ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 004.056.5

АЛГЕБРАИЧЕСКИЕ АСПЕКТЫ ЭФФЕКТИВНОЙ РЕАЛИЗАЦИИ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Червяков Н.И., Бабенко М.Г., Кучеров Н.Н.
Северо-Кавказский федеральный университет, Ставрополь, РФ
E-mail: chervyakov@yandex.ru

В статье исследуются методы защиты конфиденциальной информации, обрабатываемой с использованием облачных вычислений. Показано, что для обеспечения безопасности облачных вычислений можно эффективно использовать гомоморфные шифры с применением системы остаточных классов. Построенные схемы гомоморфного шифрования позволяют выполнять арифметические операции в облаках с шифр-текстами. Исследуется зависимость безопасности от количества информации, известной облачным провайдерам при облачном сговоре. Проводится анализ безопасности зашифрованных данных с использованием гомоморфного шифра при сговоре облачных сервисов, а также при различных вычислительных моделях. Предлагается решение проблемы безопасности при передаче и хранении информации в облачных структурах.

Ключевые слова: гомоморфное шифрование, системы остаточных классов, облачные вычисления, схемы разделения секрета, алгоритм Монтгомери

Введение

Облачные вычисления являются новой технологией, которая охватывает параллельные, распределенные и грид-вычисления. Облачные вычисления могут обеспечить следующие три вида сервисных режимов.

1. Программное обеспечение как услуга SaaS. Потребителю предоставляются программные средства – приложения провайдера, выполняемые на облачной инфраструктуре. Приложения доступны с различных клиентских устройств через интерфейс тонкого клиента, такой как браузер (например электронная почта с Web-интерфейсом). Потребитель не управляет и не контролирует саму облачную инфраструктуру, на которой выполняется приложение, будь то сети, серверы, операционные системы, системы хранения или даже некоторые специфичные для приложений возможности. В ряде случаев потребителю может быть предоставлена возможность доступа к некоторым пользовательским конфигурационным настройкам.

2. Платформа как услуга PaaS. Потребителю предоставляются средства для развертывания на облачной инфраструктуре создаваемых потребителем или приобретаемых приложений, разрабатываемых с использованием поддерживаемых провайдером инструментов и языков программирования.

3. Инфраструктура как услуга IaaS. Потребителю предоставляются средства обработки данных, хранения, сетей и других базовых вычислительных ресурсов, на которых потребитель может развертывать и выполнять произвольное программное обеспечение, включая операционные системы и приложения. Потребитель не управляет и не контролирует саму облачную инфраструктуру, но может контролировать операционные системы, средства хранения, развертываемые приложения и, возможно, обладать ограниченным контролем над выбранными сетевыми компонентами.

Для всех этих услуг у пользователей нет необходимости в управлении или контроле облачной инфраструктуры, в том числе сети, сервера, операционной системы, хранения и даже функций приложений. Общие ресурсы, программное обеспечение и другая информация предоставляются на компьютеры по сети. Основным путем развития облачных вычислений является решения проблемы качества обслуживания и проблемы надежности.

В связи с увеличением доступности широкополосного доступа к Internet, развитием систем виртуализации, распределенных вычислений с кластерами серверов на первый план выходит система повсеместного доступа к вычислительным ресурсам – облачным вычислениям. Под облачными вычислениями ИТ-индустрия понимает

предоставляемые третьей стороной приложения для использования по интернету. При помощи технологии облачных вычислений ИТ-менеджеры имеют возможность предоставлять услуги пользователям более быстрыми, гибкими и экономически эффективными способами. Облачные вычисления наряду с техническими преимуществами имеют недостатки, из-за которых многие потенциальные пользователи еще не используют рассматриваемую технологию. Проблема облачных технологий заключается в том, что зашифрованные данные могут только храниться в облаке, так как облачные серверы не могут выполнять вычисления над зашифрованными данными без их предварительной расшифровки. Гомоморфное шифрование позволяет проводить расчеты над зашифрованными данными без их предварительной расшифровки. При обработке конфиденциальных данных с использованием криптографических методов для обеспечения защиты информации от ненадежных серверов возможно передавать ключи для расшифровки данных только доверенным серверам [1; 3-4; 6-9].

Для решения задачи обеспечения безопасности в облачных средах современные алгоритмы симметричного и асимметричного шифрования не подходят, так как не позволяют обеспечить безопасность обрабатываемой информации в облаках. Использование гомоморфного шифрования позволяет обеспечить конфиденциальность обрабатываемой информации и результата вычислений. При реализации вычислительных алгоритмов с использованием гомоморфных шифров возникает задача, связанная с переводом алгоритма в базис операций, поддерживаемый гомоморфным шифром. Исходя из вышесказанного приобретает актуальность задача использования и эффективной реализации гомоморфных шифров.

Гомоморфное шифрование

Информация в облаке хранится в зашифрованном виде. Для эффективной обработки зашифрованной информации необходимо исключить доступ третьих лиц к информации. Таким образом, пользователь не сможет отправить облаку данные для вычислений без предварительной зашифровки. Предположим, что провайдер сможет выполнять любые произвольные вычисления над размещенными данными без предварительного декодирования.

В этом случае гомоморфное шифрование позволяет трансформировать шифр тексты $C(m)$ от сообщения m в шифр тексты $C(f(m))$ из вычислительного сообщения m, не раскрывая сообщения. Первую гомоморфную схему шифрования, известную как конфиденциальный гомоморфизм, предложил Rivest, Alderman и Dertouzos [13] в 1978 году. Схема шифрования называется полностью гомоморфной, если, зная значения $E_n(a)$ и $E_n(b)$, без расшифровывания можно вычислить значение $E_n(f(a,b))$, где f – функция, заданная над множеством операций $(+, \times, \oplus)$, без использования секретного ключа. Схемы гомоморфного шифрования могут быть классифицированы по сложению и умножению.

Аддитивные схемы гомоморфного шифрования – это схемы, в которых шифр тексты вычисляется как сумма простых текстов. Криптосистема Pailler [10] и криптосистемы Goldwasser-Micalli [6] являются аддитивными схемами гомоморфного шифрования.

В мультипликативных гомоморфных схемах шифрования шифр тексты рассчитываются как произведение простых текстов. Мультипликативными гомоморфными схемами являются системы RSA [12] и криптосистемы Эль-Гамаля [14]. Для реализации алгоритмов обработки информации, хранящейся в облаке, необходимо использовать полностью гомоморфное шифрование (ПГШ), потому что ПГШ позволяет выполнять все виды операций над зашифрованными данными без их расшифровки.

Gentry в [2] предложил схему гомоморфного шифрования вида $c = pq + m$, где c – зашифрованный текст; m – сообщение открытого текста; q – случайное число; p – ключ. Эта функция шифрования гомоморфна относительно сложения, вычитания и умножения. Отсюда появляется новое отношение c и m, представляющее собой остаток c по отношению к модулю p.

Система остаточных классов (СОК) используется для достижения повышения производительности, так как можно реализовывать параллельные алгоритмы. СОК определена в терминах множества взаимно простых модулей. Через P обозначим множество модулей

$$P = \{p_1, p_2, ..., p_n\} \text{ и } GSD(p_i, p_j) = 1, \ for\ i \neq j .$$

Динамический диапазон равен $P = \prod_{i=1}^{n} p_i$. Любое целое число в классе вычетов Z_P может быть представлено в СОК:

$$X \xrightarrow{COK} (x_{p1}, x_{p2}, ..., x_{pn}),$$

где $x_{p_i} = x \bmod p_i$. Представление СОК гомоморфно относительно сложения, вычитания и умножения. Другими словами,

$$X \otimes Y \Leftrightarrow \left(x_{p_1} \otimes y_{p_1}, x_{p_2} \otimes y_{p_2}, ..., x_{p_n} \otimes y_{p_n}\right).$$

Основное применение гомоморфное шифрование получит в области облачных вычислений. Если клиент зашифрует свои данные с помощью гомоморфного шифрования, то он сможет использовать ненадежное облако для вычислений конфиденциальных данных.

СОК создает несколько частей в данных, и операции над этими частями являются гомоморфными. Эти два свойства СОК могут быть использованы для разработки гомоморфной функции шифрования для облачных вычислений.

При использовании СОК возникает проблема обеспечения конфиденциальности данных. Для того чтобы сделать вычисления в СОК, модуль должен быть передан в облако. Если облачный сервер сможет приобрести все модули СОК каким-либо способом, то это может снизить безопасность системы как облака. Для того чтобы предотвратить такую возможность, можно добавить случайное число к модулю. Добавление случайного числа к модулям производится путем умножения модуля на случайное число $k_{p_i} = k\, p_i$ таким образом, чтобы вычисления выполнялись с использованием модулей $p'_i = p_i k_{p_i}$. В результате данные, полученные из облака, которое работает с помощью модуля p'_i, могут быть преобразованы обратно к модулю p_i с помощью леммы 1 [5; 9].

Лемма 1. Если $p_i \mid p'_i$, то справедливо сравнение: $\left(x \bmod p'_i\right) \bmod p_i = x \bmod p_i$.

Доказательство.

Пусть $c = x \bmod p_i \Rightarrow k \cdot p_i + c = x$. Тогда

$$k = k_{p_i} \frac{k-l}{r_{p_i}} + l \Rightarrow p_i' \frac{k-l}{k_{p_i}} + l p_i + c = x \Rightarrow$$

$$\Rightarrow l p_i + c = x \bmod p_i' \Rightarrow \left(x \bmod p_i'\right) \bmod p_i =$$

$$= c = x \bmod p_i.$$

Использование гомоморфного шифра, построенного на основе леммы 1, позволяет не раскрывать целиком модули системы остаточных классов. Однако в случае объединения нескольких облачных сервисов объем известной информации возрастает. Исследование вопроса, связанного с обеспечением конфиденциальности информации при объединении облачных сервисов в неразрешимое подмножество, равносильно исследованию различных вариантов облачного сговора и анализу объема информации, который узнает неразрешимое подмножество. Вопрос обеспечения конфиденциальности информации исследуем более подробно.

Общий сговор

Пусть a и b представляют собой два числа, которые должны быть сложены для получения результата облаком. Пусть также $P = \{p_1, p_2, ..., p_n\}$ набор модулей, который определяет СОК, и P задает его диапазон так, что $-\frac{P}{2} \le a, b < \frac{P}{2}$. В классе вычетов Z_P диапазон $[0, P/2)$ представляет положительные числа, и диапазон $[P/2, P)$ представляет отрицательные числа. Число x представляется как $M_p - x$, это представление, аналогичное двойным дополнениям. При вычислении облако получает доступ к частям данных a_{p_i}, b_{p_i} и модулю p_i. Для исключения получения облаком всех модулей множества P можно использовать распределение вычислений на разных облаках, как показано на рис. 1.

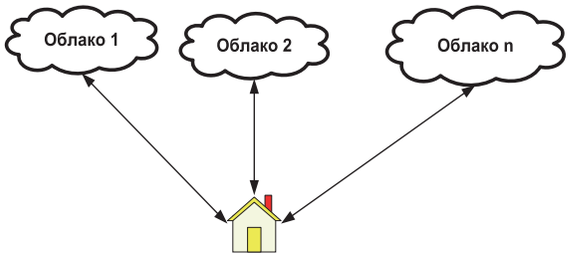

Рис. 1. Схема с вычислением на конкурирующих облаках

При данном подходе клиент производит разделение передаваемых данных на n блоков, каждый из которых включает в себя модуль p'_i и остатки от деления на $p'_i - a_i, b_i$. Затем различные блоки информации передаются различным облакам. Применение данного подхода требует облачный сговор всех облаков для восстановления множества модулей P. Можно использовать другой подход, при котором часть вычислений по некоторым модулям пользователь проводит самостоятельно, а большая часть вычислений проводится в облаке. Таким образом, исключается передача полного множества P облаку, данный подход представлен на рис. 2.

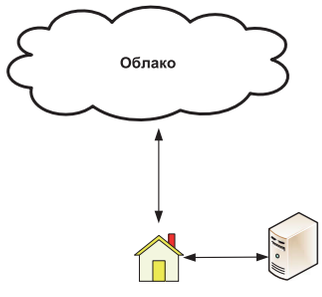

Рис. 2. Схема с вычислениями у клиента

В этом случае облаку не предоставляется доступ ко всем модулям P. Даже с такими ограничениями конфиденциальность не может быть полностью гарантирована. Облако может предсказать P в окрестности размером слова. Тогда оно может предсказать a как $a = xp_i + a_{p_i}$, так что $a < P$. Вероятность того, что облако может найти a правильно, равна p_i / P. Учитывая доступ облака к k модулям, вероятность угадывания результата может быть значительно увеличена до $\prod_{i=1}^{k} p_i / P$.

Таким образом, для обеспечения конфиденциальности информации необходимо защитить истинные значения модулей. Однако для эффективной реализации арифметических операций в облаке необходимо передавать модули СОК облаку; для обеспечения безопасности модулей выберем их так, чтобы они удовлетворяли лемме 1, тогда облаку будут переданы модули p'_i, а не p_i, что позволит обеспечить безопасность модулей СОК.

Может возникнуть задача, при которой пользователь имеет вычислительные ресурсы для проведения небольшой части вычислений и существует потребность в обеспечении высокой степени конфиденциальности передаваемой информации. Для решения данной проблемы произведем объединение двух выше представленных схем, которое позволит получить модифицированную схему, обеспечивающую высокую защищенность информации. Большая часть информации будет вычисляться на нескольких облаках, а также небольшую часть вычислений проведет пользователь, модель такой схемы представлен на рис. 3.

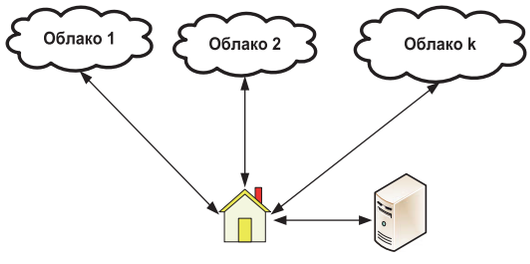

Рис. 3. Схема, при которой вычисления проводятся в облаках и клиентом

Пусть $P = \{p_1, p_2, ..., p_n\}$ – множество модулей и $|p_i| > S_P^n$, где S_P^n является минимальным размером модуля. Пусть также P_n – диапазон этой СОК, k – число модулей, переданных облакам для вычисления данных. Тогда максимальная вероятность того, что любое облако может вывести данные, равна S_P^k / P_n и $P_n \approx S_P^n$.

Пусть $f(n,k)$ представляют вероятность успеха для любого облака с k из n модулей для вывода данных, тогда $f(n,k) = 1/S_P^{n-k}$. Простой способ распределения модулей облакам является создание непересекающихся подмножеств. При использовании данного подхода вероятность успеха сговора между двумя облаками будет возрастать по экспоненте $f(n, k_1 + k_2) = 1/S_P^{n-(k_1+k_2)}$.

Наилучшим вариантом является распределение модулей, при котором вероятность успеха сговора y облаков была меньше суммы их индивидуальных вероятностей успеха, то есть $\sum_{i=1}^{y} f_i(n,k) < \frac{1}{S_P^{n-yk}}$.

Это может быть достигнуто с помощью следующей схемы с резервированием, в которой каждому из облаков будет передано $k = q + l$ модулей, где q – различные непересекающиеся модули и l – модули, являющиеся избыточными и пересекаются с модулями, переданными различным облакам.

Таким образом, если два облака сговорились, они могут собрать не $2k$ модулей, а меньше $2k$. Конечно, если все облака сговорились, то они будут иметь все модули, необходимые для взлома системы СОК.

Утверждение 1. Чтобы полностью воссоздать систему СОК, необходим сговор по крайней мере $n/q + l$ облаков. Пока этого не произойдет, система СОК является безопасной.

Доказательство. Рассмотрим сценарий, где у облаков сговор, для восстановления системы СОК. Сговор приводит к $y \cdot q$ отличию модулей и $y \cdot l$ избыточных модулей. В лучшем случае, $y \cdot l$ по модулю не совпадает с $y \cdot q$ модулей. Группа y облаков воссоздаст все модули, если $n = yl + yq$. Другими словами, $y \geq \frac{n}{q+l}$ для того, чтобы воссоздать систему СОК.

Утверждение 2. Пусть $y \geq \frac{n}{q+l}$, тогда вероятность представления значения $n - yq$ в СОК с yl модулей равна $\left(\frac{yq}{n-yq}\right) \Big/ y\left(\frac{n-q}{l}\right)$, где $\binom{k}{n} = \frac{n!}{(n-k)!\cdot k!}$.

Доказательство. Количество различных представлений числа $n - yq$ равно $\binom{y \cdot q}{n - y \cdot q}$. Количество возможных комбинаций, с учетом параметра y, равно $y\binom{n-q}{l}$, следовательно, вероятность представления значения $n - yq$ в СОК с yl модулей равна $\left(\frac{yq}{n-yq}\right) \Big/ y\left(\frac{n-q}{l}\right)$.

При вычислении операции модульного возведения в степень возникает необходимость в

многократном повторении операции модулярного умножения, так как если использовать операцию умножения в СОК, то возникает ошибка – переполнение динамического диапазона. Для построения схемы гомоморфного шифрования, поддерживающей операцию модульного умножения в СОК, используем подход, предложенный в [11].

Заключение

В ходе проведенного исследования получены следующие результаты. Исследованы методы защиты конфиденциальной информации, обрабатываемой с использованием облачных вычислений. Показано, что для обеспечения безопасности облачных вычислений можно эффективно использовать гомоморфное шифрование в СОК. Рассмотрены способы эффективной реализации арифметических операций $(+, \times, \oplus)$ в облаках над информацией, зашифрованной с использованием гомоморфных шифров. Проведен анализ безопасности зашифрованных с использованием гомоморфного шифра данных при сговоре облачных сервисов. Показано, что объем информации, узнаваемый облачным сервисом, при сговоре растет по экспоненциальному закону. Вследствие всего вышесказанного можно сделать вывод о том, что для защиты информации, обрабатываемой в облаках, эффективно использовать гомоморфные шифры на базе СОК, так как они позволяют реализовать все базовые операции, необходимые при рассмотрении большинства алгоритмов.

Работа выполнена при поддержке стипендии Президента РФ молодым ученым и аспирантам СП-1215.2016.5.

Литература

1. Dimakis A.G., Prabhakaran V., Ramchandran K. Decentralized Erasure Codes for Distributed Networked Storage // IEEE/ACM Transactions on Networking (TON). V.14, № SI, 2006. – P. 2809-2816.
2. Gentry C. Computing Arbitrary Functions of Encrypted Data // Communications of the ACM. V. 53, №3, 2010. – P. 97-105.
3. Ateniese G. et al. Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage // ACM Transactions on Information and System Security (TISSEC). V.9, №1, 2006. – P. 1-30.
4. Lin H.Y., Tzeng W.G. A Secure Decentralized Erasure Code for Distributed Networked Storage // IEEE Transactions on Parallel and Distributed Systems. V.21, №11, 2010. – P. 1586-1594.
5. Bajard J.C., Didier L.S., Kornerup P. An RNS Montgomery Modular Multiplication Algorithm // IEEE Transactions on Computers. V.47, №7, 1998. – P. 766-776.
6. Bringer J. et al. An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication // Australasian Conference on Information Security and Privacy. Springer Berlin Heidelberg, 2007. – P. 96-106.
7. Blaze M., Bleumer G., Strauss M. Divertible Protocols and Atomic Proxy Cryptography // International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 1998. – P. 127-144.
8. Mambo M., Okamoto E. Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. V.80, №1, 1997. – P. 54-63.
9. Gomathisankaran M., Tyagi A., Namuduri K. HORNS: A Homomorphic Encryption Scheme for Cloud Computing Using Residue Number System // CISS, 2011. – P. 1-5.
10. Paillier P. Publickey Cryptosystems Based on Composite Degree Residuosity Classes // International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 1999. – P. 223-238.
11. Montgomery P.L. Modular Multiplication Without Trial Division //Mathematics of Computation. V.44, №170, 1985. – P. 519-521.
12. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Publickey Cryptosystems // Communications of the ACM. V.21, №2, 1978. – P. 120-126.
13. Rivest R.L., Adleman L., Dertouzos M.L. On Data Banks and Privacy Homomorphisms // Foundations of Secure Computation. V.4, №11, 1978. – P. 169-180.
14. El-Gamal T. A Public key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // Workshop on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg, 1984. – P. 10-18.

Получено 21.11. 2016

Червяков Николай Иванович, д.т.н., профессор, Заслуженный деятель науки и техники РФ, заведующий Кафедрой прикладной математики и математического моделирования (ПМ и ММ) Северо-Кавказского федерального университета (СКФУ). Тел. (8-865) 235-48-61; E-mail: chervyakov@yandex.ru

Бабенко Михаил Григорьевич, к.ф-м.н., доцент Кафедры ПМ и ММ СКФУ. Тел. 8-918-753-56-73. E-mail: mgbabenko@ncfu.ru

Кучеров Николай Николаевич, аспирант Кафедры ПМ и ММ СКФУ. Тел. 8-928-341-92-95. E-mail: nkucherov @ncfu.ru

ALGEBRAIC ASPECTS OF EFFECTIVE IMPLEMENTATION OF METHODS FOR INFORMATION PROTECTION IN CLOUD COMPUTING BY USING RESIDUE NUMBER SYSTEM

Chervyakov N.I., Babenko M.G., Kucherov N.N.
North-Caucasus Federal University, Stavropol, Russia Federation
E-mail: chervyakov@yandex.ru

The article researches the methods of confidential information security processed with cloud computing. We demonstrated effectiveness of homomorphic encryption application with residue number system for cloud computing protection. Proposed schemes of homomorphic encryption provide to perform arithmetic operations ($+$, $\times$, $\oplus$) in cloud by ciphertext. We researched security dependence on information capacity known to cloud providers under cloudy conspiracy. Analysis of encrypted data protection is performed by using homomorphic encryption under cloudy conspiracy and various computational models. We propose solution of security problem during data transmission and cloud storage.

Keywords: homomorphic encryption, residue number system, cloud computing, secret sharing schemes, Montgomery algorithm

DOI: 10.18469/ikt.2016.14.4.01

Chervyakov Nikolai Ivanovich, North Caucasus Federal University; 1, Pushkin Street, Stavropol 355009; Head of Department of Applied Mathematics and Computer Science; Doctor of Engineering Sciences. Tel.: +79054693412. E-mail: ncherviakov@ncfu.ru.

Babenko, Mikhail Grigorevich, North Caucasus Federal University; 1, Pushkin Street, Stavropol 355009; Associate Professor at the Department of Applied Mathematics and Computer Science; Candidate of Physico-Mathematical Sciences. Tel.: +79187535673. E-mail: mgbabenko@ncfu.ru.

Kucherov Nikolay Nikolaevich, North Caucasus Federal University; 1, Pushkin Street, Stavropol 355009; Postgraduate at the Department of Applied Mathematics and Computer Science. Tel.: +79283419295. E-mail: nkucherov@ncfu.ru.

References

1 Dimakis A.G., Prabhakaran V., Ramchandran K. Decentralized erasure codes for distributed networked storage. *IEEE/ACM Transactions on Networking (TON)*, 2006, vol. 14, no. SI, pp. 2809-2816.
2. Gentry C. Computing arbitrary functions of encrypted data. *Communications of the ACM,* 2010, vol. 53, no. 3, pp. 97-105.
3. Ateniese G. et al. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security (TISSEC)*, 2006, vol. 9, no. 1, pp. 1-30.
4. Lin H.Y., Tzeng W.G. A secure decentralized erasure code for distributed networked storage. *IEEE transactions on Parallel and Distributed Systems*, 2010, vol. 21, no. 11, pp. 1586-1594.
5. Bajard J.C., Didier L.S., Kornerup P. An RNS Montgomery modular multiplication algorithm. *IEEE Transactions on Computers,* 1998, vol. 47, no. 7, pp. 766-776.
6. Bringer J. et al. An application of the Goldwasser-Micali cryptosystem to biometric authentication. *Australasian Conference on Information Security and Privacy,* Springer Berlin Heidelberg, 2007, pp. 96-106.

7. Blaze M., Bleumer G., Strauss M. Divertible protocols and atomic proxy cryptography. *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer Berlin Heidelberg, 1998, pp. 127-144.
8. Mambo M., Okamoto E. Proxy cryptosystems: Delegation of the power to decrypt cipher-texts. *IEICE transactions on fundamentals of electronics, Communications and computer sciences,* 1997, vol. 80, no. 1, pp. 54-63.
9. Gomathisankaran M., Tyagi A., Namuduri K. HORNS: A homomorphic encryption scheme for Cloud Computing using Residue Number System. *CISS*, 2011, pp. 1-5.
10. Paillier P. Public-key cryptosystems based on composite degree residuosity classes. *International Conference on the Theory and Applications of Cryptographic Techniques,* Springer Berlin Heidelberg, 1999, pp. 223-238.
11. Montgomery P.L. Modular multiplication without trial division. *Mathematics of computation,* 1985, vol. 44, no. 170, pp. 519-521.
12. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, vol. 21, no. 2, pp. 120-126.
13. Rivest R.L., Adleman L., Dertouzos M.L. On data banks and privacy homomorphisms. *Foundations of secure computation*, 1978, vol. 4, no. 11, pp. 169-180.
14. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *Workshop on the Theory and Application of Cryptographic Techniques*, Springer Berlin Heidelberg, 1984, pp. 10-18.

Received 21.11.2016

ТЕХНОЛОГИИ ТЕЛЕКОММУНИКАЦИЙ

УДК 621.391.63; 681.7.068

АНАЛИЗ ВВОДА ОПТИЧЕСКОГО СИГНАЛА «O»-ДИАПАЗОНА ЧЕРЕЗ СОГЛАСУЮЩЕЕ СТАНДАРТНОЕ ОДНОМОДОВОЕ ВОЛОКНО В ГРАДИЕНТНЫЙ МНОГОМОДОВЫЙ СВЕТОВОД С ЦЕНТРАЛЬНЫМ ГАБАРИТНЫМ ДЕФЕКТОМ ПРОФИЛЯ ПОКАЗАТЕЛЯ ПРЕЛОМЛЕНИЯ

Бурдин А.В.[1], Бурдин В.А.[1], Дмитриев Е.В.[1], Демидов В.В.[2], Дукельский К.В.[3], Жуков А.Е.[1], Минаева А.Ю.[1], Прапорщиков Д.Е.[1], Тер-Нерсесянц Е.В.[2]
[1]Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
[2]АО «Научно-исследовательский и технологический институт оптического материаловедения ВНЦ «ГОИ им. С.И. Вавилова», Санкт-Петербург, РФ
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, РФ
E-mail: bourdine@yandex.ru

В работе представлены результаты теоретического анализа перераспределения мощности оптического сигнала, возбуждаемого когерентным источником излучения в «O»-диапазоне длин волн, пигтелированного стандартным одномодовым оптическим волокном рек. ITU-T G.652, между направляемыми модами кварцевых градиентных многомодовых волоконных световодов с габаритным технологическим дефектом профиля показателя преломления в центре сердцевины.

Ключевые слова: маломодовый режим передачи сигнала, дифференциальная модовая задержка, многомодовые оптические волокна, градиентный профиль показателя преломления, технологический дефект профиля, MCVD, возбуждение мод высших порядков, радиальное смещение, угловое рассогласование

Общие положения

На сегодняшний день многомодовые оптические волокна (ММ ОВ) фактически являются основой компактных многопортовых инфокоммуникационных сетей, соединительные волоконно-оптические линии которых отличаются малой протяженностью (формально до 2 км, на практике – буквально сотни, а в ряде случаев – даже десятки метров) при одновременно высоких скоростях передачи информации [1-3].

Переход на мультигигабитные скорости требует применения в оптических модулях активного