УДК 681.3

А.М. КУДИН

КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ НЕШЕННОНОВСКИХ ИСТОЧНИКОВ ИНФОРМАЦИИ

Ключевые слова: *модели криптосистем, стойкость криптосистем, общая теория оптимальных алгоритмов, алгоритмическая теория информации Колмогорова, идеально стойкие асимметричные криптосистемы, вычислительная модель криптосистем.*

ВВЕДЕНИЕ

Актуальной в криптологии является проблема получения нетривиальных нижних оценок стойкости практически используемых криптосистем. Несмотря на значительный прогресс в исследовании теоретических основ криптографии [1–10], до сих пор не предложены методы построения криптографических преобразований (криптографических алгоритмов и криптосистем), стойкость которых ко всем возможным криптоаналитическим атакам формально доказана для «реальных» практических ситуаций (моделей). Вместо этого до сих пор применяются методы экспертных оценок стойкости (метод ad-hoc). При этом стойкость криптографического алгоритма в большинстве практических ситуаций оценивается по отношению к известным криптографическим атакам. Работы последних лет [1, 2] разделяют два главных направления развития криптографии: формальные модели и реализуемые криптографические системы. В рамках первого направления получены достаточно весомые результаты [1–4], но разработанные модели криптографических преобразований все еще не реализованы на практике. В работе [3] определены два направления решения этой задачи: построение адекватных моделей криптосистем (и реализация криптосистем в этих моделях), так называемый конструктивный путь, и второй — приближение требований практических ситуаций к имеющимся формальным моделям. В рамках второго направления, как правило, не удается построить единые методы анализа всех систем, поэтому методы адаптированы для каждого шифра (тем более системы). Одна из причин — не рассмотрены различные (кроме статистических) модели источника информации [5].

Фактически сложилась следующая ситуация: применяемые шифры достаточно стойки к известным методам криптоанализа на практике, но доказать, насколько они стойки, нельзя. Как следствие, при проектировании шифра после проверки очевидных, эмпирически известных свойств возникает новая задача проверки его на стойкость к криптоанализу, решение которой в общем случае зависит от применяемых моделей источника информации, обработки информации (передачи, хранения, изменения), криптографического преобразования, нарушителя. Разнородность этих моделей приводит к нескольким различным подходам к формальному описанию стойкости криптосистем.

МОДЕЛИ И СТОЙКОСТЬ КРИПТОСИСТЕМ

В работе [6] предложено три подхода к определению стойкости криптосистем: теоретико-информационный (нет информации для решения задачи, ресурсы противника неограниченные), теоретико-сложностной (ресурсы ограничены) и теоретико-системный (стойкость к определенным атакам).

В теоретико-информационном подходе [7–12] связывают невозможность выполнения криптоанализа с недостаточностью информации для его проведения. Наиболее известным подходом к построению криптосистем, стойких в теоретико-информационном смысле, в настоящее время является рандомизация источника открытых сообщений. При этом часто кажущиеся далекими друг от друга направления исследований [10, 11] являются частными случаями методов рандомизации источника открытых сообщений или рандомизации криптографических преобразований. Так идея «ущербных текстов» [11] является вариантом применения вероятностных кодов [12] для предварительного кодирования информации, общий

случай которых рассмотрен в работах [8, 9]. Заметим, что естественным продолжением исследований методов рандомизации является уточнение понятий «количества информации» в криптограмме относительно открытого текста и «случайности» последовательностей. В данной статье рассматривается построение математических моделей с использованием колмогоровской меры количества информации и колмогоровского определения случайной последовательности.

В теоретико-сложностном подходе [1, 13, 14] связывают невозможность выполнения алгоритма криптоанализа с недостаточностью ресурсов для его выполнения. Заметим, что решение задачи получения нижних оценок стойкости криптографических систем при теоретико-сложностном (и тем более при теоретико-системном) подходах связано с доказательством гипотезы о существовании однонаправленных функций [15], являющейся более строгой, чем известная гипотеза $P \neq NP$. Сложность определения нижних оценок стойкости в данном подходе состоит также в применении статистических критериев открытого текста совместно с методами теории сложности вычислений для оценки стойкости криптосистемы [5]. Особенно явно проявляется данное противоречие при описании асимметричных криптосистем благодаря существованию двух возможных методов криптоанализа: по известному шифртексту и по известному открытому ключу. Если для оценки стойкости относительно анализа по открытому тексту применяются методы, аналогичные тем, которые применяются к рандомизированным симметричным криптосистемам [1, 14], то общие методы оценки стойкости относительно анализа по открытому ключу практически исследовались только для частных случаев [16].

Сформулируем следующую задачу: для заданной асимметричной криптографической системы (G, E, D, X, Y), где G — множество алгоритмов генерации ключей, E, D — множества алгоритмов шифрования/расшифрования соответственно, X — множество открытых текстов, Y — множество шифртекстов, определить условия отсутствия алгоритма определения $d_i \in D$, $x_i \in X$ при известных $e_i \in E$, $y_i \in Y$ и частично известном $g_i \in G$.

Первым к решению поставленной задачи при условии $E = D$ подошел в своей фундаментальной работе Яо [13]. Он показал справедливость следующего утверждения: пусть $O(v(n))$ — любая функция $f(n)$, которая стремится к нулю быстрее, чем n^{-t} для некоторой константы $t > 0$. Существует ансамбль источников информации S_n с эффективной энтропией $H_c(S_n)$, много большей, чем классическая энтропия $H(S_n)$. Для $g(n): (\log_2 n)^2 < g(n) < n$ существует ансамбль источников такой, что $H(S_n) = g(n)$, $H_c(S_n) = n + O(v(n))$. Фактически удалось показать, что если существует так называемый идеальный генератор случайных последовательностей $G: \{0,1\}^k \to \{0,1\}^\infty$ [1], то алгоритма получения $x_i \in X$ по множествам $e_i \in E$, $y_i \in Y$ не существует для реальных источников открытых сообщений X.

Более точные модели множеств X, Y можно построить с помощью меры количества информации, заключенной в индивидуальных конечных объектах, предложенной Колмогоровым [17]. Следующая теорема [18] определяет существование пар конечных слов с «нематериализуемой» взаимной информацией.

Теорема 1. Пусть $f(n)$ — такая функция, что $f(n) = o(n)$ и $f(n) \geq \log n$ и x_n — такая последовательность, что $K(x_n) = n + O(f(n))$, где $K(x_n)$ — колмогоровская сложность последовательности. Тогда существует последовательность y_n такая, что $K(y_n) = n + O(f(n))$, $I(x_n : y_n) = an + O(f(n))$ для любых значений $0 < a < 1$ и для любой последовательности слов z_n, удовлетворяющих условию $K(z_n | x_n) = O(f(n))$, $K(z_n | y_n) = O(f(n))$, имеет место соотношение $K(z_n) = O(f(n))$. Здесь $I(x_n : y_n)$ — взаимная информация по Колмогорову.

Этот факт позволяет при построении криптосистем использовать преобразования, вносящие не статистическую, а «вычислительную (алгоритмическую)» неопределенность элементов множества X относительно известных элементов множества Y.

Брассард [19] впервые рассмотрел случай $E \neq D$ с помощью построения искусственных моделей вычислений, в которых любой алгоритм определения X по известным E, Y принадлежал бы классу NP.

Практическим развитием идей Брассара стала концепция вероятностного шифрования. За счет введения вероятностной модели вычислений, рандомизации мно-

жества X, гипотез о существовании идеальных генераторов случайных последовательностей $G:\{0,1\}^k \to \{0,1\}^\infty$ и хеш-функций $H:\{0,1\}^\infty \to \{0,1\}^k$ удалось доказать следующее утверждение [14].

Теорема 2. Пусть A — полиномиальная вероятностная машина Тьюринга, характеризующая вычислительные возможности криптоаналитика при наличии информации об открытом ключе и шифртексте; G — алгоритм генерации ключей, E,D — алгоритмы шифрования/расшифрования соответственно, X — множество открытых текстов, Y — множество шифртекстов, Q — произвольный полином. Существует криптосистема (G,E,D,X,Y) такая, что любая A определяет $x_i \in X$ при известных $e_i \in E$, $y_i \in Y$ с вероятностью не большей $1/2+1/Q(k)$, где k — выбранный параметр стойкости к криптоанализу.

Главная идея метода — рандомизация множества открытых сообщений X, за счет которой нарушается инъективность отображения $Y \to X$. Дальнейшие исследования связаны с изучением связи структур множеств X,Y при различных E,D. В работе [20] вводится свойство несохранения гомоморфизма (non-malleability) криптографического преобразования, определенное на множестве шифртекстов Y следующим образом: $\forall\, y_1, y_2 \in Y$ относительно функции f, определенной на множестве открытых текстов, не существует вероятностного алгоритма определения y_2 по известному y_1, такого, что $y_1 = E(x_1)$, $y_2 = E(f(x_1))$. Таким образом, криптографическое преобразование разрушает некоторое отношение, введенное на множестве открытых текстов.

ПОСТАНОВКА ЗАДАЧИ

В рассмотренных выше моделях стойкости асимметричных криптосистем исследовалось влияние криптографических преобразований на связь между множествами X,Y, при этом всегда существует алгоритм определения D (и соответственно $x_i \in X$) по известным $y_i \in Y$, $e_i \in E$. Рассмотрим построение асимметричных криптосистем, для которых нарушена как инъективность отображения $Y \to X$, так и отображения $D \to E$.

Теоретической основой построения и оценки стойкости таких криптографических систем предлагается выбрать общую теорию оптимальных алгоритмов [21], которая связывает существование и сложность алгоритмов с точностью задания входных данных. При этом в качестве одной из мер случайности множеств X,Y,E,D целесообразно использовать колмогоровскую меру информации.

Для решения задачи построения таких криптосистем автор в работе [22] предложил объединить построение рандомизированных асимметричных шифров и «шарад Меркля» [23]. Главная идея — внести неопределенность в связь алгоритмов шифрования и расшифрования, легко устранимую при знании дополнительной информации. Для этого увеличивалась неопределенность ключа расшифрования, только часть которого была бы связана с открытым ключом. Неопределенность зависимости ключей шифрования и расшифрования осуществлялась за счет рандомизации открытого ключа во взаимосвязи с рандомизацией открытого текста при зашифровании. При этом противник, ограниченный в вычислительных возможностях вероятностными алгоритмами полиномиальной сложности, не в состоянии определить алгоритм расшифрования, а законный пользователь таким алгоритмом обладает благодаря знанию избыточности открытого текста. Единственной стратегией противника при этом остается вычисление обратной функции связи открытого текста/шифртекста, а не функции лазейки (связи ключей шифрования/расшифрования).

Ограничением такого похода является сложность введения неопределенности в связь личного и открытого ключа на основании критерия открытого текста.

Более простым методом решения сформулированной задачи построения асимметричных криптосистем является следующий: нарушение инъективности отображений $Y \to X$ и $D \to E$ осуществляется за счет рандомизации множеств X,E; законные абоненты для расшифрования сообщений используют криптографически сильный генератор случайных последовательностей $G:\{0,1\}^k \to \{0,1\}^\infty$ с неизвестным нарушителю начальным заполнением. При этом выбор конкретных алгоритмов $e_i \in E$, $d_i \in D$ у законных абонентов управляется генератором G (например, $i = G(t)$, t — состояние генератора). Рассмотрим этот поход подробнее.

Введем следующие обозначения. Пусть заданы множества X, Y, пусть 2^Y — класс всех подмножеств множества Y. В работе [21] рассматривается оператор $S: X \times \times R_+ \to 2^Y$, где $R_+ = [0, \infty)$ — оператор решения, обладающий двумя свойствами:

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

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

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).

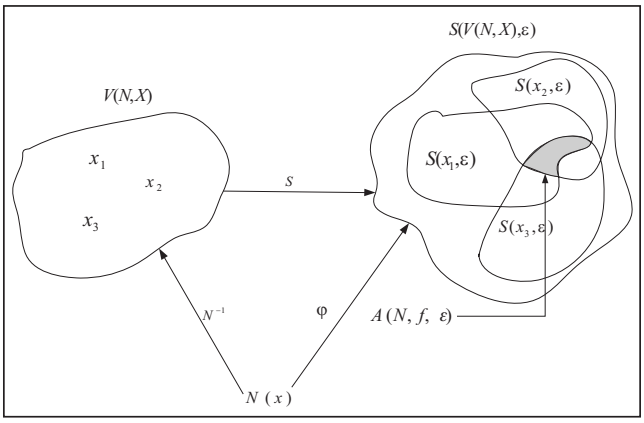

Рис. 1. Графическое изображение информационного оператора и оператора решения

Если множество $V(N,x) = \{\widetilde{x} \in X : N(\widetilde{x}) = N(x)\}$ всех элементов $\widetilde{x}$, неотличимых с помощью информационного оператора N от x, одноточечно, то оператор N устанавливает взаимно однозначное соответствие между множествами X и Y и называется полным (и неполным в противном случае). Оператор решения, применяемый к неполному информационному оператору, порождает множество $A(N, f, \varepsilon) = \bigcap_{\widetilde{x} \in V(N,x)} S(\widetilde{x}, \varepsilon)$, при этом для $\delta_1 \le \delta_2 \Rightarrow A(N,x,\delta_1) \subset A(N,x,\delta_2)$. Тогда величины $r(N,x) = \inf\{\delta : A(N,x,\delta) \neq \varnothing\}$ и $r(N) = \sup_{x \in X} r(N,x)$ $(= \inf\{\delta : A(N,x,\delta) \neq \neq \varnothing,\ \forall\, x \in X\})$ определяют нижние оценки точности решений, которые могут быть достигнуты при неполном информационном операторе. В работе [21] 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:

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

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

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

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

$$r(N_\rho) = \varepsilon,\ \exists\, \varphi : \varphi(N_\rho(x)) \in S(x, e(\varphi, N_\rho)) \quad \forall\, x \in X.$$

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

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

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

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

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

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 математической модели криптосистемы с использованием описанного выше подхода отметим, что в задачах, рассматриваемых в криптологии, нарушителю не известен открытый текст, но известна некоторая информация о нем, заключенная в криптограммах. Пусть X — источник открытых сообщений, тогда $N: X \to Y$ — оператор, описывающий криптографическое преобразование, $S: X \times R_+ \to 2^G$ — оператор криптографического анализа, G — множество оценок «истинности» открытых текстов. В зависимости от практической ситуации 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. Заметим, что для достижения идеальной стойкости криптосистемы оператор N должен быть неполным.

В качестве $\Phi(N(X))$ выбираем множество идеальных алгоритмов φ реализации оператора криптоанализа. При этом условие идеальной стойкости определяется как $r(N(X)) \ge \varepsilon > 0$, где $r(N(X))$ — радиус информации $N(x)$.

Особый интерес вызывает случай приближенной информации, т.е. сознательное внесение ошибок в процесс криптографического преобразования. При этом, как указывалось выше, при полном точном информационном операторе N оператор N_ρ может оказаться как полным, так и неполным. Это позволяет предположить существование идеальных криптосистем, которые Шеннон отнес к «практически стойким». Назовем введенную модель вычислительной моделью стойкости криптосистем.

Справедливы следующие теоремы.

Теорема 3. Для криптосистем, идеально стойких в вычислительной модели стойкости, все криптографические преобразования имеют свойство не сохранять гомоморфизм.

Доказательство. По определению для криптографического преобразования, не сохраняющего гомоморфизм $\forall\, y_1, y_2 \in Y$, и некоторой функции f, определенной на X, не существует вероятностного алгоритма $A(x_1, y_1, E, f)$, определяющего y_2, такого, что $y_1 = E(x_1)$, $y_2 = E(f(x_1))$. Поскольку для идеально стойкой в вычислительном смысле криптосистемы $r(N(X)) \ge \varepsilon > 0$, то для любых функций f, x_1, $f(x_1)$, $x_2 \ne f(x_1)$ существует такое $\varepsilon > 0$, что $E(x_1) = E(f(x_1)) = E(x_2)$. Тогда $y_2 = E(f(x_1)) = E(x_2)$, отсюда $x_2 = f(x_1)$, что противоречит предположению о $x_2 \ne f(x_1)$.

Теорема доказана.

Теорема 4. Криптосистема, идеально стойкая в вычислительной модели стойкости, также является стойкой в смысле полиномиальной неразличимости.

Рассмотрим примеры построения асимметричных криптосистем, стойких в идеальном смысле в модели вычислительной стойкости, с использованием криптографически сильного генератора случайных последовательностей.

ПРИМЕРЫ ПОСТРОЕНИЯ ИДЕАЛЬНО СТОЙКИХ АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ В ТЕРМИНАХ ОБЩЕЙ ТЕОРИИ ОПТИМАЛЬНЫХ АЛГОРИТМОВ

Пусть (G, E, D) — криптосистема RSA.

Генерация ключей. Положим вместо открытого ключа N множество $\dot{N} = \{N_1, N_2, \ldots, N_k\}$. Это соответствует ситуации, когда некоторые биты N_i неизвестны. Пусть $\dot{D} = \{d_1, d_2, \ldots, d_k\}$ — соответствующее множество личных ключей, X — множество открытых текстов, $f_r(x)$ — рандомизатор, $G: \{0,1\}^k \to \{0,1\}^\infty$ — криптографически сильный генератор случайных последовательностей с неизвестным нарушителю начальным заполнением t_0. Построение множества $\dot{N}$ можно осуществить с помощью конструктивного алгоритма: вначале строим случайные простые числа требуемого размера, затем определяем их произведения. Ясно, что этот алгоритм имеет полиномиальную сложность.

Зашифрование. Выбираем $i = G(t_0)$, где t_0 — начальное состояние, известное законным абонентам.

Вычисляем $\tilde{N} \overset{G}{\leftarrow} \dot{N}_I$. Для $x \in X$ имеем $\tilde{x} = f_r(x)$, $c = \tilde{x}^e \bmod \tilde{N}$.

Расшифрование. Пусть B — полиномиальная вероятностная машина Тьюринга с входами $\dot{N}$, $\dot{D}$, $f_r(x)$, c, $G(t_0)$, которая вычисляет x. Такая машина существует, так как существует полиномиальный алгоритм вычисления $\dot{D}$ по известному $i = G(t_0)$ и вероятностный полиномиальный алгоритм вычисления x по известному $f_r(x)$. В простейшем случае для $f_r(x) = x||\text{random}$, где random — случайное число, $||$ — операция конкатенации, применяем следующий алгоритм: $i = G(t_0)$, $\dot{x} = c^{d_i} \bmod N_i$, $\dot{x} = x||\text{random}$.

Подобный алгоритм существует и для других схем рандомизации, например для схемы Optimal asimetric encryption [24].

Оценка стойкости. Погрешность вычисления d, соответствующего выбранному при зашифровании $\tilde{N}$ (при знании c, $f_r(x)$, N, e, G) не равна 0, т.е. $r(N(\tilde{d})) > 0$. Вся информация «по Колмогорову», необходимая для точного восстановления, какой именно элемент множества $\dot{N}$ был выбран при зашифровании, заключена в t_0. Оценка практической стойкости криптосистемы зависит от мощности множества $\dot{N}$.

Для определения мощности данного множества необходимо оценить количество чисел, являющихся модулем для криптосистемы RSA размера n. Известно, что модуль $N = p \cdot q$, где p, q — классические сильные простые числа размера примерно $\sqrt{n}$, т.е. выполнены следующие условия:

$$p_1 \mid p-1,\ p_1 \ge N^{x_1},\ p_2 \mid p_1 - 1,\ p_2 \ge N^{x_2},\ p_3 \mid p+1,\ p_3 \ge N^{x_3},$$

$$\frac{1}{2} \le x_1 < 1,\ \frac{1}{2} \le x_2 < 1,\ \frac{1}{2} \le x_3 < 1;$$

$$q_1 \mid q-1,\ q_1 \ge N^{x_4},\ q_2 \mid q_1 - 1,\ q_2 \ge N^{x_5},\ q_3 \mid q+1,\ q_3 \ge N^{x_6},$$

$$\frac{1}{2} \le x_4 < 1,\ \frac{1}{2} \le x_5 < 1,\ \frac{1}{2} \le x_6 < 1.$$

Получим верхнюю оценку количества чисел p, q. Для этого заметим, что вероятность того, что случайно выбранное число независимо от размера будет иметь наибольший делитель, больший или равный N^x, $\frac{1}{2} \le x < 1$, равна $\ln x$ [25]. Количество простых чисел в интервале $[a, b]$ находится по формуле $\pi(b) - \pi(a) = \int_a^b \frac{dt}{\ln t}$. Тогда, принимая во внимание, что для получения верхних оценок события существования делителей p_1, p_2, p_3 (q_1, q_2, q_3) выбранных размеров можно считать независимыми, получаем

$$\pi_s(a,b) = -\ln x_1 \cdot \ln x_2 \cdot \ln x_3 \cdot \int_a^b \frac{dt}{\ln t},$$

где $\pi_s(a,b)$ — количество сильных простых чисел p в интервале $[a,b]$, $\frac{1}{2} \le x_1, x_2, x_3 < 1$. Таким образом, верхняя оценка мощности множества $\dot{N}$ определяется как $\pi_s(a,b)^2$. Для применяемых размеров модулей RSA (2048 бит) эта оценка приблизительно равна 10^{600}. Подобный метод можно применить для построения идеально стойкой в вычислительном смысле схемы Диффи–Хеллмана.

ЗАКЛЮЧЕНИЕ

Предложенные методы построения идеально стойких в вычислительной модели криптосистем достаточно эффективны при практической реализации. Результаты сравнения предложенного похода с известными можно представить в виде таблицы, отображающей основные характеристики криптосистем, построенных в их рамках.

Таблица 1

Характеристики	Подход, связанный с классической теорией информации	Подход, связанный с вычислительной энтропией	Подход, связанный с алгоритмической теорией информации Колмогорова и общей теорией оптимальных алгоритмов
Мера информации	Энтропия $H(X)$	Эффективная энтропия $H_C(X)$	Колмогоровская сложность $KS(X)$
Условия существования совершенных КС	$H(X) \le H(K)$, $I(X,Y) = I(X,K) = 0$	$H_C(X) \le H_C(K)$	$KS(X) \le H(K)$, $r(N,x) > \varepsilon$
Условия существования идеальных КС	$I(X,Y) < H(X)$	$H_C(K) > 0$, $H_C(X) > 0$	$I(X:K) = 0$, $I(X:Y) = 0$, $r(N_\rho, x) > \varepsilon$

Из таблицы видно, что при применении в качестве меры информации криптогоровской сложности, а в качестве показателя стойкости, — чебышевского радиуса информации, удается выделить новый класс криптографических преобразований, основанный на внесении неопределенности в связь ключей шифрования/расшифрования.

СПИСОК ЛИТЕРАТУРЫ

1. Goldwasser S., Bellare M. Lecture Notes on Cryptography. — Cambridge, Massachusetts, 2001. — 283 c.
2. Abadi M., Rogaway P. Reconciling two views of cryptography (The computational soundness of formal encryption) / J. of Cryptology. — 2002. — **15**, N 2. — P. 103–127.
3. Grigoriev D., Hirsch E.A., Pervyshev K. A Complete Public-Key Cryptosystem / Groups-Complexity-Cryptology. — 2009. — **1**, N 1. — P. 1–12.
4. Pliam J.O. The disparity between work and entropy in cryptology // available from iacr.eprint/024.
5. Кудин А.М. Ограничения современных моделей описания криптосистем / Вісн. Держ. ун-ту інформаційно-комунікаційних технологій. — 2008. — **6**, № 2. — С. 144–146.
6. Rueppel, Rainer A. Analysis and design of stream ciphers. With a foreword by James L. Massey // Com. and Contr. Engineer. Ser. — Berlin: Springer-Verlag, 1986. — 244 p.
7. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. — М.: Изд-во иностр. лит., 1963. — С. 333–369.
8. Wyner A.D. The wire-tap channel // Bell Syst. Techn. J. — 1975. — **54**. — P. 1355–1388.
9. Maurer U. Information-theoretic cryptography // Advances in Cryptology — CRYPTO'99, Proceedings. — Berlin: Springer-Verlag, 1999. — P. 47–64.
10. Рябко Б.Я., Фионов А.Н. Быстрый метод полной рандомизации сообщений // Проблемы передачи информации. — 1997. — **33**, вып. 3. — С. 3–14.
11. Мищенко В.А., Виланский Ю.В. Ущербные тексты и многоканальная криптография. — Мн.: Энциклопедикс, 2007. — 292 с.
12. Алексейчук А.Н. Математическая модель и задачи анализа стойкости вероятностно-криптографических систем в системах защиты информации // Захист інформації. — 2001. — № 3. — С. 5–12.
13. Yao A.C. Theory and application of trapdoor functions / 23rd Annual Sympos. on Foundat. of Comput. Sci. — Chicago, 1982. — P. 80–91.
14. Goldwasser S., Micali S. Probabilistic Encryption // J. of Comput. and System Sci. — 1984. — N 28. — P. 270–299.
15. Левин Л. Односторонние функции // Проблемы передачи информации. — 2003. — 39(1).
16. Maurer U., Wolf S. The Diffie-Hellman protocol / from www.iacr.eprint/078.pdf
17. Колмогоров А.Н. Три подхода к определению понятия «Количество информации» / Новое в жизни, науке, технике. Сер. «Математика и кибернетика». — 1991. — № 1. — С. 24–29.
18. Успенский В., Верещагин Н., Шень А. Колмогоровская сложность. — 2004. — 325 с.
19. Brassard G. Relativized cryptography // IEEE Trans. on Inform. Theory. — 1983. — **IT-29**, N 6. — P. 877–890.
20. Dolev D., Dwork C., Naor M. Non-malleable cryptography // Proc. of Twenty-third Annual ACM sympos. on Theory of Comput. — New Orleans, Lousiana,Us, 1991. — P. 542–552.
21. Трауб Д., Васильковский Г., Вожьняковский Х. Информация, неопределенность, сложность. — М.: Мир, 1988. — 184 с.
22. Кудин А.М. Об одном классе криптографических преобразований для модели источников информации Колмогорова // Праці міжнар. симпозіуму «Питання оптимізації обчислень ПОО-XXXV». — Київ: Ін-т кібернетики ім. В.М. Глушкова НАН України, 2009. — **1**. — С. 394–399.
23. Merkle R. Secure communications over insecure channels // CACM. — Apr. 1978. — P. 294–299.
24. Bellare M., Rogaway P. Optimal asymmetric encryption // Advances in cryptology. — LCNCS — 1994. — **950**. — P. 92–111.
25. Knut D.E., Trabb-Pardo L. Analysis of a simple factorization algorithm // Theoret. Comput. Sci. — 1976. — **3**. — P. 321–348.

Поступила 15.02.2010