сылок между субъектом и информационной системой и промежуточная их обработка обеими сторонами. В результате этих действий обе стороны обмена должны удостоверить, что они являются теми, за кого себя выдают.

В результате работы изучены средства защиты персональных данных от несанкционированного доступа, в основе работы которых лежит использование криптографических методов и алгоритмов защиты информации. Изучена сфера применения этих средств в компании ООО «Цинтур». Также получены практические навыки работы с данными средствами.

### Библиографические ссылки

1. *Соколов А. В.*, *Шаньгин В. Ф.* Защита информации в распределенных корпоративных сетях и системах. М. : ДМК, 2002. 450 с.

## РЕАЛИЗАЦИЯ КРИПТОСИСТЕМЫ ПЭЙЕ НА ЭРЛАНГЕ

*А. Н. Комиссаров*, *Д. А. Подкорытов*, *С. О. Суханинский*
(Курган, КГУ, cerg121@yandex.ru)

В настоящее время все более активно развиваются технологии облачных вычислений. Основными причинами такого развития являются доступность, низкая стоимость и вычислительная эластичность данной технологии. Также у компаний и физических лиц появляется возможность значительно уменьшить расходы на инфраструктуру информационных технологий. Но несмотря на все эти преимущества, существует реальная угроза раскрытия конфиденциальных данных, хранящихся в облачной инфраструктуре, так как у ее провайдера появляется возможность неконтролируемого доступа к обрабатываемым данным.

Единственным действенным решением этой проблемы может служить шифрование всей конфиденциальной информации перед передачей в облако. К сожалению, все распространенные в настоя-

щее время криптографические алгоритмы не позволяют производить произвольные вычисления над зашифрованными данными, существенно ограничивая возможности использования облачных ресурсов. В связи с необходимостью повышения безопасности облачных вычислений становится важным создание эффективных алгоритмов полностью гомоморфного шифрования, позволяющего производить произвольные вычисления над данными без предварительной расшифровки.

Под гомоморфным шифрованием понимается криптографический примитив (функция или семейство функций, которые используются как составной элемент при построении криптосистем или криптографических протоколов и обладают определенным криптографическим свойством), представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо алгебраических операций над открытыми текстами.

Пусть $E(k, m)$ – функция шифрования, где $m$ – открытый текст, $k$ – ключ шифрования. Для данных фиксированных $k$ и $m$ криптограмма $E(k, m)$ может быть случайной величиной. В таких случаях говорят о вероятностном шифровании. Функция $E$ гомоморфна относительно операции $op$ (под $op$ понимается какая-то конкретная математическая операция) над открытыми текстами, если существует эффективный алгоритм $M$, который, получив на вход любую пару криптограмм вида $E(k, m_1)$, $E(k, m_2)$, выдает криптограмму $c$ такую, что при дешифровании $c$ будет получен открытый текст $m_1 op m_2$.

Как правило, рассматривается следующий важнейший частный случай гомоморфного шифрования. Для данной функции шифрования $E$ и операции $op1$ над открытыми текстами существует операция $op2$ над криптограммами такая, что из криптограммы $E(k, m_1) op2 E(k, m_2)$ при дешифровании извлекается открытый текст $m_1 op1 m_2$.

Гомоморфное шифрование как криптографический примитив может найти широкое применение в криптографии и в разработке математических методов защиты информации. Прежде всего следу-

ет выделить такую интересную с прикладной точки зрения задачу, как вычисления над зашифрованными данными. Конфиденциальные данные хранятся в зашифрованном виде. Для выполнения вычислений над ними данные можно расшифровать, произвести необходимые операции, и затем результаты вновь зашифровать. Но для этого требуются защищенная аппаратура и организационные меры по хранению секретных ключей. Вычисления над зашифрованными данными, если они возможны, помогают избежать всех этих проблем.

Криптосистема Пэйе является системой вероятностного шифрования. Из всех известных криптосистем с открытым ключом данная обладает наиболее интересными для прикладного использования гомоморфными свойствами:

1) произведение двух криптограмм является криптограммой суммы соответствующих открытых текстов, т. е. при дешифровании криптограммы $E(k, m_1) \times E(k, m_2) \bmod n^2$ будет получен открытый текст $m_1 + m_2 \bmod n$;

2) ту же самую сумму можно получить, умножив криптограмму $E(k, m_1)$ на $g^{m_2}$, т. е. при дешифровании криптограммы $E(k, m_1) \times$ $\times g^{m_2} \bmod n^2$ будет получен открытый текст $m_1 + m_2 \bmod n$;

3) открытый текст, содержащийся в криптограмме, можно умножить на константу $d$, возведя эту криптограмму в степень $d$, т. е. при дешифровании криптограммы $E(k, m)^d \bmod n^2$ будет получен открытый текст $d \times m \bmod n$. В частности, в качестве константы $d$ можно задать другой открытый текст $m'$ и тем самым получить криптограмму произведения $m \times m' \bmod n$.

Последнее свойство не является свойством гомоморфности функции шифрования относительно операции умножения открытых текстов.

Шифрование выполняется следующим образом: пусть $p$ и $q$ – два больших простых числа и пусть $n = p \times q$ и $\lambda = \text{НОК}(p-1, q-1)$.

Выберем случайное число $g$, причем $g < n^2$, и вычислим

$$\mu = \left( L\left( g^{\lambda} \bmod n^2 \right) \right)^{-1} \bmod n,$$

где $L(u) = \dfrac{u-1}{n}$.

Поскольку при выбранном $\lambda$ выполняется сравнение $u \equiv 1 \bmod n$, определение корректно, так как $L(u) = \dfrac{u-1}{u \bmod n} = \dfrac{u-1 \bmod n}{u \bmod n}$ есть целое число.

Открытым ключом криптосистемы служит пара $k = (n, g)$, а секретным ключом – пара $(\lambda, \mu)$. Для шифрования открытого текста $m \in Z_n$ (множество целых чисел $n$) выбирается случайное число $r$, причем $r < n^2$, и вычисляется шифртекст по формуле

$$c = (g^m \times r^n) \bmod n^2.$$

Дешифрование криптограммы $c$ выполняется по формуле

$$m = L(c^\lambda \bmod n^2) \times \mu \bmod n.$$

В рамках данной работы была разработана реализация описанного выше алгоритма в виде модулей на языке Erlang. Erlang – функциональный язык программирования с динамической типизацией, предназначенный для создания распределенных вычислительных систем. Данный язык имеет ряд преимуществ, таких как параллелизм, кроссплатформенность и отказоустойчивость. Поддержка работы со сверхдлинными числами и прозрачность кода сделали Erlang идеальным инструментом для реализации криптосистемы Пэйе.

В настоящее время множество исследователей работают над созданием законченного решения, позволяющего безопасно обрабатывать конфиденциальные данные в облаках. Полностью гомоморфное шифрование способно исключить необходимость хотя бы частичной расшифровки данных для произведения вычислений над ними.

## ЛАТИНСКИЙ КВАДРАТ И ЕГО ПРИМЕНЕНИЕ

*В. С. Провков, Д. С. Дорохов*
(Екатеринбург, УрГУПС, www.usurt.ru)

Латинский квадрат – это квадратная матрица порядка $n$, каждая строка и каждый столбец которой являются перестановкой элементов конечного множества $S$, состоящего из $n$ элементов. Наиболее