствии с (11) будет равна единице (p = 1).

Теперь рассмотрим построение аналога для пяти раундов шифрования (рис. 3). Так как третий раунд не будет являться последним, то нельзя будет произвести замену значений YL3 и XR3 на известные значения выходов CL и CR. В данном случае для получения трехраундового аналога объединим уравнения (3) и (4), где в уравнении (4) заменим YL3[18] на XR4[18] ⊕ XR2[18]. Получим:

$$PR[32]\oplus PL[18]\oplus XR3[32]\oplus XR4[18]=K1[32]\oplus K3[32]. \quad (8)$$

Ранее определено, что вероятность аналога (8) будет равна единице (p=1). Мы получили в аналоге (8) два неизвестных значения XR3[32] и XR4[18]. Теперь надо для следующих раундов построить аналоги таким образом, чтобы эти значения сократились. Для того, чтобы сократилось значение XR3[32] необходимо для 4 раунда подобрать такую пару векторов, чтобы на выходе функции F был задействован 32-й бит. Так как выход функции F получается в результате циклического сдвига выходов S-блоков влево на 11 позиций, то 32 бит на выходе F функции на самом деле является третьим битом на выходе S3 блока замены (рис. 3).

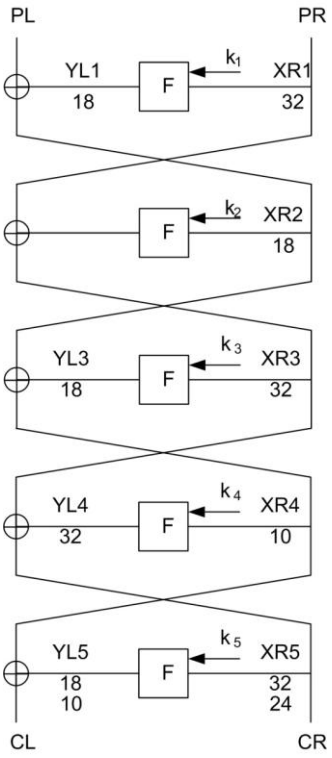

Рис. 3. Анализ 5 раундов

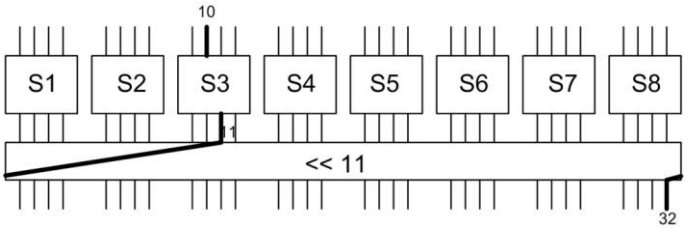

Рис. 4. Преобразование входного бита для анализа 5 раундов

В соответствии с таблицей анализа [2], для того чтобы получить такой выход, необходимо использовать входной вектор, равный 4, что соответствует задействованию 10-го бита входного сообщения XR. Таким образом, для 4 раунда будет использован аналог

$$XR4[10] \oplus XR3[32] \oplus XR5[32] = K4[10]. \quad (9)$$

Объединив уравнения (8) и (9), получим

$$PR[32] \oplus PL[18] \oplus XR4[10] \oplus XR5[32] \oplus XR4[18] = K1[32] \oplus K3[32] \oplus K4[10]. \quad (10)$$

Вероятность итогового 4-раундового аналога определим в соответствии с формулой (6), и получим p=0.

Далее, в пятом раунде рассмотрим сразу два аналога для того, чтобы исключить из (10) значения XR4[10] и XR4[18]. Как и выше, определим каким образом можно получить данные значения на выходе 5 раунда шифрования (рис. 5). Построим аналоги для 5 раунда шифрования:

$$XR5[32] \oplus XR4[18] \oplus XR6[18] = K5[32]; \quad (11)$$

$$XR5[24] \oplus XR4[10] \oplus XR6[10] = K5[10]. \quad (12)$$

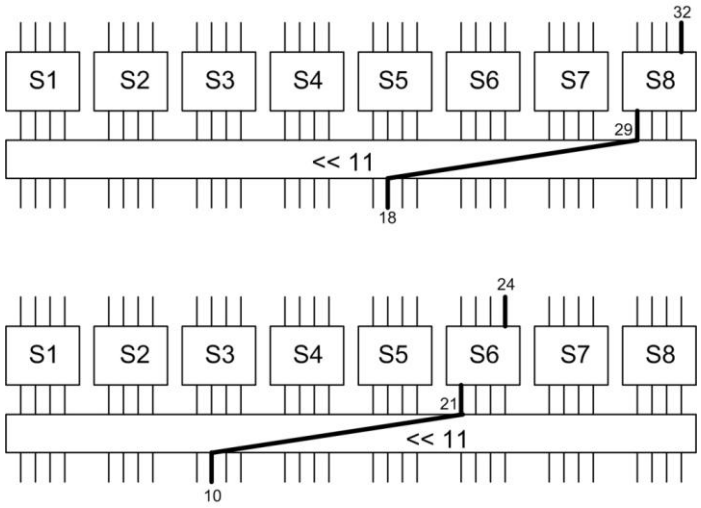

Рис. 5. Преобразование входного бита для анализа 7 раундов

Объединив уравнения (10), (11) и (12), получим итоговый аналог для 5 раундов шифрования, который в соответствии с (6) будет выполняться с вероятностью p = 0.

$$PR[32]\oplus PL[18]\oplus XR6[18] \oplus XR5[24] \oplus XR6[10]=$$
$$= K1[32]\oplus K3[32] \oplus K4[10] \oplus K5[32] \oplus K5[10]. \quad (13)$$

Если рассматривать 5 раунд в качестве последнего раунда шифрования, то можно произвести замену значений XR6 и XR5 соответственно на известные выходные значения CL и CR. Тогда выражение (13) преобразуется к виду:

$$PR[32]\oplus PL[18]\oplus CL[18] \oplus CR[24] \oplus CL[10]=$$
$$= K1[32]\oplus K3[32] \oplus K4[10] \oplus K5[32] \oplus K5[10]. \quad (14)$$

В левой части выражения (14) использованы известные значения входа и выхода, вероятность аналога равна нулю.

Аналогичным образом можно перейти к рассмотрению 8 раундов алгоритма шифрования ГОСТ (рис. 6). На рис. 7 показано соответствие ранее не рассмотренных входных и выходных значений для функции F. В результате будут использованы следующие линейные аналоги (все отдельно взятые аналоги в соответствии с таблицей анализа [2] выполняются с вероятностью p=0).

Для шестого раунда

$$XR6[29] \oplus XR5[24] \oplus XR7[24] = K6[29]. \quad (15)$$

Для седьмого раунда

$$XR7[12] \oplus XR6[29] \oplus XR8[29] = K7[12]; \quad (16)$$

$$XR7[32] \oplus XR6[18] \oplus XR8[18] = K7[32]; \quad (17)$$

$$XR7[24] \oplus XR6[10] \oplus XR8[10] = K7[24]. \quad (18)$$

Для восьмого раунда

$$XR8[10] \oplus XR7[32] \oplus XR9[32] = K8[10]; \quad (19)$$

$$XR8[21] \oplus XR7[12] \oplus XR9[12] = K8[21]. \quad (20)$$

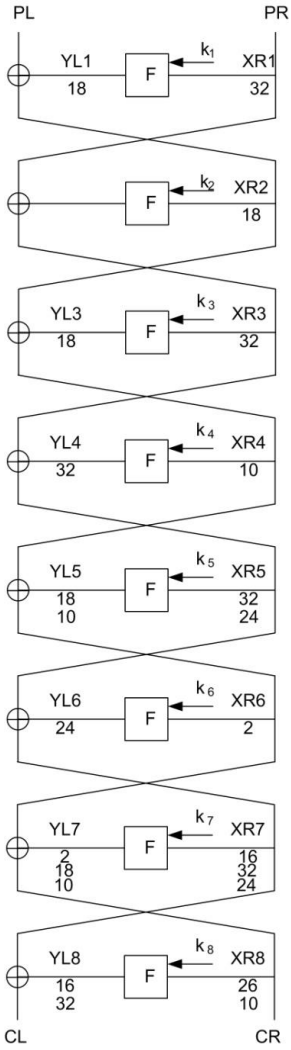

Рис. 6. Анализ 8 раундов

Объединив выражение (13) с выражениями (15)–(20), а также заменив значения XR8 и XR9 соответственно на известные выходные значения CR и CL, получим:

$$PR[32] \oplus PL[18] \oplus CR[29] \oplus CR[18] \oplus CL[32] \oplus CR[21] \oplus CL[12] =$$
$$= K1[32] \oplus K3[32] \oplus K4[10] \oplus K5[32] \oplus K5[10] \oplus K6[29] \oplus K7[12] \oplus$$
$$\oplus K7[32] \oplus K7[24] \oplus K8[10] \oplus K8[21]. \quad (21)$$

Выражение (21) является результирующим аналогом для 8 раундов рассматриваемого алгоритма шифрования ГОСТ и выполняется с вероятностью p=0.

Как можно видеть, построение аналогов осуществляется достаточно просто и может иметь различные варианты построения. Аналогичная ситуация будет сохраняться и при анализе алгоритма ГОСТ, в котором используется 8 разных блоков замены при том условии, что все эти блоки являются слабыми по отношению к линейному криптоанализу.

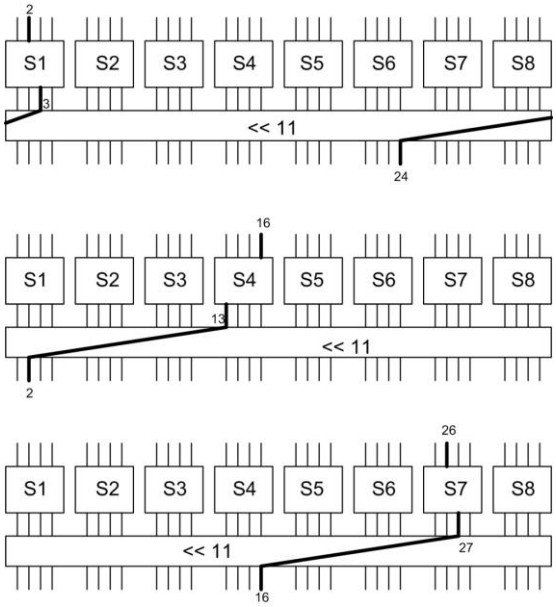

Рис. 7. Преобразование входного бита для анализа 8 раундов

Выводы. Представлен алгоритм построения эффективных линейных статистических аналогов на основе использования слабых блоков замены по отношению к линейному криптоанализу для алгоритма ГОСТ 28147-89. Работа данного алгоритма проверена на примере использования алгоритма шифрования ГОСТ 28147-89, для которого это представляет особую актуальность в связи с использованием нефиксированных S-блоков.

В результате исследования получен универсальный инструмент для быстрого определения полного списка слабых блоков по отношению в линейному криптоанализу, который может быть, например, использован при разработке новых алгоритмов шифрования. Во-вторых, при использовании данного алгоритма можно легко получить полный список блоков, не рекомендованных к использованию для алгоритма ГОСТ, что может быть полезно для тех, кто пользуется данным шифром, но не владеет навыками криптоанализа.

Дальнейшее исследование в данной области будет направлено на решение проблемы быстрого построения линейных аналога при использовании различных наборов S-блоков, а так же на комплексную оценку устойчивости алгоритма шифрования ГОСТ и других блочных шифров, малоизученных по отношению к линейному криптоанализу.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Matsui M.*, Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology – EUROCRYPT'93, Springer-Verlag, 1998. – 386 p.
2. *Бабенко Л.К., Ищукова Е.А*. Анализ алгоритма ГОСТ 28147089: поиск слабых блоков // Известия ЮФУ. Технические науки. – 2014. – № 2 (151). – С. 129-138.
3. *Babenko L.K., Ishchukova E.A., Maro E.A.* Theory and Practice of Cryptography Solutions for Secure Information Sysmems. GOST Encryption Algorithm and Approaches to its Analysis. IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) Book Series, USA, 2013. – P. 34-62.

4. *Babenko L.K., Ishchukova E.A., Maro E.A.* Research about Strength of GOST 28147-89 Encryption Algorithm. – Proceedings of the 5th international conference on Security of information and networks (SIN 2012). – ACM, New York, NY, USA, 2012. – P. 138-142.
5. *Babenko L.K., Ishchukova E.A.* Differential Analysis of GOST Encryption Algorithm. – Proceedings of the 3rd International Conference of Security of Information and Networks (SIN 2010). – ACM, New York, NY, USA,2010. – P. 149-157.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@fib.tsure.ru; 347928, г. Таганрог, ул. Чехова, 2, корпус "И"; тел.: 88634312018; кафедра безопасности информационных технологий; профессор.

Ищукова Евгения Александровна – e-mail: jekky82@mail.ru; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Babenko Lyudmila Klimentevna – Southern Federal University; e-mail: blk@fib.tsure.ru; Block "I", 2, Chehov street, Taganrog, 347928, Russia; phone: +78634312018; the department of security of information technologies; professor.

Ischukova Evgeniya Aleksandrovna – e-mail: jekky82@mail.ru; phone: +78634371905; the department of security of information technologies; associate professor.

УДК 681.3.06

А.В. Бессалов, А.А. Дихтенко, О.В. Цыганкова

ПЛОТНОСТЬ КАНОНИЧЕСКИХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ СО СВОЙСТВОМ ИЗОМОРФИЗМА К ФОРМЕ ЭДВАРДСА

Кривые в форме Эдвардса наиболее интересны с точки зрения практических приложений. Удобство программирования и рекордная производительность – главные преимущества кривых данного класса перед прочими известными формами представления эллиптических кривых. В работе поставлена задача определения точного числа канонических кривых изоморфных кривым Эдвардса над простым полем. Для ее решения предложен прием, основанный на замене параметров (a, b) канонической кривой парой параметров (a, c), где c – единственный в поле корень кубического уравнения. Таким образом, найдены условия существования канонических кривых, изоморфных кривым в форме Эдвардса над простым полем. Также доказаны две леммы в теории квадратичных вычетов, построенной на схеме Гаусса. На основе полученных условий и доказанных лемм приведены точные формулы расчета числа эллиптических кривых с ненулевыми параметрами a и b, изоморфных кривым Эдвардса. Доказано, что для больших полей плотность таких кривых близка к 0,25.

Каноническая эллиптическая кривая; кривая Эдвардса; кривая кручения; параметры кривой; изоморфизм; квадратичный вычет; квадратичный невычет.

A.V. Bessalov, A.A. Dikhtenko, O.V. Tsygankova

DENSITY OF THE CANONICAL ELLIPTIC CURVES HAVING A PROPERTY OF THE ISOMORPHISM TO AN EDWARDS FORM

Edwards curves are the most interesting in terms of practical applications. The ease of programming and the best performance are their main advantages before other known forms of elliptic curves representation. A problem of determining the precise number of canonical elliptic curves which are isomorphic to Edwards curves over a prime field is posed in the paper. An approach is proposed by authors in order to solve the problem. The approach is based on substitution of canonical curve parameters (a, b) by a parameters pair (a, c), where c – is the cubic equation unique root in a field. As a result the conditions for existence canonical curves isomorphic to