L.K. Babenko, A.V. Trepacheva

Security Analysis of One Solution for Secure Private Data Storage in a Cloud

Keywords: fully homomorphic encryption, security analysis, cloud computing.
The paper analyzes the security of one recently proposed secure cloud data base architecture. We present an attack on it binding the security of whole solution with the security of particular encryption schemes, used in it. We show this architecture is vulnerable and consequently the solution is unviable.

Л.К. Бабенко, А.В. Трепачева

АНАЛИЗ ЗАЩИЩЕННОСТИ ОДНОЙ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ[1]

Введение

Популярной современной технологией являются облачные вычисления, которые подразумевают хранение и обработку баз данных пользователей на удаленных серверах. Основная проблема этой технологии – проблема конфиденциальности данных, хранящихся на сервере. Хорошее решение для неё – шифрование данных клиента, позволяющее обрабатывать данные в зашифрованном виде без знания секретного ключа. Это так называемое полностью гомоморфное шифрование (ПГШ) [1].

На данный момент предложено много полностью гомоморфных криптосистем (ПГК), но пока не предложено ни одной доказуемо криптостойкой и при этом позволяющей эффективно вычислять над зашифрованными данными все необходимые для БД операции: +, *, <, >, поиск и т.д. (см. [2]). В связи с этим возник вопрос о том, как организовать реальную защищенную облачную БД, в которой бы данные шифровались перед отправкой на сервер, и возможно было бы проводить все необходимые вычисления над ними эффективно в зашифрованном виде.

В работе [3] сделана попытка решить эту проблему. Основная идея архитектуры защищенной облачной БД [3] в том, что в зависимости от того, какие операции нужно вычислять над столбцами в таблице, они шифруются по-разному. Для сравнения и сортировки применяется так называемое шифрование сохраняющее порядок E_{OPE} (ШСП) [4], для +, * гомоморфное E_{FHE}, для поиска по ключевым словам детерминированное E_{DET} (ДШ). Пользователь перед отправкой таблиц на сервер указывает, какие операции нужно будет вычислять над каждым столбцом. В соответствии с этим доверенный для пользователя прокси-сервер шифрует данные. Помимо этого, прокси-сервер преобразовывает обычные SQL-запросы пользователя к запросам к зашифрованной БД, а также расшифровывает ответы облачного сервера. За счет прокси-сервера для пользователя и облачного сервера работа с БД происходит так же, как в случае незашифрованной БД.

В реализации данной архитектуры авторы [3] для шифрования данных использовали ранее предложенные ими криптосистемы: ШСП [4], ПГК [5], ДШ [6].

В [7, 8] была представлена эффективная атака с известным открытым текстом на ПГК [5], требующая для раскрытия ключа знания одной пары (открытый текст, шифртекст). А также в [7, 8] рассмотрены случаи, когда на ПГК [5] возможно провести атаку только по шифртекстам. Уже в связи с этим СУБД [3] является уязвимой, так как

[1] Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта №15-07-00597 А.

можно атаковать все столбцы, зашифрованные на ПГК [5] (злоумышленником считается администратор облачной БД). Однако если неизвестно ни одной пары (открытый текст, шифртекст), то время взлома каждого гомоморфно зашифрованного столбца $\approx O(t^2)\cdot T_{KPA}$, где t число строк в таблице, $T_{KPA}=O(d^3\cdot\log(n))$ время работы атаки с известным открытым текстом на ПГК [5], d, n параметры ПГК [5], $n=p\cdot q\in\mathbf{Z}$ RSA-модуль, $\log(p),\log(q)\geq 512$, $d\in\mathbf{Z}, d>1$. Здесь мы рассмотрим вопрос о том, как особенности СУБД [4] позволяют сократить время атаки на гомоморфно зашифрованные столбцы БД.

Уязвимость СУБД [3]

Предположим, что над столбцом M таблицы T, хранящим целочисленные данные в диапазоне $[0,p-1]$, нужно вычислять +,*,<,>. Тогда в зашифрованной таблице T_{encr}, хранящейся в облачной БД, окажутся два столбца Col_1 и Col_2, шифрующие одинаковый набор $m_0,...,m_{t-1}$, но разными шифрами – ШСП [4] ($E_{OPE}(m_0),...,E_{OPE}(m_{t-1})$) и ПГШ [5] ($E_{FHE}(m_0),...,E_{FHE}(m_{t-1})$). Если $\exists i,j,i\neq j,m_i=m_j$, то криптоаналитик может обнаружить это, так как ШСП [4] детерминированное и $m_i=m_j\Rightarrow E_{OPE}(m_i)=E_{OPE}(m_j)$. При этом ПГШ [5] вероятностное и $\Rightarrow \Pr\left[E_{FHE}(m_i)\neq E_{FHE}(m_j)\right]\approx 1$. Таким образом, к криптоаналитику попадут два разных шифртекста одного и того же открытого текста на одном ключе. Тогда криптоаналитик может получить нетривиальный шифртекст $E_{FHE}(m_i)-E_{FHE}(m_j)=E_{FHE}(0)$, провести атаку с известным открытым текстом [7,8] и дешифровать $E_{FHE}(m_0),...,E_{FHE}(m_{t-1})$.

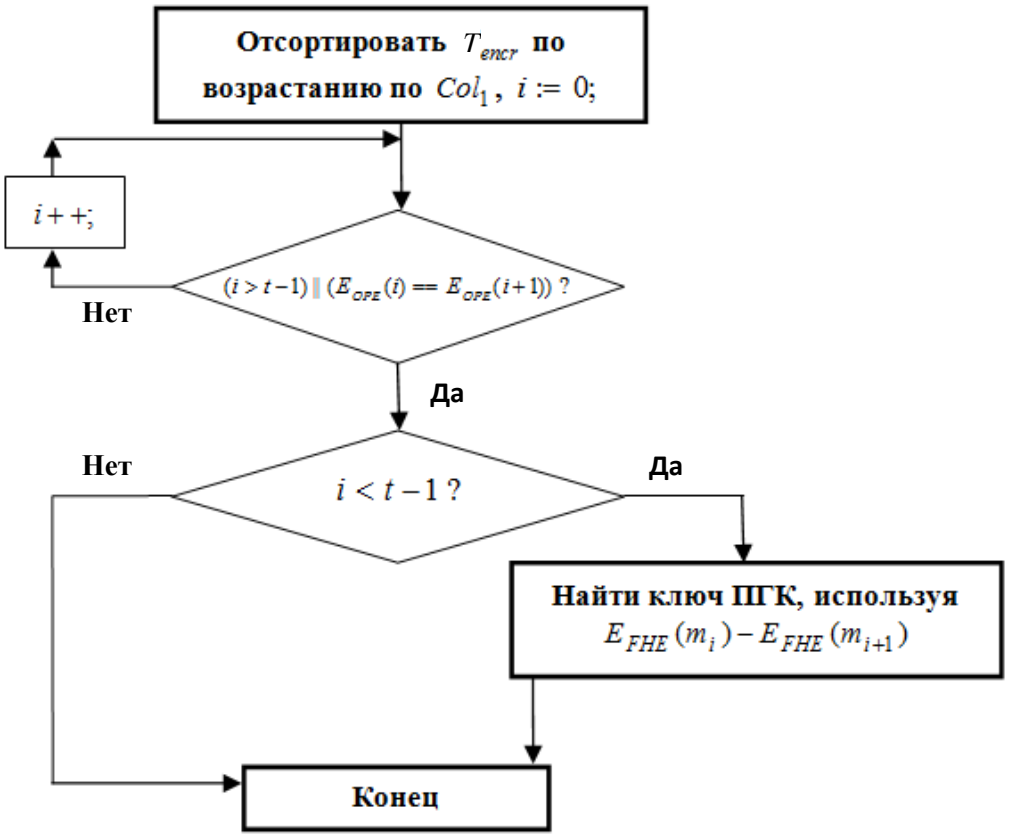

Рис. 1. Блок-схема Алгоритма 1

Пусть криптоаналитику известно, что Col_1 и Col_2 шифруют столбец M разными шифрами. Алгоритм 1 взлома Col_1 и Col_2 представлен на рис. 1.

Вероятность успеха Алгоритма 1 можно вычислить по формуле $\Pr_{t,p,\varsigma} = 1 - \sum_{S_{i_1,\ldots,i_t} \subseteq [0,p-1]} t! \cdot \Pr_{\varsigma}[m_{i_1}] \cdot \ldots \cdot \Pr_{\varsigma}[m_{i_t}]$, где ς вероятностное распределение на M.

В табл. приведены значения $\Pr_{t,p,\varsigma}$ для $\log(p) = 512$, $\varsigma = DN_{[0,p-1],0,700}$, где DN дискретное нормальное распределение на $[0, p-1]$.

Таблица

t	$\Pr_{t,p,\varsigma}$
200	0,98

Если использовать сортировку слиянием, то время взлома Col_1, Col_2 будет $\approx O(t \cdot \log t) \cdot T_{COMP} + T_{KPA}$, где T_{COMP} время вычисления операции сравнения над шифртекстами ШСП [4].

Стратегия атаки на СУБД [3] и алгоритм оценки её успеха

Опишем общую стратегию атаки на СУБД [3]. Поскольку злоумышленник не знает, какие столбцы в T_{encr} шифруют одно и то же, то Алгоритм 1 приходится модифицировать, введя в него перебор. Атака состоит из двух основных этапов:

Злоумышленник в соответствие с поступающими SQL-запросами разбивает множество C столбцов T_{encr} на подмножества $C_{OPE}, C_{FHE}, C_{DET}$ в соответствии с типами шифрования.

Для $\forall Col \in C_{OPE} \cup C_{DET}$ выполняются следующие действия: 1) T_{encr} сортируется по возрастанию по столбцу Col; 2) осуществляется поиск такого $i \in [0, t-2]$, что $Col[i] = Col[i+1]$; 3) для $\forall Col' \in C_{FHE}$ вычисляется шифртекст $Col'[i+1] - Col'[i]$ и на него проводится атака с известным открытым текстом из работы [5].

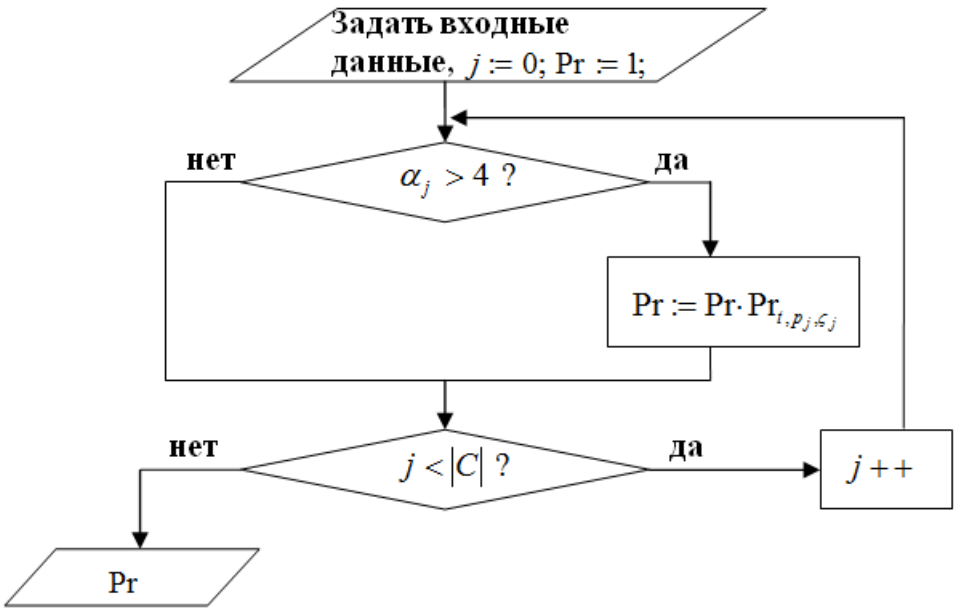

Рис. 2. Алгоритм оценки риска использования СУБД [3]

Вычислительная сложность атаки $\approx(O(t\cdot\log t)\cdot T_{COMP}\cdot+T_{KPA}\cdot|C_{FHE}|)\cdot|C_{OPE}\cup C_{DET}|$. Заметим, что в случае непосредственной атаки сразу на гомоморфные столбцы (без использования дополнительной информации) сложность будет $\approx O(t^2)\cdot T_{KPA}\cdot|C_{FHE}|$. Так как обычно для БД характерно соотношение $t>>|C|$, то предложенная атака работает быстрее.

На рис. 2 представлена блок-схема алгоритма оценки риска использования СУБД [3] для случая однотабличной БД. Результатом работы алгоритма является вероятность успешного взлома всех столбцов, зашифрованных гомоморфно. Входные данные для алгоритма следующие: число строк t, для $\forall j\in C$ задается: 1) диапазон значений $[0,p_j]$; 2) 3-битное число α_j, в котором наличие в каждом бите единицы, соответствует необходимости шифровать столбец j с помощью E_{OPE} (0-й бит), E_{DET} (1-й), E_{FHE} (2-й); 3) вероятностное распределение ς_j.

Выводы

Выявлена уязвимость и описана общая стратегия атаки на СУБД [3], позволяющая взломать все гомоморфно зашифрованные столбцы. Успех определяется вероятностным распределением на открытых данных. Одним из возможных путей ликвидации уязвимости является использование ПГШ, стойкого против атак с известным открытым текстом. Другой путь – пересмотр архитектуры СУБД. В дальнейшем планируется осуществить конкретную реализацию описанной стратегии атаки.

СПИСОК ЛИТЕРАТУРЫ:

1. Gentry C. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.
2. Guellier. Can Homomorphic Cryptography ensure Privacy? PhD thesis, Inria; IRISA; Supelec Rennes, equipe Cidre; Universite de Rennes 1, 2014.
3. Shatilov K., Boiko V., Krendelev S., Anisutina D. and Sumaneev A. Solution for secure private data storage in a cloud. In Computer Science and Information Systems (FedCSIS). 2014 Federated Conference on, pp. 885–889. IEEE, 2014.
4. Usoltseva M., Krendelev S. and Yakovlev M. «Order preserving encryption schemes based on arithmetic coding and matrices» in Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, M. P. M. Ganzha L. Maciaszek, Ed., ser. Annalsof Computer Science and Information Systems, vol. 2,IEEE, 2014, pp. 891–899.
5. Zhirov, Zhirova O. and Krendelev S.F. Practical fully homomorphic encryption over polynomial quotient rings. In Internet Security (WorldCIS), 2013 World Congress on. Pp. 70–75. IEEE, 2013.
6. Egorova V., Chechulina D., Krendelev S.F. (2013) New View on Block Encryption (Unpublished) URL: https://db.tt/vnE9wfgj (дата обращения: 1.02.2016).
7. Trepacheva A.V. Known plaintext attack on a fully homomorphic cryptosystem based on factorization // Труды конференции CTCrypt, 3–5 июня, 2015.
8. Трепачева А.В. О криптоанализе одной полностью гомоморфной криптосистемы на основе задаче факторизации // Журнал БИТ (безопасность информационных технологий). 2015. № 4. С. 19–25.

REFERENCES:

1. Gentry C. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.
2. Guellier. Can Homomorphic Cryptography ensure Privacy? PhD thesis, Inria; IRISA; Supelec Rennes, equipe Cidre; Universite de Rennes 1, 2014.
3 Shatilov K., Boiko V., Krendelev S., Anisutina D. and Sumaneev A. Solution for secure private data storage in a cloud. In Computer Science and Information Systems (FedCSIS). 2014 Federated Conference on, pp. 885–889. IEEE, 2014.
4. Usoltseva M., Krendelev S. and Yakovlev M. «Order preserving encryption schemes based on arithmetic coding and matrices» in Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, M. P. M. Ganzha L. Maciaszek, Ed., ser. Annalsof Computer Science and Information Systems, vol. 2,IEEE, 2014, pp. 891–899.
5. Zhirov, Zhirova O. and Krendelev S.F. Practical fully homomorphic encryption over polynomial quotient rings. In Internet Security (WorldCIS), 2013 World Congress on. Pp. 70–75. IEEE, 2013.
6. Egorova V., Chechulina D., Krendelev S. F. (2013) New View on Block Encryption (Unpublished) URL: https://db.tt/vnE9wfgj (Accessed on 1.02.2016).

7. Trepacheva A.V. Known plaintext attack on a fully homomorphic cryptosystem based on factorization // Proceedings of CTCrypt, 3-5 июня, 2015.
8. Trepacheva A.V. About cryptanalysis of one fully homomorphic cryptosystem based on factorization problem // BIT magazine. 2015. № 4. P. 19–25.