УДК 512.5

Олійник М. А.

DOI: https://doi.org/10.18523/2617-7080420213-6

ЗАСТОСУВАННЯ МЕДОВОГО ШИФРУВАННЯ ДО СХЕМИ ЦИФРОВОГО ПІДПИСУ ШНОРРА

Стійкість криптосистем значною мірою залежить від надійності захисту секретних ключів, які в них використовуються. Зокрема, процедура генерування останніх повинна повертати достатньо різноманітні ключі, щоб їх не можна було підібрати за допомогою атаки повного перебору (brute–force attack). Медове шифрування використовують як додатковий бар'єр захисту ключів криптосистем для сповільнення атаки повного перебору. Як і для «криптографії білої скриньки» (White box cryptography), існують різні схеми медового шифрування залежно від того, на що спрямовано додатковий захист. Потреба додатково захищати таємні ключі виникає у системах віддаленого доступу, у контексті надання доступу до інформації авторизованим користувачам.

У цій статті побудовано схеми додаткового захисту ключів системи цифрового підпису Шнорра, наведено псевдокод відповідних алгоритмів, проаналізовано складність атаки повним перебором.

Ключові слова: медове шифрування, стійкість, схема цифрового підпису Шнорра.

Вступ

Медове шифрування створює додатковий бар'єр для захисту від brute-force атаки (повного перебору), спрямованої на злам ключів, паролів, пін-кодів, номерів кредитних карток тощо.

Багато сучасних криптосистем використовують слабке шифрування, яке в основному базується на виборі користувачами певних паролів. Більшість користувачів обирають «бідні» (ненадійні) паролі, які досить легко підібрати методом brute-force атаки (тобто перебираючи всі можливі варіанти). Тому виникає потреба у додатковому захисті цих паролів.

З іншого боку, довжина пароля часто обмежена, а оскільки ключі шифрування генеруються за паролем, це також призводить до того, що методом брутальної атаки легше підібрати ключ.

Ідея шифрування, яке б забезпечило належний додатковий захист, полягає в побудові такої системи, щоб суперник не був здатен відновити початковий текст навіть після перебору всіх можливих варіантів паролів/ключів. Основана на концепції систем-приманок, вона видає на виході повідомлення, які важко відрізнити від правдивих. Такі повідомлення називають *медовими*, адже, подібно до солодкої маси, але в термінології комп'ютерної безпеки, вони «затягують» суперника у глухий кут.

Медове шифрування може бути використане для додаткового захисту не тільки паролів, але й ключів криптосистем. Часто ключі вибираються випадковим чином і можуть бути вразливими до повного перебору (як, наприклад, у випадку криптосистеми RSA, вибір пари простих чисел-«близнюків» в якості закритого ключа може привести до легкого розкриття системи). Безпека медового шифрування, способи його побудови і застосування розглянуті в роботах [2; 3; 5; 6].

Синтаксис і семантика медового шифрування аналогічні до симетричних криптосистем. Алгоритм шифрування, який за допомогою ключа і відкритого тексту утворює криптотекст, є випадковим. Дешифрування відновлює відкритий текст із криптотексту. Відмінність від звичайної симетричної криптосистеми полягає у тому, як медове шифрування поводить себе при дешифруванні, коли хтось намагається за допомогою неправильного ключа дешифрувати криптотекст. Замість того, щоб видати якийсь шум або помилку, дешифрування видасть відкритий текст, який виглядає правдоподібним.

У цій статті розглянуто схему цифрового підпису Шнорра, для якої описано схему медового шифрування для додаткового захисту ключа.

Загальна схема медової криптосистеми. Нехай $\mathcal{K}$ і $\mathcal{M}$ — множини ключів і повідомлень відповідно. Для загальності вважаємо, що $\mathcal{K}$ містить стрінги $\{0,1\}^*$ різної довжини. Медове шифрування складається з пари алгоритмів

$$(HEnc, HDec),$$

з яких перший є алгоритмом шифрування, а другий — дешифрування. Шифрування $HEnc$ приймає на вхід ключ $K \in \mathcal{K}$, повідомлення $M \in \mathcal{M}$, деякі однорідні випадкові біти, і виводить зашифрований текст C. Дешифрування $HDec$ приймає на вхід ключ $K \in \mathcal{K}$ і зашифрований текст C, і повертає повідомлення $M \in \mathcal{M}$.

Зазначимо, що дешифрування є успішним, якщо для всіх $M \in \mathcal{M}$ і $K \in \mathcal{K}$ ймовірність $P = [HDec_K(HEnc_K(M)) = M] = 1$.

Від звичайного процесу шифрування і дешифрування пари алгоритмів

$$(HEnc, HDec)$$

відрізняються тим, що у випадку введення зашифрованого тексту C не з множини криптотекстів алгоритм дешифрування видає не помилку, а деяке повідомлення M_1, відмінне від M, але дуже «подібне» до M. Скажімо, в [1] запропоноване медове шифрування для криптосистеми RSA, яке спрямоване на захист ключів. При дешифруванні неправильного повідомлення зловмисник отримає пару простих чисел, які не є ключами криптосистеми RSA. Цю ідею ми використаємо для побудови медового шифрування, спрямованого на захист криптосистеми Рабіна.

Надійність медового шифрування. Для того, щоб формалізувати поняття безпеки медового шифрування, використаємо поняття атаки відновлення повідомлень (message recovery attack). Наша мета полягає в тому, щоб, враховуючи шифрування повідомлення, ймовірність того, що будь-який супротивник відновить правильне повідомлення, була незначною. Але це можливо тільки тоді, коли як повідомлення, так і ключі мають високу ентропію. Тим не менш, ми можемо конкретно виміряти перевагу відновлення повідомлення будь-якого супротивника, і зробимо це, щоб показати, що зловмисники не можуть досягти більшої переваги, ніж $1/2^{\mu}$, де μ — мінімальна ентропія розподілу ключів p_k.

Визначимо успішність супротивника $\mathcal{A}$ проти схеми медового шифрування як

$$\mathbf{Adv}_{HE,p_m,p_k}(\mathcal{A}) = \\ = P[\text{зловмисник підібрав ключ при розподілах } p_m \ , p_k \ ],$$

де p_m —розподіл повідомлень на множині $\mathcal{M}$.

Схема цифрового підпису Шнорра

Розглянемо алгоритм цифрового підпису, що базується на схемі цифрового підпису Шнорра.

Припустимо, що учасниками процесу підписування є Аліса й Боб.

Генерування ключів. Виберемо велике просте число p таким чином, що в числа $p-1$ є великий простий дільник q. Далі виберемо таке число $h \neq 0$, для якого $h^q \equiv 1 \mod p$.

Аліса вибирає випадковим чином число $a, 1 \leq a \leq q-1$, і обчислює $v = (h^a)^{-1} \mod p$. Таким чином отримує ***відкритий ключ*** v і ***таємний ключ*** a, причому $h^a v \equiv 1 \mod p$.

Процес генерування підпису з боку Аліси можна описати послідовно такими діями:

1) вибір випадкового числа $r, 1 \leq r \leq q-1$;
2) обчислення $X = h^r \mod p$;
3) обчислення $s_1 = f(MX)$, де M — повідомлення, f — деяка хеш-функція, MX — результат конкатинації M і X;
4) обчислення $s_2 = (r + as_1) \mod q$;
5) створення пари $S = (s_1, s_2)$, де S — підпис.

Підтвердження підпису. Після отримання від Аліси повідомлення M і підпису $S = (s_1, s_2)$, Боб обчислює $Z = h^{s_2} v^{s_1} \mod p$ і перевіряє, чи справджується $s_1 = f(MZ)$.

Коректність протоколу доводиться таким чином:

$$Z = h^{s_2} v^{s_1} = h^{r+as_1+kq} v^{s_1} = \\ = h^r (h^q)^k (h^a v)^{s_1} \equiv h^r \mod p = X.$$

Застосування медового шифрування до схеми цифрового підпису Шнорра. Для ймовірнісної системи цифрового підпису, якою є схема Шнорра, необхідно надати додатковий захист щодо таємного ключа a, оскільки зберігання його у відкритому вигляді є ненадійним.

«Заховаємо» таємний ключ a в числовий набір $(p_1, ..., p_t)$.

Нехай $\mathbb{O}_q$ — множина цілих чисел у діапазоні від 1 до $q-1$.

Псевдокод, який описує алгоритм шифрування $Enc(a)$, має вигляд:

$(p_1, ..., p_t) \leftarrow \mathbb{O}_q^t$
For $i = 1$ to $t-1$ do
  If $IsPrime(p_i)$ then break
$p_t \leftarrow p_i \cdot a \mod q$
$return(p_1, ..., p_t)$.

Шифрування приймає на вхід ціле число a і генерує послідовність цілих чисел із проміжку $[1, q-1]$. Якщо серед $t-1$ чисел із цієї множини є хоча б одне просте, замінимо останнє число в послідовності на добуток цього простого і a. Якщо серед $t-1$ чисел із цієї множини простих немає, замінимо останнє число на добуток передостаннього і a.

Псевдокод, який описує алгоритм дешифрування $Dec(p_1, ..., p_t)$, має вигляд:

$i \leftarrow 1$
while $\neg IsPrime(p_i)$
  $i \leftarrow i + 1$
  If $i = t - 1$ then $a \leftarrow p_i^{-1} \cdot p_t$
$p \leftarrow p_i^{-1} \cdot p_t \mod q$
$return(a)$.

Дешифрування приймає на вхід вектор цілих чисел довжини t і повертає таємний ключ a. Якщо вектор введений зловмисником і не містить у собі замасковане число a, дешифрування повертатиме результат множення останнього числа на обернене по модулю q до першого простого числа, якщо таке існує в наборі, або передостаннього числа в наборі. Отже, при спробі штучно підібрати таємний ключ шляхом повного перебору зловмисник отримає число, подібне до a (а саме, якесь число з проміжку $[1, q-1]$), але яке він не зможе використати під час спроби підробки підпису Аліси.

Разом вищеописані шифрування та дешифрування складають схему **Schn–HE**.

Надійність медового шифрування, застосованого до схеми цифрового підпису Шнорра. Доведемо таку теорему.

Теорема 1. *Припустимо, що* **Schn–HE** *— це схема медового шифрування, застосованого до схеми цифрового підпису Шнорра. Тоді для довільного зловмисника* $\mathcal{A}$

$$\mathbf{Adv}_{HE}(\mathcal{A}) \leq \frac{1}{q-1}(1 - \frac{2}{3l})^{t-2},$$

де $q \in [2^{l-1}, 2^l)$.

Доведення. Скористаємось постулатом Бертнанда, тобто використаємо факт, що

$$\pi(2^l) - \pi(2^{l-1}) > \frac{2^{l-1}}{3l}$$

для всіх l, де l — таке число, для якого $q \in [2^{l-1}, 2^l)$. Тоді ймовірність вибрати просте число з інтервалу $[2^{l-1}, 2^l)$ буде $\frac{2}{3l}$. Для двох чисел з послідовності $(p_1, ..., p_t)$ вгадати, що $p_t = p_i \cdot a \mod q$, дорівнює $\frac{1}{q-1}$. Отже, ймовірність вгадати розв'язок, якщо жодне інше число не є простим,

$$(1 - \frac{2}{3l})^{t-2} \cdot \frac{1}{q-1}.$$

Оскільки при атаці повного перебору зловмисник перебирає всі можливі варіанти, і випадок, коли в наборі $(p_1, ..., p_t)$ тільки одне просте число, є найбільш сприятливим для нього, ймовірність вгадати розв'язок за усіх інших обставин буде меншою, тобто

$$\mathbf{Adv}_{HE}(\mathcal{A}) \leq \frac{1}{q-1}(1 - \frac{2}{3l})^{t-2} = g(t).$$

Оскільки функція $g(t)$ є незначною, ми вважаємо успіх зловмисника незначним.

Список літератури

1. Juels Ari, Ristenpart Thomas. Honey Encryption: Security Beyond the Brute-Force Bound. Nguyen P.Q., Oswald E. (eds.). *Advances in Cryptology — EUROCRYPT 2014. Lecture Notes in Computer Science,* vol 8441. Springer, Berlin, Heidelberg.
2. Joo-Im Kim, Ji Won Yoon. Honey chatting: a novel instant messanging system robust to eavedropping over communication. 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).
3. Jaeger Joseph, Ristenpart Thomas, Tang Qiang. Honey Encryption Beyond Recovery Security. *Advances in Cryptology – EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I,* pp.758–788.
4. Moriarty K., Kaliski B., Rusch A. (eds.). Password-Based Cryptography Specification. Internet Engineering Task Force, 2017.
5. Ji Won Yoon, Hyoungshick Kim, Hyun-Ju Jo, Hyelim Lee, Kwangsu Lee. Visual Honey encryption: Application to Steganography. *IH and MMSec 2015 - Proceedings of the 2015 ACM Workshop on Information Hiding and Multimedia Security.* Pp. 65–74.
6. Beunardeau Marc, Ferradi Houda, Geraud Remi, Naccache Gavid. Honey encryption for language. Cryptology ePrint Archive: Report 2017/031.
7. Shanks Daniel. Five Number-theoretic Algorithms. Proceedings of the Second Manitoba Conference on Numerical Mathematics. 1973. Pp. 51–70.
8. Вербіцький О.В. Вступ до криптології. ВНТЛ : Львів, 1998.

References

1. A. Juels and T. Ristenpart, Honey Encryption: Security Beyond the Brute-Force Bound, in: *Advances in Cryptology — EUROCRYPT 2014. Lecture Notes in Computer Science,* vol 8441, edited by P.Q. Nguyen, E. Oswald (Springer, Berlin, Heidelberg).
2. Joo-Im Kim and Ji Won Yoon, Honey chatting: a novel instant messanging system robust to eavedropping over communication. 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP).
3. Joseph Jaeger, Thomas Ristenpart and Qiang Tang, Honey Encryption Beyond Recovery Security, in: *Advances in Cryptology – EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I,* pp.758–788.

4. K. Moriarty, B. Kaliski, A. Rusch, editors, *Password-Based Cryptography Specification* (Internet Engineering Task Force, 2017).
5. Ji Won Yoon, Hyoungshick Kim, Hyun-Ju Jo, Hyelim Lee and Kwangsu Lee. Visual Honey encryption: Application to Steganography in: *IH and MMSec 2015 - Proceedings of the 2015 ACM Workshop on Information Hiding and Multimedia Security*, pp. 65–74.
6. Marc Beunardeau, Houda Ferradi, Remi Geraud and Gavid Naccache. *Honey encryption for language* (Cryptology ePrint Archive: Report 2017/031).
7. Daniel Shanks, *Five Number-theoretic Algorithms. Proceedings of the Second Manitoba Conference on Numerical Mathematics* (1973), pp. 51–70.
8. О.В. Вербіцький, *Вступ до криптології* (ВНТЛ: Львів, 1998).

M. Oliynyk

HONEY ENCRYPTION APPLIED TO SCHNORR SIGNATURE SCHEME

The security of any cryptosystem mostly depends on the reliability of the protection of secret keys used in it. In particular, key generation procedure must give a variety of keys so that they cannot be picked up by a brute-force attack. Honey encryption is used as an additional barrier of cryptosystems' keys protection to slow down a brute-force attack. As in the case of " white box cryptography", different honey encryption schemes are considered depending on what the additional protection is aimed at. The need to additionally protect secret keys arises in remote access systems, when it is necessary to provide access to information to authorized users.

The idea of encryption, which would provide adequate additional protection, is to build a system so that the attacker will not be able to recover the original text, even after searching through all possible options for passwords or keys. Based on the concept of lure systems, this system outputs messages that are difficult to distinguish from the true ones. Such messages are called it honey, which, like the sweet substance, but in computer security terminology, " drag " the opponent into a dead end.

This article constructs schemes for additional key protection of the Schnorr Signature Scheme, describes the pseudocodes of the corresponding algorithms, analyzes the complexity of a brute-force attack. This scheme requires additional protection against the a secret key because storing it in the open is unreliable. With the proposed encryption algorythm, we can "hide" a into a sequence of integers, and extract it back with the proposed decryption algorythm. If the sequence is entered by an attacker and does not contain a masked number a, decryption algorythm will return the result of multiplying the last number by the inverse q to the first prime number, if any, in the set, or the penultimate number in the set. Therefore, when trying to artificially pick up a secret key by a brute-force attack, the attacker will get a number similar to a but which he will not be able to use when trying to forge Alice's signature.

Keywords: honey encryption, security, Schnorr Signature Scheme.

Матеріал надійшов 07.10.2021