КОМПЬЮТЕРНАЯ МАТЕМАТИКА

УДК 681.3

А.М. КУДИН

МОДЕЛЬ ОЦЕНКИ СТОЙКОСТИ МОДУЛЕЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ К КРИПТОАНАЛИЗУ ПО ПОБОЧНЫМ КАНАЛАМ

Рассмотрены модели оценки стойкости реализации криптосистем относительно атак криптоанализа по побочным каналам. Предлагается модель на базе общей теории оптимальных алгоритмов. Особенностью предложенной модели является ее применимость к криптографическим модулям в распределенных вычислительных системах.

Введение. Известно [1, 2], что существует несколько уровней абстракции при проектировании и анализе стойкости криптографических систем: от абстрактной математической модели криптографического преобразования (например, алгебраические и вероятностные модели шифра) до модели средства криптографической защиты информации (средства КЗИ) и криптосистемы, состоящей из них, с точки зрения их реализации на конкретной программно-аппаратной платформе. Первые модели в основном анализируются методами классического криптоанализа, вторые – криптоанализа с использованием информации из побочных каналов (далее – криптоанализ по побочным каналам, англ. – side-channel cryptoanalisys). Таким образом, в криптоанализе по побочным каналам исследуется влияние косвенной информации, полученной при работе криптосистемы, на ослаблении стойкости к частичному или полному взлому криптографической системы [2, 3]. Очевидно, что методы криптоанализа по побочным каналам зависят от архитектуры и особенностей реализации вычислительной системы, в рамках которой реализовано средство КЗИ (криптосистема). Развитие идеологии распределенных вычислительных систем и их наиболее современного варианта – облачных вычислительных систем, существенно меняют постановки задач анализа

стойкости средств КЗИ (криптосистем)	относительно методов криптоанализа по

побочным каналам и синтеза стойких средств КЗИ (криптосистем). В статье приводится новая формальная модель решения обозначенных задач для некоторых частных случаев.

Анализ известных методов оценки стойкости к атакам по побочным каналам

Анализ существующих моделей оценки стойкости от атак по побочным каналам проводится с учетом того, что вначале необходимо построить математическую модель некоторого физического процесса, в результате которого получается косвенная информация о секретных параметрах. Этим они отличаются от моделей оценки стойкости криптографических преобразований, в которых, как правило, изначально рассматриваются математические отношения. Такими физическими процессами могут быть время выполнения в средстве КЗИ арифметических операций или других операций с участием ключа (так называемые «временные» атаки [3]), изменения мощности, потребляемой модулем КЗИ в различные моменты времени (атаки измерения потребляемой мощности [3]), электромагнитных или акустических сигналов, излучаемых при работе модуля КЗИ. При этом измерения параметров этих физических процессов проводится или в нормальном режиме функционирования модуля (обычные или пассивные атаки), или в аварийных режимах, связанных с внешними дестабилизирующими воздействиями или подачей на вход некорректных исходных данных (так называемые активные атаки или атаки на основе генерируемых ошибок) [4]. Дополнительно к этому измерения могут осуществляться непосредственно (простые атаки) и с учетом нескольких наблюдений, выбранных адаптивно (разностные атаки).

Разнородность этих физических процессов, а также методов измерения их параметров и определяет нетривиальность задачи построения универсальных моделей оценки стойкости модулей КЗИ к атакам по побочным каналам. С другой стороны, построение таких универсальных моделей – актуальная задача, поскольку методы оценки модулей КЗИ, зависящих от конкретных программно-аппаратных платформ практически неприменимы для распределенных и «облачных» вычислительных систем.

Определимся с понятиями «распределенная вычислительная система» и «облачные вычисления», которые будем использовать в дальнейшем. Под «распределенной вычислительной системой» [5] будем понимать систему, в которой технология обработки локальных и удаленных информационных ресурсов не различается. Следуя этому, информационные ресурсы могут храниться и обрабатываться на любом подмножестве $U_t \subseteq U$ вычислительных узлов системы (здесь U – множество всех вычислительных узлов системы). Для каждого информационного ресурса $i \in I$ в каждый момент времени t таким образом определено отображение $i \to U_t$.

Для определения «облачных вычислений» в настоящее время не выработано единого понятия, однако согласно предварительной терминологии NIST [6], понятие «облачных вычислений» характеризуется через пять основных свойств

обработки информации, три модели предоставления ресурсов и четыре модели использования облачной системы. Этими свойствами являются: самообслуживание пользователей «по запросу» (grid computing), эластичные (то есть такие, которые предоставляются в необходимом объеме) вычислительные мощности, единое пространство вычислительных ресурсов любого типа без ограничения их географического местоположения, широкополосные мобильные сети и точно измеримые вычислительные ресурсы. Ресурсы облачных систем могут использоваться в режимах «система как сервис» (PaaS), «программное обеспечение как сервис» (SaaS), «инфраструктура как сервис» (IaaS). Использование облачных систем клиентами может осуществляться в виде частного облака (все ресурсы принадлежат клиенту или используются клиентом «в лизинге»), общественное облако (ресурсы принадлежат некоторому сообществу), публичное облако (ресурсы принадлежат провайдеру вычислительных услуг), гибридное облако. Ясно, что в этих условиях происходит максимальная унификация программного и аппаратного обеспечения вычислительных систем, в том числе и модулей КЗИ. Отсюда следует, что требования к защите модулей повышаются из-за увеличения числа потенциальных нарушителей, а значит задача построения универсальных моделей оценки стойкости модулей КЗИ актуальна.

Очевидно, первоочередным для построения универсальной модели является обобщенная модель возникновения побочного канала при работе модуля КЗИ. В работе [7] предлагается строить такую модель на основании следующих предположений-аксиом.

Аксиома 1. Утечка косвенной информации, которую можно использовать в криптоанализе по побочным каналам происходит только в рамках вычислительного процесса.

Аксиома 2. Одни и те же вычисления могут приводить к разной утечке информации на разных компьютерах.

Аксиома 3. Утечка информации зависит от выбранного метода измерений.

Аксиома 4. Утечка зависит от внутренней конфигурации устройства.

Аксиома 5. Вся утечка информации, которая вычисляется путем наблюдения физического процесса, сопровождающего функционирование устройства, может быть эффективно вычислена из внутреннего состояния устройства.

С использованием этих аксиом и понятия функции утечки секретного параметра $\lambda(S): S \to L$, где S – искомый секретный параметр, являющийся реализацией равномерной случайной величины $S \xleftarrow{R} \{0,1\}^k$, а L – множество значений косвенной информации об S (например, весов Хэмминга S), в работе [8] вводятся различные формальные модели оценки стойкости модулей КЗИ. Если в качестве меры используется энтропия, то мы получаем теоретико-информационные модели, если эффективность распознавания S вероятностным полиномиальным алгоритмом – теоретико-сложностные.

Теоретико-информационные модели успешности атак по побочным каналам

Формальные теоретико-информационные модели успешности атак по побочным каналам, универсальные относительно атаки, как правило, оценивают отклонение распределения искомой случайной величины (ключа или другого секретного параметра) от априорного (как правило, равномерного) распределения за счет наблюдения поведения другой случайной величины (дополнительной информации, получаемой в ходе работы устройства). Наиболее простой моделью можно считать следующую [8].

Пусть S – искомый секретный параметр, являющийся реализацией равномерной случайной величины $S \xleftarrow{R} \{0,1\}^k$. Тогда криптоанализ по побочным каналам успешен, если для любой произвольной функции $\lambda(S)$, называемой «функцией утечки» условное распределение $\mathrm{P}(S \mid \lambda(S))$ отлично от равномерного.

Легко показать, что достоинствами данной модели является простота доказательства существования слабостей к криптоанализу по побочным каналам при *известной функции утечки,* а недостатками – сложность осуществления доказательства отсутствия слабостей к криптоанализу по побочным каналам *для всех функций утечки* и сложности оценки практической осуществимости атак. Кроме того, рассмотренная модель не применима для случая атак второго и более высоких порядков [9].

Более сложные модели рассматривают возможность многократного измерения состояния побочного канала информации. Пусть O_S^q – измерения величины S, полученные за q запросов к криптографическому модулю. Тогда мера стойкости определяется через матрицу взаимной информации $\mathbf{I}(S; O_S^q)$.

Модели успешности атак по побочным каналам на основе теории вычислительной сложности

Теоретико-информационные модели определяют принципиальную возможность осуществления атак по побочным каналам на модули КЗИ, но имеющаяся информация может оказаться не реализуемой эффективными вычислительными алгоритмами. В силу этого применяются модели, определяющие возможность распознавания S вероятностным полиномиальным алгоритмом. Рассмотрим одну из них.

Пусть f_K – модуль КЗИ со встроенным секретным ключом $K \in \{0,1,\ldots G-1\}$. Пусть $A_{f_K,\lambda}(t,q)$ – вероятностный полиномиальный алгоритм атаки по побочному каналу со временем t, количеством запросов к f_K равным q, функцией утечки λ. Введем следующий алгоритм распознавания $\mathbf{KeR}_{f_K,A}$:

шаг 1. $K \xleftarrow{R} \{0,1,\ldots,G-1\}$,

шаг 2. $K^* \leftarrow A_{f_K,\lambda}(t,q)$,

шаг 3. Если $K = K^*$ то вернуть 1 и останов,

шаг 4. Иначе вернуть 0 и останов.

Тогда мера стойкости вводится как успешность работы алгоритма распознавания или «выигрыша» противника:

$$\mathbf{ADV}_{f_K,A}(t,q) = P(\mathbf{KeR}_{f_K,A} = 1).$$

$$\mathbf{ADV}_{f_K}(t,q) = \max_{A,\lambda}\{\mathbf{ADV}_{f_K,A}(t,q)\}.$$

Недостатком этого класса моделей следует считать отсутствие связи эффективности алгоритма распознавания с качеством информации, получаемой по побочному каналу.

Рассмотрим модель оценки стойкости, которая позволяет объединить достоинства теоретико-информационных и теоретико-сложностных моделей, а также учитывать качество информации, получаемой по побочному каналу.

Модель оценки стойкости средств КЗИ к атакам по побочным каналам на основе общей теории оптимальных алгоритмов

Теоретической основой такой модели оценки стойкости модулей КЗИ к атакам по побочным каналам предлагается выбрать общую теорию оптимальных алгоритмов [10], которая связывает существование и сложность алгоритмов с точностью задания входных данных. При этом в качестве одной из мер случайности множеств X, Y целесообразно использовать колмогоровскую меру информации.

Введем следующие обозначения. Пусть заданы множества X, Y. Пусть 2^Y – класс всех подмножеств множества Y. В работе [10] 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 (рисунок).

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 $\delta_1 \le \delta_2 \Rightarrow$ $\Rightarrow A(N, x, \delta_1) \subset A(N, x, \delta_2)$. Тогда величины $r(N, x) = \inf\{\delta : A(N, x, \delta) \neq \varnothing\}$ и $r(N) = \sup_{x \in X} r(N, x)$ определяют нижние оценки точности решений, которые могут быть достигнуты при неполном информационном операторе.

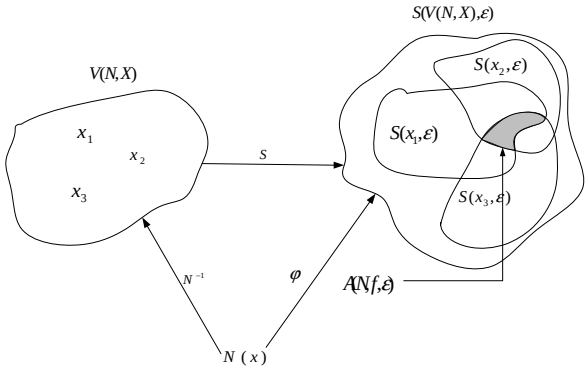

РИСУНОК. Информационный оператор и оператор решения

В работе [10] 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 отличие от точного информационного оператора, оператор N_ρ определяется через оператор информационной ошибки $E : H \times R_+ \to 2^H$, обладающий двумя свойствами:

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

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

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 $r(N_\rho) = 0$.

Обозначим X – значение секретной случайной величины, которое нужно определить в результате атаки по побочному каналу, тогда $N(X)$ – информация, известная по наблюдениям величины X, $S : X \times R_+ \to 2^G$ оператор (в частном случае – функция) утечки информации, G – множество значений функции утечки. В зависимости от практической ситуации в качестве множества G могут использоваться, например, веса Хемминга, значение бита четности и т. д. Заметим, что для достижения стойкости криптографического модуля к атаке по побочным каналам системы оператор N должен быть неполным.

В качестве $\Phi(N(X))$ выбираем множество идеальных алгоритмов φ реализации оператора атаки. При этом условие стойкости 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 измерения. При этом, как указывалось выше, при полном точном информационном операторе N оператор N_ρ может оказаться как полным, так и неполным.

Заметим, что предложенная модель хорошо ориентирована на оценку стойкости криптографических модулей в распределенных и «облачных» вычислительных системах благодаря возможности моделирования ситуации вычисления модулей КЗИ на разных узлах системы (из-за свойства информационного оператора учитывать «качество» информации с точки зрения точности решения задачи оператором решения).

А.М. Кудін

МОДЕЛЬ ОЦІНКИ СТІЙКОСТІ МОДУЛІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ДО КРИПТОАНАЛІЗУ ЗА ПОБІЧНИМИ КАНАЛАМИ

Розглянуті моделі оцінки стійкості реалізації криптосистем щодо атак криптоаналізу за побічними каналами. Пропонується модель оцінки стійкості на базі загальної теорії оптимальних алгоритмів. Особливістю запропонованої моделі є можливість її застосування для криптографічних модулів у розподілених обчислювальних системах.

A.M. Kudin

SECURITY ESTIMATION MODEL FOR CRYPTOGRAPHIC MODULE AGAINST SIDE-CHANNEL CRYPTOANALYSIS

Models for estimation of security of cryptosystem implementation are considered against side-channel attacks cryptoanalysis. A model for estimation of security is proposed on the basis of general optimal algorithm theory. A peculiarity of the model proposed is its applicability for cryptographic modules in distributed computer systems.

1. *Задирака В.К., Кудин А.М., Людвиченко В.А., Олексюк А.С.* О технологии криптографической защиты информации на специальных цифровых носителях // Управляющие системы и машины. – 2010. – № 4. – С. 77–83.
2. *Jean-Jacques Quisquater* Side channel attacks State-of-the-art October 2002 // www.psu.citeseer.edu.
3. *Paul Kocher.* Rational Paranoia: Securing unusually high-threat Systems // RSA 2003 Conference. – www.cryptography.com
4. *Certin Kaya Koc.* Cryptographic engineering / Springer Science+Business Media, LLC 2009. – 528 p.
5. *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с.
6. *Peter Mell, Tim Grance.* Effectively and Securely Using the Cloud Computing Paradigm // http://csrc.nist.gov/groups/SNS/cloud-computing/index.html
7. *Micali S., Reyzin L.* Physically Observable Cryptography // Proceedings of TCC 2004. – Lecture Notes in Computer Science. – 2004. – **2951**. – P. 278–296.
8. *Francois-Xavier Standaert, Tal G. Malkin, Moti Yung.* A formal practice-oriented model for analysis of side-channel attacks // www.psu.citeseer.edu.
9. *Kerstin Lemke-Rust and Christof Paar.* Gaussian mixture models for higher-order side channel analysis //www.psu.citeseer.edu.
10. *Трауб Д., Васильковский Г., Вожьняковский Х.* Информация, неопределенность, сложность. – М.: Мир, 1988. – 184 с.

Получено 18.04.2011

Об авторе:

Кудин Антон Михайлович,

кандидат технических наук, старший научный сотрудник,
докторант Института кибернетики имени В.М. Глушкова НАН Украины.