УДК 681.3:519.72:003.26

В.К. ЗАДИРАКА, А.М. КУДИН

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ В КРИПТОГРАФИИ И СТЕГАНОГРАФИИ

Ключевые слова: *распределенные вычислительные системы, облачные вычисления, криптография, многоразрядная арифметика, метод Карацубы, криптоанализ по побочным каналам, общая теория оптимальных алгоритмов.*

1. Особенности облачных информационно-коммуникационных технологий, определяющие новые постановки задач криптографии. Облачные информационно-коммуникационные системы (ОИКС) являются одной из реализаций теоретической концепции распределенных вычислительных систем [1]. Объектом исследований облачные системы стали недавно, поэтому существует несколько определений ОИКС. В статье использованы два основных определения, отличающиеся аспектом рассмотрения облачных систем: функциональное [2] и технологическое [3]. Согласно функциональному определению ОИКС рассматривают с точки зрения предоставляемых ими возможностей и относят к ним системы, в которых:

— определяются такие особенности обработки информации, как самообслуживание пользователей по запросу (grid computing), эластичные (предоставляемые в любом нужном объеме) вычислительные мощности, единое пространство динамически распределяемых вычислительных ресурсов любого типа (без ограничений на географическое расположение), возможность удаленного доступа к ресурсам системы с требуемой скоростью без ограничения на географическое расположение пользователя (что обусловливает использование высокоскоростных мобильных сетей), точно измеримые вычислительные ресурсы;

— существуют такие модели предоставления услуг, как программное обеспечение (прикладное программное обеспечение, в том числе системы управления базами данных) в качестве сервиса (SaaS, DbaaS), платформа (операционная система и т.д.) в качестве сервиса (PaaS), инфраструктура (физические вычислительные ресурсы и виртуальные машины, управляющие ими) в качестве сервиса (IaaS);

— имеются такие варианты использования информационных ресурсов системы, как частное облако (ресурсы принадлежат клиенту или используются им в лизинге), общественное облако (ресурсы принадлежат некоторому сообществу, характерный пример — социальные сети), публичное облако (ресурсы принадлежат провайдеру облачных услуг), гибридное облако.

В основе технологического определения облачных вычислений лежит совместное применение двух технологий: измеримые распределенные вычисления по запросу, которые берут начало в грид-технологии [3], и виртуализация, позволяющая эффективно решать задачу миграции программного обеспечения между гетерогенными элементами распределенной системы. Исходя из этих определений, можно выделить основные особенности облачных информационно-коммуникационных технологий, обусловливающие новые постановки описанных далее задач криптографии.

Для облачных вычислительных систем (ОВС) характерно наличие асимметричных вычислений — мощного облака с практически неограниченными вычислительными возможностями и множества терминальных устройств (в том числе

мобильных), которые ставят проблему так называемой «легковесной (низкоресурсной) криптографии» [4]. Это определяет задачу создания «наращиваемых» по стойкости криптопримитивов, способных решать сложные задачи в облаке и минимальные в терминале. Фактически это обобщение требований, выдвигаемых к гомоморфным криптосистемам.

В ОВС повышается актуальность эффективного решения задачи обработки зашифрованных данных, которая позволяет обеспечить такое свойство криптографического преобразования, как гомоморфность [5]. Однако известно [6], что оно снижает стойкость криптосистемы. Это обусловливает постановку задач создания оптимальных по стойкости гомоморфных криптосистем.

Упомянутая выше асимметрия мощности ОВС определяет новые постановки задач безопасной реализации криптосистем. Для распределенных вычислительных систем в общем и для облачных в частности изменяется модель возникновения побочного канала для модулей криптографической защиты информации. Главная особенность такой модели в [7] — возможность моделирования ситуации, когда агенты, составляющие криптосистему, работают на разных узлах распределенной системы. Для ОВС к атакам по побочным каналам добавляются атаки, связанные с функционированием криптографических модулей в среде виртуальной машины, а также направленные на криптографические модули гипервизора.

Для эффективной работы в составе облака криптосистема должна обеспечивать эластичность предоставления услуг, а значит, реализоватся по одной из технологий, поддерживающих облачные вычисления. Технология реализации криптосистем, которая может применяться для облаков, описана в [7, 8]. Фактически предложенная в этих работах концепция специальных цифровых носителей информации является вариантом построения криптосистемы как множества взаимодействующих мобильных агентов. Как и в классической агентно-ориентированной парадигме построения распределенных вычислительных систем, каждая часть цифрового носителя является интеллектуальным агентом, способным подстраиваться под изменяющиеся внешние условия. Наиболее эффективна в этом случае модель, в которой мобильные агенты, реализующие криптосистему любой сложности, формируются из криптопримитивов в зависимости от функциональности. Криптосистема, созданная по такому принципу, способна работать с распределенными данными и изменять (наращивать и снижать) свою эффективность без потери стойкости. При этом эффективность оценивается не только быстродействием, но и расходом «ценных» ресурсов (например, случайных последовательностей и ключей). Нерешенной проблемой является построение минимально достаточного множества криптопримитивов и автоматическое определение стойкости криптопротоколов и криптосистем, созданных из этих криптопримитивов. Эта проблема повышает также актуальность направления исследований формального анализа стойкости криптографических протоколов.

Реализацию криптосистем по агентной парадигме можно осуществить с использованием XML-шаблонов. Атаки на XML-данные принципиально отличны от атак на другие форматы хранения данных, поскольку сами данные могут содержать инструкции по своей обработке. При этом обработка исключительных ситуаций, ошибок и сбоев тоже, как правило, управляется самими данными в автоматическом режиме. Последнее предоставляет широкие возможности для осуществления атак на реализацию [9–11]. В этом случае нерешенной проблемой является отсутствие эффективной по быстродействию формальной методики оценки текущего состояния защищенности от атак на реализацию.

Новые возможности использования ОВС для криптоанализа ограничиваются проблемой раскрытия целей и методик криптоанализа перед провайдером услуг ОВС. Поэтому возникают новые постановки задач, связанные с определением перечня вычислительных задач, существенных для криптоанализа, изучение которых в совокупности не позволяло бы восстанавливать задачу криптоанализа в целом. Фактически речь идет о частном виде задачи разделения секрета.

В ОВС в силу массовости применения стандартных криптографических модулей уточняются постановки традиционных задач (в частности, построение автоматических систем управления ключами с варьируемой стойкостью).

Теоретической основой для решения поставленных выше задач является общая теория оптимальных алгоритмов [12–14] и теория алгоритмической информации Колмогорова [15–17].

2. Аспекты решения задачи построения криптосистем и стеганосистем для ОВС. В работах [18–19], посвященных проблемам безопасности в облачных системах, методы решения задач, поставленных в разд. 1 статьи, существенно отличаются в зависимости от модели предоставления услуг. Поэтому все последующие методы решения предложены для наиболее сложной модели — SaaS (программное обеспечение как сервис), при этом основное внимание уделяется:

— прозрачности и верифицируемости описанных методов и технологий для пользователя облака;

— адаптивности методов к моделям ценности информации, метаданным систем защиты и к увеличению нагрузки на вычислительные ресурсы;

— асимметричности вычислительных моделей в ОВС, т.е. наличию маломощных вычислительных узлов с последовательной моделью вычислений (пользовательские терминалы) и мощных вычислительных узлов с параллельной моделью вычислений (центры обработки данных);

— многократному использованию стандартных виртуальных машин различными пользователями с разными полномочиями доступа к информации;

— сложности использования в рамках виртуальной машины физических источников случайных чисел.

Изложенные требования являются частным случаем для криптографических и стенографических систем, вытекающие из общей модели угроз ОВС, рассмотренной в [20]. Остановимся на требованиях адаптивности к нагрузкам и асимметричности вычислительных моделей. Эти требования обусловливают актуальность исследований в области низкоресурсной [4] криптографии [21–22]. Развитием идей, предложенных в этих работах, являются адаптивные к асимметричной вычислительной модели и входным данным алгоритмы многословной арифметики, поиска простых чисел и базовые операции реализации стеганографических преобразований.

Рассмотрим алгоритм многословного умножения, являющийся базовым для многих криптографических и стеганографических преобразований.

Классический алгоритм Карацубы легко распространяется на случай деления множителей на $r+1$, $r>1$, равных частей [23] (для $r=2$ — это метод Тоома–Кука). В этом случае время выполнения умножения двух n-разрядных чисел оценивается как $(T(r+1)n) \le (2r+1)T(n)+cn$. В ОИКС вычисления не только асимметричны, но и должны удовлетворять требованию точной измеримости. Поэтому актуально исследование асимметричного метода быстрого умножения Карацубы, когда нужно оптимальным способом разбить множители на неравные части в зависимости от разрядности слова привлекаемых вычислительных ресурсов и их стоимости. Заметим, что в отличие от метода Ш. Винограда [24], ориен-

тированного на случай умножения, в котором размерность одного операнда в три раза меньше другого, в данной статье рассмотрены операнды равного размера, но разбитые на несколько неравных частей. Идея предлагаемого метода состоит в том, что операнды длиной n разбиваются на две части: длиной $k_1 \cdot n / s_1$ и $n - k_1 \cdot n / s_1$, где s_1 — длина слова существующего вычислительного ресурса, k_1 — количество слов операнда для данного вычислительного ресурса, определяемое из условия его граничной производительности. Оставшиеся части операндов длиной $n - k_1 \cdot n / s_1$ продолжаем последовательно разбивать, применяя для выбора их оптимального размера метод динамического программирования. Оптимальный выбор на каждом шаге определяется следующими векторами: размеров слов вычислительных ресурсов $(s_2, s_3, s_4, \ldots)$, количества обрабатываемых слов $(k_2, k_3, k_4, \ldots)$, стоимости данных ресурсов $(c_2, c_3, c_4, \ldots)$.

Следующая задача исследования состоит в построении из базовых криптографических примитивов необходимых криптографических механизмов. Базовыми являются идеальные генератор псевдослучайной последовательности $G : \{0,1\}^k \to \{0,1\}^\infty$ и хэш-функция $H : \{0,1\}^\infty \to \{0,1\}^k$. Построение симметричной криптографической системы с использованием данных примитивов возможно. Для асимметричных криптосистем дополнительным примитивом, очевидно, должна стать слабая односторонняя функция, определенная как честная функция $f : \{0,1\}^n \to \{0,1\}^{m(n)} (n \le q(m(n)))$, где $q(m(n))$ — любой полином, удовлетворяющая двум условиям:

— существует вероятностный алгоритм полиномиальной сложности, вычисляющий $f(x) \ \forall x \in \{0,1\}^n$;

— для любого вероятностного алгоритма полиномиальной вычислительной сложности A, который использует на входе случайную строку 1^n длины n, существует полином p такой, что для всех $n \ge n_0$ имеем

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

Известно [25], что существование слабых односторонних функций необходимо и достаточно для существования сильных, тем не менее неясно, достаточно ли этого для реализации доказуемо стойких асимметричных криптосистем [26].

Построение стеганографических систем в ОВС — мало изученный вопрос. Как показано в [27], важнейшей задачей реализации стегосистемы и повышения ее стойкости к стеганоанализу является выбор или построение контейнеров. При формировании контейнеров стеганосистем в ОВС необходимо комплексно использовать все виды избыточности систем: функциональную (возможность выполнения задач системы более чем одним методом), информационную (наличие избыточной информации, например в базах данных, информационных хранилищах и т.п.), представления данных (избыточность кодирования). В настоящее время лучше исследован последний вид избыточности для мультимедийных данных и практически не исследован вопрос использования избыточности первых двух видов.

3. Технологии применения криптографических и стеганографических систем в ОВС. Остановимся на некоторых аспектах решения задачи оценки стойкости криптосистем и стеганосистем к атакам по побочным каналам для облачных вычислений. Рассмотрим постановку задачи, аналогичную приведенной в [7, 20].

Для сообщения m вычисляется хэш-функция $h(m)$ и цифровая подпись $S = h(m)^d \bmod N_{rsa}$, где N_{rsa} — модуль системы RSA, d — секретный ключ вы-

работки подписи, e — открытый ключ верификации подписи. При этом $e \cdot d \equiv 1 \bmod \lambda(N_{rsa})$, где $\lambda(N_{rsa})$ — обобщенная функция Эйлера. Предположим, что для вычисления степени используется бинарный алгоритм, а для вычисления остатка по модулю — метод Монтгомери без применения китайской теоремы об остатках. Тогда общая схема алгоритма возведения в степень имеет следующий вид:

вход: $m, N_{rsa}, d = (d_{n-1}, \dots, d_0)_2$, $h: \{0,1\}^* \to Z / Z_{N_{rsa}}$;

выход: $S = h(m)^d \bmod N_{rsa}$;

$R_0 \leftarrow h(m)$;

для $j = n-2$, $j \le 0$, $j = j-1$ повторить;

$R_0 \leftarrow R_0^2 \bmod N_{rsa}$;

если $(d_j = 1)$, то $R_0 \leftarrow h(m) \cdot R_0 \bmod N_{rsa}$;

конец цикла.

Возвращаем R_0.

Заметим, что при использовании метода Монтгомери в результате имеем число в отрезке $[0, 2 \cdot N_{rsa}]$ и для получения корректного остатка по модулю необходимо одно дополнительное вычитание N_{rsa}.

В работе [10] рассмотрена следующая схема временной атаки. Последняя строится итеративно от старших бит к младшим в предположении, что известны старшие биты $d_{n-1}, \dots, d_{n-k+1}$. Цель атаки — установить значение бита d_{n-k}. Предположим, что $d_{n-k} = 1$. Случайно выбираем t сообщений $m_1, \dots, m_t$. Зная $d_{n-1}, \dots, d_{n-k+1}, d_{n-k}$ и N_{rsa}, можно разбить эти сообщения на два множества: $M_0 = \{m_i \mid R_0 \cdot h(m) \bmod N_{rsa}\}$ и $M_1 = \{m_i \mid R_0 \cdot h(m) \bmod N_{rsa}\}$ соответственно не требующего и требующего дополнительного корректирующего вычитания для вычисления модуля при $j = n-k$. Выбирая сообщения из множеств M_0 и M_1, определяем среднее время выработки цифровой подписи τ_0 и τ_1 для каждого из множеств соответственно. Если $\tau_0 \approx \tau_1$, то предположение $d_{n-k} = 1$ неверно и полагаем $d_{n-k} = 0$. Если $\tau_1 > \tau_0$ и $\tau_1 - \tau_0 \approx \tau_{\text{sub}}$, где τ_{sub} — время операции вычитания, то предположение верно и $d_{n-k} = 1$.

Оценивая мощность данной атаки, необходимо отметить два важных момента: предполагается априорное знание некоторых старших бит ключа; время выработки цифровой подписи для различных сообщений измеряется в общем случае неточно и зависит от множества случайных факторов. В результате стойкость криптосистемы к данной атаке зависит от априорной информации и согласно методу ее получения описывается различными моделями и показателями. Это неизбежно приводит к практическим сложностям оценки.

Применим к оценке стойкости криптосистемы к данной атаке на реализацию подход, предложенный в [7]. В качестве информационного оператора выберем оператор $N: \widetilde{D} \to X$, $X = < AI, \tau >$, где AI — априорная информация о значении d; τ — информация, полученная из побочного временного канала (или по мощности); $\widetilde{D}$ — множество значений показателя d. Мощность множества $V(N, d, \tau) = \{\widetilde{d} \in \widetilde{D} : N(\widetilde{d}) = N(d)\}$ всех элементов $\widetilde{d}$, не отличимых с помощью информационного оператора N от d, определяет принципиальную стойкость к атаке, а глобальный радиус информации $r(N)$ и множество алгоритмов $\Phi(N(\widetilde{D}))$ реализации атаки — показатель практической сложности ее осуществления. При этом в общем случае оператор N не всегда полностью дает точное значение d, а в зависимости от точности измерения τ еще и не является точным. Показатель стойкости к атаке определяется оператором утечки информации

$S:\widetilde{D}\times\mathbb{R}_+\to 2^G$ (в частном случае — функцией), где G — множество значений функции утечки.

Поясним, почему $r(N)$ определяет практическую сложность осуществления атаки по побочным каналам. Это следует из того, что $r(N)=\sup_{d\in\widetilde{D}}(\inf_\tau V(N,d,\tau))$. При дополнительном уточнении реализуемости атаки возможен выбор множества $\Phi(N(\widetilde{D}))$. Действительно, только в случае выбора $\Phi(N(\widetilde{D}))$ как множества идеальных, оптимальных по точности или центральных алгоритмов получаем из [13]: $\inf_{\varphi\in\Phi(n)} e(\varphi,N)=r(N)$, где $e(\varphi,N)$ — глобальная погрешность алгоритма φ, т.е. точная нижняя граница погрешности идеального алгоритма совпадает с $r(N)$, при другом выборе $\Phi(N(\widetilde{D}))$ информация N может не позволить однозначно определить d. В приведенном примере атаки по побочному временному каналу на дискретное возведение в степень очевидно, что $r(N)=\tau_{\text{sub}}$ при $AI=\varnothing$ (априорная информация может отсутствовать, так как старший бит d, как правило, однозначно определяется размерностью N_{rsa}).

Описанный алгоритм атаки не всегда относится к множеству центральных алгоритмов в силу равномерного случайного выбора $m_1,\dots,m_t$, поэтому точного определения d можно не достичь и при $\tau_1-\tau_0\approx\tau_{\text{sub}}>\tau_e$, где τ_e — погрешность измерения времени, которая в ОВС принимает достаточно большие значения.

В заключение отметим, что новые свойства облачных информационно-коммуникационных систем такие, как эластичность и точная измеримость вычислений, приводят к новым постановкам задач в области защиты информации, в частности при проектировании, оценке стойкости и реализации криптографических и стеганографических систем. Асимметричность вычислений для облачных информационно-коммуникационных систем обусловливает новые постановки задач эффективных по быстродействию и ресурсам построения алгоритмов многословной арифметики, проектированию криптографических протоколов и разработки методов безопасной реализации криптографических и стеганографических модулей. Приведенные в статье постановки задач и методы решения некоторых из них подтверждают необходимость пересмотра многих традиционных подходов, принятых в теории защиты информации, криптографии и стеганографии.

СПИСОК ЛИТЕРАТУРЫ

1. Таненбаум Э., Ван-Стеен М. Распределенные системы. Принципы и парадигмы. — Спб.: Питер, 2003. — 877 с.
2. Bhaskar Prasad Rirnal, Eunrni Choi, Ian Lumb. A taxonomy and survey of cloud computing systems // Proc. 2009 Fifth Intern. Joint Conf. INC, IMS and IDC. — IEEE Comp. Society Washington DC, USA, 2009. — P. 44–51.
3. grid.kpi.ua/files/2012-4.pdf.
4. www.ecrypt.eu.org/documents/D.VAM.2.pdf.
5. Gentry C. Fully homomorphic encryption using ideal lattice / Proc. 41st ACM Symp. Theory of Comp. — New York: ACM, 2009. — P. 169–178.
6. Кудін А.М. Порівняльний аналіз математичних моделей стійкості криптосистем // Наукові вісті НТУУ «КПІ». — 2010. — № 4(72). — С. 86–90.
7. Кудин А.М. Модель оценки стойкости модулей криптографической защиты информации к криптоанализу по побочным каналам // Компьютерная математика. — 2011. — № 2. — С. 59–66.
8. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: Навчальний посібник / В.К. Задірака, А.М. Кудін, В.О. Людвиченко, О.С. Олексюк / Київ–Тернопіль: Підручники та посібники, 2007. — 272 с.

9. О технологии криптографической защиты информации на специальных цифровых носителях / В.К. Задирака, А.М. Кудин, В.А. Людвиченко, А.С. Олексюк // Управляющие системы и машины. — 2010. — № 4. — С. 77–83.
10. www.ipa.go.jp/1047_Side_Channel_report.pdf.
11. Certin Kaya Kos. Cryptographic engineering / New York: Springer Science+Business Media, LLC 2009. — 528 p.
12. Трауб Дж., Вожьняковский Х. Общая теория оптимальных алгоритмов: Пер. с англ. — М.: Мир, 1983. — 382 с.
13. Трауб Дж., Васильковский Г., Вожьняковский Х. Информация, неопределенность, сложность. — М.: Мир, 1988. — 184 с.
14. Сергієнко І.В., Задірака В.К., Литвин О.М. Елементи загальної теорії оптимальних алгоритмів та суміжні питання. — К.: Наук. думка, 2012. — 400 с.
15. Колмогоров А.Н. Три подхода к определению понятия «Количество информации» / Новое в жизни, науке, технике. Сер. «Математика и кибернетика». 1991. — № 1. — С. 24–29.
16. Верещагин Н.К., Успенский В.А., Шень А. Колмогоровская сложность и алгоритмическая случайность. — М.: МЦНМО, 2013. — 576 с.
17. Колмогоровская сложность и криптография // Алгоритмические вопросы алгебры и логики. Сб. ст. к 80-летию со дня рождения акад. С.И. Адяна. Тр. МИАН, 274, МАИК, М.: 2011. — С. 210–221.
18. Subashini S., Kavitha V. A survey on security issues in service delivery models of cloud computing // J. Network and Comput. Appl. — 2011. — **34**, N 1. — P. 1–11.
19. A trusted computing environment model in cloud architecture / Xiao-Yong Li, Li-Tao Zhou, Yong Shi, Yu Guo // Proc. Ninth Intern. Conf. Mach. Learn. and Cybern. — Qingdao, 11–14 July, 2010. — P. 2843–2848.
20. Задирака В.К., Кудин А.М. Особенности реализации криптографических и стеганографических систем по принципу облачных вычислительных технологий // Искусственный интеллект. — 2012. — № 3. — С. 438–444.
21. Задирака В.К., Кудін А.М. Построение программно-аппаратных комплексов арифметики сверхбольших чисел / Комп'ютерна математика. Оптимізація обчислень: Зб. наук. праць НАНУ, ІК ім.. В.М. Глушкова. — К.: 2001. — Т.1. — С. 158–163.
22. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозрядних чисел: Наукове видання. — К.: б.в., 2003. — 264 с.
23. Кнут Д.Э. Искусство программирования, том 2. Получисленные алгоритмы. Третье изд. — М.: Вильямс, 2000. — 830 с.
24. Keshab K. Parhi. VLSI digital signal processing systems: Design and implementation. — New York: John Wiley & Sons, 1998. — 808 p.
25. Goldwasser S., Micali S. Probabilistic encryption // J. Comput. and Syst. Sci. — 1984. — № 28. — P. 270–299.
26. Кудин А.М. Однонаправленные функции с информационно невычислимой лазейкой // Прикладная радиоэлектроника. — 2012. — **11**, № 2 — С. 245–249.
27. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: СОЛОН-ПРЕСС, 2009. — 265 с.

Поступила 22.02.2013