DOI 10.52209/1609–1825_2022_1_333 УДК 004.9

# Методы безопасной облачной обработки матричных уравнений большой размерности

[1]**ЕРГАЛИЕВА Бану Бакытжановна,** *докторант, banu.yergaliyeva@gmail.com,*
[1]***СЕЙТКУЛОВ Ержан Нураханович,** к.ф.-м.н., директор НИИ ИБиК, yerzhan.seitkulov@gmail.com,*
[1]**ТАШАТОВ Нурлан Наркенович,** *к.ф.-м.н., доцент, tash.nur@mail.ru,*
[1]**САТЫБАЛДИНА Дина Жагыпаровна,** *к.ф.-м.н., зав. кафедрой, dinasaty@gmail.com,*
[1]*Евразийский национальный университет им. Л.Н. Гумилева, Казахстан, 010008, Нур-Султан, ул. Сатпаева, 2,*
**автор-корреспондент.*

***Аннотация.*** *Целью исследования является разработка новых методов облачной обработки матричных уравнений большой размерности, стойких к активным и пассивным атакам. Исследованы новые методы безопасной облачной обработки больших данных с использованием альтернативных (не криптографических) технологий защиты информации и доказывается их стойкость к атакам. Как правило, для обеспечения безопасности клиент-серверного взаимодействия используются стандартные криптографические протоколы. Эти криптографические методы эффективны в задачах хранения больших данных, но не всегда являются приемлемыми в задачах безопасной обработки больших данных. Например, хорошо известные математические методы гомоморфного шифрования до сих пор не имеют практического применения из-за огромных вычислительных затрат на стороне клиента. Поэтому возникла задача использовать альтернативные методы безопасного аутсорсинга в задачах обработки больших данных. В статье представлены новые методы и технологии защиты информации при обработке больших данных на примере решений матричных уравнений большой размерности.*

***Ключевые слова:*** *информационная безопасность, обработка больших данных, безопасный аутсорсинг, клиент-серверное взаимодействие, решение матричных уравнений.*

**Введение**

Теория безопасного аутсорсинга научных вычислений бурно развивается в различных областях, так как в современных условиях обработку больших данных уже невозможно представить без использования мощных вычислительных ресурсов. Именно поэтому ведущие ученые в области информационной безопасности предлагают самые разные методики безопасного аутсорсинга научных вычислений [1-11].

Целью исследования является разработка новых методов облачной обработки матричных уравнений большой размерности, стойких к активным и пассивным атакам [9]. При этом под активной атакой подразумевается случай, когда в процесс клиент-серверного взаимодействия вмешивается злоумышленник, который перехватывает информацию и посылает клиенту ложную информацию. А пассивная атака – это случай, когда не происходит перехват информации третьими лицами, но сервер непреднамеренно отправляет ошибочную информацию клиенту. Такие случаи возможны при сбоях интернета, помехи связи и т.д.

Суть научной проблемы заключается в том, что клиент не может передавать внешним серверам (вычислительные машины) все данные исходной вычислительно-сложной задачи, так как она может содержать секретные параметры. Поэтому клиенту вначале нужно преобразовать исходную задачу в совершенно другую задачу, где уже секретная информация не может быть обнаружена на внешнем сервере или перехвачена злоумышленником. Полученная новая вычислительно-сложная задача отправляется на сервер для его решения. Затем результат облачной обработки вычислительно-сложной задачи передается клиенту. Из этого промежуточного результата клиент самостоятельно обязан вычислить результат исходной вычислительно-сложной задачи за приемлемое для него время.

Данному клиент-серверному взаимодействию можно придать следующий протокольный вид.

*Протокол Z:*

Предположим, что клиенту необходимо решить вычислительно-сложную задачу $Z$, зависящую от секретного параметра $\alpha$: $Z(\alpha)$. Предположим, что существует алгоритм (или схема) $A$ для решения задачи $Z(\alpha)$, который может быть эффективно реализован на сервере.

Шаг 1. Клиент осуществляет декомпозицию алгоритма $A$ на два алгоритма $B$ и $C$ так, что выполняются следующие условия:

- Реализация алгоритмов $B$ и $C$ позволяет решить задачу Z;

- Алгоритм $B$ может зависеть от секретного параметра, а алгоритм $C$ либо вовсе не зависит от секретного параметра $\alpha$, либо время, необходимое серверу для выявления секрета из алгоритма $C$, неприемлемо для него.

- Клиент может вычислить $C$ достаточно быстро за приемлемое для него время.

Шаг 2. Клиент реализовывает на своем маленьком компьютере алгоритм $B$, а серверу передает алгоритм $C$.

Шаг 3. Сервер реализовывает алгоритм $B$, и результат вычисления передает обратно клиенту.

Шаг 4. Клиент, получив результат вычисления $B$, решает задачу $Z(\alpha)$.

**Методы обработки матричных уравнений большой размерности**

Рассмотрим матричное уравнение следующего вида:

$$A_{nn}X_{nm} = B_{nm}, \qquad (1)$$

где $A_{nn}$, $X_{nm}$ и $B_{nm}$ – матрицы вида

$$A_{nn} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix};$$

$$X_{nm} = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \dots & x_{2m} \\ \dots & \dots & \dots & \dots \\ x_{n1} & x_{n2} & \dots & x_{nm} \end{pmatrix};$$

$$B_{nm} = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ b_{21} & b_{22} & \dots & b_{2m} \\ \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{nm} \end{pmatrix}.$$

Здесь матрица $A_{nn}$ – квадратная матрица размерности $n*n$, матрица $B_{nm}$ – матрица размерности $n*m$. А матрица $X_{nm}$ – искомая матрица, которую требуется найти. Для однозначности решения уравнения (1) предположим, что $\det|A_{nn}| \neq 0$.

**Задача № 1.** Предположим, что требуется приближенно решить уравнение (1) с помощью сервера, при этом матрица $B_{nm}$ – является секретным параметром клиента, а матрица $A_{nn}$ не является секретом. Искомое решение также должно оставаться в секрете.

Следующий протокол решает эту задачу:

Протокол 1.

Шаг 1. Клиент случайным образом выбирает матрицу $D_{nm}$ следующего вида:

$$D_{nm} = \begin{pmatrix} d_{11} & d_{12} & \dots & d_{1m} \\ d_{21} & d_{22} & \dots & d_{2m} \\ \dots & \dots & \dots & \dots \\ d_{n1} & d_{n2} & \dots & d_{nm} \end{pmatrix}.$$

Далее вычисляет композицию двух матриц

$$A_{nn}D_{nm} \equiv W_{nm},$$

а также разность двух матриц: $-W_{nm} + B_{nm} \equiv L_{nm}$. Теперь клиент матрицу $L_{nm}$ отправляет серверу. А матрицу $D_{nm}$ клиент держит в секрете.

Шаг 2. Сервер решает уравнение

$$A_{nn}Y_{nm} = \begin{pmatrix} l_{11} & l_{12} & \dots & l_{1m} \\ l_{21} & l_{22} & \dots & l_{2m} \\ \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & \dots & l_{nm} \end{pmatrix} \equiv L_{nm},$$

относительно неизвестной матрицы

$$Y_{nm} = \begin{pmatrix} y_{11} & y_{12} & \dots & y_{1m} \\ y_{21} & y_{22} & \dots & y_{2m} \\ \dots & \dots & \dots & \dots \\ y_{n1} & y_{n2} & \dots & y_{nm} \end{pmatrix}.$$

Теперь сервер найденное решение $Y^0_{nm}$ уравнения отправляет обратно клиенту.

Шаг 3. Клиент находит искомое решение уравнения (1) путем сложения двух матриц

$$X^0_{nm} = D_{nm} + Y^0_{nm}.$$

Проверка. Действительно, имеет место цепочка равенств

$$A_{nn}X^0_{nm} = A_{nn}(D_{nm} + Y^0_{nm}) = A_{nn}D_{nm} + A_{nn}Y^0_{nm} =$$
$$= W_{nm} + (B_{nm} - W_{nm}) = B_{nm}.$$

Таким образом, $X^0_{nm}$ решение уравнения (1).

Безопасность. Так как сервер получает только разность двух секретных матриц $B_{nm} - W_{nm} \equiv L_{nm}$, то определить секретную матрицу $B_{nm}$ он не сможет. Кроме того, как видим из вычисления, искомое решение уравнения (1) также остается в секрете.

Верификация. Клиент может проверить полученное решение от сервера путем умножения матрицы $A_{nn}$ на матрицу $Y^0_{nm}$, которое приближенно должно совпасть с матрицей $L_{nm}$. Это легко сделать, так как предполагается, что такие операции как «умножения» и «сложения» матриц являются легко вычислимой задачей для клиента. Таким образом, данный протокол является стойким к пассивной атаке, так как целостность полученной информации легко верифицируется. Стойкость к активной атаке также обеспечивается данным протоколом, так как процедура верификации, как видим, позволяет проверить правильность полученного решения о сервере, даже если вмешивается перехватчик информации.

**Задача № 2.** Предположим, что требуется приближенно решить уравнение (1) с помощью сервера, при этом матрица $B_{nm}$ – не является секретным параметром клиента, а матрица $A_{nn}$ наоборот является секретом. Искомое решение также должно оставаться в секрете.

Данную задачу с помощью сервера можно решить следующим протоколом.

Протокол 2.

Шаг 1. Клиент выбирает случайным образом

квадратную матрицу $D_{nn}$, таким образом, чтобы $\det|D_{nn}| \neq 0$. Теперь производит замену переменных

$$X_{nm} = D_{nn} Y_{nm}.$$

Далее клиент вычисляет композицию двух матриц

$$A_{nn} D_{nn} = W_{nn}.$$

Теперь клиент отправляет уравнение $W_{nn} Y_{nm} = B_{nm}$ серверу.

Шаг 2. Сервер решает уравнение $W_{nn} Y_{nm} = B_{nm}$ относительно неизвестной матрицы $Y_{nm}$, и пусть $Y^0_{nm}$ есть решение этого уравнения, которое теперь отправляется клиенту.

Шаг 3. Клиент находит решение $X^0_{nm}$ исходного уравнения (1) по формуле

$$X^0_{nm} = D_{nn} Y^0_{nm}.$$

Проверка. Действительно, имеет место цепочка равенств

$$A_{nn} X^0_{nm} = A_{nn} (D_{nn} Y^0_{nm}) = W_{nn} Y^0_{nm} = B_{nm}.$$

Таким образом, $X^0_{nm}$ решение уравнения (2). Далее, так как $\det|D_{nn}| \neq 0$, то решение уравнения $W_{nn} Y_{nm} = B_{nm}$ существует и однозначно.

Безопасность. Так как сервер получает только произведение двух секретных матриц $A_{nn} * D_{nn} \equiv W_{nn}$, то определить секретную матрицу $A_{nn}$ он не сможет. Кроме того, как видим из вычисления, искомое решение уравнения (1) также остается в секрете.

Верификация. Клиент проверяет полученное решение от сервера путем умножения матрицы $W_{nn}$ на матрицу $Y^0_{nm}$, которое приближенно с заранее определенной точностью должно совпасть с матрицей $B_{nm}$. Данный протокол также является стойким к пассивной атаке и активной атакам, так как целостность и правильность полученной информации от сервера легко верифицируется на стороне клиента.

**Задача № 3.** Предположим, что требуется приближенно решить уравнение (1) с помощью сервера, при этом обе матрицы $B_{nm}$ и $A_{nn}$ являются секретными параметрами клиента. Искомое решение также должно оставаться в секрете.

Данную задачу с помощью сервера решим по следующему протоколу.

Протокол 3.

Шаг 1. Клиент выбирает случайным образом квадратную матрицу $D_{nn}$, таким образом, чтобы $\det|D_{nn}| \neq 0$. Теперь производит замену переменных

$$X_{nm} = D_{nn} Y_{nm}.$$

Далее клиент вычисляет композицию двух матриц

$$A_{nn} D_{nn} = W_{nn}.$$

И получает уравнение вида $W_{nn} Y_{nm} = B_{nm}$. Далее клиент выбирает случайную матрицу $R_{nn}$, такую, что $\det|R_{nn}| \neq 0$, и умножает слева на эту матрицу, тогда клиент получает

$$R_{nn} W_{nn} Y_{nm} = R_{nn} B_{nm}.$$

Обозначим $R_{nn} W_{nn} = Q_{nn}$, $R_{nn} B_{nm} = L_{nm}$. В итоге клиент получает уравнение $Q_{nn} Y_{nm} = L_{nm}$. Это уравнение отправляется серверу для решения относительно неизвестной матрицы $Y_{nm}$.

Шаг 2. Сервер решает уравнение $Q_{nn} Y_{nm} = L_{nm}$ относительно неизвестной матрицы $Y_{nm}$, и пусть $Y^0_{nm}$ есть решение этого уравнения, которое отправляется клиенту.

Шаг 3. Клиент находит решение $X^0_{nm}$ исходного уравнения (1) по формуле

$$X^0_{nm} = D_{nn} Y^0_{nm}.$$

Проверка. Действительно, имеет место цепочка равенств

$$A_{nn} X^0_{nm} = A_{nn} (D_{nn} Y^0_{nm}) = W_{nn} Q^{-1}_{nn} L_{nm} =$$
$$= W_{nn} W^{-1}_{nn} R^{-1}_{nn} R_{nn} B_{nm} = B_{nm}.$$

Таким образом, $X^0_{nm}$ решение уравнения (2). Далее, так как $\det|D_{nn}| \neq 0$ и $\det|R_{nn}| \neq 0$, то решение уравнения $Q_{nn} Y_{nm} = L_{nm}$ существует и однозначно.

Безопасность. Так как сервер получает только произведение трех секретных матриц $R_{nn} * A_{nn} * D_{nn} \equiv Q_{nn}$, а также произведение двух секретных матриц $R_{nn} * B_{nm} \equiv L_{nm}$, то определить секретные матрицы $A_{nn}$ и $B_{nm}$ он не сможет. Кроме того, как видим из вычисления, искомое решение уравнения (1) также остается в секрете.

Верификация. Клиент проверяет полученное решение от сервера путем умножения матрицы $Q_{nn}$ на матрицу $Y^0_{nm}$, которое приближенно с заранее определенной точностью должно совпасть с матрицей $L_{nm}$.

**Выводы**

В работе представлены новые методы безопасной облачной обработки больших данных на примере решения матричных уравнений большой размерности. Все представленные протоколы являются стойкими к пассивной и активной атакам, так как на стороне клиента проводится процедура верификации за приемлемое время. В последующих работах мы представим эффективные программные реализации данных протоколов.

***Источник финансирования***

*Данная работа выполнена при финансовой поддержке грантового финансирования МЦРИАП, No. AP06850817.*

## СПИСОК ЛИТЕРАТУРЫ


1. Yerzhan N. Seitkulov, Seilkhan N. Boranbayev, Gulden B. Ulyukova, Banu B. Yergaliyeva, Dina Satybaldina Methods for secure cloud processing of big data // Indonesian Journal of Electrical Engineering and Computer Science, Vol. 22, No. 3, June 2021, pp. 1650-1658, DOI: 10.11591/ijeecs.v22.i3.pp.1650-1658.
2. Seitkulov Ye. New methods of secure outsourcing of scientific computations // The Journal of Supercomputing, Springer US, Print ISSN 0920-8542. – 2013. – Vol. 65, Issue 1. – pp. 469-482.
3. Jianhua Yu, Xueli Wang, Wei Gao Improvement and applications of secure outsourcing of scientific computations // Journal of Ambient Intelligence and Humanized Computing. – 2015. – Vol. 6, Issue 6. – pp. 763-772.
4. Xing Hu, Chunming Tang Secure outsourced computation of the characteristic polynomial and eigenvalues of matrix / Journal of Cloud Computing, Springer Berlin Heidelberg, 4:7 DOI 10.1186/s13677-015-0033-9, 2015, ISSN 2192-113X. – URL: https://eprint.iacr.org/2014/442.pdf
5. Cong Wang, Kui Ren, Jia Wang Secure Optimization Computation Outsourcing in Cloud Computing: A Case Study of Linear Programming // IEEE Transactions on Computers. – 2016. – Vol. 65, Issue 1. – pp. 216-229.
6. Vyas R., Singh A., Singh J., Soni G., Purushothama B.R.: Design of an efficient verification scheme for correctness of outsourced computations in cloud computing // Security in Computing and Communications, Springer, 2015. – Vol. 536. – pp. 66-77.
7. Atallah M., Frikken K. Securely outsourcing linear algebra computations // In: Proceedings of ASIACCS. New York. – 2010. – pp. 48-59.
8. Benjamin D., Atallah M. Private and cheating-free outsourcing of algebraic computations // Proceedings of 6th conference on privacy, security, and trust (PST). – 2008. – pp. 240-245.
9. Tsutomu Matsumoto, Koki Kato, Hideki Imai Speeding Up Secret Computations with Insecure Auxiliary Devices // CRYPTO 1988: Advances in Cryptology – CRYPTO' 88. – 1998. – pp. 497-506.
10. Thierry Mefenza, Damien Vergnaud Cryptanalysis of Server-Aided RSA Protocols with Private-Key Splitting // Published 2018. – URL: https://www.di.ens.fr/~mefenza/Cryptanalysis%20of%20Server-Aided%20RSA.pdf (дата обращения 2020.10.09).
11. Kai Zhou, Afifi M.H., Jian Ren ExpSOS: Secure and Verifiable Outsourcing of Exponentiation Operations for Mobile Cloud Computing // IEEE Transactions on Information Forensics and Security. – 2017. – Vol. 12, Issue 11. – pp. 2518-2531.


### *Үлкен өлшемді матрицалық теңдеулерді қауіпсіз бұлтты өңдеу әдістері*


[1]***ЕРҒАЛИЕВА Бану Бақытжанқызы,*** *докторант, banu.yergaliyeva@gmail.com,*
[1]****СЕЙТҚҰЛОВ Ержан Нұраханұлы,*** *ф.-м.ғ.к., АҚҚ ҒЗИ директоры, yerzhan.seitkulov@gmail.com,*
[1]***ТАШАТОВ Нұрлан Наркенұлы,*** *ф.-м.ғ.к., доцент, tash.nur@mail.ru,*
[1]***САТЫБАЛДИНА Дина Жағыпарқызы,*** *ф.-м.ғ.к., кафедра меңгерушісі, dinasaty@gmail.com,*
[1]*Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қазақстан, 010008, Нұр-Сұлтан, Сәтпаев көшесі, 2,*

**автор-корреспондент.*



***Аңдатпа.*** *Зерттеудің мақсаты – белсенді және пассивті шабуылдарға төзімді үлкен өлшемді матрицалық теңдеулерді бұлттық өңдеудің жаңа әдістерін әзірлеу. Ақпаратты қорғаудың баламалы (криптографиялық емес) технологияларын пайдалана отырып, үлкен деректерді қауіпсіз бұлттық өңдеудің жаңа әдістерін зерттеп, олардың шабуылдарға төзімділігін дәлелдейміз. Әдетте стандартты криптографиялық хаттамалар клиент-сервер байланысын қамтамасыз ету үшін қолданылады. Бұл криптографиялық әдістер үлкен деректерді сақтау тапсырмалары үшін тиімді, бірақ әрқашан үлкен деректерді өңдеу тапсырмаларын орындауға жарамайды. Мысалы, гомоморфты шифрлаудың белгілі математикалық әдістері клиенттік жағынан үлкен есептеу шығындарына байланысты әлі де практикалық қолданылмайды. Сондықтан үлкен ақпаратты өңдеу тапсырмаларында қауіпсіз аутсорсингтің балама әдістерін қолдану міндеті туындады. Мақалада үлкен көлемді матрицалық теңдеулерді шешу мысалында үлкен мәліметтерді өңдеу кезінде ақпаратты қорғаудың жаңа әдістері мен технологиялары ұсынылған.*



***Кілт сөздер:*** *ақпараттық қауіпсіздік, үлкен деректерді өңдеу, қауіпсіз аутсорсинг, клиент пен сервердің өзара әрекеттесуі, матрицалық теңдеулерді шешу.*


### *Methods for Secure Cloud Processing of Matrix Equations of Large Dimension*


[1]***YERGALIYEVA Banu,*** *doctoral student, banu.yergaliyeva@gmail.com,*
[1]*****SEITKULOV Yerzhan,*** *Cand. of Phys. and Math. Sci., Director of IS&C Institute, yerzhan.seitkulov@gmail.com,*
[1]***TASHATOV Nurlan,*** *Cand. of Phys. and Math. Sci., Associate Professor, tash.nur@mail.ru,*
[1]***SATYBALDINA Dina,*** *Cand. of Phys. and Math. Sci., Head of Department, dinasaty@gmail.com,*
[1]*L.N. Gumilyov Eurasian National University, Kazakhstan, 010008, Nur-Sultan, Satpayev Street, 2,*

**corresponding author.*



***Abstract.*** *The aim of the study is to develop new methods for cloud processing of matrix equations of large dimensions that are resistant to active and passive attacks. Explore new methods of secure cloud processing of big data using alternative (non-cryptographic) information protection technologies and prove their resistance to attacks. Typically,*

*standard cryptographic protocols are used to secure client-server communication. These cryptographic techniques are effective for big data storage tasks, but are not always suitable for secure big data processing tasks. For example, the well-known mathematical methods of homomorphic encryption still have no practical application due to the huge computational costs on the client side. Therefore, the task arose to use alternative methods of secure outsourcing in big data processing tasks. The article presents new methods and technologies for protecting information in the processing of big data on the example of solving matrix equations of large dimensions.*

***Keywords:*** *information security, big data processing, secure outsourcing, client-server interaction, solution of matrix equations.*

## REFERENCES

1. Yerzhan N. Seitkulov, Seilkhan N. Boranbayev, Gulden B. Ulyukova, Banu B. Yergaliyeva, Dina Satybaldina Methods for secure cloud processing of big data // Indonesian Journal of Electrical Engineering and Computer Science, Vol. 22, No. 3, June 2021, pp. 1650-1658, DOI: 10.11591/ijeecs.v22.i3.pp.1650-1658.
2. Seitkulov Ye. New methods of secure outsourcing of scientific computations // The Journal of Supercomputing, Springer US, Print ISSN 0920-8542. – 2013. – Vol. 65, Issue 1. – pp. 469-482.
3. Jianhua Yu, Xueli Wang, Wei Gao Improvement and applications of secure outsourcing of scientific computations // Journal of Ambient Intelligence and Humanized Computing. – 2015. – Vol. 6, Issue 6. – pp. 763-772.
4. Xing Hu, Chunming Tang Secure outsourced computation of the characteristic polynomial and eigenvalues of matrix / Journal of Cloud Computing, Springer Berlin Heidelberg, 4:7 DOI 10.1186/s13677-015-0033-9, 2015, ISSN 2192-113X. – URL: https://eprint.iacr.org/2014/442.pdf
5. Cong Wang, Kui Ren, Jia Wang Secure Optimization Computation Outsourcing in Cloud Computing: A Case Study of Linear Programming // IEEE Transactions on Computers. – 2016. – Vol. 65, Issue 1. – pp. 216-229.
6. Vyas R., Singh A., Singh J., Soni G., Purushothama B.R.: Design of an efficient verification scheme for correctness of outsourced computations in cloud computing // Security in Computing and Communications, Springer, 2015. – Vol. 536. – pp. 66-77.
7. Atallah M., Frikken K. Securely outsourcing linear algebra computations // In: Proceedings of ASIACCS. New York. – 2010. – pp. 48-59.
8. Benjamin D., Atallah M. Private and cheating-free outsourcing of algebraic computations // Proceedings of 6th conference on privacy, security, and trust (PST). – 2008. – pp. 240-245.
9. Tsutomu Matsumoto, Koki Kato, Hideki Imai Speeding Up Secret Computations with Insecure Auxiliary Devices // CRYPTO 1988: Advances in Cryptology – CRYPTO' 88. – 1998. – pp. 497-506.
10. Thierry Mefenza, Damien Vergnaud Cryptanalysis of Server-Aided RSA Protocols with Private-Key Splitting // Published 2018. – URL: https://www.di.ens.fr/~mefenza/Cryptanalysis%20of%20Server-Aided%20RSA.pdf (дата обращения 2020.10.09).
11. Kai Zhou, Afifi M.H., Jian Ren ExpSOS: Secure and Verifiable Outsourcing of Exponentiation Operations for Mobile Cloud Computing // IEEE Transactions on Information Forensics and Security. – 2017. – Vol. 12, Issue 11. – pp. 2518-2531.