УДК 621.391:519.2

А.Н. АЛЕКСЕЙЧУК

НЕАСИМПТОТИЧЕСКИЕ НИЖНИЕ ГРАНИЦЫ ИНФОРМАЦИОННОЙ СЛОЖНОСТИ СТАТИСТИЧЕСКИХ АТАК НА СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Аннотация. Предложен метод получения нижних границ информационной сложности статистических атак на блочные или поточные шифры. Метод основан на применении неравенства Фано и в отличие от известных не использует каких-либо асимптотических соотношений, приближенных формул или эвристических предположений об исследуемом шифре. Полученные границы информационной сложности для одних видов атак имеют классический вид, а для других — позволяют ввести обоснованные параметры, характеризующие стойкость симметричных криптосистем к таким атакам.

Ключевые слова: симметричная криптография, проверка статистических гипотез, статистическая атака, блочный шифр, поточный шифр, корреляционная атака, информационная сложность, неравенство Фано.

ВВЕДЕНИЕ

Атаки, основанные на статистических методах, образуют широкий класс наиболее мощных атак на симметричные криптосистемы (поточные и блочные шифры). К ним относятся разностные [1, 2], линейные [3], обобщенные линейные [4], билинейные [5] атаки на блочные шифры и их многочисленные обобщения и усовершенствования (см., например, [6, 7] и ссылки к ним), а также корреляционные атаки на поточные шифры [8, 9].

Традиционной математической основой для построения статистических атак является теория проверки статистических гипотез: каждая атака, по сути, является статистической процедурой проверки двух или большего числа гипотез, связанных с возможными значениями неизвестного криптографического параметра. При этом эффективность атаки определяется ее информационной сложностью (data complexity) — наименьшим объемом данных, необходимых для различения указанных гипотез с заданной достоверностью (средней или максимальной вероятностью ошибки).

Одной из центральных проблем в области статистического криптоанализа является получение обоснованных оценок информационной сложности, которые позволяют установить, от каких параметров, связанных с алгоритмом шифрования, зависит эффективность той или иной атаки. Наиболее существенные недостатки, присущие известным методам получения оценок информационной сложности статистических атак, состоят в следующем.

Классические выражения для информационной сложности разностных, линейных, обобщенных линейных атак [2–4] основаны на эвристических предположениях (гипотезах о стохастической эквивалентности, строгой различимости ключей и т.п.), проверить которые на практике, как правило, невозможно. Остается нерешенным вопрос о том, насколько необходимы эти предположения для обоснования стойкости блочных шифров относительно статистических атак.

Кроме того, в большинстве работ рассматриваются исключительно различающие атаки (что соответствует случаю проверки двух гипотез). При этом приводятся асимптотические формулы для информационной сложности атак, в доказательствах которых используются приближенные соотношения (например, нормальное приближение распределения суммы независимых случайных величин) без явных оценок погрешностей (см. [7], где подробно аргументированы недостатки такого подхода к выводу оценок информационной сложности).

Математически корректное обоснование неасимптотических нижних границ информационной сложности дано в [10] для разностной и линейной различающих атак и в [11–13] — для атак более общего вида.

В настоящей статье предлагается простой и эффективный метод получения нижних границ информационной сложности статистических атак, не имеющий указанных недостатков. Метод базируется на применении неравенства Фано в рамках общей статистической модели, которая позволяет одновременно описывать атаки, направленные на восстановление ключей, различающие атаки на блочные шифры и корреляционные атаки на синхронные поточные шифры. В отличие от известных методов предложенный в данной работе используется в случае произвольного (конечного) числа гипотез, не требует информации о виде (shape) статистических критериев, применяемых при проведении атак, и не использует асимптотических соотношений, приближенных формул или эвристических предположений об исследуемом шифре. В случае (многомерных) линейных, обобщенных линейных, билинейных и разностных атак полученные границы информационной сложности имеют классический вид. Для других видов атак эти границы позволяют ввести обоснованные параметры, характеризующие стойкость симметричных криптосистем к таким атакам.

В качестве отдельного результата отметим усиление леммы Ваденеи [10, лемма 15], позволяющее улучшить ранее известные границы информационной сложности ряда статистических атак на симметричные криптосистемы [11–13].

ПОСТАНОВКА ЗАДАЧИ И ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Большинство статистических атак на поточные или блочные шифры можно описать с помощью следующей общей модели.

Пусть S, S', Z — конечные множества, состоящие не менее чем из двух элементов; $\psi : S \to S'$ — сюръективное отображение; $(p(s) : s \in S)$ — распределение вероятностей на множестве S такое, что $p(s) > 0$ для любого $s \in S$. Пусть также для каждого $s \in S$ задана последовательность распределений вероятностей $P_{1,s}, P_{2,s}, \ldots$ на множестве Z. Наблюдается случайная последовательность $Z^{(t)} = Z_1, \ldots, Z_t$, распределенная по закону $P_s\{Z^{(t)} = z^{(t)}\} = P_{1,s}(z_1) \cdots P_{t,s}(z_t)$, $z^{(t)} = (z_1, \ldots, z_t) \in Z^t$, где параметр s выбран случайно в соответствии с распределением $(p(s) : s \in S)$ и неизвестен. Требуется восстановить значение $\psi(s)$ по реализации случайной последовательности $Z^{(t)}$ или, что равносильно, проверить справедливость одной из гипотез $H_{s'}: s \in \psi^{-1}(s')$, где $s' \in S'$.

Произвольный критерий для проверки указанных гипотез определяется как отображение $D : Z^t \to S'$. Вероятность ошибки критерия D определяется по формуле $\delta(D) = \sum_{s \in S} p(s) P_s\{D(Z^{(t)}) \neq \psi(s)\}$. Известно (см., например, [14]), что оптимальным (имеющим наименьшую вероятность ошибки) является байесовский критерий (ставящий в соответствие последовательности $z^{(t)} \in Z^t$ произвольный фиксированный элемент $\psi(s^*) \in S'$, для которого достигается максимум условной вероятности

$$P(s' / z^{(t)}) = \frac{\sum_{s \in \psi^{-1}(s')} p(s) P_s(z^{(t)})}{\sum_{s \in S} p(s) P_s(z^{(t)})}$$

по всем $s' \in S'$), однако в дальнейшем рассматриваются любые критерии. Основная задача состоит в том, чтобы для любого $\delta \in (0, 1/2)$ оценить наименьший объем t выборки, необходимый для различения гипотез $H_{s'}$ $(s' \in S')$ с вероятностью ошибки, не превышающей δ.

Справедлива следующая теорема.

Теорема 1. Пусть D — произвольный критерий для проверки гипотез $H_{s'}$ ($s' \in S'$), где $\delta(D) \le \delta < 1/2$. Тогда имеет место неравенство

$$t \ge \frac{H(S') - \delta \log (|S'|-1) - h(\delta)}{\max\limits_{1 \le i \le t} \{I(S; Z_i)\}}, \tag{1}$$

где

$$H(S') = -\sum_{s' \in S'} \left(\sum_{s \in \psi^{-1}(s')} p(s) \right) \log \left(\sum_{s \in \psi^{-1}(s')} p(s) \right)$$

является энтропией распределения вероятностей, индуцированного на множестве S' распределением $(p(s): s \in S)$ и отображением ψ, $h(\delta) = -\delta \log \delta - (1-\delta) \log (1-\delta)$, а

$$I(S; Z_i) = \sum_{s \in S} p(s) \sum_{z \in Z} P_{i,s}(z) \log \frac{P_{i,s}(z)}{P_i(z)}$$

является (средней) взаимной информацией между случайными величинами S и Z_i, $P_i(z) = \sum\limits_{s \in S} p(s) P_{i,s}(z)$, $z \in Z$, $1 \le i \le t$.

Доказательство. Рассмотрим взаимную информацию $I(\psi(S); D(Z^{(t)}))$ между случайными величинами $\psi(S)$ и $D(Z^{(t)})$. Согласно известным свойствам взаимной информации и энтропии (см., например, [15]) имеем

$$I(\psi(S); D(Z^{(t)})) \le I(S; D(Z^{(t)})) \le I(S; Z^{(t)}) = H(Z^{(t)}) - H(Z^{(t)} / S) \le$$

$$\le \sum_{i=1}^{t} H(Z_i) - H(Z^{(t)} / S) = \sum_{i=1}^{t} H(Z_i) - \sum_{i=1}^{t} H(Z_i / S),$$

где последнее равенство вытекает из условия независимости случайных величин $Z_1, \ldots, Z_t$ при условии $\{S = s\}$ для каждого s. Следовательно,

$$I(\psi(S); D(Z^{(t)})) \le \sum_{i=1}^{t} I(S; Z_i) \le t \cdot \max_{1 \le i \le t} \{I(S; Z_i)\}. \tag{2}$$

Далее, согласно неравенству Фано (см., например, [15, лемма 3.8])

$$H(\psi(S) / D(Z^{(t)})) \le \delta(D) \log (|\psi(S)|-1) + h(\delta(D)) \le \delta \log (|S'|-1) + h(\delta),$$

откуда вытекает, что

$$I(\psi(S); D(Z^{(t)})) = H(\psi(S)) - H(\psi(S) / D(Z^{(t)})) \ge$$

$$\ge H(S') - \delta \log (|S'|-1) - h(\delta). \tag{3}$$

Из формул (2), (3) следует неравенство (1).

Теорема доказана.

Рассмотрим теперь произвольные распределения вероятностей P_1 и P_2 на множестве Z, $P_2(z) > 0$ для любого $z \in Z$. Обозначим

$$D(P_1 || P_2) = \sum_{z \in Z} P_1(z) \log \frac{P_1(z)}{P_2(z)}, \tag{4}$$

$$\chi^2(P_1, P_2) = \sum_{z \in Z} \frac{(P_1(z) - P_2(z))^2}{P_2(z)}. \tag{5}$$

Величина (4) называется информационной дивергенцией (или расстоянием Кульбака–Лейблера), а величина (5) — расстоянием χ^2 между распределениями P_1 и P_2 (см., например, [14]). Отметим, что в случае, когда P_2 совпадает с равно-

мерным распределением U_Z на множестве Z, величина

$$\Delta(P_1) = \chi^2(P_1, U_Z) = |Z|^{-1} \sum_{z \in Z} (P_1(z)|Z| - 1)^2$$

представляет собой так называемую квадратичную евклидову несбалансированность (squared Euclidean imbalance) распределения вероятностей P_1 [16].

Величины (4) и (5) связаны неравенством

$$D(P_1 || P_2) \le \frac{1}{\ln 2} \chi^2(P_1, P_2), \tag{6}$$

которое следует из оценки $\ln x \le x - 1$, $x > 0$, и соотношений

$$D(P_1 || P_2) = \frac{1}{\ln 2} \sum_{z \in Z} P_1(z) \ln \frac{P_1(z)}{P_2(z)} \le \frac{1}{\ln 2} \sum_{z \in Z} P_1(z) \left(\frac{P_1(z)}{P_2(z)} - 1 \right) = \frac{1}{\ln 2} \chi^2(P_1, P_2).$$

Использовав формулу (6) и теорему 1, нетрудно получить следующий результат.

Теорема 2. Пусть в условии теоремы 1 $p(s) = |S|^{-1}$, $|\psi^{-1}(s')| = |S| \cdot |S'|^{-1}$ для любого $s' \in S'$. Тогда справедливо неравенство

$$t \ge \frac{(1-\delta)\log|S'| - h(\delta)}{\max\limits_{1 \le i \le t} \left\{ |S|^{-1} \sum\limits_{s \in S} \Delta(P_{i,s}) \right\}} \ln 2, \tag{7}$$

где $\Delta(P_{i,s}) = |Z|^{-1} \sum\limits_{z \in Z} (P_{i,s}(z)|Z| - 1)^2$, $s \in S$, $1 \le i \le t$.

Доказательство. Обозначим U_Z равномерное распределение вероятностей на множестве Z. Поскольку $p(s) = |S|^{-1}$ для любого $s \in S$, то

$$I(S; Z_i) = H(Z_i) - H(Z_i / S) \le \log|Z| - H(Z_i / S) =$$

$$= \log|Z| - \sum_{s \in S} |S|^{-1} H(P_{i,s}) = |S|^{-1} \sum_{s \in S} D(P_{i,s} || U_Z), \ 1 \le i \le t.$$

Отсюда на основании неравенства (6) получим, что

$$I(S; Z_i) \le \frac{1}{\ln 2} |S|^{-1} \sum_{s \in S} \chi^2(P_{i,s}, U_z) = \frac{1}{\ln 2} |S|^{-1} \sum_{s \in S} \Delta(P_{i,s}), \ 1 \le i \le t.$$

Кроме того, из условия теоремы следует, что $H(S') = \log|S'|$. Подставив полученные соотношения в формулу (1), получим неравенство (7).

Теорема доказана.

Следующая теорема устанавливает нижнюю границу параметра t для случая двух гипотез, имеющих одинаковые априорные вероятности.

Теорема 3. Пусть в условии теоремы 1 $S = S_0 \cup S_1$, где $S_0 \cap S_1 = \varnothing$, $p(s) = 1/2 \cdot |S_j|^{-1}$, если $s \in S_j$, $j \in S' = \{0, 1\}$ и $\psi(s) = j$ для любого $s \in S_j$, $j \in S'$. Тогда справедливо неравенство

$$t \ge \frac{2(1 - h(\delta)) \ln 2}{\max\limits_{1 \le i \le t} \left\{ |S_0|^{-1} \sum\limits_{s \in S_0} \Delta(P_{i,s}) + |S_1|^{-1} \sum\limits_{s \in S_1} \Delta(P_{i,s}) \right\}}, \tag{8}$$

где $\Delta(P_{i,s}) = |Z|^{-1} \sum\limits_{z \in Z} (P_{i,s}(z)|Z| - 1)^2$, $s \in S$, $1 \le i \le t$.

Доказательство. Из условия теоремы следует, что

$$I(S;Z_i)=H(Z_i)-H(Z_i/S)\le \log|Z|-H(Z_i/S)=$$

$$=\log|Z|-1/2\cdot\sum_{s\in S_0}|S_0|^{-1}H(P_{i,s})-1/2\cdot\sum_{s\in S_1}|S_1|^{-1}H(P_{i,s})=$$

$$=1/2\cdot\left(|S_0|^{-1}\sum_{s\in S_0}D(P_{i,s}||U_Z)+|S_1|^{-1}\sum_{s\in S_1}D(P_{i,s}||U_Z)\right),\ 1\le i\le t.$$

Следовательно, на основании неравенства (6)

$$I(S;Z_i)\le\frac{1}{2\ln 2}\left(|S_0|^{-1}\sum_{s\in S_0}\Delta(P_{i,s})+|S_1|^{-1}\sum_{s\in S_1}\Delta(P_{i,s})\right),\ 1\le i\le t.$$

Кроме того, из условия теоремы вытекает, что $H(S')=\log|S'|=1$. Подставив указанные соотношения в формулу (1), получим неравенство (8).

Теорема доказана.

Отметим простоту обоснования неравенств (1), (7), (8) и общность условий, при которых они справедливы. Далее приведены примеры применения этих неравенств к оцениванию информационной сложности различных статистических атак на симметричные криптосистемы.

НЕАДАПТИВНЫЕ АТАКИ НА БЛОЧНЫЕ ШИФРЫ

Пусть $\mathfrak{F}$ — блочный шифр со множеством открытых (шифрованных) сообщений X, множеством ключей K и семейством шифрующих преобразований $(F_k: k\in K)$. Рассмотрим атаку d-го порядка на шифр $\mathfrak{F}$, обобщающую ряд известных атак, в частности (многомерные) линейные, обобщенные линейные и билинейные атаки [3–5, 10–13, 16–18].

Атака строится на основе пары отображений $\varphi: X^d\times X^d\to Z$, $\psi: K\to S'$, где Z, S' — конечные множества, отображение φ отлично от константы, а отображение ψ удовлетворяет условию $|\psi^{-1}(s')|=|K|\cdot|S'|^{-1}$ для любого $s'\in S'$. Предполагается, что на множестве K задано равномерное распределение вероятностей, а на множестве X^d — произвольное распределение $P^{(d)}$, $d\in\mathbf{N}$. При проведении атаки противник имеет доступ к оракулу F_k с неизвестным (выбранным случайно и равновероятно из множества K) ключом k. Противник генерирует независимые в совокупности наборы открытых сообщений $X_i=(X_{i,1},\dots,X_{i,d})$, каждый из которых распределен по закону $P^{(d)}$, получает наборы $F_k(X_i)=(F_k(X_{i,1}),\dots,F_k(X_{i,d}))$ и вычисляет значения $Z_i=\varphi(X_i,F_k(X_i))$, $1\le i\le t$. Целью противника является восстановление значения $\psi(k)$ по известной последовательности $Z^{(t)}=Z_1,\dots,Z_t$.

Ясно, что описанная атака сводится к рассмотренной ранее задаче проверки гипотез $H_{s'}$, $s'\in S'$, если положить $S=K$, $p(k)=|K|^{-1}$ и $P_{i,k}(z)=$ $=P^{(d)}\{\varphi(X_i,F_k(X_i))=z\}$, где $k\in K$, $z\in Z$, $1\le i\le t$. При этом распределение вероятностей $P_{i,k}$ не зависит от i и имеет квадратичную евклидову несбалансированность

$$\Delta(P_k)=|Z|^{-1}\sum_{z\in Z}(|Z|P^{(d)}\{\varphi(X,F_k(X))=z\}-1)^2, \tag{9}$$

где $X=(X_1,\dots,X_d)$ — случайный вектор, распределенный на множестве X^d по закону $P^{(d)}$, $F_k(X)=(F_k(X_1),\dots,F_k(X_d))$, $k\in K$. Таким образом, на основании теоремы 2 получаем следующий результат.

Утверждение 1. Наименьший объем выборки, необходимый для проведения описанной ранее атаки с вероятностью ошибки, не превышающей $\delta \in (0, 1/2)$, удовлетворяет неравенству

$$t \geq \frac{(1-\delta)\log|S'| - h(\delta)}{|K|^{-1}\sum\limits_{k\in K}\Delta(P_k)}\ln 2, \tag{10}$$

где $\Delta(P_k)$ определяется по формуле (9).

Отметим, что в случае, когда $d = 1$, множества X, K, Z и S' являются векторными пространствами над некоторым конечным полем (соответственно абелевыми группами), а φ и ψ — линейными отображениями (соответственно гомоморфизмами абелевых групп), описанная атака представляет собой многомерную линейную атаку типа алгоритма 1 Матцуи, при этом формула (10) принимает классический вид [3, 16–18]. Вместе с тем эта формула содержит явную зависимость информационной сложности атаки от вероятности ошибки δ, а ее доказательство не использует каких-либо эвристических допущений или приближенных равенств.

Рассмотрим теперь различающую атаку на блочный шифр $\mathfrak{F}$, аналогичную приведенной ранее атаке. Пусть Φ — случайное отображение, которое с вероятностью $1/2$ является случайной равновероятной подстановкой на множестве X (гипотеза H_0) или случайным равновероятным шифрующим преобразованием шифра $\mathfrak{F}$ (гипотеза H_1). Требуется различить гипотезы H_0 и H_1 по известной реализации случайной последовательности $Z^{(t)} = Z_1, \ldots, Z_t$, где $Z_i = \varphi(X_i, \Phi(X_i))$, а φ и X_i определены ранее, $1 \leq i \leq t$.

Обозначим $\sigma(X)$ симметрическую группу подстановок на множестве X и зададим S как дизъюнктное объединение множеств $\sigma(X)$ и K. Положим $S' = \{0, 1\}$; $p(s) = 1/2 \cdot |\sigma(X)|^{-1}$ и $\psi(s) = 0$, если $s \in \sigma(X)$; $p(s) = 1/2 \cdot |K|^{-1}$ и $\psi(s) = 1$, если $s \in K$. Непосредственно из теоремы 3 вытекает следующий результат.

Утверждение 2. Наименьший объем выборки, необходимый для проведения указанной различающей атаки с вероятностью ошибки, не превышающей $\delta \in (0, 1/2)$, удовлетворяет неравенству

$$t \geq \frac{2(1-h(\delta))\ln 2}{|K|^{-1}\sum\limits_{k\in K}\Delta(P_k) + |X|!^{-1}\sum\limits_{F\in\sigma(X)}\Delta(P_F)}, \tag{11}$$

где $\Delta(P_k)$ определяется по формуле (9), $\Delta(P_F)$ — квадратичная евклидова несбалансированность распределения вероятностей $P_F(z) = P^{(d)}\{\varphi(X, F(X)) = z\}$, $z \in Z$, а $X = (X_1, \ldots, X_d)$ — случайный вектор, распределенный на множестве X^d по закону $P^{(d)}$, $F(X) = (F(X_1), \ldots, F(X_d))$, $F \in \sigma(X)$.

Отметим, что рассмотренная атака обобщает ряд известных различающих атак на блочные шифры [6, 7, 10–13, 16, 17]. В случае, когда $d = 1$, $X = \{0, 1\}^n$, $Z = \{0, 1\}$, а φ является линейной булевой функцией, упомянутая атака сводится к традиционной линейной различающей атаке. При этом $|X|!^{-1}\sum\limits_{F\in\sigma(X)}\Delta(P_F) = (2^n - 1)^{-1}$ и формула (11) принимает классический вид. Для случая многомерных линейных атак эта формула уточняет известные границы их информационной сложности [16–18], однако в отличие от последних содержит явную зависимость информационной сложности атаки от вероятности ошибки δ и не базируется на каких-либо приближенных равенствах.

Пусть R — конечное коммутативное кольцо с единицей; A — $t\times n$-матрица с линейно независимыми столбцами над кольцом R; s — неизвестный вектор, выбранный случайно равновероятно из некоторого множества $S\subseteq R^n$; $\xi_1,\dots,\xi_t$ — последовательность независимых случайных величин, распределенных на кольце R по закону $p_\xi(z)=P\{\xi_i=z\}$, $z\in R$, $1\le i\le t$. Требуется восстановить вектор s по известной реализации случайной последовательности $Z^{(t)}=Z_1,\dots,Z_t$, где $Z_i=A_is+\xi_i$, A_i — i-я строка матрицы A, A_is — скалярное произведение векторов A_i и s над кольцом R, $1\le i\le t$.

К решению этой задачи приводит построение корреляционных (в частности, быстрых корреляционных) атак на синхронные поточные шифры, причем, как правило, R является полем из двух элементов [8, 9]. В случаях $R=\mathbf{GF}(2^N)$ и $R=\mathbf{Z}/(2^N)$ методы решения упомянутой задачи приведены в работах [19–23].

Для получения нижней границы объема данных, необходимых для восстановления вектора s с заданной вероятностью ошибки, воспользуемся теоремой 2, полагая $S'=S$, $Z=R$, $\psi(s)=s$ для любого $s\in S$ и $P_{i,s}(z)=p_\xi(z-A_is)$, $z\in Z$, $1\le i\le t$.

Утверждение 3. Пусть распределение p_ξ отлично от равномерного распределения вероятностей на кольце R. Тогда наименьший объем выборки, необходимый для восстановления вектора s с вероятностью ошибки, не превышающей $\delta\in(0,1/2)$, удовлетворяет неравенству

$$t\ge\frac{(1-\delta)\log|S|-h(\delta)}{\Delta(p_\xi)}\ln 2, \tag{12}$$

где $\Delta(p_\xi)=|R|^{-1}\sum\limits_{z\in R}(|R|\,p_\xi(z)-1)^2$.

Формула (12) уточняет приближенную границу информационной сложности корреляционной атаки, приведенную в [21] для случая $R=\mathbf{GF}(2^N)$, $S=R^n$, однако в отличие от последней границы содержит явную зависимость информационной сложности от вероятности ошибки δ и не базируется на каких-либо приближенных равенствах.

УСИЛЕНИЕ ЛЕММЫ ВАДЕНЕИ

Рассмотрим важный частный случай поставленной ранее задачи проверки гипотез H_s $(s\in S')$, когда $S'=S=Z=\{0,1\}$, $\psi(s)=s$ для любого $s\in S$ и $P_{i,s}(1)=1-P_{i,s}(0)=p_s$, $i=0,1,\dots$, где $p_0=p<p_1=1/2$. Тогда последовательность $Z^{(t)}=Z_1,\dots,Z_t$ является схемой Бернулли с параметрами (t,p_s), где $p_s=p<1/2$, если $s=0$ (т.е. справедлива гипотеза H_0), и $p_s=1/2$, если $s=1$ (т.е. справедлива гипотеза H_1).

Обозначим

$$d(t,p)=\max_{A\subseteq\{0,1\}^t}\left\{\left|\sum_{z\in A}(p^{wt(z)}(1-p)^{t-wt(z)}-2^{-t})\right|\right\}$$

расстояние по вариации между распределениями случайной последовательности $Z^{(t)}$ при условии справедливости гипотез H_0 и H_1 соответственно. Так называемая лемма Ваденеи [10, лемма 15] утверждает, что

$$d(t,p)\le 2\sqrt{t}(1-2p),\quad p\in(0,1/2). \tag{13}$$

Эта лемма используется в [10–13] и полезна при решении задач обоснования стойкости поточных и блочных шифров относительно ряда статистических атак.

Использовав теорему 1, покажем, что верхнюю границу (13) можно усилить. А именно имеет место следующая теорема.

Теорема 4. Справедливо неравенство

$$d(t, p) \le \sqrt{3}/2 \cdot \sqrt{t}(1-2p), \quad p \in (0, 1/2). \tag{14}$$

Доказательство. Обозначим δ_* вероятность ошибки оптимального (байесовского) критерия для проверки гипотез H_0 и H_1. Тогда

$$d(t, p) = 1 - 2\delta_*. \tag{15}$$

Далее согласно теореме 1 наименьший объем выборки, необходимый для различения гипотез H_0 и H_1 с вероятностью ошибки, не превышающий δ_*, удовлетворяет неравенству $t \ge \dfrac{1-h(\delta_*)}{\max\limits_{1\le i\le t}\{I(S; Z_i)\}}$. При этом

$$I(S; Z_i) = H(Z_i) - H(Z_i / S) \le \log|Z| - H(Z_i / S) =$$
$$= 1 - 1/2 \cdot (H(P_{i,0}) + H(P_{i,1})) = 1/2 \cdot (1 - h(p)),\ 1 \le i \le t,$$

откуда следует, что

$$t \ge \frac{2(1-h(\delta_*))}{1-h(p)}. \tag{16}$$

Отметим, что для любого $x \in (0, 1)$ справедливы следующие неравенства:

$$\frac{1}{\ln 4}(1-2x)^2 \le 1 - h(x) \le \frac{3}{2\ln 4}(1-2x)^2. \tag{17}$$

Действительно, полагая $y = 2x - 1$ и используя разложение логарифмической функции в ряд Тейлора, получаем, что

$$h(x) = h\left(\frac{1+y}{2}\right) = -\frac{1}{\ln 2}\left(\frac{1+y}{2}\ln\left(\frac{1+y}{2}\right) + \frac{1-y}{2}\ln\left(\frac{1-y}{2}\right)\right) =$$

$$= -\frac{1}{\ln 2}\left(\frac{1+y}{2}\ln(1+y) + \frac{1-y}{2}\ln(1-y) - \ln 2\right) =$$

$$= 1 - \frac{1}{\ln 4}\left((1+y)\sum_{k=1}^{\infty}\frac{(-1)^{k-1}y^k}{k} - (1-y)\sum_{k=1}^{\infty}\frac{y^k}{k}\right) = 1 - \frac{1}{\ln 4}\sum_{k=1}^{\infty}\frac{y^{2k}}{k(2k-1)}.$$

Итак, справедливо равенство $1 - h(x) = \dfrac{1}{\ln 4}\sum\limits_{k=1}^{\infty}\dfrac{(1-2x)^{2k}}{k(2k-1)}$, из которого непосредственно следует нижняя граница (17). Далее,

$$1 - h(x) = \frac{1}{\ln 4}\sum_{k=1}^{\infty}\frac{(1-2x)^{2k}}{k(2k-1)} \le \frac{(1-2x)^2}{\ln 4}\sum_{k=1}^{\infty}\frac{1}{k(2k-1)} \le$$

$$\le \frac{(1-2x)^2}{\ln 4}\left(1 + \sum_{k=2}^{\infty}\frac{1}{k(2k-2)}\right) = \frac{(1-2x)^2}{\ln 4}\left(1 + \frac{1}{2}\cdot\sum_{k=2}^{\infty}\frac{1}{k(k-1)}\right) = \frac{3}{2}\cdot\frac{(1-2x)^2}{\ln 4},$$

откуда следует верхняя граница (17).

Использовав неравенства (16), (17), получим, что $t \ge \dfrac{4(1-2\delta_*)^2}{3(1-2p)^2}$. Отсюда на основании формулы (15) вытекает неравенство (14).

Теорема доказана.

Отметим, что согласно границе (14) наименьший объем выборки, необходимый для различения упомянутых гипотез H_0 и H_1, по крайней мере в $16/3$ раз больше, чем утверждает лемма Ваденеи. Это позволяет улучшить известные оценки информационной сложности статистических атак, доказательства которых базируются на лемме Ваденеи [10–13].

Полученные ранее границы информационной сложности статистических атак на блочные шифры имеют классический вид в случае (многомерных) линейных, обобщенных линейных и билинейных атак. Вместе с тем для некоторых видов атак (например, разностных) эти границы отличаются от классических и оказываются слишком грубыми. Далее предлагается метод построения границ информационной сложности статистических атак в указанном случае.

Рассмотрим описанную различающую атаку на блочный шифр $\mathfrak{F}$. Отметим, что эта атака состоит в проверке справедливости одной из двух гипотез: H_0 и H_1, по известной реализации случайной последовательности $Z^{(t)} = Z_1, \dots, Z_t$, где $Z_i = \varphi(X_i, \Phi(X_i))$, а φ, Φ и X_i определены ранее, $1 \le i \le t$.

Особенностью рассматриваемой атаки является то, что количество гипотез равно двум; при этом вероятность ошибки δ_* оптимального критерия их различения удовлетворяет равенству

$$1-2\delta_* = d(P_0, P_1), \tag{18}$$

где $d(P_0, P_1)$ — расстояние по вариации между распределениями случайной последовательности $Z^{(t)}$ при условии справедливости гипотез H_0 и H_1 соответственно.

Для любых $k \in K$, $F \in \sigma(X)$, $z \in Z$ обозначим

$$p_k(z) = P^{(d)}\{\varphi(X, F_k(X)) = z\}, \;\; p_F(z) = P^{(d)}\{\varphi(X, F(X)) = z\},$$

где $X = (X_1, \dots, X_d)$ — случайный вектор, распределенный на множестве X^d по закону $P^{(d)}$, $F_k(X) = (F_k(X_1), \dots, F_k(X_d))$, $F(X) = (F(X_1), \dots, F(X_d))$. Справедливы равенства

$$P_0(z_1, \dots, z_t) = \frac{1}{|X|!} \sum_{F \in \sigma(X)} p_F(z_1) \cdots p_F(z_t),$$

$$P_1(z_1, \dots, z_t) = \frac{1}{|K|} \sum_{k \in K} p_k(z_1) \cdots p_k(z_t),$$

где $(z_1, \dots, z_t) \in Z^t$. При этом

$$d(P_0, P_1) = 1/2 \sum_{(z_1, \dots, z_t) \in Z^t} |P_0(z_1, \dots, z_t) - P_1(z_1, \dots, z_t)|. \tag{19}$$

Теорема 5. Пусть $Z = \{0, 1\}$. Тогда наименьший объем выборки, необходимый для проведения рассматриваемой различающей атаки с вероятностью, не превышающей δ_*, удовлетворяет неравенству

$$t \ge \frac{1-2\delta_*}{\overline{p}_K + \overline{p}_F}, \tag{20}$$

где $\overline{p}_K = \dfrac{1}{|K|} \sum\limits_{k \in K} P^{(d)}\{\varphi(X, F_k(X)) = 1\}$, $\overline{p}_F = \dfrac{1}{|X|!} \sum\limits_{F \in \sigma(X)} P^{(d)}\{\varphi(X, F(X)) = 1\}$.

Доказательство. На основании формул (18), (19) имеем

$$1-2\delta_* = 1/2 \sum_{(z_1, \dots, z_t) \in \{0,1\}^t} \left| \frac{1}{|X|!} \sum_{F \in \sigma(X)} p_F(z_1) \cdots p_F(z_t) - \frac{1}{|K|} \sum_{k \in K} p_k(z_1) \cdots p_k(z_t) \right| =$$

$$= 1/2 \sum_{(z_1,\dots,z_t)Z^t} \left| \frac{1}{|X|!}\frac{1}{|K|} \sum_{\substack{F\in\sigma(X),\\ k\in K}} (p_F(z_1)\cdots p_F(z_t) - p_k(z_1)\cdots p_k(z_t)) \right| \le$$

$$\le \sum_{\substack{F\in\sigma(X),\\ k\in K}} \frac{1}{|X|!}\frac{1}{|K|} \left(1/2 \sum_{(z_1,\dots,z_t)\in\{0,1\}^t} \left| p_F(z_1)\cdots p_F(z_t) - p_k(z_1)\cdots p_k(z_t) \right| \right).$$

Отсюда, используя неравенство

$$1/2 \sum_{(z_1,\dots,z_t)\in\{0,1\}^t} | p_F(z_1)\cdots p_F(z_t) - p_k(z_1)\cdots p_k(z_t)| \le t/2 \sum_{z\in\{0,1\}} | p_F(z) - p_k(z)|,$$

в справедливости которого нетрудно убедиться с помощью индукции по t, получаем, что

$$1-2\delta_* \le t \sum_{\substack{F\in\sigma(X),\\ k\in K}} \frac{1}{|X|!}\frac{1}{|K|} |p_F(1) - p_k(1)| \le$$

$$\le t \left(\sum_{F\in\sigma(X)} \frac{1}{|X|!} p_F(1) + \sum_{k\in K} \frac{1}{|K|} p_k(1) \right) = t\,(\overline{p}_K + \overline{p}_F).$$

Таким образом, имеет место неравенство (20).

Теорема доказана.

В качестве примера применения полученной теоремы рассмотрим классическую разностную атаку на блочный шифр $\mathfrak{F}$ [10]. В этом случае $X = \{0,1\}^n$, $d = 2$ и для фиксированного дифференциала $(\alpha, \beta) \in \{0,1\}^n \times \{0,1\}^n \setminus \{(0,0)\}$ распределение $P^{(d)}$ является равномерным на множестве $\{(x, x\oplus\alpha): x \in V_n\}$, а отображение $\varphi: X^2 \times X^2 \to \{0,1\}$ определяется следующим образом:

$$\varphi(x_1, x_2, y_1, y_2) = 1 \Leftrightarrow x_1 \oplus x_2 = \alpha,\ y_1 \oplus y_2 = \beta,\ x_1, x_2, y_1, y_2 \in X.$$

Из данных определений следует, что

$$p_k(1) = P_X\{F_k(X\oplus\alpha)\oplus F_k(X) = \beta\},\ \ p_F(1) = P_X\{F(X\oplus\alpha)\oplus F(X) = \beta\},$$

где X — случайный вектор с равномерным распределением на множестве $\{0,1\}^n$. Таким образом, $\overline{p}_K$ и $\overline{p}_F$ совпадают с классическими (средними) вероятностями дифференциала (α, β) блочного шифра $\mathfrak{F}$ и случайной равновероятной подстановки F соответственно:

$$\overline{p}_K = \frac{1}{|K|} \sum_{k\in K} P_X\{F_k(X\oplus\alpha)\oplus F_k(X) = \beta\},$$

$$\overline{p}_F = \frac{1}{|X|!} \sum_{F\in\sigma(X)} P_X\{F(X\oplus\alpha)\oplus F(X) = \beta\}.$$

Кроме того, справедливо равенство $\overline{p}_F = (2^n - 1)^{-1}$, и на основании теоремы 5 информационная сложность рассматриваемой атаки ограничена снизу значением $\dfrac{1-2\delta_*}{\overline{p}_K + (2^n-1)^{-1}}$, которое по порядку величины совпадает с классической границей сложности различающей разностной атаки на блочные шифры [10, лемма 12].

ЗАКЛЮЧЕНИЕ

Основными результатами статьи являются неасимптотические нижние границы информационной сложности статистических атак на блочные и поточные шифры. Эти границы получены с помощью неравенства Фано на основе общей статистической модели, описывающей практически все известные виды атак. В отличие от известных предложенный метод построения границ информационной сложности применяется в случае произвольного (конечного) числа статистических гипотез, не требует информации о виде статистических критериев, применяемых при проведении атак, и не использует асимптотических соотношений, приближенных формул или эвристических предположений об исследуемом шифре.

В случае (многомерных) линейных, обобщенных линейных, билинейных и разностных атак полученные границы информационной сложности имеют классический вид. Для других видов атак эти границы позволяют ввести обоснованные параметры, характеризующие стойкость симметричных криптосистем относительно описанных атак. Это важно при создании общей теории обоснования стойкости симметричных криптосистем относительно статистических методов криптоанализа.

СПИСОК ЛИТЕРАТУРЫ:

1. Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems *Journal of Cryptology*. 1991. Vol. 4, N 1. P. 3–72.
2. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis. *Advances in Cryptology — EUROCRYPT'91*: Proc. Springer Verlag, 1991. P. 17–38.
3. Matsui M. Linear cryptanalysis methods for DES cipher. *Advances in Cryptology — EUROCRYPT'93*: Proc. Springer Verlag,. 1994. P. 386–397.
4. Harpes C., Kramer G.G., Massey J.L. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma. *Advances in Cryptology — EUROCRYPT'95*: Proc. Springer Verlag, 1995. P. 24–38.
5. Courtois N.T. Feistel schemes and bi-linear cryptanalysis. *Advances in Cryptology — CRYPTO'04*: Proc. Springer Verlag,. 2004. P. 23–40.
6. Blondeau C., Gérard B., Tillich J.-P. Accurate estimates on the data complexity and success probability for various cryptanalysis. *Desigh, Codes and Cryptography*. 2011. Vol. 59(1–3). P. 3–34.
7. Samajder S., Sarkar S. Rigorous upper bounds on data complexities of block cipher cryptanalysis. Cryptology ePrint Archive, Report 2015/916. URL: http://eprint.iacr.org/2015/916.
8. Canteaut A. Fast correlation attacks against stream ciphers and related open problems. *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*. ITW 2005. E-Proc. 2005. P. 49–54.
9. Meier W. Fast correlation attacks: methods and countermeasures. *Lecture Notes in Computer Science — FSE'2011*: Proc. Springer Verlag. 2011. P. 55–67.
10. Vaudenay S. Decorrelation: a theory for block cipher security. *Journal of Cryptology*. 2003. Vol. 16, N 4. P. 249–286.
11. Алексейчук А.Н., Шевцов А.С. Показатели и оценки стойкости блочных шифров относительно статистических атак первого порядка. *Реєстрація, зберігання і обробка даних*. 2006. Т. 8, вип. 4. С. 53–63.
12. Алексейчук А.Н., Проскуровский Р.В., Шевцов А.С. Аналитические оценки и достаточные условия стойкости блочных шифров и комбинирующих генераторов гаммы с неравномерным движением относительно статистических методов криптоанализа *Прикладная радиоэлектроника*. 2007. Т. 6, № 2. С. 264–273.
13. Blondeau C., Bay A., Vaudenay S. Protecting against multidimensional linear and truncated differential cryptanalysis by decorrelation. Cryptology ePrint Archive, Report 2015/380. URL: http://eprint.iacr.org/2015/380.

14. Боровков А.А. Математическая статистика. Москва: Наука, 1984. 472 с.

15. Чисар И., Кернер Я. Теория информации. Теоремы кодирования для дискретных систем без памяти. Москва: Мир, 1985. 397 с.

16. Baigneres T., Junod P., Vaudenay S. How far we go beyond linear cryptanalysis? *Advances in Cryptology — ASIACRYPT'04*. Proc. Springer Verlag, 2004. P. 432–450.

17. Baigneres T., Stern J., Vaudenay S. Linear cryptanalysis of non binary ciphers (with an application to SAFER). *Selected Areas in Cryptography — SAC'07:* Proc. Springer Verlag, 2007. P. 184–211.

18. Hermelin M., Cho J.Y., Nyberg K. Multidimensional linear cryptanalysis of reduced round Serpent. *Lecture Notes in Computer Science — ACISP'2008*: Proc. Springer Verlag, 2008. P. 203–215.

19. Johansson T., Jonsson F. Correlation attacks on stream ciphers over GF(2^N). *International Symposium on Information/Theory — ISIT'2001*: Proc. Springer Verlag, 2001. P. 140.

20. Jonsson F. Some results on fast correlation attacks Ph.D. Thesis, Lund University, Sweden, 2002.

21. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. Cryptology ePrint Archive, Report 2016/311. URL: http://eprint.iacr.org/2016/311.

22. Алексейчук А.Н., Игнатенко С.М. Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Реєстрація, зберігання і обробка даних*. 2005. Т. 7, № 1. С. 21–29.

23. Алексейчук А.Н., Игнатенко С.М. Нижняя граница вероятности восстановления истинного решения системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. 2006. № 4. С. 6–12.

Надійшла до редакції 14.12.2016

А.М. Олексійчук

НЕАСИМПТОТИЧНІ НИЖНІ МЕЖІ ІНФОРМАЦІЙНОЇ СКЛАДНОСТІ СТАТИСТИЧНИХ АТАК НА СИМЕТРИЧНІ КРИПТОСИСТЕМИ

Анотація. Запропоновано метод отримання нижніх меж інформаційної складності статистичних атак на блокові чи потокові шифри. Метод базується на застосуванні нерівності Фано та на відміну від раніше відомих не використовує будь-яких асимптотичних співвідношень, наближених формул або евристичних припущень про досліджуваний шифр. Отримані межі інформаційної складності для низки видів атак мають класичний вигляд, а для інших видів дозволяють ввести обґрунтовані параметри, що характеризують стійкість симетричних криптосистем до цих атак.

Ключові слова: симетрична криптографія, перевірка статистичних гіпотез, статистична атака, блоковий шифр, потоковий шифр, кореляційна атака, інформаційна складність, нерівність Фано.

A.N. Alekseychuk

NON-ASYMPTOTIC LOWER BOUNDS FOR THE DATA COMPLEXITY OF STATISTICAL ATTACKS ON SYMMETRIC CRYPTOSYSTEMS

Abstract. A method is proposed for obtaining the lower bounds of data complexity of statistical attacks on block or stream ciphers. The method is based on the Fano inequality and, unlike the available methods, doesn't use any asymptotic relations, approximate formulas or heuristic assumptions about the considered cipher. For a lot of known types of attacks the obtained data complexity bounds have the classical form. For other types of attacks these bounds allow us to introduce reasonable parameters that characterize the security of symmetric cryptosystems against these attacks.

Keywords: symmetric cryptography, statistical hypotheses testing, statistical attack, block cipher, stream cipher, correlation attack, data complexity, Fano's inequality.

Алексейчук Антон Николаевич,
доктор техн. наук, доцент, ведущий научный сотрудник научно-исследовательского центра Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехниический институт имени Игоря Сикорского», e-mail: alex-dtn@ukr.net.