УДК 004.056:004.62

Оценка криптостойкости полностью гомоморфных систем

©А.Е. Малинский

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Облачные вычисления являются одной из самых востребованных на текущий период технологий на рынке информационных услуг. Однако безопасность облачных вычислений опирается на доверие к поставщику облачных услуг. В отсутствии доверия данную задачу могут решить системы полностью гомоморфного шифрования. Эти системы позволяют производить операции над зашифрованными данными без выполнения операции расшифрования [1]. Таким образом, поставщик облачных услуг выполняет требуемые операции при сохранении конфиденциальности данных клиента. В данной статье рассмотрены уязвимости, присущие полностью гомоморфным системам. В ходе исследования получены оценки по стойкости полностью гомоморфных систем, а так же алгоритмы для дешифровки зашифрованных сообщений для произвольных реализаций полностью гомоморфного шифрования. Алгоритм дешифровки зашифрованных сообщений позволил оценить сверху количество гомоморфных систем. Данный результат указывает на отсутствие безопасного полностью автоморфного шифрования.

Ключевые слова: облачные вычисления, гомоморфизм, криптография, шифрование.

Введение в полностью гомоморфное шифрование. Пусть даны два множества двоичных векторов X и Y. Без ограничения общности положим, что $|X| = 2^n$, $|Y| = 2^m$, $n \leq m$. Пусть $\lambda(x_1, x_2, \ldots, x_i)$ — произвольная функция от i переменных, где $x_i \in X$, $\lambda(x_1, x_2, \ldots, x_i) \in X$. Тогда полностью гомоморфное шифрование — это пара отображений

$$f : X \xrightarrow{f} Y, \qquad y = f(x) \tag{1}$$

$$f^{-1} : Y \xrightarrow{f^{-1}} X, \quad x = f^{-1}(y), \tag{2}$$

таких что $\forall\lambda(x_1, x_2, \ldots, x_i)$, выполняются следующие условия:

$$f^{-1}(f(\lambda(x_1, x_2, \ldots, x_i))) \equiv \lambda(x_1, x_2, \ldots, x_i) \tag{3}$$

$$\exists\lambda_f(y_1, y_2, \ldots, y_i) : \lambda(x_1, x_2, \ldots, x_i) \equiv f^{-1}(\lambda_f(y_1, y_2, \ldots, y_i)). \tag{4}$$

Уравнение (3) гарантирует, что при шифровании значения произвольной функции и последующем расшифровании результат останется неизменным. Уравнение (4) позволяет отображать произвольную операцию над множеством X в операцию над множеством Y.

Отметим, что по построению гомоморфное шифрование может отображать лишь базисные операции, т.е. такие операции, через которые можно выразить все функции. Таким образом, условие отобра-

жения всех возможных функций и отображение базисных функций являются эквивалентными.

Анализ защищенности полностью гомоморфных систем. В связи с тем что полностью гомоморфное шифрование отображает любую функцию λ на пространство Y, оно отображает в том числе и:

1. Побитная сумма по модулю 2: $x_1 \oplus x_2 \xrightarrow{f} y_1 \underset{f}{\oplus} y_2$
2. Побитная конъюнкция: $x_1 \wedge x_2 \xrightarrow{f} y_1 \underset{f}{\wedge} y_2$
3. Побитное отрицание: $\neg x_1 \xrightarrow{f} \underset{f}{\neg} y_1$
4. Битовый сдвиг: $x_1 \gg 1 \xrightarrow{f} y_1 \underset{f}{\gg} 1$

Отметим, что битовый сдвиг является единственной рассматриваемой функцией, которая связывает разряды векторов между собой.
Предположим, что был осуществлен перехват шифротекста y. Тогда нетрудно заметить, что

$$f(0) = y \underset{f}{\oplus} y \tag{5}$$

$$f(2^n - 1) = y \underset{f}{\vee} \underset{f}{\neg} y \tag{6}$$

$$f(2^0) = (f(2^n - 1) \underset{f}{\gg} n - 1) \tag{7}$$

$$f(2^i) = (f(2^n - 1) \underset{f}{\gg} n - i - 1) \underset{f}{\oplus} (f(2^n - 1) \underset{f}{\gg} n - i), i > 0 \tag{8}$$

В том случае, если $|X| \equiv |Y|$, т.е. $n \equiv m$, i-й бит открытого текста находится следующим образом:

$$f^{-1}(y) \wedge 2^i \equiv \begin{cases} 0, & \text{если } y \underset{f}{\wedge} f(2^i) \equiv f(0) \\ 1, & \text{иначе.} \end{cases} \tag{9}$$

Таким образом, не имея ключа шифрования возможно получение открытого текста. Количество гомоморфных операций для получения образов 2^i равно $\omega_{\underset{f}{\oplus}} + \omega_{\underset{f}{\neg}} + \omega_{\underset{f}{\vee}} + \omega_{\underset{f}{\gg}} = (1+n-1)+1+1+(n-1) = 2n+$ $+1$. Проверка бит затрачивает n гомоморфных операций и n обычных операций сравнения.

Если $n > m$, необходимо доработать предыдущий метод: количество образов для каждого прообраза может быть более одного.

Если вероятность получения образа фиксированного прообраза равномерно распределена, то можем выполнить полный перебор образов $f(0)$ следующим путем.

1. Перехватываем k шифротекстов.
2. Получаем k новых образов $f(0) = y_k \underset{f}{\oplus} y_k$.

3. Получаем $C_k^2, C_k^3, \ldots, C_k^{k-1}, C_k^k$ образов всеми возможными суммами $\bigoplus\limits_{f}{}_i\, y_i$.
4. В результате получаем 2^k образов $f(0)$.

Обозначим множество всех найденных различных $f(0)$ как Θ. Тогда i-й бит открытого текста находится следующим образом:

$$f^{-1}(y) \wedge 2^i \equiv \begin{cases} 0, & \text{если } y \underset{f}{\wedge} f(2^i) \in \Theta \\ 1, & \text{иначе.} \end{cases} \tag{10}$$

Данный способ позволяет получить максимально 2^k образов $f(0)$ по k шифротекстам. Если данное множество велико, целесообразно применение атаки с предвычислениями, а именно метод радужных таблиц.

В качестве начального столбца необходимо выбрать k различных начальных значений $f(0)$. Функцию перехода выбираем как сумму текущего элемента с подсуммой первого столбца. Выбирая длину строки таблицы порядка $\dfrac{2^k}{k}$ получаем уменьшение хранимого множества Θ до $2k$ элементов.

В случае неравномерной вероятности распределения образов фиксированного прообраза, атака аналогична, но возможно ее завершение за меньшее время, т.к. существует такой образ $f(0)$, вероятность перейти в который после определенного количества операций $\underset{f}{\oplus}$ стремится к нулю.

Анализ количества гомоморфизмов. Алгоритм дешифрования можно использовать для вычисления верхней оценки количества полностью гомоморфных систем.

Рассмотрим два случая.

1) $n = m$. Задавая одно отображение $x \xrightarrow{f} y$ с помощью дешифрования можно получить все образы 2^i, что позволяет построить образ y произвольного x. Таким образом верхняя оценка количества полных гомоморфизмов

$$|X \xrightarrow{f} Y| \leq 2^n \cdot 2^m = 2^{n+m}. \tag{11}$$

2) $n < m$. Первым шагом находим по одному экземпляру всех образов аналогично предыдущему случаю. Затем необходимо учесть оставшиеся $2^m - 2^n$ образов. Образ может не иметь прообраза. Данная задача аналогична распределению шаров в урны, причем урны могут быть пустыми. Тогда верхняя оценка количества полных гомоморфных систем:

$$|X \xrightarrow{f} Y| \leq 2^{n+m} \cdot (n+1)^{2^m - 2^n}. \tag{12}$$

Заключение. Итогом данного исследования является отсутсвие полного автоморфного шифрования, ведь невозможно обеспечить требуемый уровень секретности. Полностью гомоморфные системы возможны при достаточной разнице размерностей пространств прообразов и образов. Однако данное условие требует больших вычислительных ресурсов, что при текущем уровне технологического развития критично. Решением данной проблемы является аппаратная реализация работы над шифротекстами.

Следует отметить, что при отсутствии какой-либо базовой операции общий подход к атаке становится невозможен. Таким образом, целесообразно проводить построения гомоморфных систем под конкретные задачи, которые будут решаться над шифротекстами.

ЛИТЕРАТУРА

[1] Craig Gentry. A fully homomorphic encryption scheme. Stanford University, 2009.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом: Малинский А.Е. Оценка криптостойкости полностью гомоморфных систем. *Инженерный журнал: наука и иновации*, 2013, вып. 11. URL: http://engjournal.ru/catalig/it/security/995.html

Антон Евгеньевич Малинский — выпускник факультета «Информатика и системы управления» МГТУ им. Н.Э. Баумана. e-mail: anton@malinskiy.com