захстана, Сингапура, Украины. Более 280 участников — студенты, около 120 — школьники, остальные участники — любители криптографии и профессионалы.

Участникам олимпиады было предложено 15 задач. Математические задачи олимпиады посвящены вопросам исследования дифференциальных характеристик S-блоков; взаимосвязи простейших операций, использующихся для построения шифра: циклического сдвига и сложения по модулю 2^k ; построению специальных линейных подпространств в $\mathbb{F}_2^n$; поиску числа решений уравнения $F(x) + F(x+a) = b$ над конечным полем $\mathbb{F}_{2^n}$ и APN-функциям. Были и игровые задачи, такие, как крипто-квест, дешифрование секретных сообщений, анализ музыкального шифра. Детально задачи и их решения обсуждаются в [1, 2]. При этом работа [2] содержит не только разбор всех задач, но и комментарии к решениям участников, организационные моменты олимпиады, списки призёров.

Победителями олимпиады стали участники из Новосибирска, Омска, Москвы, Санкт-Петербурга, Саратова, Минска (Беларусь) и Лёвена (Бельгия): 15 участников в первом туре и 11 команд-победительниц во втором туре. Награждение призёров состоялось в Новосибирском государственном университете в декабре.

NSUCRYPTO задумана как ежегодное мероприятие. В следующий раз она пройдёт в ноябре 2015 г. (см. www.nsucrypto.nsu.ru). Приглашаем всех желающих принять в ней участие! Например, участники конференции Sibecrypt могут выбрать категорию «любитель/профессионал».

ЛИТЕРАТУРА

1. Agievich S., Gorodilova A., Kolomeec N., Nikova S., et al. Mathematical problems of the First international student's Olympiad in cryptography NSUCRYPTO // IV Симпозиум «Современные тенденции в криптографии» CTCrypt'15, Казань, 3–5 июня 2015 г.
2. Agievich S., Gorodilova A., Kolomeec N., Nikova S., et al. Problems, solutions and experience of the first international student's Olympiad in cryptography // Прикладная дискретная математика. 2015. № 3(29).

УДК 519.95

DOI 10.17223/2226308X/8/28

АТАКА ПО ШИФРТЕКСТАМ НА ОДНУ ЛИНЕЙНУЮ ПОЛНОСТЬЮ ГОМОМОРФНУЮ КРИПТОСИСТЕМУ¹

А. В. Трепачева

Описывается новая стратегия атаки по шифртекстам на одну линейную полностью гомоморфную криптосистему, чья защищённость обосновывается с привлечением сложности задачи факторизации больших чисел. Приводятся теоретические и практические оценки вероятности раскрытия секретного ключа с использованием данной атаки. Проводится анализ связи трудности факторизации чисел и защищённости криптосистемы против атаки по шифртекстам, на основе которого предлагается более эффективная модификация криптосистемы.

Ключевые слова: *полностью гомоморфное шифрование, задача факторизации чисел, атака по шифртекстам.*

Введение

В связи с распространением облачных сервисов задача построения полностью гомоморфных криптосистем (ПГК), позволяющих проводить произвольные вычисления

¹Работа поддержана грантом РФФИ № 15-07-00597-а.

над данными в зашифрованном виде, приобрела большую актуальность. Основным направлением в данной области является построение ПГК, основанных на теории решёток и методике Джентри [1]. Однако существующие на данный момент ПГК этого типа обладают низкой вычислительной эффективностью и являются непригодными для практики [1]. Поэтому не прекращаются поиски альтернативного варианта ПГК, не использующей метод Джентри и являющейся эффективной и криптостойкой. В частности, активно предлагаются ПГК, основанные на задаче факторизации чисел. В данной работе анализируется одна недавно предложенная ПГК этого вида из [2]. Описывается атака по шифртекстам (АШ) на ПГК [2], основанная на решении системы линейных уравнений и не рассмотренная ранее в литературе. Приводятся оценки вероятности её успеха в зависимости от различных параметров.

1. Полностью гомоморфная криптосистема из [2] и её основные свойства

Опишем ПГК, предложенную в [2]. Для зашифрования открытого текста $m \in \mathbb{Z}_n$ составляется матрица $D = \text{diag}(m, r) \in \mathbb{Z}_n^{2 \times 2}$, где $n = pq$, p, q — простые числа, $\log(p) = \log(q) \geq 512$ (т.е. n трудно факторизовать), $r \in \mathbb{Z}_n$ выбран по равномерному распределению, $\text{diag}(m, r)$ — диагональная матрица с m, r на главной диагонали. Шифртекст вычисляется как $C = K^{-1}DK \in \mathbb{Z}_n^{2 \times 2}$, где $K \in \mathbb{Z}_n^{2 \times 2}$ — секретный ключ. Ясно, что m — собственное число C , имеющее собственный вектор $v_1 = K^{-1}e_1 \in \mathbb{Z}_n^2$, где $e_1 = (1, 0)$. Для расшифрования вычисляется $s = Cv_1$, а затем $m = s_1/v_{1,1}$. Описанная криптосистема — ПГК, так как в ней произведению и сумме шифртекстов соответствуют произведение и сумма открытых текстов. При этом операции над шифртекстами вычислительно эффективны (умножение и сложение матриц). Это делает данную ПГК очень интересной с практической точки зрения. Однако ПГК [2] совершенно нестойка к атаке по известным открытым текстам. По перехваченной паре (m, C) можно составить систему линейных уравнений $(C - mI)x = 0$, множество решений которой имеет базис $\{v_1\}$ с вероятностью ≈ 1 , и поэтому наличие даже одной пары (m, C) компрометирует [2]. Больше информации об атаке по известным открытым текстам на ПГК [2] можно найти в [3].

2. Атака по шифртекстам на ПГК [2]

Предположим, противник перехватил последовательность $C_i \in \mathbb{Z}_n^{2 \times 2}$, $i = 1, \dots, t$, шифрующих $m_i \in \mathbb{Z}_n$, $i = 1, \dots, t$, на ключе K . Ясно, что m_i — корень характеристического полинома $\text{char}_i(x) \in \mathbb{Z}_n[x]$, составленного для C_i . Так как n трудно факторизовать, нахождение корней $\text{char}_i(x)$ в общем случае трудно. Этим свойством в [2] и обосновывается защищённость ПГК. Однако на самом деле это работает, только если вероятностное распределение $\mathbb{D}$, заданное на пространстве открытых текстов $P = \mathbb{Z}_n$, является близким к равномерному. Если же, к примеру, $\mathbb{D}$ таково, что $\mathbf{P}\{m_i > \sqrt{n}\} = 0$, то, согласно [3], m_i можно найти из $\text{char}_i(x)$.

Рассмотрим другую стратегию АШ на ПГК [2]. Противнику предлагается решить систему линейных уравнений

$$(C_i - C_j)x = 0 \quad (1)$$

для $i = 1, \dots, t$, $j = 1, \dots, t$, $i \neq j$. Ясно, что если существуют i, j , такие, что $m_i = m_j$, то соответствующая система уравнений (1) имеет решение $v_1 = K^{-1}e_1 \in \mathbb{Z}_n^2$. Оценим вероятность $\Pr_t$ того, что существует хотя бы одна пара i, j , такая, что $m_i = m_j$. Для этого понадобится следующая лемма.

Лемма 1. Вероятность появления $\tilde{m} \in \mathbb{Z}_n$ хотя бы дважды в последовательности $\{\tilde{m}_k : k = 1, \dots, w\}$, где $\tilde{m}_k \in \mathbb{Z}_n$ сгенерированы по вероятностному распределению $\mathcal{D}$,

равна $\tilde{\text{Pr}}_{\mathcal{D},w}(\tilde{m}) = 1 - (1 - p_{\tilde{m}})^w - w(1 - p_{\tilde{m}})^{w-1}p_{\tilde{m}}$, где $p_{\tilde{m}}$ — вероятность появления $\tilde{m}$ в соответствии с $\mathcal{D}$.

Распределение $\mathcal{D}$ здесь считается таким, что все m_i независимы друг от друга. Легко видеть тогда, что $\text{Pr}_t = 1 - \prod_{\alpha=0}^{n-1} (1 - \tilde{P}r_{\mathcal{D},t}(\alpha)) = 1 - \prod_{\alpha=0}^{n-1} ((1 - p_\alpha)^t + t(1 - p_\alpha)^{t-1}p_\alpha)$, где p_α — вероятность появления $\alpha \in \mathbb{Z}_n$ согласно $\mathcal{D}$. Другие ненулевые решения, кроме v_1 , у системы (1) появляются, только если $r_i - r_j \notin \mathbb{Z}_n^*$. Последнее может произойти с вероятностью $\text{Pr} = 1 - \phi(n)/n$, так как $r_i - r_j$ — равномерно распределённая на $\mathbb{Z}_n$ величина. В силу выбора n можно считать, что $\text{Pr} \approx 0$, поэтому вероятность успеха описанной атаки равна Pr_t .

Для любого $\mathcal{D}$ справедливо $\lim_{t \rightarrow \infty} \text{Pr}_t = 1$. Однако атака оказывается практичной не для любого $\mathcal{D}$ из-за большого размера $P = \mathbb{Z}_n$. Наилучшим образом она работает для дискретного гауссова распределения $\mathcal{D} = \mathcal{D}_{\mathbb{Z}_n, \mu, \sigma^2}$, где μ — математическое ожидание; σ^2 — дисперсия и $\sigma^2 \ll n$. В таблице приведены значения Pr_t для разных t при n с $\log(n) = 1024$ и $\sigma^2 \ll n$; указаны также практические оценки вероятности $\tilde{\text{Pr}}_t$ найти v_1 с помощью описанной стратегии, полученные при тестировании реализации атаки. Для получения каждой $\tilde{\text{Pr}}_t$ проводилось 10^4 независимых испытаний.

t	Pr_t	$\tilde{\text{Pr}}_t$
50	0,88	0,85
70	0,955	0,945
90	0,998	0,99
120	1	0,99999

3. Связь трудности факторизации больших чисел и защищённости криптосистемы

В [2] доказано, что умение правильно расшифровывать $C \in \mathbb{Z}_n^{2 \times 2}$ позволяет факторизовать n . Однако для того чтобы строго связать криптостойкость с задачей факторизации, необходимо и обратное утверждение. Но оно не выполняется, так как если известны p, q , то из этого не следует корректное расшифрование C . Действительно, по китайской теореме об остатках $\text{char}(x)$ для C имеет четыре корня, и чтобы выбрать из них открытый текст, придётся привлечь $\mathcal{D}$. Исходя из этого, можно модифицировать ПГК [2]. Пусть n задается как $n = \prod_{k=1}^l p_k^{d_k}$, где p_k — простые числа, $p_i \neq p_j$. Решить уравнение $\text{char}(x) = 0$ теперь нетрудно, так как n можно факторизовать. Однако количество решений равно 2^l . При знании $\mathcal{D}$ для выбора открытого текста среди этих решений необходимо $\geq 2^l$ операций. Если положить $l = 120$, то перебор окажется настолько велик, что атака на $\text{char}(x)$ будет нереализуемой. Причём вычислительная сложность этого перебора эквивалентна сложности факторизации 1024-битного RSA модуля (с использованием метода решета числового поля), т. е. сложность атаки на $\text{char}(x)$ остаётся такой же. При этом размер n можно уменьшить, подобрав нужным образом p_k , $k = 1, \dots, l$; в результате ПГК [2] становится более эффективной.

Заключение

Предложена атака по шифртекстам на ПГК [2], основанная на решении системы линейных уравнений. Её практичность обусловлена распределением $\mathcal{D}$ на пространстве открытых текстов. Если $\mathcal{D}$ сильно отлично от равномерного, например $\mathcal{D}$ — гауссово распределение с небольшой дисперсией, то атака работает успешно. Для практики

это представляет интерес, так как в реальных приложениях $\mathcal{D}$ часто является именно таким. Обнаружено, что отсутствие строгой сводимости криптостойкости ПГК [2] к задаче факторизации позволяет использовать модуль n более скромных размеров без ухудшения защищённости. Это делает ПГК [2] более быстродействующей.

ЛИТЕРАТУРА

1. *Guellier A.* Can Homomorphic Cryptography ensure Privacy? PhD thesis, Inria; IRISA; Supélec Rennes, équipe Cidre; Université de Rennes 1, 2014.
2. *Kipnis A. and Hibshoosh E.* Efficient methods for practical fully homomorphic symmetric-key encryption, randomization and verification // IACR Cryptology ePrint Archive. 2012. No. 637.
3. *Vizár D. and Vaudenay S.* Analysis of chosen symmetric homomorphic schemes // Central European Crypto Conference, Budapest, Hungary, 2014, EPFL-CONF-198992.