УДК 519.72:003.26

ОДНОНАПРАВЛЕННЫЕ ФУНКЦИИ С ИНФОРМАЦИОННО НЕВЫЧИСЛИМОЙ ЛАЗЕЙКОЙ

А.М. КУДИН

Рассматривается текущее состояние исследований в области построения однонаправленных функций и однонаправленных функций с лазейкой. Предлагается подход к построению однонаправленных функций с лазейкой, в котором лазейка неоднозначно связана с параметром функции и результатом вычисления функции.

Ключевые слова: теоретико-информационная стойкость криптосистем, стойкость асимметричных криптосистем, односторонние функции в криптографии, односторонние функции с потерей информации, общая теория оптимальных алгоритмов.

ВВЕДЕНИЕ

Одновременно с появлением идеи и первых реализаций принципа асимметричной криптографии начались исследования существования формального доказательства стойкости этих криптосистем к криптоанализу [1-15]. В отличие от симметричной криптографии, где существует прямая связь меры информативности шифртекста о ключе (открытом сообщении) [13] и криптографическими преобразованиями, в асимметричных криптосистемах эта статистическая мера информации с шифрующим преобразованием напрямую не связана. Достаточно быстро были установлены проблемы со стойкостью асимметричных криптосистем, следующих из этого факта: нестойкость систем при зашифровании источников открытого текста с малой энтропией, наличия информации об открытом тексте в шифртексте, вычислимой за полиномиальное время, алгоритмическая различимость за полиномиальное время шифртекстов, полученных от разных открытых текстов (для одного ключа зашифрования) [5]. Также было доказано [2] сводимость первых двух проблем к третьей и предложена новая концепция стойкости асимметричных криптосистем – концепция вероятностного шифрования, являющаяся вариантом применения метода рандомизации открытого текста перед зашифрованием. Стойкость при этом оценивалась через невозможность для вероятностного полиномиального алгоритма распознавания различных открытых текстов, соответствующих заданному шифртексту. Для введенного определения стойкости (в дальнейшем получившего абривиатуру PI (Polynomial Indistinguishability) стойкости) была получена нижняя граница увеличения длины открытого текста при рандомизации [4]. Недостатком данного подхода к оценке стойкости являлась сложность введения количественной меры, который удалось преодолеть, введя понятие семантической стойкости (абривеатура S (SemanticSecurity)) через модели теории игр. Количественной мерой стало так называемое «преимущество противника», определяемое через модуль разности вероятности случайного угадывания открытого текста и угадывания открытого текста по имеющимся шифртексту и открытому ключу. Дальнейшие исследования позволили установить взаимосвязь между обоими определениями и рассматривать стойкость относительно выбранного открытого текста (абривиатура CPA-стойкость (chosen plaintext security)). При этом оставалась проблема существования множества шифртекстов, для которых система не обеспечивала достаточную стойкость, т.е. определение стойкости было неравномерным относительно множества шифртекстов.

Более строгое и общее определение стойкости было введено относительно адаптивно выбранного шифртекста (абривиатура CCA-стойкость (chosen cipher text security)). Последнее определение позволило на основе вычислительной модели со случайным оракулом вплотную приблизиться к решению вопроса о существовании формального доказательства стойкости криптосистем «почти для всех» шифртекстов.

Все вышеперечисленные определения (PI, S, CPA, CCA-стойкости) оставались формальными моделями, не связанными напрямую с методами построения новых асимметричных криптосистем, удовлетворяющих этим определениям стойкости. Основной причиной этого явилось пересмотр не самого подхода к построению однонаправленных функций с лазейкой (ОДФЛ), а изменения структуры криптосистем. Заметим, что особенно характерно это проявилось при изучении стойкости криптосистем и протоколов типа «протоколов с неполным или нулевым разглашением секрета» [5]. Следствием этого явились появление новых моделей стойкости и требований к асимметричным криптографическим преобразованиям [3,4,6] (требования не сохранения гомоморфизма на множестве шифртекстов, требования анонимности ключа и т.п.) без пересмотра требований к ОДФЛ. Одной из первых идей, пересматривающими само построения ОДФЛ, явилась идея отказа от инъективности функции зашифрования, а также предложенные на этой основе ОДФЛ с потерей информации [8], вычислительная модель стойкости, основанная на использовании общей теории оптимальных алгоритмов [9-14].

В данной статье рассматриваются подходы к построению однонаправленных функций

с лазейкой для асимметричных криптосистем, стойких в теоретико-информационном смысле. Анализируются известные методы односторонних функций с лазейкой с потерей информации [8,16] и однонаправленные функции с информационно неопределенной лазейкой, предложенные автором [9-14].

1. КЛАССИЧЕСКИЕ ПОНЯТИЯ ОДНОСТОРОННИХ ФУНКЦИЙ И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

Введем некоторые определения, нужные для дальнейшего изложения.

Определение 1. Честная функция – функция $f:\{0,1\}^n \to \{0,1\}^{m(n)}$, если $n \le q(m(n))$, где $q(x)$ некоторый полином степени не выше k_0, для всех n. Степень полинома определяется вычислительными возможностями противника.

Определение 2.

Функция $\nu:\mathbb{N}\to\mathbb{R}$ называется «пренебрежимо малой функцией», если для $\forall c \ge 0$ существует k_c такое, что $\nu(k) < k^{-c}$ для всех $k \ge k_c$.

Определение 3.

Сильной односторонней функцией называется честная функция $f:\{0,1\}^n \to \{0,1\}^{m(n)}$, если:

1) Существует вероятностный алгоритм полиномиальной вычислительной сложности, вычисляющий $f(x)$ для $\forall x \in \{0,1\}^n$

2) для любого вероятностного алгоритма полиномиальной вычислительной сложности A существует пренебрежительно малая функция, что для всех $n \ge n_0$

$$P(f(z)=y; x \xleftarrow{R} \{0,1\}^n; y \leftarrow f(x); z \leftarrow A(1^n; y)) < \nu_A(n).$$

Определение 4.

Слабой односторонней функцией называется честная функция $f:\{0,1\}^n \to \{0,1\}^{m(n)}$, если:

1) Существует вероятностный алгоритм полиномиальной вычислительной сложности, вычисляющий $f(x)$ для $\forall x \in \{0,1\}^n$

2) для любого вероятностного алгоритма полиномиальной вычислительной сложности A существует полином p такой, что для всех $n \ge n_0$

$$P(f(z)\ne y; x \xleftarrow{R} \{0,1\}^n; y \leftarrow f(x); z \leftarrow A(1^n; y)) \ge 1/p(n).$$

Пример – умножение на множестве целых чисел (с обратной функцией факторизации). Грубая оценка доли чисел, являющихся произведением двух простых чисел приблизительно равного размера – $1/k^2$ (исходя из приблизительной вероятности того, что число длиной k бит будет простым $O(1/k)$).

Вообще говоря, имеет смысл говорить о семействе (множестве) односторонних функций с параметром длины входа, т.к. на практике конкретная длина входа зависит от возможностей вычисления обратной функции. Вместо определения множества функций можно определить адаптивный (в простейшем случае зависящий от размера входа) алгоритм вычисления обратной функции. Разница между двумя определениями в том, что для слабой односторонней функции мы требуем существования только некоторой не пренебрежительно малой части входов, на которых трудно вычислить обратную функцию. Для сильной требуем трудности вычисления обратной функции для всех, кроме незначительной части входов.

При этом существование слабых односторонних функций необходимо и достаточно для существования сильных. Кроме этого, известен простой метод [2], позволяющий строить сильные односторонние функции из слабых:

Пусть $f_1(x_1 \dots x_N) = f(x_1) \| \dots \| f(x_N)$ – сильная односторонняя функция, если $N = 2kp(k)$, $\forall x_i$ длиной k и $f(x_i)$ – слабые односторонние функции.

Заметим, что доказательство справедливо только для последовательной модели вычислений и только если информация, полученная при вычислении функции от одного аргумента не используется для вычислении функции от другого аргумента.

Определение 5.

Неравномерной (non-uniform) односторонней функцией называется функция

$f:\{0,1\}^n \to \{0,1\}^{m(n)}$, если:

1) Существует вероятностный алгоритм полиномиальной вычислительной сложности, вычисляющий $f(x)$ для $\forall x \in \{0,1\}^n$

2) для любого полиномиального по памяти алгоритма A и любого полинома q и всех $n > n_0$

$$P(f(z)\ne y; x \xleftarrow{R} \{0,1\}^n; y \leftarrow f(x); z \leftarrow A(y)) \ge 1/q(n).$$

Заметим, что поскольку для инвертирования функции используется алгоритм, полиномиальный по используемой памяти, то требования честности функции можно опустить.

Можно показать, что неравномерная односторонняя функция является сильной односторонней функцией.

Возможно, но не очень вероятно, что существует сильная односторонняя функция, которая не является неравномерной односторонней функцией.

2. ПОСТАНОВКА ЗАДАЧИ

Односторонние функции в криптографии рассматриваются под углом теории алгоритмов: не должно существовать эффективного в среднем (вероятностного) алгоритма криптоанализа по времени, но не по точности [14]. С другой стороны рассматривается недостаточность взаимной информации (даже уже в смысле Колмогорова) для восстановления одного слова по другому. Необходимо показать, что учет количества информации по Колмогорову об аргументе одностороннего криптографического преобразования с лазейкой позволяет увеличить эффективность криптосистемы, или с точки зрения «расширения» аргумента (увеличения его длины или с точки зрения длин ключей).

Такая постановка задачи связана с оценкой зависимости вида обратной функции от входных данных и оценки алгоритма вычисления обратной функции в случае **неравномерного** распределения входов. Вероятность успеха этого алгоритма зависит от распределения входов.

Фактически задача сводится к анализу распределения прообразов односторонней функции. При этом граничным случаем является равномерное распределение открытого текста (в случае его рандомизации или без избыточного кодирования). Но это является тривиальным случаем, поскольку при равномерном распределении открытого текста легко получить теоретико-информационную стойкость. С другой стороны, данный случай рассматривать не нужно, т.к. законный получатель тоже не получит никакой информации даже расшифровав сообщение. Естественно также не рассматривать случай, когда метод кодирования или параметры рандомизации являются долговременным ключом.

3. ОДНОСТОРОННИЕ ФУНКЦИИ С ПОТЕРЕЙ ИНФОРМАЦИИ

В модели lossy trapdoor function [8] (функции с потерей информации) неопределенность все равно вносится в открытый текст (функция становится не инъективной) путем предварительного шифрования (линейного, путем умножения на матрицу), а не в само шифрующее преобразование, как в вычислительной модели стойкости.

Основные отличия – 1) это конструкция «черного ящика» более эффективная, чем общая парадигма неинтерактивных нулевых знаний 2) эта конструкция позволяет строить стойкие в смысле атак по выбранному шифртексту (англ. CCA) криптосистемы основанные на **наихудшем случае** проблемы решеток.

Проблема в том, что достижения семантической стойкости в стандартной модели требуется внешний источник случайности (независимый от шифруемого сообщения). Главная проблема в том, что для инвертирования обратной функции требуется полный вход (т.е. случайность и шифртекст), а для расшифрования желательно, чтобы было достаточно только шифртекста. Интуитивно чувствуется, что нужна более сильная конструкция, чем семантическая стойкость. ОДФЛ с потерей информации (ОДФЛПИ) ведет себя одним из двух способов (неотличимых вероятностным полиномиальным алгоритмом друг от друга): первый – обычный, второй – размер образа существенно меньше, чем прообраза (например, размер входа n, размер образа $n/2$). Пусть

$$x \xleftarrow{random} \{0,1\}^n,\ c=(c_1,c_2)=(f(x),m\oplus h(x)).$$

Здесь $h(x)$ – ядро односторонней функции $f(x)$. Расшифрование: $m=c_2\oplus h\left(f^{-1}(c_1)\right)$.

Практически криптосистемы на основе ОДФЛПИ отличаются от предыдущих конструкций с рандомизацией открытого текста (например, вычислительной модели стойкости) фактически только тем, что открытый текст **не участвует в асимметричном шифровании**: практически вместо шифрования текста с помощью лазейки вырабатывается общая шифрующая гамма (или приводится к одному состоянию генератор псевдослучайной последовательности). При этом, поскольку размерность входных данных для генератора может быть меньшей, чем выхода, то при обратная функция является не инъективной, т.е. создается информационная неопределенность открытого текста и шифртекста.

Для реализациообщей схемы (framework) ОДФЛ с потерей информации можно использовать любую семантически стойкую криптосистему, обладающую несколькими специальными свойствами. Первое из таких свойств – система должна быть аддитивно гомоморфной, (*т.е. шифрование должно сохранятьоперацию сложения двух открытых текстов, т.е.* $(M_1\circ M_2\to C_1+C_2)$. Открытый текст рассматривается как n мерный вектор, перед шифрованием происходит предварительное кодирование ОТ («расширение ОТ») путем умножения его на матрицу ($M\cdot x$). Матрица должна быть обратимой, также выполняется ($I\cdot x=x$), для инъективной функции матрица ненулевая, для ОДФЛ с потерей информации – матрица нулевая. Дополнительно к этому криптосистема обладает двумя свойствами: остается стойкой при повторном использовании случайности для разных ключей, во-вторых гомоморфная операция изолирует случайность (т.е. случайность входного шифртекста зависит только от случайности выходного шифртекста). Концепция ОДФЛПИ может быть реализована на основании варианта системы Эль-Гамаля. Напомним, что зашифрование в криптосистеме Эль Гамаля при открытом ключе $h=\alpha^z \bmod p$ и секретном z осуществляется следующим образом: $r\in_R[1,p-1], c_1=\alpha^r \bmod p, c_2=x\cdot h^r \bmod p$. Обозначим как $E_h(x,r)$ зашифрование x при выбранном открытом ключе и случайном $r\in_R\{0,1\}$.

Расшифрование – $x=c_2\cdot(c_1^{\,z})^{-1} \bmod p$.

Вариант криптосистемы Эль-Гамаля, рассматриваемый в ОДФЛПИ отличается процессами зашифрования и расшифрования, а именно– зашифрование $c_1=\alpha^r \bmod p, c_2=\alpha^x\cdot h^r \bmod p$, расшифрование $x=\log_\alpha(c_2/c_1^{\,z})$. Здесь в качестве входных данных принимаются биты $x=\{0,1\}$ (или другой «небольшой» размер входных данных), поэтому вычисление дискретного логарифма производится путем простого перебора. Хорошо известно, что данный вариант криптосистемы обладает S стойкостью при условии сложности задачи распознавания Диффи-Хеллмана (DDH). Эта система является также аддитивно гомоморфной относительно операции:

$$E_h(x,r)\circ E_h(x',r')=E_h(x+x',r+r')$$

где операция $\circ$ означает покоординатное умножение шифртекстов и уязвимой относительно добавления величины $v\in Z_p$ даже без знания

открытого ключа. Рассмотренное определение односторонних функций с лазейкой и потерей информации не учитывает возможность введения неоднозначности (нарушение свойства инъективности отображения) в зависимость лазейки и открытых параметров для вычисления функции. Поэтому ниже рассматривается идея построения ОДФЛ, в которых алгоритм вычисления обратной функции без лазейки не просто **не реализуется вероятностным алгоритмом полиномиальной сложности**, **но не существует**.

4. ОДНОНАПРАВЛЕННЫЕ ФУНКЦИИ С ИНФОРМАЦИОННО НЕОПРЕДЕЛЕННОЙ ЛАЗЕЙКОЙ

Введем следующие обозначения. Пусть заданы множества X, Y. Пусть 2^Y – класс всех подмножеств множества Y. В работе [12] рассматривается оператор $S: X \times R_+ \to 2^Y$, где $R_+ = [0,\infty)$, называемый оператором решения и обладающий двумя свойствами:

$$S(x,0) \neq \varnothing, \forall x \in X,$$

$$\delta_1 \le \delta_2 \Rightarrow S(x,\delta_1) \subset S(x,\delta_2), \ \forall \delta_1, \delta_2 \in R_+, x \in X.$$

Для заданного $\varepsilon \ge 0$ элемент $y \in Y$, удовлетворяющий условию $y \in S(x,\varepsilon)$ называется ε – приближением. Задача поиска ε – приближения рассматривается при условии отсутствия полной (и, в общем случае точной) информации об элементе x, о котором известна некоторая информация $N(x)$, где: $N: X \to Y$ – информационный оператор в терминологии общей теории оптимальных алгоритмов, а Y – образ множества X. Зная $N(x)$ необходимо найти ε – приближение к x (рис. 1).

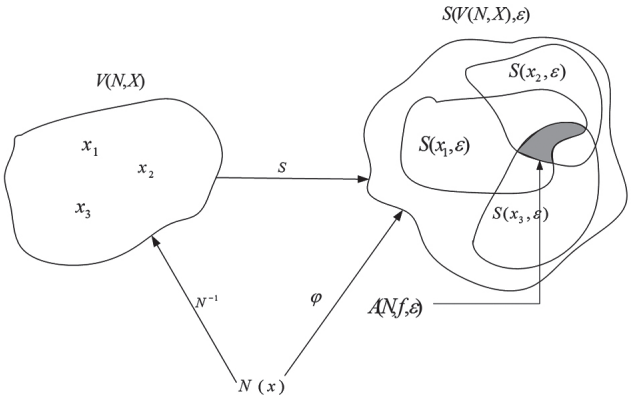

Рис. 1. Информационный оператор и оператор решения

Если множество

$$V(N,x) = \{\tilde{x} \in X : N(\tilde{x}) = N(x)\}$$

всех элементов $\tilde{x}$ неотличимых с помощью информационного оператора N от x состоит из одного элемента, то оператор N устанавливает взаимно-однозначное соответствие между множествами X и Y, и называется полным (и неполным в противном случае). Оператор решения, примененный к неполному информационному оператору, порождает множество

$$A(N,f,\varepsilon) = \bigcap_{\tilde{x} \in V(N,x)} S(\tilde{x},\varepsilon),$$

при этом для $\delta_1 \le \delta_2 \Rightarrow A(N,x,\delta_1) \subset A(N,x,\delta_2)$. Тогда величины

$$r(N,x) = \inf\{\delta : A(N,x,\delta) \neq \varnothing\}$$

$$\text{и } r(N) = \sup_{x \in X} r(N,x)$$

определяют нижние оценки точности решений, которые могут быть достигнуты при неполном информационном операторе.

В работе [15] доказано, что на классе идеальных алгоритмов

$$\Phi(N): N(x) \to G,$$

с введенными определениями локальной $e(\varphi,N,x) = \inf\{\delta : \varphi(N(x)) \in A(N,x,\delta)\}$ и глобальной $e(\varphi,N) = \sup_{x \in X} \varepsilon(\varphi,N,x)$ погрешностей информация $N(x)$ позволяет найти ε – приближение для произвольного $x \in X$ тогда и только тогда, когда выполняется одно из условий:

$$r(N) < \varepsilon,$$

$$r(N) = \varepsilon, \exists \varphi : \varphi(N(x)) \in S(x,\varepsilon(\varphi,N)), \forall x \in X.$$

В случае приближенной информации N_ρ (ρ – мера погрешности) результаты для нижних оценок определяются аналогично:

$$r(N_\rho) < \varepsilon,$$

$$r(N_\rho) = \varepsilon, \exists \varphi : \varphi(N_\rho(x)) \in S(x,\varepsilon(\varphi,N_\rho)),$$

$$\forall x \in X.$$

В отличии от точного информационного оператора, оператор N_ρ определяется через оператор информационной ошибки $E: H \times R_+ \to 2^H$, обладающий двумя свойствами:

$$E(h,0) = \{h\}, \forall h \in H,$$

$$\delta_1 \le \delta_2 \Rightarrow E(h,\delta_1) \subset E(h,\delta_2), \ \forall \delta_1, \delta_2 \in R_+, h \in H.$$

Приближенный оператор $N_\rho : X \to H$ удовлетворяет условию:

$$N_\rho(x) \in E(N(x),\rho), \forall x \in X.$$

Заметим, что если точный информационный оператор N неполон, то N_ρ тоже неполон, если же N полон, то N_ρ может оказаться как полным, так и неполным. Если оператор N_ρ полон, то $r(N_\rho) = 0$.

При построении ОДФЛ с использованием вышеописанного подхода отметим, что множество определения функции X может быть задано неполно и неточно. Тогда $N: X \to Y$ – информационный оператор, описывающий лазейку, без точности и полноты определения которого вычисление обратной функции, определенной оператором решения $S: X \times R_+ \to 2^G$ с необходимой точностью невозможно. Здесь G – множество оценок близости вычисленного значения обратной функции к «истинному», которое было задано. В зависимости от практической ситуации при построении асимметричной криптосистемы в качестве множества G могут

использоваться, например, апостериорные вероятности элементов множества X (как в теории информации Шеннона); множество предполагаемых открытых текстов или множество состояний конечного автомата, описывающего источник открытых сообщений X.

Выбором множества $\Phi(N(X))$ определяются вычислительные модели, которые могут быть использованы для вычисления обратной функции. При этом условие невозможности вычисления обратной функции без знания дополнительной информации о лазейке определяется как $r(N(X)) \geq \varepsilon > 0$, где $r(N(X))$ – радиус информации $N(X)$.

Особый интерес вызывает случай приближенной информации, т.е. сознательное внесение ошибок в процесс вычисления функции. При этом, как указывалось выше, при полном точном информационном операторе N оператор N_ρ может оказаться как полным, так и неполным.

В работе [14] приводится пример построения асимметричной криптосистемы, основанной на такой односторонней функции с информационно невычислимой лазейкой на базе модифицированной системы RSA.

Литература

[1] *G. Brassard* Relativized cryptography / IEEE Transactions on information theory. – V. IT-29. - Num.6. – 1983. – P. 877-890.

[2] *S. Goldwasser, S. Micali* Probabilistic Encryption / Journal of Computer and System Sciences. – №28, 1984. – P. 270-299.

[3] *D. Dolev, C. Dwork, M. Naor* Non-malleable cryptography / Proceedings of twenty-third annual ACM symposium on theory of computing. – New Orleans, Lousiana,Us,1991. – P. 542-552.

[4] *M. Bellare, P. Rogaway* Optimal asymmetric encryption / Advances in cryptology. – LCNCS V.950, 1994. – P. 92-111.

[5] *S. Goldwasser, M. Bellare* Lecture Notes on Cryptography. – Cambridge,Massachusetts, 2001. – 283 с.

[6] *M. Bellare, A. Boldyreva, A. Desai, D. Pointcheval* Key-privacy in public-key encryption. – ASIACRYPT 2001. – LCNS 2248. – pp. 566-582.

[7] *M. Abadi, P. Rogaway*. Reconciling two views of cryptography (The computational soundness of formal encryption) / Journal of Cryptology. – 2002. – Vol. 15. – № 2. – P. 103-127.

[8] *Chris Peikert Brent Waters* Lossy trapdoor functions and their applications Electronic Colloquium on Computational Complexity, Report No. 80 (2007)

[9] *Кудин А.М.* Оценка стойкости криптосистем с использованием Чебышевского радиуса информации / Искусственный интеллект. – № 4, 2002. – С. 568-573.

[10] *Кудин А.М.* Вычислительные модели стойкости криптосистем / Праці міжнародного симпозіуму «Питання оптимізації обчислень (ПОО-XXXIII)», присвяченого 50-річчю створення ІК ім. В.М. Глушкова НАН України. – К., 2007. – С. 150-152.

[11] *Кудин А.М.* Ограничения современных моделей описания криптосистем / Вісник Державного університету інформаційно-комунікаційних технологій. – Т. 6. – № 2. – 2008. – С. 144-146.

[12] *Кудін А.М.* Порівняльний аналіз математичних моделей стійкості криптосистем // Наукові вісті НТУУ «КПІ». – № 4 (72). – 2010. – С. 86-90.

[13] *Кудин А.М.* Криптографические преобразования нешенноновских источников информации // Кибернетика и системный анализ. – № 5. – 2010. – С.143-149.

[14] *Задирака В.К., Кудин А.М.* Анализ стойкости криптографических и стеганографических систем на основе общей теории оптимальных алгоритмов // JOURNAL OF QAFQAZ UNIVERSITY MathematisandComputerScience. – № 2. – 2010. – P.47-57.

[15] Д. *Трауб, Г. Васильковский, Х. Вожьняковский* Информация, неопределенность, сложность. – М.: Мир, 1988. – 184 с.

[16] *Л. Левин* Односторонние функции / Проблемы передачи информации. – 39(1), 2003.

Поступила в редколлегию 25.04.2012

Кудин Антон Михайлович, кандидат технических наук, старший научный сотрудник, доцент кафедры Физико-технического института Национального технического университета Украины «КПИ», докторант Института кибернетики им. В.М. Глушкова НАН Украины. Область научных интересов: теоретическая криптография, теория информации, основания асимметричной криптографии, методы реализации криптографических систем.

УДК 519.72:003.26

Односпрямовані функції з лазівкою, для обчислення якої не вистачає інформації / А.М. Кудін // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 245–249.

Розглядається сучасний стан досліджень в галузі побудови односпрямованих функцій та односпрямованих функцій із лазівкою. Пропонується підхід до побудови односпрямованих функцій із лазівкою, в якому лазівка неоднозначно пов'язана із параметром функції та результатом обчислення функції.

Ключові слова: теоретико-інформаційна стійкість криптосистем, стійкість асиметричних криптосистем, односпрямовані функції в криптографії, односпрямовані функції в криптографії з втратою інформації, загальна теорія оптимальних алгоритмів.

Іл. 01. Бібліогр.: 16 найм.

UDC 519.72:003.26

One-way functions with an informationally noncomputable trapdoor / A.M. Kudin // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 245–249.

The current state of researches of constructing one-way and trapdoor functions is considered. An approach is proposed to construct the trapdoor functions, in which the trapdoor is ambiguously related with a parameter of the function and function result.

Keywords: information theoretical security of cryptosystems, security of asymmetric cryptosystems, one-way functions in cryptography, lossy trapdoor functions, general theory of optimal algorithms.

Fig. 01. Ref.: 16 items.