УДК 004.052.42

DOI: 10.18372/2073-4751.78.18955

Верба О.А., к.т.н.,
orcid.org/0000-0001-5752-5121,
e-mail: olverba@gmail.com,
Дайко І.В.,
e-mail: igordaiko1604@gmail.com

МЕТОД КРИПТОГРАФІЧНО СТРОГОЇ ІДЕНТИФІКАЦІЇ З БЛОКУВАННЯМ ПОВТОРНОГО ВИКОРИСТАННЯ ПАРОЛІВ

**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»**

Вступ

Поява перших комп'ютерних мереж започаткувала виникнення технологій віддаленої інформаційної взаємодії. Подальший прогрес технологій Інтернету надав процесам дистанційної взаємодії якісно нового рівня. Потужним імпульсом розширення їх використання в усіх сферах людської діяльності стало явище пандемії Ковід-19. Після його закінчення технологія віддаленої інформаційної взаємодії продовжує динамічно розвиватися.

Вагому роль в ефективності використання цієї технології відіграє забезпечення інформаційної безпеки віддаленої взаємодії. Ключовим елементом при цьому виступає достовірна ідентифікація учасників віддаленої взаємодії [1]. Сучасний етап розвитку технологій віддаленої інформаційної взаємодії характеризується рядом чинників, які вимагають адекватного вдосконалення методів ідентифікації.

Значною мірою розширення застосування технологій віддаленої інформаційної взаємодії відбувається за рахунок таких сфер, як банківська справа, дистанційне надання різноманітних послуг на комерційній основі, адміністративне управління. Специфіка цих застосувань потребує підвищеного рівня захисту від спроб отримання незаконної вигоди шляхом підміни легальних користувачів, тобто атак на засоби їх ідентифікації.

З іншого боку, високими темпами зростає кількість користувачів систем надання різноманітних послуг в реальному часі. Це вимагає прискорення процесів ідентифікації.

Наведені чинники зумовлюють актуальність вдосконалення механізмів ідентифікації віддалених користувачів як в ракурсі підвищення рівня захищеності, так і в плані прискорення відповідних комп'ютерних процедур.

Таким чином, наукова задача підвищення ефективності ідентифікації віддалених користувачів є актуальною та практично вагомою з огляду на особливості сучасного етапу розвитку комп'ютерних технологій.

Аналіз відомих методів криптографічно строгої ідентифікації.

Широкий спектр сучасних застосувань технології дистанційної інформаційної взаємодії зумовив велику кількість моделей, які їх описують. В рамках поточної роботи розглядається модель віддаленої взаємодії великої кількості користувачів з однією системою, яка надає їм певні послуги чи ресурси на комерційній основі. Вказана модель відповідає широкому коду практичних систем, таких, зокрема, як оператори мобільного зв'язку, інтернет-послуг, зосереджені бази даних та багато інших.

Характерними рисами ідентифікації в таких системах є її односторонній характер, а також те. що її швидкість практично повністю визначається часом реалізації відповідних процедур на боці системи [2]. Мета атак в таких системах полягає в отриманні незаконного доступу до ресурсів чи послуг, які вона надає користувачам. Об'єктами атак може виступати як канал обміну даними, так і пам'яті системи, я якій зберігається інформація, пов'язана з

ідентифікацію користувачів. Атаки на канал [3] можуть бути пасивними (перехоплення паролю легального користувача на центрах комутації мережі Інтернет) або активними, які зводяться з витісненню користувача з сеансу віддаленої взаємодії з системою. Цей тип атак отримав назву "*middle attacks*".

Методи ідентифікації традиційно поділяються на криптографічно слабкі, напівслабкі та криптографічно строгі [1]. Перші передбачають незмінний пароль, який зберігається в пам'яті системи. Відповідно, ідентифікація здійснюється щляхом простого порівняння отриманого від користувача паролю з тим, що зберігається в пам'яті. Очевидно, що така схема вразлива до всіх зазначених вище видів атак. В напівслабких схемах ідентифікації в пам'яті системи зберігається хеш-сигнатура пароля користувача і , відповідно, ідентифікація здійснюється через порівняння результату хеш-перетворення над отриманим від користувача паролем та хеш-сигнатурою, що зберігається в пам'яті. Це захищає від зовнішніх атак на пам'ять системи.

Найбільший рівень захисту забезпечує криптографічно строга ідентифікація, яка базується на теоретичній концепції "нульових знань" (*Zero Knowledge Identification*). Ця концепція має за основу дві умови [1]:

- користувач має у своєму розпорядженні криптографічний механізм генерації правильних сеансових паролів, які змінюються в кожному сеансі ідентифікації;
- система має в своєму розпорядженні криптографічний механізм, який надає змогу проводити перевірку правильності отриманих від користувача паролів, але не дозволяє системі самій генерувати правильні паролі.

Остання умова означає, що в системі не тільки не зберігається інформації, яка дає змогу генерувати правильні сеансові паролі, але й сама система не здатна імітувати надання послуг користувачу з застосуванням підробного правильного паролю. Вказана властивість дозволяє більш чітко регламентувати процедури віддаленого надання платних послуг та сервісів [4].

Для практичної реалізації теоретичної концепції "нульових знань" запропоновано низку методів, які можна розділити на два класи в залежності від виду незворотних перетворень на яких вони базуються. Переважна більшість методів криптографічно строгої ідентифікації які використовують незворотні перетворення булевої алгебри реалізують ідею пов'язаних між собою незворотними перетвореннями сеансових паролів, які утворюють ланцюжок. Фактично ці методи ідентифікації базуються на доведенні того, що користувач в новому сеансі той же самий, що працював з системою в рамках минулого сеансу взаємодії.

В найпростішому варіанті в якості незворотного перетворення використовується хеш-перетворення [5]. Користувач на етапі авторизації в системі генерує увесь список із m сеансових паролів: $P_m, P_{m-1},\ldots,P_1, P_0$. При цьому останній пароль P_m обирається випадковим чином, а всі інші формуються у вигляді: $\forall i \in \{0,1,\ldots,m\text{-}1\}$: $P_i = H(P_{i-1})$. В систему надсилається код P_0. Для ідентифікації абонента в першому сеансі дистанційної взаємодії він надсилає в систему код P_1. система виконує хеш-перетворення над отриманим сеансовим паролем: $S=H(P_1)$ та порівнює отриманий результат S з кодом P_0, що зберігається в системі: якщо вони співпадають, то ідентифікація вважається успішною і код P_0 в пам'яті системи замінюється на код отриманого паролю P_1. При подальших сеансах взаємодії з системою користувача, його ідентифікація виконується аналогічним чином. Після m сеансів проводиться нова авторизація абонента. Система, маючи в розпорядженні попередній пароль P_i не може, в силу незворотності стандартизованого хеш-перетворення, згенерувати правильний пароль P_{i+1}.

Крім хеш-перетворень, в якості незворотного перетворення запропоновано використання стандартизованих шифроблоків типу *DES* або *AES* [6]. Інший

варіант побудови незворотних перетворень в схемі ланцюжка паролів, а саме використання генераторів псевдовипадкових двійкових послідовностей запропоновано в роботі [7]. Таке рішення дозволяє не тільки реалізувати криптографічно строгу ідентифікацію віддаленого користувача але й здійснювати поточне шифрування даних обміну, що забезпечує ефективний захист від *middle attacks*.

Найбільш вагома перевага розглянутих методів криптографічно строгої ідентифікації на основі булевих незворотних перетворень полягає в високій швидкодії. Всі вони орієнтовані на використання стандартизованих засобів, що забезпечує можливість їх швидкої реалізації на криптопроцесорах. Іншою перевагою є автоматичне блокування повторного використання зловмисником правильного паролю, який потенційно може бути перехоплений.

Очевидними недоліками цих технологій криптографічно строгої ідентифікації виступають обмеженість числа m сеансових паролів, необхідність тривалого їх зберігання в пам'яті користувача, а також жорсткі вимоги до синхронізації процедур ідентифікації.

Вказані недоліки відсутні в методах ідентифікації, які реалізують криптографічну концепцію нульових знань з використанням незворотних перетворень теорії чисел. На практиці найбільшого поширення набули методи *FESIS* [8], *Guillou-Quisquater* [9] та *Schnorr* [10] .

Зокрема, в методі *Guillou-Quisquater* [9], користувач, на етапі авторизації обирає два простих числа p та q, добуток яких утворює модуль M: $M=q\cdot p$. Крім того, користувач обирає два числа D та u, після цього визначає значення W такого, що виконується умова: $W\cdot D^u \bmod M = 1$. Числа u та W надсилаються системі в якості відкритого ключа.

Процес ідентифікації полягає в тому, що абонент генерує випадкове число Y та обчислює першу компоненту сеансового паролю : $Q_1=Y^u \bmod M$; обчислене значення Q_1 надсилається системі, яка випадковим чином обирає $s < u$ та надсилає це число користувачеві. Останній, отримавши від системи число s, обчислює код другої компоненти сеансового паролю у вигляді: $Q_2 = Y\cdot D^s \bmod M$; обчислене значення Q_2 надсилається системі. Після отримання обох компонент коректного сеансового паролю віддалена система обчислює $R = Q_2^u\cdot W^s \bmod M$, обчислене значення порівнюється зі значенням першої компоненти сеансового паролю Q_1: якщо $R=Q_1$ то ідентифікація вважається успішною.

Розглянутий метод дозволяє використовувати практично необмежену кількість сеансових паролів і їх генерація здійснюється безпосередньо перед початком сеансу дистанційної взаємодії.

До недоліків методу можна віднести низьку швидкодію, зумовленою тим, що системі доводиться обчислювати модулярний добуток двох модулярних експонент $Q_2^u\cdot W^s \bmod M$ над числами великої розрядності.

Серйозним недоліком також є те, що і сама система і зовнішній зловмисник можуть повторно використати згенеровані користувачем паролі. Дійсно, система змозі першу компоненту $Q_{1,l}$ сеансового паролю користувача на l-тому сеансі зберегти в пам'яті, разом з числом s_l , яке надсилала йому, а також другу компоненту $Q_{2,l}$ сеансового паролю, яку на l-тому сеансі надсилав системі користувач. Ці дані можуть бути повторно використані системою для імітації звернення користувача в систему на h-тому сеансі; $h>l$. Подібним чином, зовнішній зловмисник, що має змогу прослуховувати канал обміну даними між системою та користувачем на l-тому сеансі їх віддаленої взаємодії, може запам'ятати коди $Q_{1,l}$, s_l, $Q_{2,l}$ і використати їх повторно для отримання доступу до ресурсів системи під виглядом легального користувача.

Аналогічні недоліки мають і інші відомі схеми криптографічно-строгої ідентифікації, що використовують незворотні перетворення теорії чисел.

Відомі також методи ідентифікації, що реалізують теоретичну концепцію

нульових знань з використанням незворотних перетворень на кінцевих полях Галуа $GF(2^n)$ [11, 12]. В силуц того, що обчислення на полях Галуа виконуються значно швидше, ці методи дозволяють на порядок прискорити ідентифікацію в порівнянні з відомими методами *FESIS* [8], *Guillou-Quisquater* [9] та *Schnorr* [10]. Проте, вони також не забезпечують захисту від повторного використання сеансового паролю системою для імітації надання користувачу послуг або зовнішнім зловмисником

Таким чином, проведений огляд відомих технологій реалізації криптографічно строгої ідентифікації показав, що для значної їх частини, зокрема тих, які використовують незворотні перетворення теорії чисел, недоліком є обмежений рівень захищеності, зумовлений можливістю для системи і зовнішнього зловмисника повторно використати сеансові паролі користувача.

Мета досліджень

Мета досліджень полягає в підвищенні ефективності криптографічно строгої ідентифікації за рахунок підвищення рівня захищеності шляхом блокування можливості повторного використання правильних сеансових паролів користувача, а також шляхом прискорення ідентифікації на боці системи.

Організація комбінованого використання незворотних перетворень модулярної арифметики та ланцюжка паролів

Для досягнення поставленої мети пропонується метод криптографічно строгої ідентифікації віддалених користувачів, оснований на комбіневаному використанні незворотних перетворень модулярної арифметики та утворення ланцюжка функціонально пов'язаних сеансових паролів.

Використання ланцюжка функціонально пов'язаних паролів дозволяє ефективно вирішити задачу блокування повторного їх використання зовнішнім зловмисником або самою системою.

Розроблений метод криптографічно строгої ідентифікації базується на комбінованому використанні стандартизованого хеш-перетворення $H(X)$ та операцій модулярного експоненціювання над числами, довжина n яких значно перевищує розрядність процесора. На практиці значення розрядності n чисел, що використовуються в методі становить не менше 4096. Хеш-перетворення $H(X)$ формує m-розрядний код хеш-сигнатури. Якщо в якості хеш-перетворення $H(X)$ використовується стандартизованого хеш-алгоритм *SHA*-256 [1], то m=256.

Запропонований метод включає в себе дві процедури: авторизацію віддаленого користувача в системі та його ідентифікацію на початку кожного сеансу віддаленої взаємодії.

Процедура авторизації віддаленого користувача включає в себе виконання наступної послідовності дій.

1. Користувач формує пару ключів: секретний $K_1 = < U,M >$ та відкритий $K_2 = < W, M >$. Розрядність модуля M і компоненти U секретного ключа K_1 дорівнює n, в той час, як довжина компоненти W відкритого ключа K_2 становить 3-4 біти. Формування ключів K_1 та K_2 здійснюється в такій послідовності:

1.1. Випадковим чином обирається просте ціле число W більше двох. Обране число W являє собою частину відкритого ключа K_2.

1.2. Обираються два простих числа p и q так, щоб раніше обране число W не було подільником чисел q-1 та p-1. Модуль M формується як добуток двох обраних простих чисел: $M = q \cdot p$.

1.3. Компонента U закритого ключа K_1 обирається як мультиплікативна інверсія W: $U=W^{-1}$ по модулю $(q\text{-}1)\cdot(p\text{-}1)$, тобто, таким чином, щоб $U \cdot D \bmod (q\text{-}1)\cdot(p\text{-}1) = 1$.

2. Користувач формує випадкове m-розрядне число Y, яке, як і секретний ключ K_1, зберігає в пам'яті.

3. Обране число Y та відкритий ключ K_2 користувач шифрує відкритим ключем системі і надсилає їй.

4. Система приймає від користувача коди Y та K_2, дешифрує їх своїм секретним ключем і зберігає в пам'яті.

Таким чином, після виконання описаної процедури авторизації на боці користувача зберігається закритий ключ $K_1 = < U,M >$ та m-розрядне число Y. На боці системи зберігається відкритий ключ $K_2 = < W,M >$ та число Y.

Ключовий момент описаної процедури генерації відкритого K_2 та закритого K_1 ключів схемі ідентифікації користувачем полягає в тому, що число u розрядів компоненти W на порядки менше за довжину модуля M, яка для практичних застосувань дорівнює або більша за 4096.

Робота запропонованої і описаної вище процедури авторизації користувача в системі може бути ілюстрована наступним прикладом.

Наприклад, в якості числа W може бути обрано 3-х розрядне число $5=101_2$. Тоді в якості двох простих чисел q та p, таких, що q-1 і p-1 не діляться на W=5 можуть бути обрані прості числа q=53 та p=59. Очевидно, що q-1=52 та p-1=58 не діляться на 5. Відповідно, модуль $M= q \cdot p = 53 \cdot 59 = 3127$, а довжина циклу експоненціювання при такому значенні модуля складає $(q\text{-}1)\cdot(p\text{-}1)= 52 \cdot 58 = 3016$. Мультиплікативна інверсія W^{-1} числа W=5 по модулю $(q\text{-}1)\cdot(p\text{-}1)$ дорівнює $U= W^{-1} \ mod \ 3016 = 2413$. Дійсно: $2413 \cdot 5 \ mod \ 3016 = 1$. Таким чином, сформований закритий ключ $K_1 = < 2413, 3127>$.

Процедура ідентифікації користувача перед початком кожного сеансу віддаленої взаємодії за запропонованим методом включає виконання наступної послідовності дій.

1. Користувач формує m-розрядне число X в результаті виконання хеш-перетворення над m-розрядним кодом Y: $X=H(Y)$. Отриманий код X зберігається в пам'яті користувача як число Y для використання в наступному сеансі ідентифікації: $Y = X$.

2. Користувач обчислює код сеансового паролю P з використання свого секретного ключа K_1 у вигляді: $P=X^U \ mod \ M$ і надсилає його системі.

3. Система, після отримання паролю P від користувача, з використання його відкритого ключа K_2 обчислює код $G=P^W \ mod \ M$.

4. Система виконує хеш-перетворення над збереженим в пам'яті m-розрядним кодом числа Y: $L=H(Y)$ і порівнює отриманий m-розрядний код L з обчисленим кодом G: якщо $L=G$, то ідентифікація вважається успішною: користувачу надається зумовлених його статусом права доступу до ресурсам системи, при цьому отриманий код G замінює в пам'яті системи код Y: $Y=G$.

Робота наведеної процедури ідентифікації може бути ілюстрована наступним прикладом. Нехай, на початку сеансу віддаленої взаємодії в пам'яті користувача зберігається число Y=23 та закритий ключ $K_1 = < 2413, 3127>$. В пам'яті системи також зберігається число Y=23 та відкритий ключ $K_2 = < 5, 3127>$.

На початку сеансу віддаленої взаємодії користувач, у відповідності з п.1 процедури, здійснює хеш-перетворення над числом Y=23. Якщо припустити, що $H(23)$=31, то обчислення значення X= 31. Це число користувач зберігає в змінній Y для наступного сеансу взаємодії з системою. Згідно п.2 процедури, користувач обчислює код сеансового паролю P з використання свого секретного ключа K_1 у вигляді: $P=X^U \ mod \ M = 31^{2413} \ mod \ 3127 = 692$ і надсилає його системі. В рамках виконання п.3 описаної процедури, система після отримання від користувача паролю P=692, обчислює значення $G=P^W \ mod \ M = 692^5 \ mod \ 3127 = 31$ з використанням компонентів W=5 і M=3127 відкритого ключа K_2. Згідно з п.4 процедури, система виконує хеш-перетворення над збереженим в пам'яті кодом числа Y=23 з отриманням числа L: $L=H(Y)=H(23)=31$.

Система порівнює отриманий в результаті перетворення код L=31 з обчисленим в рамках попереднього п.3 кодом G=31. Оскільки коди L та G збігаються, то ідентифікація вважається успішною. Код G=31 зберігається в пам'яті системи в комірці Y: $Y=G$=31.

Схема запропонованого методу криптографічно строгої ідентифікації з

комбінованим використанням незворотних перетворень модулярної арифметики з асиметричним об'ємом обчислень на хеш-перетвореннями показана на рис. 1.

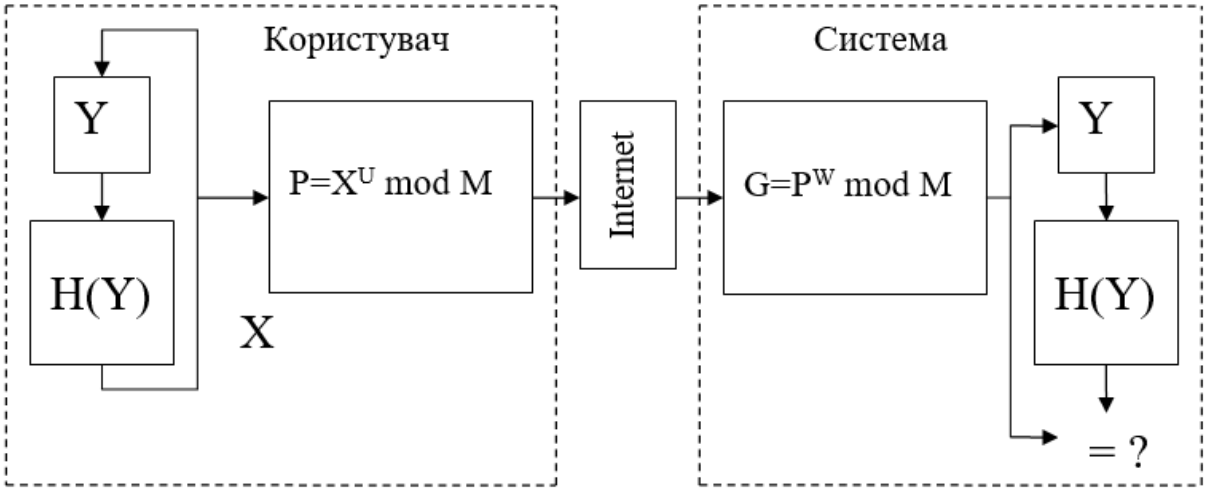

Рис. 1. Схема ідентифікації з комбінованим використанням асиметричної криптографії та ланцюжка сеансових паролі

Запропонований метод ідентифікації віддалених користувачів повною мірою задовольняє умовам криптографічної концепції "нульових знань". Дійсно,

Дійсно, користувач має криптографічний механізм формування правильних сеансових паролів у вигляді його обчислення як результату модулярного експоненціювання $P=X^U \bmod M$ з використанням секретної компоненти U. З іншого боку, система має у своєму розпорядженні спеціальний криптографічний механізм перевірки правильності паролів щляхом обчислення модулярної експоненти $G=P^W \bmod M$ над отриманим від користувача паролем з використанням компонентів W та M відкритого ключа K_2.

При цьому**,** система не здатна самостійно сформувати таке число S для якого виконується умова $S^W \bmod M = H(Y)$ в силу того, що вона на знає простих чисел, добуток яких утворює модуль, і, відповідно не знає довжини циклу модулярного експоненціювання.

Таким чином, запропонований метод ідентифікації віддалених користувачів задовольняє базовим умовам теоретикної концепції "нульових знань" і, відповідно, є криптографічно строгим.

Оцінка ефективності

Розробка направлена на підвищення ефективності криптографічно строгої ідентифікації за рахунок підвищення рівня захищеності та прискорення її обчислювальної реалізації на боці системи.

Підвищення рівня захищеності в порівнянні з відомими схемами криптографічно строгої ідентифікації досягається за рахунок виключення можливості повторного використання згенерованого користувачем правильного паролю.

В відомих методах криптографічно строгої ідентифікації, що базуються на незворотних перетвореннях теорії чисел, таких, зокрема як *FESIS* [8], *Guillou-Quisquater* [9] та *Schnorr* [10] існує небезпека того, що згенерований користувачем сеансовий пароль може бути перехоплено зловмисником і повторно використати для отримання незаконного доступу до ресурсів системи.

Для блокування повторного використання правильних паролів користувача в запропо нованому методі застосовується ланцюжок хеш-перетворень. Це означає, що послідовність кодів $X_1, X_2, \ldots$, які застосовуються користувачем для генерації правильних паролів в кожному із сеансів віддаленої взаємодії з системою, пов'язані між собою хеш-перетворенням: $\forall i \in \{2,3,..\}$: $X_i = H(X_{i-1})$; $X_1 = H(Y)$. Відповідно, якщо на i-тому сеансі віддаленої взаємодії користувач застосовував сеансовий пароль P_i, який генерувався

користувачем як $P_i = X_i^U \bmod M$, то система обчислювала $G = P_i^W \bmod M = X_i$. Отриманий код $G = X_i$ порівнювався з результатом хеш-перетворення попереднього X_{i-1}, тобто умовою успішності ідентифікації виступало виконання умови $X_i = H(X_{i-1})$.

Якщо зловмисник для незаконної ідентифікації під виглядом легального користувача, що здійснює ідентифікацію на j–тому сеансі надсилає системі раніше перехоплений пароль P_i, то система після отримання такого паролю обчислює $G = P_i^W \bmod M = X_i$. Проте в пам'яті системи на j-тому сеансі зберігається значення $Y = X_{j-1}$. Відповідно, система порівнює обчислене значення $G = X_i$ з результатом хеш-перетворення $Y = X_{j-1}$. Ймовірність, того, що два m-розрядні різні коди $X_{i-1} \neq X_{j-1}$ є колізуючими, тобто мають однаковий код хеш-перетворення $H(X)$: $H(X_{i-1}) = H(X_{j-1})$ становить 2^{-m}. Зокрема, якщо в якості хеш-перетворення використовується стандартизований хеш-алгоритм *SHA*-256, значення m=256 і ймовірність того, що $H(X_{i-1}) = H(X_{j-1})$ дорівнює $2^{-256} \approx 10^{-77}$. В практичному плані це означає, що $X_i \neq H(X_{j-1})$ і, відповідно, результат ідентифікація з застосуванням раніше використаного сеансового паролю є негативним. Таким чином, доведено, що запропонована схема криптографічно-строгої ідентифікації, на відміну від відомих, які базуються на незворотних перетвореннях теорії чисел, не дозволяє зловмиснику застосовувати раніше використані легальним користувачем сеансові паролі. Це має результатом підвищення рівня захищеності ідентифікації на основі теоретичної концепції “нульових знань”.

Ще одна вагома для практики перевага запропонованого методу криптографічно строгої ідентифікації в порівнянні з відомими схеми, що мають за основу незворотні перетворення теорії чисел, полягає в прискоренні ідентифікації на боці системи.

Підвищення швидкості криптографічно-строгої ідентифікації на боці системи дає змогу їй обслуговувати більшу кількість користувачів і зменшити час встановлення інформаційного контакту між системою та користувачами, що сприяє збільшенню рівня психологічного комфорту для останніх. Крім того, пришвидшення ідентифікації дозволяє більш ефективно здійснювати її повторні цикли для протидії *middle* атакам.

В запропонованому методі криптографічно строгої ідентифікації час її виконання на стороні системи визначається тривалістю T_1 обчислення модулярної експоненти $P^W \bmod M$. Чисельне значення T_1 за умови рівної ймовірності нулів і одиниць в коді експоненти W та використання класичного алгоритму модулярного експоненціювання становить $T_1 = 1.5 \cdot u \cdot t_m$, де u – розрядність коду експоненти W, а t_m – час виконання операції модулярного множення над n-розрядними числами. Особливість запропонованого методу, яка забезпечує прискорення ідентифікації на стороні системи, полягає в асиметрії довжини коду експоненти, що використовується на стороні системі і користувачем. Система обчислює модулярну експоненту малої розрядності $u << n$, в той час, як користувач здійснює модулярне експоненціювання при розрядності коду експоненти близької до n, тобто на чотири порядки більшої ніж система. Відповідно, тривалість обчислення модулярної експоненти на стороні системи і користувача відрізняються в n/u раз. Проте, час обчислення модулярної експоненти користувачем не є критичним для ідентифікації, тому, що система являє собою систему масового обслуговування (СМО) і, відповідно, її показники визначаються часом обслуговування системою запитів користувачів. Зокрема, в найпростішому випадку, середній час t_0 затримки заявки в системі масового обслуговування визначається як $t_0 = (\mu - \lambda)^{-1}$ [13], де μ – інтенсивність обслуговування системою, а λ – інтенсивність звернень користувачів до системи. Ссп співвідношення наведених інтенсивностей характеризує завантаженість ρ СМО: $\rho = \lambda/\mu$. Якщо час ідентифікації системою користувача зменшується в n/u раз, то коефіцієнт γ

прискорення ідентифікації з позицій теорії СМО визначається формулою:

$$\gamma = \frac{\mu\cdot\frac{n}{u}-\lambda}{\mu-\lambda} = \frac{\frac{n}{u}-\rho}{1-\rho} \approx \frac{n}{u\cdot(1-\rho)}. \qquad (1)$$

Наприклад, при типових для практики значеннях параметрів, що входять до формули (1): n=4096, u=4 та ρ = 0.6, коефіцієнт γ прискорення ідентифікації користувача з урахуванням того, що система являю собою СМО дорівнює γ = 2569.

Порівняння швидкодії запропоновано методу з відомими схемами криптографічно строгої ідентифікації також показує, що застосування асиметричної розрядності ключів дозволяє значно прискорити процес встановлення системою ідентичності віддаленого користувача. Зокрема, в схемі *Guillou-Quisquater* на боці системи обчислюється значення добутку двох експонент: $g = a^s \cdot v^e \bmod M$, де коди експонент s та e мають розрядність n. Відповідно, час T_S ідентифікації системою користувача в цій схемі визначається виразом: $T_S = 3\cdot n\cdot t_m$. Коефіцієнт β пришвидшення ідентифікації запропонованого методу в порівнянні з розглянутою схемою визначається формулою:

$$\beta = \frac{T_S}{T_1} = \frac{3\cdot n\cdot t_m}{1.5\cdot u\cdot t_m} = 2\cdot\frac{n}{u}. \qquad (2)$$

При типових для практики значеннях n=4096 та u=4 коефіцієнт β прискорення ідентифікації за запропонованим методом у порівнянні з відомою схемою криптографічно строгої ідентифікації *Guillou-Quisquater*, що базується на незворотних перетвореннях теорії чисел становить β = 2048.

При цьому не враховується, що в запропонованому методі здійснюється ще хеш-перетворення коду Y, що зберігається в пам'яті системи. Проте обчислювальна реалізація цього хеш-перетворення практично не впливає на швидкодію в силу того, що час його виконання на декілька порядків менший за час обчислення модулярної експоненти $G=P^W \bmod M$.

Дійсно, при використанні для реалізації хеш-перетворення стандартизованого хеш-алгоритму *SHA*-256 число процесорних операцій можна оцінити доволі просто. Хеш-алгоритм *SHA*-256 передбачає виконання 64 циклів на кожному із яких виконується 32 процесорні операції (6 операцій циклічних зсувів, 15 операцій арифметичного додавання та 11 логічних операцій). Тобто, для реалізації хеш-перетворення потрібно 2048 процесорних операцій.

Одна операція модулярного множення 4096-розрядних чисел при її реалізації на 32-розрядному процесорі з використанням редукції Монтгомері потребує 128^2 = 16384 процесорних множень, $2\cdot128^2+4096\cdot128 = 557056$ операцій процесорного додавання, $4096\cdot128 = 524288$ процесорних операцій логічного зсуву, що в сумі становить 1128728 процесорних операцій. Для обчислення модулярної експоненти $G=P^W \bmod M$ при u=4 середня кількість операцій модулярного множення становить $1.5\cdot4 = 6$, що в підсумку потребує $6\cdot1128728 = 6766368$ процесорних операцій. Це більш ніж в 3000 раз більше в порівнянні з реалізацією хеш-перетворення *SHA*-256.

Таким чином, наведений аналіз ефективності запропонованого методу криптографічно-строгої ідентифікації, що базується на комбінованому використанні незворотних перетворень теорії чисел та ланцюжка паролів, показав, що поставлена ціль досліджень досягнута. Метод виключає можливість повторного використання зловмисником перехопленого ним сеансового пароля легального користувача. Крім того, за рахунок асиметричної довжини відкритого та закритого ключів досягається значне (на 3 порядки) прискорення ідентифікації користувача системою.

Висновки

В результаті проведених досліджень, направлених на підвищення ефективності ідентифікації в рамках криптографічної концепції "нульових знань" за рахунок збільшення рівня захищеності та прискорення процесу підтвердження

ідентичності віддалених користувачів системою отримані такі результати.

Теоретично обґрунтовано та розроблено метод криптографічно строгої ідентифікації віддалених користувачів, який відрізняється тим, що для формування сеансових паролі використовуються коди, що утворюються ланцюжком хеш-перетворень, тобто кожен наступний сеансовий пароль пов'язаний з попереднім, за рахунок чого виключається можливість повторного використання зловмисником раніше надісланого легальним користувачем паролю. Це підвищує рівень захищеності ідентифікації.

Крім того, для прискорення процесу ідентифікації на боці системи, запропоновано обчислення модулярної експоненти з показником, довжина якого на порядки менша в порівнянні з тим, що використовується при модулярному експоненціюванні на боці користувача. Це дозволяє прискорити реалізацію криптографічно-строгої ідентифікації для широкого кола практичних застосувань, в яких система обслуговує велику кількість віддалених користувачів. Теоретично доведено і експериментально підтверджено, що для цих застосувань прискорення процесів ідентифікації практично визначається співвідношенням розрядностей кодів експоненти на боці користувача та системи.

Запропонований метод орієнтовано для підвищення ефективності криптографічно строгої ідентифікації великої кількості віддалених користувачів системами колективного доступу.

Література

1. Schneier B. Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd ed. New York : John Wiley & Sons, Inc., 1996. 784 p.

2. Han M. et al. Zero-knowledge identity authentication for internet of vehicles: Improvement and application. *PLoS ONE*. 2020. Vol. 15, no. 9. P.217–247.

3. Conti M., Dragoni N., Lesyk V. A Survey of Man in the Middle Attacks. *IEEE Communications Surveys and Tutorials*. 2016. Vol. 18, no. 3. P. 2027–2051. DOI: 10.1109/COMST.2016.2548426.

4. Васильєва М. Д., Дайко І. В., Саницький А. П. Метод швидкої ідентифікації віддалених абонентів на основі концепції нульових знань. *Наука і техніка сьогодні*. 2024. № 3(31). С. 791–803. DOI: 10.52058/2786-6025-2024-3(31)-791-804.

5. Lamport L. Password Authentication with Insecure Communication. *Communications of the ACM*. 1981. Vol. 24, no. 11. P. 770–772.

6. Bardis N., Doucas N., Markovskyi O. Zero-Knowledge Identification Method Based on Block Ciphers. *2017 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO)* : proceedings, Prague, Czech Republic, 20–22 May 2017 / IEEE. 2017. P. 307–311. DOI: 10.1109/ICCARO.2017.63.

7. Русанова О. В., Дайко І. В. Метод криптографічно строгої ідентифікації віддалених абонентів на базі генераторів псевдовипадкових послідовностей. *Проблеми управління та інформатизації*. 2023. № 1(77). С. 68–79. DOI: 10.18372 /2073-4751.76.18244.

8. Feige U., Fiat A., Shamir A. Zero knowledge proofs of identity. *Journal of Cryptology*. 1988. Vol. 1, no. 2. P. 77–94.

9. Method for Identification Subscribers and for Generating and Verifying Electronic Signatures in data Exchange System : patent no. 4995082 : H04K 1/00. No. 484127; filed 23.02.1990. published 19.02.1991.

10. Guillou L. C., Quisquater J. J. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory. *Lecture Notes in Computer Science. Vol. 330. Advances in Cryptology – EUROCRYPT '88. Workshop on the Theory and Application of Cryptographic Techniques, Davos, Switzerland, May 25-27, 1988. Proceedings* / ed. by G. Goos, J. Hartmanis. Berlin, 1988. P. 123–128.

11. Марковський О. П., Лефтеріс Захаріудакіс, Максимук В. Р. Використання алгебри полів Галуа для реалізації

концепції нульових знань при ідентифікації та автентифікації віддалених. *Електронне моделювання*. 2017. № 6. С.96–110.

12. Марковський О. П., Дайко І. В. Метод криптографічно строгої ідентифікації на основі незворотних перетворень на основі табличних перетворень на полях Галуа. *Адаптивні системи автоматичного управління*. 2024. Том. 1, № 44. С. 127–141. DOI: 10.20535/1560-8956.44.2024.302429.

13. Голоскоков О. Є., Голоскокова О. А., Мошко Є. О. Основи теорії експоненційних систем масового обслуговування : навч. посіб. Харків : НТУ "ХПІ", 2017. 312 с.

Верба О.А., Дайко І.В.

МЕТОД КРИПТОГРАФІЧНО СТРОГОЇ ІДЕНТИФІКАЦІЇ З БЛОКУВАННЯМ ПОВТОРНОГО ВИКОРИСТАННЯ ПАРОЛІВ

Теоретично обґрунтовано та розроблено метод криптографічно строгої ідентифікації віддалених користувачів з комбінованим використанням незворотних перетворень модулярної алгебри та функціонально пов'язаних сеансових паролів, за рахунок чого виключається можливість їх повторного використання зловмисником.

Крім того, для прискорення процесу ідентифікації на боці системи, запропоновано використання асиметричних за обсягом обчислень незворотних перетвореннях модулярної алгебри. Наведено математичне обґрунтування запропонованого методу та числові приклади, які ілюструють його роботу.

Теоретично та експериментально доведено, що запропонований метод дозволяє блокувати повторне використання паролів користувача, в також на 2-3 порядки прискорити процес його ідентифікації на боці системи.

***Ключові слова**: ідентифікація на основі концепції нульових знань; криптографічно строга ідентифікація; криптографічні алгоритми на основі незворотних перетворень модулярної алгебри; ланцюжки пов'язаних паролів.*

Verba O.A., Daiko I.V.

METHOD FOR CRYPTOGRAPHICALLY STRICT IDENTIFICATION WITH PASSWORD REUSE BLOCKING

A method for cryptographically strict identification of remote users with the combined use of irreversible transformations of modular arithmetic and functionally interconnected session passwords is theoretically justified and developed, which eliminates the possibility of their reuse by an attacker.

In addition, to speed up the identification process on the system side, it is proposed to use irreversible transformations of modular algebra that are asymmetric in the volume of calculations.

A mathematical justification for the proposed method and numerical examples that illustrate its operation are given. It has been theoretically and experimentally proven that the proposed method makes it possible to block the reuse of user passwords, as well as speed up the process of identification by the system by 2-3 orders of magnitude.

***Keywords**: Zero Knowledge identification; cryptographically strong identification; identification based on irreversible transformations of modular arithmetic; chains of related passwords.*