УДК 004.056

Марковський О.П.,
Ван Хуаі, Гарасимович Г.В.

ОРГАНІЗАЦІЯ ЗАХИЩЕНОГО ОБЧИСЛЕННЯ МОДУЛЯРНОЇ ЕКСПОНЕНТИ З ВИКОРИСТАННЯМ АДИТИВНОГО МАСКУВАННЯ

ORGANIZE MODULAR EXPONENTIATION SECURE COMPYTATIONBY USING ADDITIVE MASKING

У статті пропонується метод виконання модулярного експоненціювання у хмарних системах із захистом даних та коду експоненти. Запропонований метод дозволяє розділити процедуру модулярного експоненціювання на дві складові: одна, менша частина, виконується користувачем, а інша, більша за обсягом, реалізується на віддалених обчислювальних потужностях. Детально описані математичні принципи пропонованого методу організації захищеного обчислення, викладена відповідна формалізована методика. Наведено числові приклади віддаленого захищеного обчислення модулярної експоненти.

Ключові слова: модулярне експоненціювання, обчислення в хмарі, криптографія, захищені обчислення.

In this paper a method for the performing the calculations required for modular exponentiation using remote or distant computational resources. The proposed method operates by separating the procedure for modular exponentiation in two components. The first component which is computationally simple is performed on the user terminal and the second and computationally complex component, is executed on powerful cloud computational resources. The details of the proposed distributed calculation are presented. Hence, the methodology for the organization of the calculations is analyzed. The calculation is illustrated by means of a simple numerical example.

Key words: modular exponentiation, cloud computing, cryptography, secure computations.

Актуальність теми дослідження. Однією з найбільш знакових подій у розвитку комп’ютерної обробки даних стала поява хмарних технологій. У вирішальній мірі ці прогресивні технології з’явились завдяки динамічному розвитку засобів телекомунікацій та Інтернету. Хмарні технології дозволяють надавати на комерційній основі широкому колу користувачів значні за обсягом обчислювальні потужності, ресурси пам’яті, а також програмне забезпечення. Можливість віддаленого доступу до таких ресурсів істотно підвищує рівень інформатизації в усіх сферах людської діяльності. Разом з тим, розвиток хмарних технологій породжує ряд проблем, одна з яких полягає в потенційній небезпеці надання ресурсів для вирішення завдань, пов'язаних із зломом протоколів криптографічного захисту. Таким чином, впровадження хмарних технологій об'єктивно знижує рівень захищеності існуючих протоколів, що вимагає адекватного підвищення рівня їх захищеності [1].

В основі більшості існуючих протоколів криптографічного захисту інформації лежать незворотні перетворення теорії чисел, базовою математичною операцією яких є модулярне експоненціювання, тобто обчислення $A^E \mathrm{mod} M$ [1]. Рівень захищеності цих протоколів повністю визначається розрядністю використовуваних в операції модулярного експоненціювання чисел.

На сьогодні в більшості протоколів використовується розрядність 2048 [2], очевидним шляхом підвищення рівня захищеності є збільшення розрядності до 4096 або 8192. Зростання розрядності має наслідком експоненційне зростання обчислювальної складності реалізації мережевих протоколів захисту інформації. Ця проблема стає особливо відчутною для малопотужних термінальних і мобільних пристроїв, що підтримують мережеві протоколи. Виконання на таких пристроях модулярного експоненціювання на розрядностях, більших за 2048, може призвести до порушення часових рамок роботи протоколу.

Виходячи з цього, актуальним стає завдання підвищення продуктивності операції модулярного експоненціювання на малопотужних термінальних і мобільних пристроях, що підтримують протоколи криптографічного захисту.

Постановка проблеми. Один з можливих варіантів вирішення цієї проблеми полягає в залученні для обчислення експоненти значних за обсягом обчислювальних ресурсів хмарних технологій. Необхідною умовою реалізації вказаної можливості є виключення можливості доступу до секретних елементів операції модулярного експоненціювання. Іншими словами, при обчисленні $A^E \mathrm{mod} M$ необхідно врахувати, що M є частиною відкритого ключа і, відповідно, може передаватися в явному вигляді, компонент E є секретним ключем, компонент A є секретними даними і, відповідно, їхня передача по мережі в явному вигляді має бути виключена. Тобто виникає задача організації віддаленого обчислення модулярної експоненти таким чином, щоб більша за обсягом частина обчислень виконувалася на віддалених обчислювальних потужностях і при цьому не передавалася інформація, яка дає змогу дістати доступ до значень секретних елементів операції – даних та коду експоненти.

Таким чином, наукова задача організації віддаленого обчислення модулярної експоненти, що виключає передачу секретних даних, є актуальною і важливою на сучасному етапі розвитку інформаційних технологій.

Аналіз останніх досліджень і публікацій. Проблемі захисту даних користувача в системах віддаленої обробки присвячено в останні роки значну кількість робіт. Основна проблема полягає в тому, що не існує єдиного підходу до захисту даних у процесі їх обробки. Фактично переважна частина виконаних досліджень вирішує проблему захисту даних тільки для окремих класів обчислювальних задач, наприклад, для лінійної алгебри, обробки зображень і т.п. [2].

Головна проблема, на вирішення якої направлені виконані дотепер дослідження, полягає у використанні спеціальних методів шифрування, які б дозволяли отримувати коректний результат шляхом дешифрування результатів віддаленої обробки зашифрованих даних. З наведеного слідує, що не існує універсальних методів шифрування даних перед їх віддаленою обробкою, які не залежать від операцій обробки сигналів. Це означає, що для кожного виду обробки сигналів слід окремо розробляти метод шифрування та дешифрування.

Фактично опубліковані до теперішнього часу дослідження можна підрозділити на два класи. До першого класу належать роботи, які для окремого класу задач вирішують задачу виключення можливостей доступу до даних, що обробляються віддалено на непідконтрольних обчислювальних потужностях.

Виділення недосліджених частин загальної проблеми. Розроблені дотепер методи захищеного обчислення модулярної експоненти дозволяють близько 70% обчислень реалізувати на віддалених обчислювальних потужностях, а близько 30% - на обчислювальній платформі користувача. Для підвищення ефективності захищених обчислень потрібно підвищити питому вагу обчислень, що виконуються на віддалених комп'ютерних системах.

Постановка завдання. Метою роботи є підвищення ефективності захищеного обчислення модулярної експоненти на віддалених обчислювальних потужностях за рахунок збільшення питомої ваги об'єму обчислень, що виконуються на них і, відповідно, зменшення долі обчислень, які реалізуються користувачем, що дозволяє зменшити час модулярного експоненціювання чисел, розрядність яких значно перевищує розрядність процесора, і тим самим, прискорити обчислювальну реалізацію протоколів криптографічного захисту інформації.

Викладення основного матеріалу. Організація адитивного маскування коду експоненти. В якості найпростішого методу організації захищеного обчислення модулярної експоненти можна використати розкладання коду експоненти на випадкові адитивні складові. Для цього код експоненти E пропонується спочатку трансформувати до вигляду:

$$y = a + b \quad (1)$$

Потім пропонується випадковим чином розділити отриманий код T на h адитивних складових:

$$\delta_0, \delta_1,...,\delta_{h-1}: \; T = \delta_0, + \delta_1 +... +\delta_{h-1}.y = a + b \quad (2)$$

Тоді, за умови, що код A не є секретним (наприклад, у викладених у першому розділі протоколах ідентифікації віддалених користувачів), процедура віддаленого обчислення може бути представлена у вигляді такої послідовності дій:

1. Користувач вибирає випадкове мале ξ та трансформує код експоненти E наступним чином $T=E- \xi$.

2. Користувач випадковим чином розділяє отриманий код T на h адитивних складових $\delta_0, \delta_1,...,\delta_{h-1}: \; T = \delta 0, + \delta 1 +... +\delta h-1$.

3. Користувач посилає в систему код A та набір $\delta_0, \delta_1,...,\delta_{h-1}$.

4. Система обчислює:

$$r_0 = A^{\delta_0} \bmod M\,,\; r_1 = A^{\delta_1} \bmod M\,,...,\; r_{h-1} = A^{\delta_{h-1}} \bmod M$$

5. Одночасно користувач обчислює $D = A\xi \; mod \; M$

6. Користувач отримує від системи обчислені значення $r_0, r_{1, \dots}, r_{h-1}$.

7. Користувач отримує результат у вигляді $R = (r0 \cdot r1, \cdot \dots \cdot, rh-1 \cdot D) \; mod \; M$.

В окремому випадку розкладення коду експоненти на адитивні складові може бути виконано у вигляді суміжних розрядів, що містять у собі, відповідно, $n_0, n_1,...,n_{h-1}$ двійкових розрядів так, що $n_0 + n_1 +...+n_{h-1} = n$. Група δ_0 включає в себе перші n_0 двійкові розряди коду експоненти $\delta_0 = \{e_0, e_1,...,e_{n_0-1}\}$, група δ_1 містить наступні n_1 розрядів: $\delta_1 = \{e_{n_0}, e_{n_0+1},...,e_{n_1-1}\}$; і так далі. Тоді розряди групи δ_0

утворюють число g_0, розряди групи δ_1 утворюють число g_1, розряди групи δ_{h-1} утворюють число g_{h-1}:

$$\forall l \in \{0,1,..., h-1\} : g_l = \sum_{j=0}^{n_l-1} e_{n_0+n_1+...+n_{l-1}+j} \cdot 2^j$$

Відповідно, код експоненти E може бути представлений у вигляді суми адитивних складових [22]:

$$E = g_0 + g_1 \cdot 2^{n_0} + g_2 \cdot 2^{n_0+n_1} + ... + g_{h-1} \cdot 2^{m-n_{h-1}} = \sum_{l=0}^{h-1} g_l \cdot 2^{\sum_{j=0}^{l-1} n_j}$$

Якщо увести позначення $w_0=1$, $w_1 = 2^{n_0}$, $w_2 = 2^{n_0+n_1}$,..., $w_{h-1} = 2^{n_0+n_1+n_2+...+n_{h-2}}$, то експонента E може бути представлена у більш компактному вигляді:

$$E = \sum_{l=0}^{h-1} g_l \cdot w_l$$

Відповідно, операція модулярного експоненціювання $A^E \ mod \ M$ може бути представлена у вигляді добутку:

$$A^E \bmod M = ((A^{g_0} \bmod M)^{w_0} \cdot (A^{g_1} \bmod M)^{w_1} \cdot ... \cdot (A^{g_{h-1}} \bmod M)^{w_{h-1}}) \bmod M =$$

$$= (\prod_{l=0}^{h-1} (A^{g_l} \bmod M)^{w_l} \bmod M) \bmod M$$

Кожен з цих добутків може обчислюватися віддалено, незалежно від іншого, на віддалених обчислювальних потужностях без пересилки їм секретних кодів A та E. Для цього пропонується наступна організація обчислення модулярної експоненти $A^E \ mod \ M$:

1) Користувач обчислює $R_0 = A^{g_0} \bmod M$, $R_1 = A^{g_1} \bmod M$,..., $R_{h-1} = A^{g_{h-1}} \bmod M$.

2) Обчислені значення $R_1,...,R_{h-1}$ і $w_1,...,w_{h-1}$ користувач відсилає в віддалену комп'ютерну систему.

3) Комп'ютерна система паралельно обчислює $D_1 = R_1^{w_1} \bmod M$, $D_2 = R_2^{w_2} \bmod M$ ..., $D_{h-1} = R_{h-1}^{w_{h-1}} \bmod M$, після цього обчислені значення повертаються користувачеві.

4) Користувач обчислює остаточний результат у такому вигляді: $A^E \bmod M = (R_0 \cdot \prod_{i=1}^{h-1} D_i \bmod M) \bmod M$.

Запропонована організація обчислення модулярної експоненти на віддалених комп'ютерних системах може бути проілюстрована таким прикладом для A, E і M малої розрядності.

Нехай модуль M=143, A=96. $E = 93_{10} = 1011101_2$. $A^E \ mod \ M = 96^{93} \bmod 143 = 83$. Нехай 7-розрядний код експоненти E ділиться на три фрагменти: 3-розрядний та два 2-розрядні: n_0= 3, n_1=2, n_2 = 2, δ_0={1,0,1}, δ_1={1,1}, δ_2={1,0}. Тоді g_0=5, g_1=3, g_2=2, w_0=1, $w_1 = 2^3$=8, $w_2 = 2^{3+2}$=32. $R_0 = 96^5 \bmod 143 = 109$, $R_1 = 96^3 \bmod 143 = 138$, $R_2 = 96^2 \bmod 143 = 64$.

Обчислені значення R_1=138, R_2=64, а також значення w_1= 8, w_2= 32, відсилаються у віддалену комп'ютерну систему. Там паралельно обчислюються

$D_1 = 138^8 \bmod 143 = 92$ та $D_2 = 64^{32} \bmod 143 = 92$, які повертаються користувачеві. Останній обчислює $A^E \bmod M = (R_0 \cdot D_1 \cdot D_2) \bmod M = (109 \cdot 92 \cdot 92) \bmod 143 = 83$.

При обчисленні модулярної експоненти $A^E \ mod \ M$ за класичним алгоритмом[4] виконується n кроків, на кожному з яких реалізується модулярне піднесення до квадрату та модулярне множення на A, якщо поточний двійковий розряд коду експоненти дорівнює одиниці. Відповідно, середня кількість N_0 операцій модулярного множення становить $N_0 = 1.5 \cdot n$.

Таким чином, при запропонованій організації обчислення модулярної експоненти кількість операцій модулярного множення, що виконуються користувачем, скорочується приблизно втричі. Це підтверджено експериментальними дослідженнями. Разом з тим, за кодами $R_0, R_1, \ldots, R_{h-1}$, що передаються у віддалену комп'ютерну систему, практично неможливо відновити секретні коди експоненти E та числа A.

Висновки. Доведено, що для маскування секретного коду А в процесі обчислень може бути використане лише мультиплікативне маскування, для якого доцільно використовувати постійне число. Це відкриває можливості для застосування передобчислень, що виконуються лише один раз. Теоретично показано, що для захисту коду експоненти Е найбільш доцільним є використання адитивного маскування, оскільки при застосуванні мультиплікативного маскування на порядки зростає складність обчислень.

Теоретично обґрунтована можливість вибору в якості маски спеціальних кодів, числове значення яких може бути визначено через функцію Ейлера за допомогою узагальнення Ейлера малої теореми Ферма для криптографічних алгоритмів, модуль яких утворюється як добуток двох простих чисел.

Список використаних джерел

1. Boroujerdi N. Cloud Computing: Changing Cogitation about Computing / N. Boroujerdi, S. Nazem. // IJCSI International Journal of Computer Science Issues, - Vol. 9, - Issue 4. -2012.- No 3.- PP. 169-180.

2. Xiaofeng Chen. New Algorithms for Secure Outsourcing of Modular Exponentiations / Xiaofeng Chen, Jin Li, Jianfeng Ma, Qiang Tang, Wenjing Lou // ESORICS 2012, LNCS 7459, - 2012.- PP. 541–556.

3. Can Xiang. Verifiable and Secure Outsourcing Schemes of Modular Exponentiations Using One Untrusted Cloud Server and Their Application. / Can Xiang // IACR Cryptology ePrint Archive 2014: PP.500.- https://eprint.iacr.org/2014/500.pdf

4. Костенко Ю. В. Метод защищенного модулярного экспоненцирования на удаленных компьютерных системах. / Ю.В. Костенко, А.П. Марковский, О.В. Русанова. // Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка. К.: ТОО „ВЕК+".- № 64.- 2016.- С. 51-54.

ДОВІДКА ПРО АВТОРІВ

Марковський Олександр Петрович – доцент, кандидат технічних наук, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Markovskyi Oleksandr – associate professor, candidate of engineering sciences, Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

E-mail: markovskyy@i.ua

O. P. Markovskyi ,
Van Huai,
H. V. Harasymovych

ORGANIZE MODULAR EXPONENTIATION SECURE COMPYTATIONBY USING ADDITIVE MASKING

Target setting. The natural way to restore cryptographic resilience of information security systems of this class in similar conditions is to increase the bit depth n of the numbers utilized. However, as mentioned above, increasing of bit depth significantly slows down calculations, related to information security functions. This situation may be overcome by using computing resources of cloud systems for modular exponentiation, in such a manner that that when calculating the A^E mod M, the secret exponent E code and the processed number A are not disclosed.

The principle difficulty in tackling this problem lies in the fact that there exists no general approach for guaranteeing data protection during processing. Methods for data protection depend heavily on the nature of the operations employed during processing. In other words, data security technologies require a homomorphic encryption procedure for the remote data encryption process [4]. For this reason, a number of different solutions for the secure remote implementation of solutions to problems of different categories, such as linear algebra or image processing have been proposed.

Consequently, amongst the targets of algorithms for the remote implementation of modular exponentiation should be the direct coordination of parallel solutions to this problem in systems with multiple processors.

The purpose of the present research is to develop a method for the secure implementation of the modular exponentiation operation in cloud systems, with the capability for parallelism.

As a result of the research proposed, a simple technological approach was proposed for exploiting cloud computing resources in order to increase the speed of calculations of the fundamental operation that is required for most data security protocols. This operation is modular exponentiation. The acceleration of the calculation is achieved by means of the transfer of a significant proportion of the complexity involved to computing resources available via the use of cloud technologies.

The method proposed involves the execution of part of the calculations on user equipment and another part in remote computational resources. During the cloud processing, the secrecy of both the data and the user key is preserved.

Itwasshownbymeansofboththeoreticalandpracticalcalculationsthatthevolumeofth eoperationsrequired to be performed by the users is reduced by approximately a factor of three times. This reduction results in a significant increase in the speed of implementation of cryptographic mechanisms, by use of the significant processing resources made available by the contemporary cloud resources.

The proposed method is oriented to user applications that operate on portable computing terminals with small processing power and connected to the internet.

Key words: modular exponentiation, cloud computing, cryptography, secure computations.