Список литературы

1. Polylactide-Based Block Copolymeric Micelles Loaded with Chlorin e6 for Photodynamic Therapy: In Vitro Evaluation in Monolayer and 3D Spheroid Models/ P. Kumari [et al.] //Molecular Pharmaceutics. 2017. № 11. V. 14. P. 3789-3800.
2. Nanoparticles as vehicles for delivery of photodynamic therapy agents/D. Bechet [et al.] //Trends in biotechnology.2008. №11.V.26. P.612-621.
3. Зорин В.П., Хлудеев И.И., Зорина Т.Е. Распределение порфириновых сенсибилизаторов между белковыми и клеточными элементами крови//Биофизика. 2000. №.2. Т. 45. С. 313-319.

УДК 004.056.5

ЗАЩИТА ДАННЫХ В МЕДИЦИНСКИХ СИСТЕМАХ НА ОСНОВЕ РАСПРЕДЕЛЕННОГО ГОМОМОРФНОГО КОДИРОВАНИЯ

С. Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Аннотация. Цифровая медицина открывает перспективу взаимодействия двух или более объектов, занятых в услугах медицинской помощи. Заинтересованные стороны могут связаться друг с другом на «уровне операций» «доверительных отношений», причем потенциальная ответственность в таком отношении ограничена только связью «уровня операций». Необходимым условием является защита данных в соответствии с принятой политикой безопасности.

Ключевые слова: гомоморфное отображения, разделение секрета, китайская теорема об остатках, модулярные вычисления

Abstract. Digital medicine offers the prospect of the interaction of two or more objects involved in medical care services. Interested parties can communicate with each other at the “transaction level” of a “trust relationship”, and the potential liability in this respect is limited only by the “transaction level” link. The prerequisite is data protection in accordance with the accepted security policy.

Keywords: homomorphic mappings, secret separation, Chinese remainder theorem, modular calculations

Введение

Благодаря прозрачной, интегрированной информационной среде информация становится легко доступной и быстро обрабатываемой. Политика защиты медицинской информации при многостороннем обмене включает с себя административные, физические, и технические меры безопасности, чтобы защитить частные (личные) и секретные данные от неправомочного раскрытия, разрушения, или модификации во время сбора, обработки, передачи или хранения с учетом.

Одно из возможных направлений развития систем защиты данных связано с алгоритмами распределенного преобразования на основе метода разделения секрета и гомоморфного криптокодирования

Алгоритм гомоморфной защиты данных

Если $(G_1,\otimes)$ и $(G_2,\otimes)$ две группы, тогда функция $f: G_1 \to G_2$ определяет гомоморфизм группы, если $f(x*y) = f(x) \otimes f(y)$, для всех $x, y \in G_1$ [1].

Различают *частичное гомоморфное криптокодирование*, когда имеют место аддитивный $Enc(x) + Enc(y) = Enc(x+y)$ гомоморфизм и мультипликативный гомоморфизм $Enc(x) \times Enc(y) = Enc(x \times y)$ Полное гомоморфное кодирования позволяет использовать произвольные вычисления в алгоритмах защиты данных.

Алгоритм криптозащиты на основе полного гомоморфизма.

1. Секретный ключ p определяется как большое простое число.
2. Выбирается большое целое q .
3. Выбирается малое целое $r < p/2$.
4. Операция криптокодирования бинарных данных m определяется как
$$c = qp + 2r + m \text{ для } m \in \{0,1\}.$$
5. Операция декодирования выполняет $(c \bmod p) \bmod 2 = m$.

Алгоритм вычисления отображений на основе метода разделения секрета

1. Выбирается число t и массив данных преобразуется в новый массив B в виде матрицы из m строк и t столбцов.

2. Для каждой *k*-й строки матрицы, для заданного значения x, вычисляется полином

$$s_k(x) = s_0 + s_1 x + \ldots + s_{t-1} x^{t-1} (\mathrm{mod}\ p).$$

Результаты вычислений образуют m строк массива A_x.

3. Массив A_x преобразуется в матрицу размером $a \times b$, которая является возвращаемым отображением.

4. Изменяя значение x и повторяя шаги 2 и 3 алгоритма, формируются множество n различных отображений.

Предположим, что имеется n различных отображений и используется (t, n)-схема разделения секрета [2]. Любая комбинация из t различных отображений позволяет построить алгоритм восстановления. Определим массив $X = \{x_0, x_1, \ldots, x_{t-1}\}$ для хранения значений x, соответствующих выбранным t отображениям.

Алгоритм восстановления массива данных по отображениям.

1. Все A_x -матрицы t отображений преобразуются в массивы длиной m.

2. Элемент с номером i каждого массива задается как $s_i(x_l)$, где l – индекс соответствующего массива, а x_l представляет собой l-й элемент массива X. В результате формируются t значений. $s_i(x_0), s_i(x_1), \ldots, s_i(x_{t-1})$.

3. Составляется система уравнений следующего вида

$$s_i(x_0) \equiv s_0^i + s_1^i x_0 + \ldots + s_{t-1}^i x_0^{t-1} (\mathrm{mod}\ p),$$

$$\ldots$$

$$s_i(x_{t-1}) \equiv s_0^i + s_1^i x_{t-1} + \ldots + s_{t-1}^i x_{t-1}^{t-1} (\mathrm{mod}\ p).$$

Решение системы уравнения дает значения $s_0^i, \ldots, s_{t-1}^i$, являющиеся элементами *i*-й строки восстанавливаемого массива B.

4. Шаги 2 и 3 алгоритма повторяются, до тех пор, пока все элементы каждого массива не будут вычислены, что дает полный восстановленный массив B.

5. Массив B размером $m \times t$ преобразуется в массив исходного размера $H \times W$, что дает восстановление исходного массива данных.

Моделирование в среде матлаб дает следующие результаты (рис. 1)

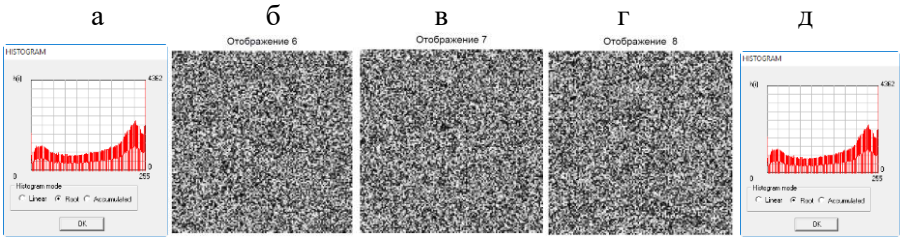

Рис. 1. Моделирования алгоритма разделения секрета:
а) – исходное изображение; б, в,г) – гомоморфная кодировка изображения алгоритмом разделения секрета; д) – восстановленное изображение

Заключение

Применение гомоморфного кодирования позволяет решить задачу защиты данных от методов криптоанализа на основе параллельных алгоритмов обработки. Защита пространственно распределенных данных основана на невозможности вычислить точно *t*-й корень системы из $(t-1)$ уравнений при криптоанализе алгоритма разделения секрета

Список литературы

1. Gentry, C. Fully homomorphic encryption using ideal lattices. In Symposium on Theory of Computing/ C.Gentry, – STOC 2009, ACM, 169–178, 2009.

Distributed Storage scheme Based on Secret Sharing Schemes/ Shuang Wang, School of Electrical and Computer Engineering, University of Oklahoma, Tulsa, OK, USA