Дерандомизационная криптостойкость гомоморфного шифрования[1]

А.В. Трепачева <alina1989malina@ya.ru>
Южный федеральный университет,
344006, Россия, г. Ростов-на-Дону, ул. Большая Садовая, д. 105/42

Аннотация. В статье освещается проблематика построения и анализа систем криптографической защиты облачных вычислений на основе гомоморфного шифрования. Рассматриваются минимальные требования, которым должна удовлетворять гомоморфная криптосистема, чтобы быть пригодной для практического использования. Для этого вводится новое понятие – шифрование, стойкое к дерандомизации, а также объясняются связи этого понятия с классическими общепринятыми определениями криптостойкости, а также с защищенностью в целом облачной системы. Показываются примеры простых гомоморфных криптосистем, как удовлетворяющие требованию стойкости к дерандомизации, так и не обладающие этим свойством. В заключение делается вывод о применимости данных криптосистем в облачных вычислительных системах.

Ключевые слова: защита информации; вычисления над зашифрованными данными; гомоморфное шифрование; криптоанализ; дерандомизация.

DOI: 10.15514/ISPRAS-2015-27(6)-24

Для цитирования: Трепачева А.В. Дерандомизационная криптостойкость гомоморфного шифрования. Труды ИСП РАН, том 27, вып. 6, 2015 г., стр. 381-394. DOI: 10.15514/ISPRAS-2015-27(6)-24.

1. Введение

Среди проблем, с которыми сталкиваются облачные вычисления, одними из самых актуальных и в то же время сложных для решения, являются проблемы обеспечения информационной безопасности. «Как организовать сложную обработку данных в облаке и при этом гарантировать конфиденциальность и правильность вычислений?», «Как минимизировать коммуникационную сложность используемых протоколов?», «Как обеспечить надежность конфи-

[1] Работа выполнена при поддержке гранта РФФИ №15-07-00597 А «Разработка и исследование алгоритмов полностью гомоморфного шифрования»

денциальных вычислений?» – все это вопросы, на которые до сих пор нет удовлетворительных ответов.

Причина этого состоит в том, что многие угрозы исходят от злонамеренных администраторов облачных серверов, а также от хакеров которые несмотря на защитные экраны и контрмеры получают доступ к данным, а специализированные криптосистемы, позволяющие организовать вычисления над зашифрованными данными (а также доказательство правильности этих вычислений) без их расшифрования пока что недостаточно изучены и мало применяются на практике. Известные применения включают проекты CryptDB [1], Cipherbase [2], BigQuery [3], Always Encrypted [4], защищенная облачная БД исследователей из Новосибирска [5].

Что же это за шифрование, которое позволяет проводить вычисления над зашифрованными данными без расшифрования? Самым общим классом таких систем является т.н. шифрование, сохраняющее свойства (англ. Property-preserving encryption, PPE), сокращенно ШСС. ШСС позволяет проводить вычисления над зашифрованными данными так, что только владелец секретного ключа может воспользоваться их результатами и получить их так, как если бы все эти вычисления проводились на его локальном компьютере над незашифрованными данными. Простейшим примером такого шифрования является детерминированное шифрование, или шифр простой замены. Криптограммы такого шифра можно сравнивать на равенство без расшифрования. Более сложные примеры включают шифрование, сохраняющее порядок (ШСП) [6], поисковое шифрование (ПШ), гомоморфное шифрование (ГШ) [7]. Среди криптосистем гомоморфного шифрования выделяют т.н. полностью гомоморфное шифрование (ПГШ), которое позволяет *теоретически* проводить *любые* вычисления над зашифрованными данными без их расшифрования.

Например, в архитектуре CryptDB сочетается использование трёх видов шифрования для поддержания всей функциональности: традиционное блочное шифрование, гомоморфное шифрование и шифрование, сохраняющее порядок. Однако поддерживаемая функциональность оставляет желать лучшего: например, невозможно сделать какие-либо более-менее сложные арифметические (например, статистические) вычисления над данными – их можно только просуммировать или умножить на какую-то фиксированную открытую (известную) константу. Это происходит вследствие того, что используемая в CryptDB гомоморфная криптосистема – криптосистема Пэйе [7] имеет такой ограниченный набор функциональных возможностей. Такое решение было принято для гарантирования безопасности, поскольку эта криптосистема считается обладающей достаточным уровнем криптостойкости. Впрочем, в настоящее время существует уже довольно большое количество криптосистем, поддерживающих бóльшие гомоморфные свойства и обладающих какими-либо доказанными в соответствии со стандартными криптографическими предположениям свойствами криптостойкости. Проблема, однако, состоит в

том, чтобы определить, *насколько безопасно применять ту или иную гомоморфную криптосистему в конкретной практической ситуации*?

Таким образом, в данной работе рассматривается следующая задача: предложить критерии, позволяющие *относительно легко* определить пригодность гомоморфной криптосистемы для использования на практике и проверить некоторые известные гомоморфные криптосистемы на удовлетворение этим критериям. В частности, предлагается некоторая новая модель криптостойкости, вводится понятие *дерандомизации (гомоморфной) криптосистемы*, которое является частным случаем понятия дерандомизации в криптографии [8]. В этой модели исследованы криптосистемы MORE и PORE, авторы которых – Эвиад Кипнис (Aviad Kipnis) и Элифас Хибшуш (Eliphas Hibshoosh) – рассмотрели сводимость атаки на них только по шифртекстам к решению квадратного уравнения по модулю труднофакторизуемого числа [9]. Данный выбор обусловлен тем, что для этих криптосистем есть точные сведения относительно стойкости по классическим атакам, а также и то, что в патенте [10] свои криптосистемы авторы назвали именно «методами полностью гомоморфной рандомизации». Также в этой модели исследованы криптосистемы, предложенные исследователями из Новосибирска [11].

Общая структура работы такова: в разделе 2 приведены некоторые необходимые в дальнейшем сведения и обозначения; в разделе 3 вводится формальное описание дерандомизационной стойкости после некоторого интуитивного пояснения. В разделе 4 приведено заключение.

2. Предварительные сведения и обозначения

Формально, криптосистема состоит из тройки алгоритмов $(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$. Вероятностный алгоритм KeyGen принимает на вход параметр уровня криптостойкости λ и выдает в качестве результата пару ключей – ключ зашифрования и ключ расшифрования. Алгоритмы Enc и Dec принимают на вход, соответственно, открытый текст вместе с ключом зашифрования и шифртекст вместе с ключом расшифрования (вычислительная сложность всех этих алгоритмов должна быть полиномиальна от параметра уровня криптостойкости λ). В зависимости от того, является ли алгоритм Enc вероятностным или детерминированным, вся криптосистема в целом будет являться вероятностной или детерминированной. В гомоморфной криптосистеме к этой тройке алгоритмов добавляется еще алгоритм Eval, который принимает на вход шифртексты, и в качестве результата выдает шифртекст, производя вычисления над зашифрованными данными. Как правило, гомоморфные криптосистемы допускают выполнение какого-то ограниченного набора арифметических операций над зашифрованными данными.

Проблема построения полностью гомоморфного шифрования (ПГШ), обеспечивающего гомоморфное сложение и умножение зашифрованных данных при неограниченном числе операций была поставлена впервые в работе [12], и оставалась в основном открытой до появления в свет работы Крейга Джентри в 2009 году (отличительное качество ПГШ состоит в том, что оно позволяет вычислить *любую* формулу над зашифрованными данными, поскольку любая формула выражается через сложения и умножения операндов). Впрочем, предложенное решение проблемы было эффективно лишь теоретически, поэтому вскоре после публикации Крейгом Джентри работы [13] стали появляться другие конструкции полностью гомоморфных криптосистем. Для большинства из них делались попытки обосновать их криптостойкость через сложность задач решения систем уравнений или факторизации чисел при атаке с известным открытым текстом. Эта атака является на сегодняшний день де-факто стандартом, позволяющим оценить качество ПГШ в целом, поскольку в силу гомоморфных свойств и свойства податливости (malleability) из произвольного шифртекста возможно получение шифртекста нуля.

Такая криптостойкость носит также название семантической криптостойкости и проверяется, например, через т.н. «игру» $\mathrm{DSemGame}$.

Определение 2.1. *(«Игра по угадыванию семантики»* $\mathrm{DSemGame}$*) Опишем алгоритм* $\mathrm{DSemGame}^{\mathrm{Adv}}(\lambda)$*, где* λ *– параметр уровня криптостойкости, а* Adv *– криптоаналитик.*

1. *Положить* $\mathbf{k} \leftarrow \mathrm{KeyGen}(1^{\lambda})$
2. *Генерировать* $(m_0, m_1) \leftarrow \mathrm{Adv}^{Enc_{\mathbf{k}}(\cdot)}(1^{\lambda})$ *при* $|m_0| = |m_1|$.
3. *Положить* $b \leftarrow \{0,1\}$ *и шифртекст* $c \leftarrow Enc_{\mathbf{k}}(m_b)$.
4. *Пусть* $b' \leftarrow \mathrm{Adv}^{Enc_{\mathbf{k}}(\cdot)}(c)$.
5. *Выдать 1, если* $b = b'$ *и* Adv *никогда не запрашивал* m_0 *или* m_1 *у оракула зашифрования, иначе выдать 0.*

Определение 2.2. *Криптосистема называется семантически криптостойкой, если для любого полиномиального алгоритма* Adv *при любом выборе достаточно большого параметра уровня криптостойкости* λ *выполняется*

$$\Pr\left[\mathrm{DSemGame}^{\mathrm{Adv}}(1^{\lambda}) = 1\right] \le 1/2 + negl(\lambda),$$

где вероятность случайных величин берется равномерной.

Однако некоторые авторы доказывают криптостойкость в атаке только по шифртекстам, поскольку их криптосистемы не обеспечивают стойкость в атаке с известным открытым текстом, хотя являются достаточно простыми и вычислительно эффективными, что обуславливает желание найти им какое-то применение. Дело в том, что хотя свойство податливости имеет место для всех алгебраически гомоморфных криптосистем, но фактическую опасность представляет в основном для криптосистем с небольшим пространством открытых текстов: например, если это пространство – один бит (как в исходной криптосистеме Джентри), можно произвести следующую операцию – возвести шифртекст в квадрат и прибавить полученное к исходному шифртексту, таким образом, получив шифртекст нуля. В случае же большого пространства открытых текстов (тем более, если это пространство не имеет алгебраической структуры поля) неочевидно как можно воспользоваться податливостью для взлома шифра.

В целом, можно сказать, что есть потребность в критериях, позволяющих отделить «пригодные к использованию» ПГШ криптосистемы от «непригодных» в ряде практических ситуаций. Например, можно ли использовать ПГШ в случае если, например, криптоаналитик без труда может получить некоторые соотношения между открытыми текстами, соответствующими имеющимся у него шифртекстам? В случае, если криптоаналитику известно вероятностное распределение на множестве открытых текстов? Или в ситуации (часто встречающейся в приложениях облачных баз данных), когда один и тот же набор исходных данных оказывается зашифрованным в нескольких экземплярах с использованием разных криптосистем (т.е. данные дублируются но с использованием разного шифрования – это делается для обеспечения всех необходимых операций над данными, поскольку один вид ШСС не сохраняет все необходимые свойства)?

Зададимся вопросом: *какими свойствами криптостойкости должна обладать гомоморфная криптосистема для безопасного использования в этих условиях*? Конечно, в случае использования шифра, криптостойкого против атаки по известным открытым текстам можно не беспокоится о нарушении защиты. Проблема, однако, состоит в том, что полностью гомоморфные криптосистемы с доказанными свойствами криптостойкости против атаки по известным открытым текстам пока что являются слишком вычислительно неэффективными. Вместе с тем есть вычислительно эффективные криптосистемы с доказанными свойствами стойкости против атаки только по шифртекстам, поэтому возникает резонный вопрос о возможности применения их в данной ситуации.

Будем исходить из следующего предположения: *пригодное к использованию полностью гомоморфное шифрование не может быть детерминированным*. Во-первых, оно не обеспечивает семантическую криптостойкость: если существует единственный шифртекст, соответствующий данному открытому тексту, то в игре DSemGame противник может отличить зашифрованное m_0

от m_1 , запуская алгоритм Enc и сравнивая результат со своим шифртекстом. Во-вторых, нейтральный по операции элемент в большинстве криптосистем определен единственным образом, и т.о. фактически не может быть зашифрован при таком подходе.

Исходя из сказанного, «плохой» будем считать детерминированную гомоморфную криптосистему, или *сводящуюся к таковой*. О чем идет речь? Дело в том, что вероятностную криптосистему можно преобразовать в детерминированную путем преобразования её алгоритма Enc: зафиксируем некоторый набор случайных битов, подаваемых на вход этому алгоритму и будем производить шифртексты только с этим набором. Поскольку этот набор произволен, то одной вероятностной криптосистеме можно поставить в соответствие 2^{λ} (где λ – количество случайных битов, подаваемых на вход исходному алгоритму Enc) детерминированных криптосистем, каждая из которых получается при некотором зафиксировании вектора случайных битов. Будем говорить о вышеописанном процессе как о *дерандомизации* вероятностной криптосистемы.

Пусть $\varepsilon = \{\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec}\}$ – вероятностная криптосистема, $c_1,...,c_N$ – шифртексты открытых текстов $m_1,...,m_N$, произведенные алгоритмом Enc криптосистемы ε, т.е. $c_i = \mathrm{Enc}(m_i, \mathbf{k}, r_i), i = 1,...,N$, где $\mathbf{k}$ – ключ зашифрования, r_i – случайные элементы (последовательности случайных битов). Рассмотрим детерминированную криптосистему $\varepsilon' = \{\mathrm{KeyGen}, \mathrm{Enc}', \mathrm{Dec}\}$, полученную в результате дерандомизации криптосистемы ε и обозначим как $c_1',...,c_N'$ шифртексты, производимые её алгоритмом Enc' от тех же открытых текстов $m_1,...,m_N$, т.е. $c_i' = \mathrm{Enc}'(m_i, \mathbf{k}), i = 1,...,N$. Если существует полиномиальный алгоритм, который преобразует каждое c_i в c_i' то будем говорить, что криптосистема является нестойкой к дерандомизации.

По аналогии можно ввести понятие «частичной дернадомизации» когда существует полиномиальный алгоритм преобразования шифртекстов в такие, которые были порождены с использованием *меньшего* набора случайных битов.

Конечно, сама по себе дерандомизация – это еще не полный взлом шифра, однако это показатель того, что его криптостойкость не так высока, как кажется на первый взгляд. Можно ли использовать дерандомизацию как элемент процесса полного взлома шифра? Как конкретно может быть проведена дерандомизация?

В следующем разделе попытаемся предложить модель криптостойкости, в рамках которой можно будет ответить на эти вопросы.

3. Понятие дерандомизационной криптостойкости

В литературе [8] можно встретить понятие дерандомизации алгоритмов, которое означает *эффективное* преобразование вероятностного алгоритма в детерминированный. В данной работе вводится понятие дерандомизации вероятностной криптосистемы или шифра (хотя неформально оно употреблялось, например, в [14]), которое аналогично дерандомизации алгоритмов означает *эффективное* преобразование вероятностного шифра (криптосистемы) в шифр простой замены (детерминированный).

Данное понятие имеет особое значение для полностью гомоморфных криптосистем: пригодная к использованию криптосистема такого типа *должна быть* вероятностной, поскольку в большинстве случаев нейтральные по гомоморфным операциям элементы определены единственным образом, как следствие в случае детерминированной гомоморфной криптосистем даже незначительной дополнительной информации (например, знания о том, что вероятностное распределение на множестве открытых текстов неравномерно) может оказаться достаточно для вскрытия шифрования.

Приведем пример практической ситуации, в которой возникает необходимость подобного анализа защищенности. Допустим, случается частичная утечка информации, например, нескольких бит открытого текста. В случае если уже имеются какие-то соотношения между открытыми текстами, с учетом дополнительной информации шифр может быть полностью взломан даже в случае его стойкости против атаки только по шифртекстам.

В интересующих нас случаях для раскрытия исходных данных вовсе не требуется полной определенности в соотношениях между открытыми текстами, а требуется лишь *некоторая* информация. В соответствии с этим попытаемся расширить наше представление о дерандомизации, для того чтобы это учесть.

Таким образом, приходим к следующему: дерандомизация подразумевает получение некоторой системы уравнений с участием только открытых текстов, однако эти уравнения могут иметь разное количество решений и разную степень сложности решения. Интуитивно, можно сказать, что, например, получение линейных или аффинных соотношений почти полностью разрушает конфиденциальность. Необходимо также различать случаи, когда система имеет одно решение, но, например, сложна для решения от случая, когда она имеет одно решение и легко решается.

Определение 3.1: *Систему из (более чем одного) полиномиальных уравнений*

$$\begin{cases} p_1(x_1,...,x_n,\alpha)=0 \\ ... \\ p_k(x_1,...,x_n,\alpha)=0 \end{cases} \quad (1)$$

от переменных $x_1,...,x_n,\alpha$ *назовем однопараметрической системой уравнений, если при каждом значении параметра (выбранного из переменных)* α *система* (1) *имеет единственное решение*.

Определение 3.2. *Криптосистема называется криптостойкой к дерандомизации, если не существует полиномиального алгоритма построения однопараметрической системы уравнений с участием только открытых текстов, соответствующих данным шифртекстам*.

Очевидно, что для шифра простой замены можно составить однопараметрическую систему уравнений, связывающую открытые тексты имеющихся у криптоаналитика шифртекстов, и других переменных кроме открытых текстов в системе уравнений нет. Более того, при фиксации любого открытого текста все остальные открытые тексты из системы определяются однозначно, таким образом можно любой шифртекст назначить параметром.

Определение 3.3. *Криптосистема называется криптостойкой к полной дерандомизации если не существует полиномиального алгоритма построения однозначно разрешимой системы уравнений с участием только открытых текстов, соответствующих данным шифртекстам*.

Основная цель при построении полностью гомоморфных криптосистем состоит в том, чтобы сделать их вероятностными, поскольку, к примеру, в случае шифра простой замены если для операций выполняются свойства кольца, то нейтральные элементы по умножению (единица) и сложению (ноль) определяются единственным образом и, таким образом при любом секретном ключе при зашифровании переходят сами в себя.

Определение 3.4. *Криптосистема называется криптостойкой к обобщенной дерандомизации, если не существует полиномиального алгоритма построения какой-либо нетривиальной системы уравнений с участием только открытых текстов, соответствующих данным шифртекстам*.

Естественно задаться вопросом: в каких соотношениях состоят введенные данными определениями понятия по отношению к традиционным в криптографии, таким как неразличимость шифртекстов [15], семантическая крипто-

стойкость и т. д.? Классически, от шифрования[2] требуется семантическая криптостойкость против атаки по известным открытым текстам.

Утверждение 1. *Свойство неразличимости шифртекстов криптосистемы (стойкость к атаке по известным открытым текстам) влечет криптостойкость к полной дерандомизации*.

Доказательство. Предположим, криптосистема нестойка к полной дерандомизации. Тогда криптоаналитик составляет систему уравнений, связывающих открытые тексты, соответствующие шифртекстам, а затем запускает игру $\mathrm{DSemGame}$, в которой по очереди подставляет открытые тексты в систему (при этом в одном из двух случаев система будет разрешима) и тем самым находит, какой из шифртекстов что шифрует.

Утверждение 2. *Свойство неразличимости шифртекстов криптосистемы (стойкость к атаке по известным открытым текстам) влечет криптостойкость к дерандомизации*.

Доказательство. Предположим, криптосистема нестойка к дерандомизации. Тогда криптоаналитик составляет систему уравнений, связывающих открытые тексты, соответствующие шифртекстам, а затем запускает игру $\mathrm{DSemGame}$, в которой по очереди подставляет открытые тексты в систему и находит НОД получившихся после подстановки полиномов от одной переменной α (при этом в одном из двух случаев НОД будет нетривиален, т.е.>1) и тем самым находит, какой из шифртекстов что шифрует.

Дерандомизации зачастую позволяет ответить на такие вопросы: есть ли в данной последовательности шифртекстов такие, которые шифруют один и тот же открытый текст и много ли таких шифртекстов?

Можно предложить некоторое альтернативное определение дерандомизации. Представим себе алгоритм шифрования гомоморфной криптосистемы: *в зависимости от параметра уровня криптостойкости этот алгоритм использует разное количество случайных битов при производстве шифртекстов*. Если часть из этих битов стала известна криптоаналитику, то такую ситуацию называют *утечкой битов* или *частичной утечкой информации*. Ситуация же дерандомизации с этой точки зрения представляет собой некоторый массовый

[2] Как общепринято в литературе по криптографии, считаем, что криптосистема (шифр) состоит из тройки алгоритмов генерации ключа $\mathrm{KeyGen}(1^{\lambda})$, зашифрования $\mathrm{Enc}_{\mathbf{k}}(\cdot)$ и расшифрования $\mathrm{Dec}_{\mathbf{k}}(\cdot)$.

вариант утечки битов: *для всех шифртекстов имеющихся у криптоаналитика ему открывается одинаковое число случайных битов*. Таким образом, можно предложить альтернативное определение дерандомизации. Для более формального определения вспомним, что алгоритм зашифрования $Enc_{\mathbf{k}}(\cdot)$ *вероятностной* криптосистемы использует для производства шифртекста кроме секретного ключа еще и набор из λ случайных битов.

Определение 3.2'. *Криптосистема является стойкой к дерандомизации, если для преобразования шифртекстов, произведённых алгоритмом* $Enc_{\mathbf{k}}(\cdot)$ *с использованием* λ *случайных битов, то преобразование этих шифртекстов к таким, которые произведены алгоритмом* $Enc_{\mathbf{k}}(\cdot)$ *с использованием* $\lambda' = 0$ *случайных битов, необходимо решить вычислительно сложную задачу*.

Справедлива следующая теорема.

Теорема 1. Определения 3.2 и 3.2' эквивалентны.
Доказательство будет изложено в расширенной версии статьи.

Определение 3.4'. *Криптосистема является стойкой к обобщённой дерандомизации, если для преобразования шифртекстов, произведённых алгоритмом* $Enc_{\mathbf{sk}}(\cdot)$ *с использованием* λ *случайных битов, то преобразование этих шифртекстов к таким, которые произведены алгоритмом* $Enc_{\mathbf{k}}(\cdot)$ *с использованием* $\lambda' < \lambda$ *случайных битов, необходимо решить NP-сложную вычислительную задачу.*

Теорема 2. Определения 3.4 и 3.4' эквивалентны.
Доказательство будет изложено в расширенной версии статьи.

Рассмотрим теперь примеры стойких и нестойких к дерандомизации криптосистем. Рассмотрим криптосистемы из [9].

Утверждение 3. Криптосистемы MORE и PORE являются стойкими к дерандомизации.

Утверждение 4. Криптосистема из [11] является нестойкой к дерандомизации.

Поскольку в качестве преобразования зашифрования в [11] предлагается использовать такой гомоморфизм полиномиальных колец как подстановку (композицию) полиномов, а вместе с тем известно, что для декомпозиции полиномов (с точностью до линейного члена) существуют полиномиальные алгоритмы, то можно сделать вывод о нестойкости к дерандомизации этой криптосистемы.

Замечание. На первый взгляд может показаться, что нестойкость к дерандомизации полностью гомоморфных криптосистем влечет и их нестойкость к атаке по шифртекстам (в случае нестойкости к атаке с известным открытым текстом), ввиду свойства податливости. Однако это неверно, поскольку получаемые посредством податливости шифртексты, про которые мы знаем, какому исходному тексту они соответствуют, могут оказаться «универсальными», т.е. подходящими для всех секретных ключей и таким образом не хранящими информации о секретном ключе. Таковы, например, в случае криптосистемы MORE из [9] диагональные матрицы или в случае PORE просто числа (любое число для PORE является шифртекстом самого себя на любом ключе).

4. Заключение

Были определены минимальные требования, предъявляемые к используемым на практике гомоморфным шифрам. Были введены новое понятие дерандомизации шифров и определения криптостойкости к дерандомизации. Установлены взаимосвязи введенных определений с классическими определениями стойкости в криптографии при различных атаках в общем случае и в случае полностью гомоморфных криптосистем.

Показаны примеры алгебраически гомоморфных криптосистем, являющиеся стойкими и нестойкими к дерандомизации.

Список литературы

[1]. Popa, R. A., Redfield, C., Zeldovich, N., Balakrishnan, H. CryptDB: protecting confidentiality with encrypted query processing //Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. – ACM, 2011. – С. 85-100.

[2]. A. Arasu, S. Blanas, K. Eguro, R. Kaushik, D. Kossmann, R. Ramamurthy, and R. Venkatesan. Orthogonal security with cipherbase. In CIDR, 2013.

[3]. Google Encrytped Big Query. https://github.com/google/encrypted-bigquery-client.

[4]. Always Encrypted. https://msdn.microsoft.com/en-us/library/mt163865(v=sql.130).aspx.

[5]. Shatilov, K., Boiko, V., Krendelev, S., Anisutina, D., & Sumaneev, A. Solution for secure private data storage in a cloud //Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. – IEEE, 2014. – С. 885-889.

[6]. Agrawal, R., Kiernan, J., Srikant, R., & Xu, Y. Order preserving encryption for numeric data //Proceedings of the 2004 ACM SIGMOD international conference on Management of data. – ACM, 2004. – С. 563-574.

[7]. Н. П. Варновский, А. В. Шокуров. Гомоморфное шифрование. Труды ИСП РАН, том 12, 2007 г. стр. 27-36

[8]. Barak B., Ong S. J., Vadhan S. Derandomization in cryptography //SIAM Journal on Computing. – 2007. – Т. 37. – №. 2. – С. 380-400.
[9]. Kipnis A., Hibshoosh E. Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification //IACR Cryptology ePrint Archive. – 2012. – №. 637.
[10]. Kipnis A., Hibshoosh E. Method and system for homomorphicly randomizing an input : заяв. пат. 14/417,184 США. – 2013. ().
[11]. Жиров А.О., Жирова О.В., Кренделев С.Ф.. Безопасные облачные вычисления с помощью гомоморфной криптографии. Безопасность информационных технологий, 2013, Т. 1, С. 6–12.
[12]. R. L. Rivest, L. Adleman, M. L. Dertouzos. On data banks and privacy homomorphisms //Foundations of secure computation. –Т. 4. – №. 11. – 1978. pp. 169-180.
[13]. C. Gentry. Fully homomorphic encryption using ideal lattices //Proceedings of the 41st annual ACM symposium on Symposium on theory of computing-STOC'09. – ACM Press, 2009. pp. 169-169.
[14]. Hemenway B., Ostrovsky R. Building lossy trapdoor functions from lossy encryption //Advances in Cryptology-ASIACRYPT 2013. – Springer Berlin Heidelberg, 2013. – С. 241-260.
[15]. Goldreich O. Foundations of cryptography: volume 2, basic applications. – Cambridge university press, 2004.

Derandomization Security of Homomorphic Encryption

A. Trepacheva <alina1989malina@ya.ru>
Southern Federal University,
105/42, Bolshaya Sadovaya st., Rostov-on-Don, 344006, Russia

Abstract. The paper considers the problems of developing and analysis of cloud database systems. We determine the minimal requirements for encryption to be usable in practical applications. A new notion – a non-derandomizable encryption – allows to do this and we explain the practical value of this notion as well as links between it and classical notions of cryptosystem's security, practical security of whole cloud computing system.
The derandomizable encryption essentially is equivalent to a simple substitution cipher. In other words, encryption is derandomizable if an effective algorithm exists translating it into a simple substitution cipher.
There are some features of derandomizable encryption allowing to check their properties in a simple way. For this purpose, this paper proposes an alternative definition of derandomizable encryption in terms of systems of equations, drawn up by known plaintext cryptanalysis.
Then the paper proposes definitions of generalized derandomization and full derandomization.
Briefly, the generalized derandomizable encryption allows to reduce efficiently the number of variables in system of equations composed for known plaintext attack; the fully derandomizable encryption allows to compose uniquely solvable system of equations by known plaintext attack effectively.

We show the examples of simple algebraically homomorphic cryptosystems – both derandomizable and not non-derandomizable. The paper finally concludes about usability of considered cryptosystems for practical cloud systems.

Keywords: information security, cloud computing, homomorphic encryption, secure computations, derandomization.

DOI: 10.15514/ISPRAS-2015-27(6)-24

For citation: Trepacheva A. Derandomization Security of Homomorphic Encryption. Trudy ISP RAN/Proc. ISP RAS, vol. 27, issue 6, 2015, pp. 381-394 (in Russian). DOI: 10.15514/ISPRAS-2015-27(6)-24.

References

[1]. Popa, R. A., Redfield, C., Zeldovich, N., & Balakrishnan, H. CryptDB: protecting confidentiality with encrypted query processing //Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. – ACM, 2011. – С. 85-100.

[2]. A. Arasu, S. Blanas, K. Eguro, R. Kaushik, D. Kossmann, R. Ramamurthy, and R. Venkatesan. Orthogonal security with cipherbase. In CIDR, 2013.

[3]. Google Encrytped Big Query. https://github.com/google/encrypted-bigquery-client.

[4]. Always Encrypted. https://msdn.microsoft.com/en-us/library/mt163865(v=sql.130).aspx.

[5]. Shatilov, K., Boiko, V., Krendelev, S., Anisutina, D., & Sumaneev, A. Solution for secure private data storage in a cloud //Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. – IEEE, 2014. – С. 885-889.

[6]. Agrawal, R., Kiernan, J., Srikant, R., & Xu, Y. Order preserving encryption for numeric data //Proceedings of the 2004 ACM SIGMOD international conference on Management of data. – ACM, 2004. – С. 563-574.

[7]. N. P. Varnovskij, A. V. Shokurov. Gomomorfnoe shifrovanie [Homomorphic Encryption]. *Trudy ISP RAN* [*The Proceedings of ISP RAS*], 2007, vol. 12, pp. 27-36 (in Russian).

[8]. Barak B., Ong S. J., Vadhan S. Derandomization in cryptography //SIAM Journal on Computing. – 2007. – Т. 37. – №. 2. – С. 380-400.

[9]. Kipnis A., Hibshoosh E. Efficient Methods for Practical Fully Homomorphic Symmetric-key Encrypton, Randomization and Verification //IACR Cryptology ePrint Archive. – 2012. – №. 637.

[10]. Kipnis A., Hibshoosh E. Method and system for homomorphicly randomizing an input : заяв. пат. 14/417,184 США. – 2013. ().

[11]. Zjirov A.O., Zjirova O.V., Krendelev S.Ph. Bezopasnye oblachnye vychislenija s pomoshh'ju gomomorfnoj kriptografii [Secure cloud computing with homomorphic encryption]. Bezopasnost' informacionnyh tehnologij [Security of Information Technologies], 2013, v. 1, pp. 6–12 (in Russian).

[12]. R. L. Rivest, L. Adleman, M. L. Dertouzos. On data banks and privacy homomorphisms. *Foundations of secure computation*, 1978, vol. 4, no. 11. pp. 169-180.

[13]. C. Gentry. Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st annual ACM symposium on Symposium on theory of computing-STOC'09*. – ACM Press, 2009, pp. 169-169.

[14]. Hemenway B., Ostrovsky R. Building lossy trapdoor functions from lossy encryption //Advances in Cryptology-ASIACRYPT 2013. – Springer Berlin Heidelberg, 2013. – C. 241-260.

[15]. Goldreich O. Foundations of cryptography: volume 2, basic applications. – Cambridge university press, 2004.