УДК 004.056.55

ПОРІВНЯЛЬНИЙ АНАЛІЗ БІОМЕТРИЧНИХ КРИПТОСИСТЕМ

М. С. ЛУЦЕНКО, О. О. КУЗНЕЦОВ, Д. І. ПРОКОПОВИЧ-ТКАЧЕНКО, В. П. ЗВЄРЄВ, А. О. УВАРОВА

Досліджуються існуючі біометричні криптографічні системи, які призначено, зокрема для формування надійних та безпечних псевдовипадкових послідовностей (т. з. криптографічних ключів, паролів, кодів доступу тощо). Проводиться порівняльний аналіз різних видів біометричних криптосистем (зі звільненням ключа; зі зв'язуванням ключа; з генерацією ключа), визначаються їх переваги та недоліки. Наводяться конкретні схеми та обчислювальні алгоритми використання біометричних образів для формування криптографічних ключів, обґрунтовуються перспективні напрямки подальших досліджень.

Ключові слова: біометричні образи, кодові криптосистеми, генерація криптографічних ключів.

ВСТУП

З розповсюдженням інформації через Інтернет та необхідністю збереження конфіденційних даних у відкритих мережах створення надійної інформаційної системи постає важливою та актуальною науковою задачею [1–3].

Наразі існує досить багато доказово стійких криптографічних алгоритмів, які можуть бути використані в різних інформаційних системах [3]. Однак, слід зауважити, що зазвичай досить велику роль в безпеці системи відіграють криптографічні ключі (паролі, коди доступу, тощо) які використовуються для ініціації інших криптопримітивів та для організації первинного доступу до приватної інформації. Запам’ятати криптографічно сильний ключ користувачеві фізично неможливо або вкрай складно, саме тому надійність системи часто залежить від простого для запам’ятовування користувачем секретного слова (пароля). Очевидно, що такий підхід має потенційні ризики для безпеки інформаційної системи [1–3].

Біометрична автентифікація дозволяє реалізувати механізм захисту ключових даних, використовуючи унікальні біометричні ознаки користувача [4–12]. Наразі вже розроблено кілька варіантів побудови таких систем. Наприклад, коли користувач хоче отримати доступ до захищеного ключа, йому може бути запропоновано надати відповідний біометричний зразок. Якщо цей зразок пройде верифікацію, тоді криптографічний ключ буде можливо використати [4].

Таким чином, біометрична автентифікація може замінити або вдосконалити використання кодів доступу, секретних ключів, паролів, тощо. Це забезпечує зручність, оскільки більше не потрібно запам'ятовувати чи зберігати в надійному середовищі криптостійку псевдовипадкову послідовність. До того ж, біометричні дані можуть стати повною заміною криптографічним ключам шляхом формування стійких та надійних псевдовипадкових послідовностей [9, 10, 12]. Ці ключі можуть бути використані в різноманітних програмах, включаючи доступ до віртуальних приватних мереж, шифрування файлів та автентифікації користувачів.

Слід відмітити, що біометричні системи також мають певні недоліки з практичного застосування [5, 6]. Зокрема, за результатом проведеного аналізу встановлено, що біометрична криптографія потенційно вразлива до таких поширених атак [1–4]:

– атака підміною (англ. Spoofing attack). Було продемонстровано, що іноді біометричну систему можна обманювати, застосовуючи підроблені біометричні образи;

– атака заміни (англ. Substitution Attack): біометричний шаблон повинен зберігатися для підтвердження користувача. Якщо зловмисник отримує доступ до сховища, локально або віддалено, він може перезаписати шаблон легітимного користувача;

– атака маскарад (англ. Masquerade Attack). Цифровий образ може бути створений з шаблону біометричного образу. Ця атака створює реальну загрозу для систем віддаленої автентифікації;

– атака найближчого самозванця (англ. Nearest Impostor Attack). Ця атака стосується систем, у яких використовуються шаблони. У цій атаці використовується велика множина різних біометричних шаблонів для викриття секретних даних з високою ймовірністю;

– недостатня точність багатьох біометричних систем, як з точки зору фальшивого відхилення (англ. False Reject Rate), так за оцінкою частоти помилок (англ. False Accept Rate). Високий рівень FRR створює незручності для законних користувачів і спонукає знизити поріг перевірки. Це неминуче призводить до FAR, що, в свою чергу, знижує рівень безпеки системи.

Залежно від мети застосування біометрії в криптографії виділяються кілька видів біометричних криптографічних систем [4–6]. Їхню загальну класифікацію за результатами проведеного аналізу зображено на рис. 1:

– системи зі звільненням ключа (англ. Key Release Cryptosystems);

– системи зі зв'язуванням ключа (англ. Key Binding Cryptosystems);

– системи з генерацією ключа (англ. Key Generation Cryptosystems).

Метою цієї статті є аналіз та порівняльні дослідження біометричних криптографічних систем, об-

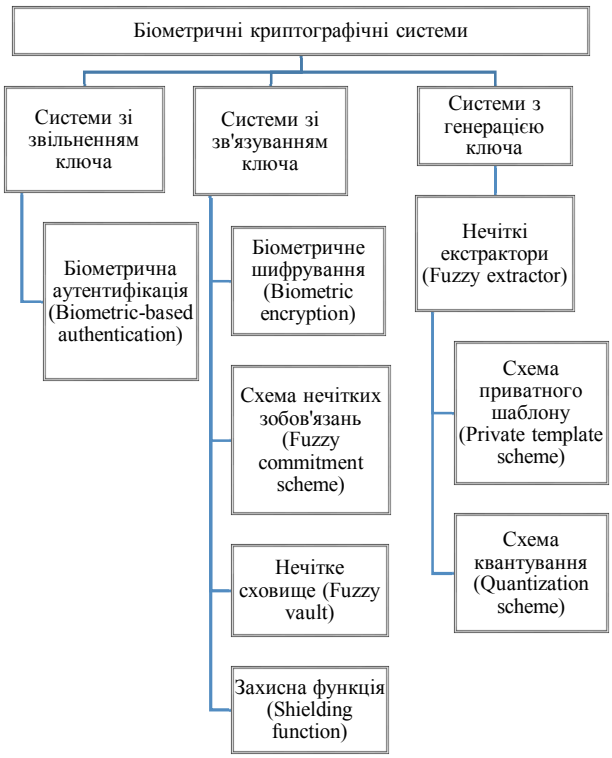

Рис. 1. Види та підвиди біометричних криптографічних систем

ґрунтування перспективних напрямків їхнього розвитку та можливого застосування.

2. БІОМЕТРИЧНІ КРИПТОСИСТЕМИ ЗІ ЗВІЛЬНЕННЯМ КЛЮЧА

У режимі звільнення ключа біометрична автентифікація здійснюється незалежно від механізму звільнення ключа, біометричний еталон і ключ зберігаються окремо один від одного, сам ключ звільняється після успішної біометричної автентифікації [4–6]. Схематичне зображення такої біометричної криптографічної системи наведено на рис. 2.

Рис. 2. Схематичне зображення біометричної криптографічної системи зі звільненням ключа

Отже, біометрична автентифікація відокремлена від криптографічної частини системи. В такому випадку, як пароль від ключа використовуються результати порівняння отриманого біометричного зображення з шаблоном. Даний вид біометричних криптосистем непридатний у більшості випадків, оскільки існує можливість заміни модуля порівняння під час виконання автентифікації. Цей метод буде добре працювати в додатках фізичного доступу, де біометричні шаблони та ключі можуть зберігатися в безпечному місці, фізично відокремленому від пристрою захоплення біометричних зображень.

3. БІОМЕТРИЧНІ КРИПТОСИСТЕМИ ЗІ ЗВ'ЯЗУВАННЯМ КЛЮЧА

У криптографічних системах такого типу ключ і біометричний еталон криптографічно пов'язані між собою [4–7]. Ключ за певним алгоритмом пов’язується з біометричним еталоном користувача і зберігається в такому вигляді в базі даних, відповідно розкрити ключ представляється можливим тільки власникові біометричних параметрів. У таких системах передбачається, проте не є необхідним, використання допоміжних даних (англ. Helper Data), для демаскування зашумлених біометричних даних. Схематично приклад біометричних систем зі зв’язуванням ключа подано на рис. 3.

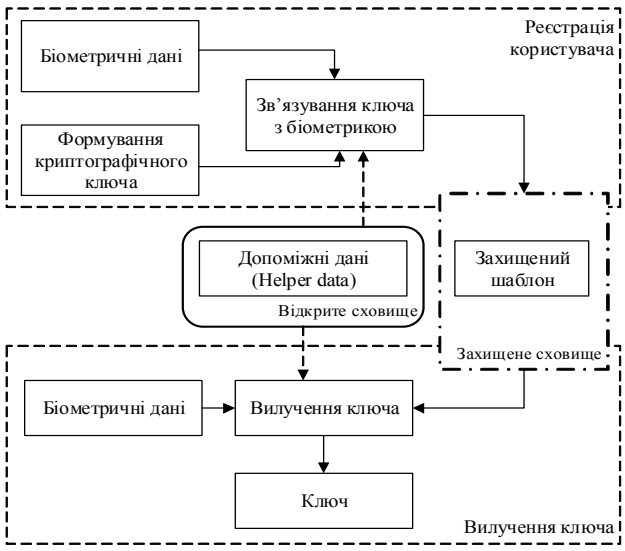

Рис. 3. Схематичне зображення біометричної криптографічної системи зі зв'язуванням ключа

Цей спосіб включає приховування криптографічного ключа в самому біометричному шаблоні реєстрації за допомогою надійного (секретного) алгоритму бітової заміни. Після успішної автентифікації користувачем цей довірений алгоритм просто витягає біти ключа, після цього ключ придатний для користування. На жаль, це означає, що криптографічний ключ буде вилучено з того ж розташування в шаблоні щоразу, коли інший користувач автентифікується системою. Таким чином, якщо зловмисник міг визначити бітові розташування, які вказують ключ, то зловмисник може

відновити вбудований ключ із будь-якого шаблону інших користувачів. Якщо зловмисник мав доступ до системи, то він міг визначити місця розташування ключа, наприклад, додаючи кількох людей у систему, використовуючи однакові ключі для кожної реєстрації. В такому випадку, злочинцю потрібно лише знайти ці місця розташування біт з загальною інформацією в шаблонах.

3.1 Біометричне шифрування

Біометричне шифрування є процесом, який надійно пов'язує криптографічний ключ з біометричним, тому що ні ключ, ні біометричні дані не можуть бути вилучені зі збереженого шаблону [7]. Криптографічний ключ генерується випадковим чином при реєстрації так, що ніхто, включаючи користувача, не знає його. Сам ключ повністю незалежний від біометрії і, отже, завжди може бути змінений або оновлений. Після отримання біометричного зразка створюється захищений шаблон, так званий «приватний шаблон» (англ. private template). По суті, криптографічний ключ шифрується за допомогою біометричного. Під час перевірки користувач представляє свій біометричний зразок, який в ході застосування до легітимного шаблоном дозволить отримати той самий ключ. Ключ відтворюється тільки в тому випадку, якщо під час перевірки представлений правильний біометричний зразок. Таким чином, біометрія служить ключем дешифрування Алгоритм розроблений так, що незначна розбіжність отриманих біометричних образів від однієї особи не впливає на коректну роботу алгоритму.

Підходи, засновані на біометричному шифруванні, чутливі до атаки змішаної заміни, атаки сходження і атаки найближчого самозванця. Більш того, зловмисник може використовувати відновлений секрет для вилучення оригінальних біометричних даних з захищених шаблонів.

Mytec1 був першою реалізацією такої біокріптографічної схеми. Пізніше Mytec2 був розроблений для забезпечення більш складного захисту шаблону відбитка пальця, що зберігається. Схематичне зображення біометричної криптографічної системи наведено на рис. 4.

3.2 Схема нечітких зобов’язань

Схема нечітких зобов'язань [8] є криптографічним алгоритмом, який забезпечує збереження біометричних даних за допомогою методів криптографії та кодування з виправленням помилок. Алгоритм пов'язує секретну інформацію з даними, щоб приховати дані і не дозволити власникові даних розкрити її більш ніж одним способом. Нечіткі схеми зобов'язань використовувалися для збереження біометричних шаблонів. Ця схема, що застосовується до біометричних шаблонів, розглядає сам шаблон без будь-якої модифікації як пошкоджене кодове слово, яке підлягає декодуванню. У таких системах для формування шаблону та вилучення даних використовується так званий свідок (або ключ шифрування). Також вважається, що для коректного функціонування алгоритму свідок може мати схожі, проте не ідентичні метрики.

Схематичне зображення біометричної криптографічної системи наведено на рис. 5.

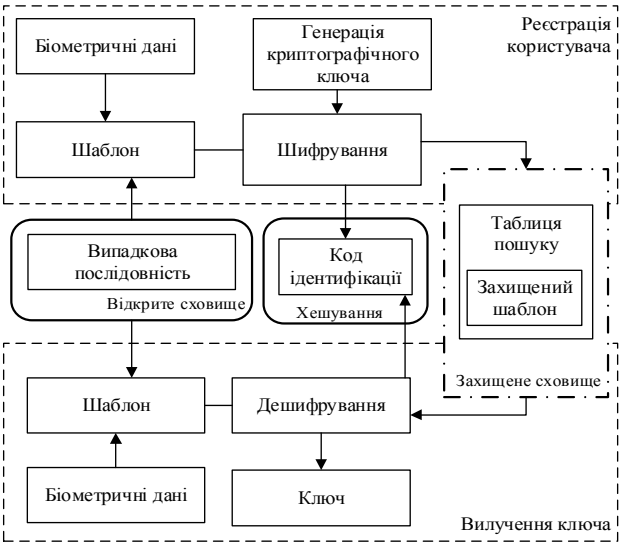

Рис. 4. Схематичне зображення біометричної криптографічної системи зі зв'язуванням ключа: біометричне шифрування

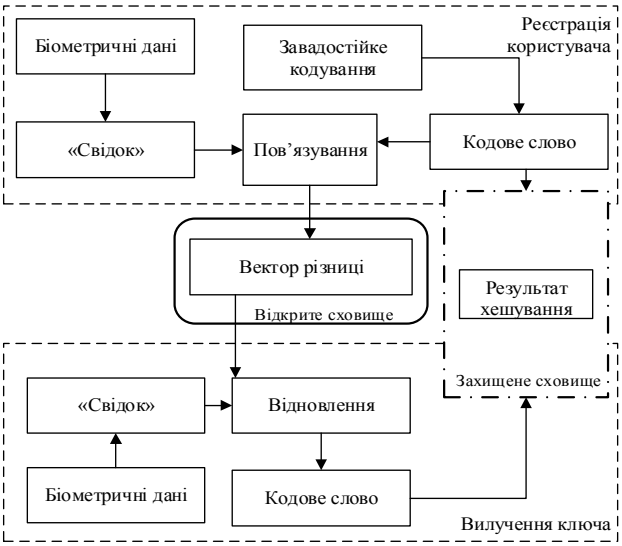

Рис. 5. Схематичне зображення біометричної криптографічної системи зі зв'язуванням ключа: схема нечітких зобов’язань

Основною слабкістю схеми нечітких зобов'язань є сприйнятливість до атак у середовищах, які залучають довірену третю сторону. Схеми нечітких зобов'язань з максимальним розміром ключів забезпечують оптимальну продуктивність для абсолютно безсистемного випадку. Також було виявлено, що нечіткі схеми зобов'язань забезпечують обмежену безпеку секретного ключа та біометричних даних у загальних випадках без пам'яті та у стаціонарних ергодичних випадках. Нечіткі схеми зобов'язань також сприйнятливі до атаки грубою силою. Атаки через множинність записів також

можуть бути використані для декодування захищених біометричних даних.

3.3 Нечіткі сховища

У своїй роботі Арі Джуэлс і Мадху Судан в 2002 році описали нову конструкцію, яку вони назвали нечітким сховищем (англ. Fuzzy vault) [9]. Узагальнено основну ідею, можна описати так. Нехай Аліса помістить деяке секретне значення k у нечітке сховище та «заблокує» його, використовуючи набір (підмножину) елементів з деякої відкритої універсальної множини A. Якщо Боб спробує «розблокувати» таке сховище, використовуючи набір B елементів (потужності підмножини A та B співпадають), то він удачно отримає секретне значення лише у випадку, якщо B подібно A. Тобто тільки, якщо A та B значною мірою є множинами, що перетинаються. Відмінною особливістю цього алгоритму за думкою авторів є те, що ця схема володіє інваріантністю порядку значень в наборах, вважається, що упорядкування підмножин A та B не впливає на роботу схеми. У такому випадку схема має доказану криптографічну стійкість до обчислювальних атак типу груба сила. Схематичне зображення біометричної криптографічної системи наведено на рис. 6.

Рис. 6. Схематичне зображення біометричної криптографічної системи зі зв'язуванням ключа: схема нечітких сховищ

Розглянемо основні принципи схеми нечіткого сховища на прикладі. Нехай Аліса – любитель кіно. Вона шукає того, хто розділяє її інтереси, але не хоче розкривати інформацію про свої уподобання всім людям. Один з підходів, який вона може зробити, полягає в тому, щоб створити набір її улюблених фільмів і опублікувати його в прихованій формі. Наприклад, Аліса може опублікувати зашифрований текст C_A, який представляє її зашифрований на наборі (в даному випадку, ключі) A телефонний номер tel_A. В цьому випадку, якщо інша людина, скажімо, Боб, склав свій список улюблених фільмів B, і якщо вони ідентичні A, він зможе розшифрувати C_A і отримати телефонний номер tel_A Аліси. Якщо ж Боб спробує розшифрувати C_A за допомогою множини даних, що відрізняються від множини інтересів Аліси, він не зможе отримати її номер телефону. Недоліком цього підходу є його точність у визначенні подібності двох множин або відсутність допущення помилок. Якщо інтереси Боба дуже схожі на інтереси Аліси, наприклад, якщо йому подобаються кілька фільмів, які Аліса не любить, то він не дізнається її телефон. Цілком ймовірно, що в цьому випадку Аліса все одно хотіла б, щоб Боб отримав її номер телефону, оскільки їх смаки дуже схожі. Автори ж пропонують поняття нечіткого сховища. Це криптографічна конструкція, відповідно до якої Аліса може заблокувати свій номер телефону tel_A, використовуючи набір даних A, помістивши його в сховище, позначене V_A. Якщо Боб намагатиметься розблокувати сховище V_A, використовуючи свій власний набір, йому це вдасться, якщо множини A та B значно перетинаються. З іншого боку, будь-який, хто намагатиметься розблокувати сховище V_A за множиною даних, що істотно відрізняються від набору Аліси, зазнає невдачі. Таким чином, нечітке сховище можна розглядати як схему перевірки помилок, у якій ключі складаються з наборів.

На думку авторів, їхня система може знайти застосування системах, в яких безпека залежить від людських чинників. Наприклад, нечіткі сховища можуть знайти застосування:

Для захисту конфіденційних даних. У такому випадку, схема може використовуватися для кола людей (наприклад, сім'ї), що володіють деякими схожими параметрами, щоб зберегти деякі дані в таємниці.

Для відновлення пароля або інших даних. Зараз поширена практика, що для відновлення пароля при реєстрації в системі користувач вигадує відповіді на деякі стандартні запитання, потім в разі відновлення пароля йому необхідно дати відповіді на ці запитання, тобто сформувати деякий набір даних, які ідентифікують системі цього користувача. Оскільки дана схема може бути застосована до набору даних, то можливо її використання для відновлення пароля користувача навіть з урахуванням того, що користувач міг дати неправильні відповіді на кілька запитань.

Біометрія. Нечіткі сховища можна застосовувати щодо біометричних зразків. Наприклад, як ключ шифрування. Аліса могла б зберігати пароль, заблокований в нечіткому сховище і зашифрований на її наборі даних отриманих з її біометричного зразка, наприклад, відбит-ка пальця, тим самим забезпечуючи стійкість системи до помилок і конфіденційність, даних що зберігаються в системі.

3.4 Захисна функція

Захисна функція або схема допоміжних даних була розроблена для забезпечення безпеки збережених

біометричних даних і гарантування конфіденційності законних користувачів [4–7]. Цей підхід дозволяє системі автентифікації перевіряти ідентичність користувача без будь-яких знань про біометричні дані користувача. Дельта-договірні і епсілон-виявляючі функції забезпечують основу цієї схеми. Функція дельта-контрактування пов'язує таємницю з біометричними даними, а функція епсилон-виявлення гарантує, що захищений шаблон відкриває лише невелику кількість інформації про випадкові та біометричні дані.

Захисна функція не стійка до атак типу спуфінг та атак грубою силою. Попередні реалізації схем такого типу виробляють ключі, які менше 50 біт. Це не відповідає мінімальним вимогам для біометричних ключів. Також такі системи сприйнятливі до атак з використанням кратності записів і перехресного нападу. Більш того, зловмисник може використовувати реконструйований секрет для отримання оригінальних біометричних даних з компрометованих допоміжних даних.

Схематичне зображення біометричної криптографічної системи наведено на рис. 7.

Рис. 7. Схематичне зображення біометричної криптографічної системи зі зв'язуванням ключа: схема захисної функції

3.5 Порівняльний аналіз біометричних криптографічних систем зі зв'язуванням ключа

Порівняння переваг та недоліків біометричних криптографічних систем зі зв'язуванням ключа наведено у Таблиці 1.

4. БІОМЕТРИЧНІ КРИПТОСИСТЕМИ З ГЕНЕРАЦІЄЮ КЛЮЧА

У такій біометричній криптосистемі ключ формується безпосередньо з біометричних даних користувача і не зберігається в базі даних [4–7, 10]. Дослідник Бодо запропонував такий метод у німецькому патенті. Цей патент передбачає, що дані, отримані з біометричних образів (по суті, біометричного шаблону), використовуються безпосередньо як криптографічний ключ.

Таблиця 1

Порівняльний аналіз біометричних криптографічних систем зі зв'язуванням ключа

	Переваги	Недоліки
Схема біометричного шифрування	1) Застосовує стандартний криптографічний алгоритм для створення безпечного біометричного шаблону 2) Зловмисник не має можливості розшифрувати захищені шаблони без знання алгоритму і криптографічного ключа	1) Існує можливість використання реконструйованого секрету для отримання оригінальних біометричних даних із захищеного шаблону 2) Не стійкі до атак змішаної заміни, атак сходження (атака маскарад) і атак найближчого самозванця, атак множинного запису
Схема нечітких зобов'язань	"Зобов'язання", отримані з біометричних даних і секретного ключа, захищають біометричний шаблон. Також секретний ключ захищений завдяки тому, що зберігається лише його хеш-значення	1) Вразливі перед усіма відомими атаками на завадостійке кодування (залежить від обраного алгоритму кодування) 2) Не стійкі до атак сходження, атак грубою силою, атак декодування та перехресних атак
Схема нечіткого сховища	Сховище не може бути декодовано без біометричних даних, які мають майже ідентичні характеристики з первинними	1) Сприйнятливі до атак грубою силою та колізій 2) Вразливі до атак вторгнень, атак зв'язків, комбінованих та ін'єкційних атак
Схема захисної функції	1) Допоміжні дані та хеш-функції захищають від відтворення біометричні дані та випадкові секрети відповідно 2) Оригінальні біометричні дані не можуть бути відновлені з захищеного шаблону без знання секретного ключа	1) Коротка довжина ключів, що отримуються 2) Можливість використання реконструйованого секрету для отримання оригінальних біометричних даних із компрометованих допоміжних даних 3) Не стійкі до атак грубою силою та перехресних атак, до атак множинного запису

Можливість не зберігати ключ, отриманий з біометричних даних, є незаперечною перевагою методу генерації криптографічних ключів з біометричних даних користувача порівняно з іншими існуючими методами. Таким чином, головною відмінністю двох останніх видів біометричних криптосистем є те, що в одному з них криптографічний ключ тільки закривається за допомогою біометричного зразка, а в іншому ключ генерується безпосередньо з біометричних даних користувача. Схематичне подане такої системи наведено на рис. 8.

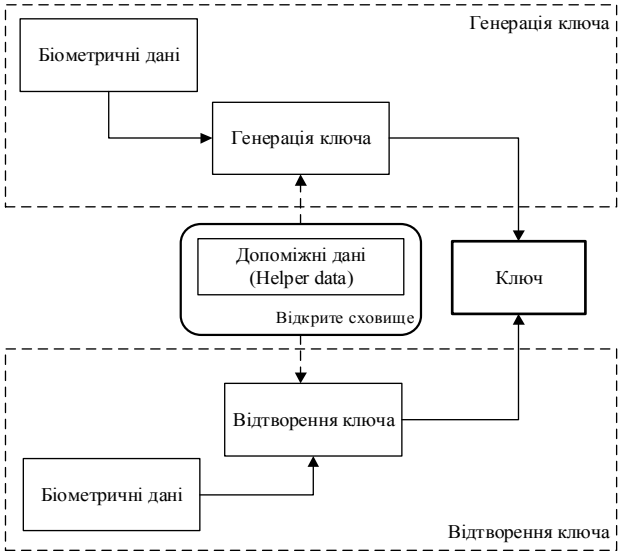

Рис. 8. Схематичне зображення біометричної криптографічної системи з генерацією ключа

Такі системи є більш безпечними, але їх важко застосовувати через навіть незначну мінливість біометричних характеристиках, оскільки необхідно з приблизно схожих даних згенеруючи той самий ключ знову і знову. Також недоліком таких систем є неможливість (або обмеженість кількості можливостей) сформувати новий ключ. Отже, якщо криптографічний ключ коли-небудь буде скомпрометований, то використання цього конкретного біометричного образу та конкретного алгоритму генерації ключа буде неможливе. У системі, де потрібне періодичне оновлення криптографічного ключа, це неприйнятно.

4.1 Нечіткі екстрактори

Найпоширенішою технологією, на якій базуються біометричні криптографічні системи з генерацією ключа, – це нечіткі екстрактори [10–12]. Базова логіка використання нечітких екстракторів схожа з логікою нечітких сховищ. Даний спосіб дозволяє однозначно відновлювати секретний ключ з неточно відтворюваних (зашумленних) біометричних даних. Метод нечітких екстракторів передбачає формування випадкової рівномірно розподіленої послідовності з початкових даних і подальше коректне її відновлення з будь-яких даних, досить схожих з початковими. Такі методи базуються на теорії інформації та завадостійкого кодування. Використовування методу нечітких екстракторів здатне компенсувати помилки, що виникають внаслідок технічної неможливості отримання однакових значень біометричних характеристик під час їхнього повторного введення користувачем. Метод нечітких екстракторів дозволяє отримувати ключ, який задовольняє всі критерії якості криптографічних ключів. У деяких реалізаціях передбачається формування ключа шляхом об'єднання допоміжних даних (отриманих з даного біометричного шаблону) та самого біометричного зразка. Допоміжні дані можуть бути отримані з заданого біометричного еталону і зберігатися у вигляді поновлюваного ключа або хеш-значення.

Загальна концепція побудови такого генератора криптографічних ключів полягає в наступному. Спочатку випадковим чином генерується бітова послідовність, яка кодується завадостійким кодом. Як завадостійкий код, що виправляє помилки, можуть використовуватися коди Хеммінга, Адамара, Боуза – Чоудхурі - Хоквінгема (БЧХ-коди), Ріда - Соломона (є окремим випадком БЧХ). Згенерована бітова послідовність може бути призначена для ідентифікації, автентифікації або генерації криптографічних ключів шифрування. Дана послідовність об'єднується з еталонними характеристиками біометричних ознак суб'єкта (біометричних еталоном).

Способи об'єднання можуть бути різними: від додавання за модулем 2 до використання алгоритмів, що більше орієнтовані на оброблювані дані. Результатом об'єднання є відкритий рядок, який може зберігатися на загальнодоступному сервері. Щоб отримати згенеровану раніше послідовність (криптографічний ключ) користувач вводить власні біометричні ознаки, які обробляються відповідним чином і «віднімаються» з відкритого рядка. Після вилучення біометричних даних отримана бітова послідовність буде змінена внаслідок нечіткості введених біометричних даних відносно еталонних. Після застосування коду, що виправляє помилки до отриманого рядка, в разі високого ступеня «схожості» висунотого біометричного образу і еталонного (тобто, якщо кількість розбіжних біт еталонних і висунутих даних не перевищує виправлячу здатність коду), буде відновлена послідовність бітів, яка і є криптографічним ключем. Описаний метод схематично зображено на рис. 9.

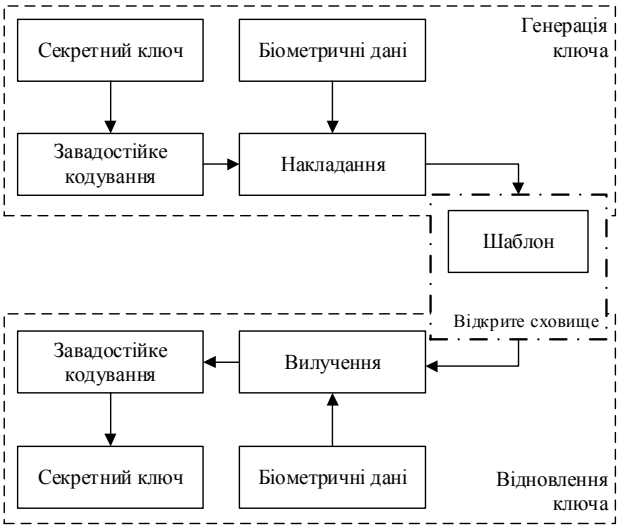

Рис. 9. Схематичне зображення методу нечітких екстракторів

Два основних підходи, що використовуються для генерації біометричних ключів – схема приватного шаблону та схема квантування.

4.2 Схема приватного шаблону

У схемах приватного шаблону (англ. Private template scheme) [10–12] використовуються допоміжні дані – послідовності бітів перевірки для виправлення помилок завадостійким кодом. Сам ключ формується безпосередньо з біометричного образу або з хешу цього біометричного образу. Наведемо як приклад алгоритм схеми приватного шаблону, в якій ключ формується з хешу.

Алгоритм генерації ключа:

1. До біометричного образу довжиною M біт, застосовується завадостійке декодування. У результаті формується вектор $Vec(V)=(V_1,V_2,...,V_n)$ для n-бітного коду, визначений як $Vec(v_i)=(v_{i,1},v_{i,2},...,v_{i,n})$, де $V_j = majority(v_{1,j},v_{2,j},...,v_{M,j})$

2. Отриманий після декодування характеристичний вектор $Vec(T)$ поєднується з вектором контрольної суми $Vec(C)$: $Vec(T)\|Vec(C)$, де вектор $Vec(C)$ є частиною коду, виправляючого помилки.

3. Для формування ключа виконується хешування $Vec(T)\|Vec(C)$ та, залежно від реалізації, з допоміжними даними

$$Key = Hash\left[Vec(T)\|Vec(C), helper\_data\right].$$

Алгоритм відтворення ключа:

1. До біометричного образу довжиною M біт, застосовується мажоритарне декодування. Формується вектор $Vec(V')=(V'_1,V'_2,...,V'_n)$ для n-бітного коду, визначений як $Vec(v'_i)=(v'_{i,1},v'_{i,2},...,v'_{i,n})$, де $V'_j = majority(v'_{1,j},v'_{2,j},...,v'_{M,j})$.

2. Отриманий після декодування характеристичний вектор $Vec(T')$ поєднується з вектором контрольної суми $Vec(C)$

$$Vec(T')\|Vec(C),$$

де вектор $Vec(C)$ є частиною коду, виправляючого помилки.

3. Для формування ключа виконується хешування $Vec(T)\|Vec(C)$ та, залежно від реалізації, з допоміжними даними

$$Key = Hash\left[Vec(T)\|Vec(C), helper\_data\right].$$

Відтворений ключ можна використовувати за призначенням.

Схематичне зображення такого алгоритму наведено на рис. 10. Експериментальні результати та аналіз безпеки показують, що схема приватних шаблонів є простою та ефективною, також слід зазначити, що під час використання такої схеми відновлення початкових біометричних даних із захищених шаблонів неможливе.

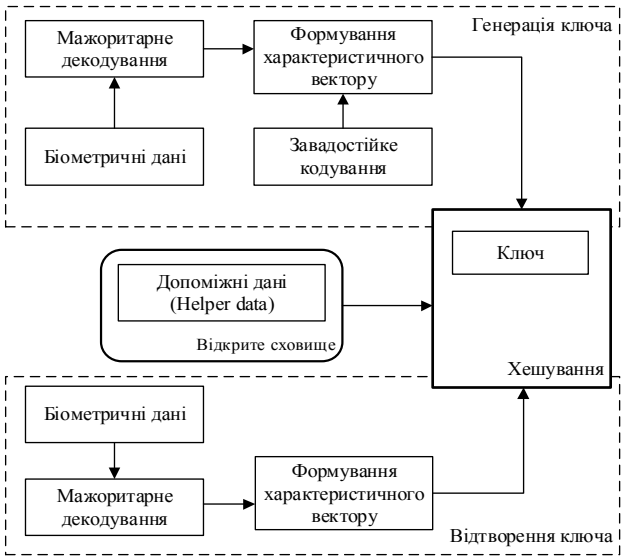

Рис. 10. Схематичне зображення біометричної криптографічної системи з генерацією ключа: схема приватного шаблону

4.3 Схема квантування

Схеми квантування (англ. Quantization scheme) [10]12] створюють біометричні ключі, використовуючи допоміжні дані та бінаризовані (або квантовані) біометричні характеристики. Унікальною особливістю схем квантування є можливість отримувати одні і ті самі ключі з досить різноманітних біометричних образів особи, навіть якщо вони отримані за допомогою різних сканерів. Результати експериментів з використанням як біометричні образи відбитків пальців показують, що до 40% відбитків створюють один і той самий криптографічний ключ, навіть коли різні сканери використовувались для захоплення відбитків пальців.

Схематично функціонування схеми квантування подано на рис. 11.

Рис. 11. Схематичне зображення біометричної криптографічної системи з генерацією ключа: схема квантування

Схеми квантування можуть бути реалізовані як мультимодальні системи; тобто унікальний ключ може бути отриманий з об'єднання двох або більше біометричних метрик.

Слабкістю схем квантування на основі допоміжних даних є можливість відновлення оригінальних біометричних зображень із захищених шаблонів. Зловмисник може отримати характеристичні вектори з захищених шаблонів, а потім відновити реальний біометричний образ. Схеми квантування, які використовують допоміжні дані, вразливі для атаки за допомогою множинності записів. Отже, існує потреба в мінімізації обсягу корисної інформації, яка може бути доступна зловмиснику, якщо система буде скомпрометована.

Для функціонування схеми квантування необхідні характеристичні вектори декількох біометричних зразків для обчислення відповідних інтервалів для кожного елемента характеристики (необхідні характеристичні вектори з реальними значеннями). Ці інтервали кодуються та зберігаються у вигляді допоміжних даних. Під час ідентифікації знову фіксуються біометричні характеристики суб'єкта та відображаються у попередньо визначені інтервали, генеруючи хеш-ключ. Для того, щоб забезпечити оновлюванні ключі або хеші, більшість схем забезпечують параметризоване кодування інтервалів. Схеми квантування дуже пов'язані з захисними функціями (англ. shielding function), оскільки обидва методи виконують квантування біометричних характеристик шляхом побудови відповідних інтервалів функцій. На відміну від захисних функцій, загальні схеми квантування визначають інтервали для кожної окремої біометричної характеристики, виходячи з її дисперсії. Це дає змогу покращувати коректування збережених допоміжних даних до характеру застосованої біометрії.

4.4 Порівняльний аналіз біометричних криптографічних систем з генерацією ключа

Порівняння переваг та недоліків криптографічних методів наведено у таблиці 2.

Таблиця 2

Порівняльний аналіз біометричних криптографічних систем з генерацією ключа

	Переваги	Недоліки
Схема приватного шаблону	1) Формує конкретні ключі безпосередньо з біометричних даних 2) Забезпечує захист шаблонів та конфіденційність користувачів, оскільки біометричні дані відсутні в системі автентифікації. 3) Використання сильних хеш-алгоритмів для генерації випадкових ключів з біометричних даних забезпечує криптографічну стійкість до атак грубою силою	Ключі не підлягають оновленню в разі компрометації
Схема квантування	1) Генерує біометричні ключі, використовуючи допоміжні дані та квантовані біометричні характеристики. 2) Можливо відновлювати одні і ті самі ключі з декількох екземплярів біометричних даних, отриманих навіть від різних джерел (сканерів, датчиків) 3) Забезпечує безпеку та конфіденційність, оскільки не зберігає інформацію про користувача, таку як біометричні дані.	Вразлива для атаки через множинність запису

5. ПОРІВНЯЛЬНИЙ АНАЛІЗ БІОМЕТРИЧНИХ КРИПТОСИСТЕМ

Проведемо аналіз переваг та недоліків зазначених вище біометричних криптографічних систем. Результати наведено у таблиці 3.

Таблиця 3

Порівняльний аналіз біометричних криптосистем

	Переваги	Недоліки
Біометричні криптографічні системи з звільненням ключа	1) Простота практичної реалізації 2) Більш надійна заміна паролів від ключів 3) Генерація ключа відбувається надійним криптографічним генератором	1) Шаблон потрібно зберігати в базі даних, що означає, що його можна викрасти 2) Криптографічний ключ має зберігатися як частина шаблону 3) Не гарантує високого рівня безпеки даних
Біометричні криптографічні системи зі зв'язуванням ключа	1) Ключ зберігається в замаскованому вигляді 2) Генерація ключа відбувається надійним криптографічним генератором 3) Допоміжні дані не містять ніякої інформації про біометричний образ та ключ, отже можуть зберігатися у відкритому доступі	1) Шаблон потрібно зберігати в базі даних, що означає, що його можна викрасти 2) Криптографічний ключ має зберігатися як частина шаблону
Біометричні криптографічні системи з генерацією ключа	1) Генерування ключів безпосередньо з біометричних шаблонів 2) Відсутність вразливостей, які існують під час зберігання ключа в сховищі 3) Допоміжні дані не містять ніякої інформації про біометричний образ та ключ, отже можуть зберігатися у відкритому доступі 4) Згенерований ключ не містить інформації власника біометричного образу	1) Біометричні характеристики не дають достатньої інформації для отримання надійного, поновлюваного ключа без використання будь-яких допоміжних даних 2) Складність створення нового ключа, при компрометації попереднього (обмеженість людини як носія біометричних образів) (у випадку, коли допоміжні дані не використовуються) 3) Вразливість перед атаками грубою силою та маскарад, атак помилкової ідентифікації

ВИСНОВКИ

Методи вилучення біометричних даних відомі досить давно. Проте саме на етапі створення постквантової криптографії біометричні криптографічні системи можуть знайти своє широке застосування та стати більш надійною заміною не лише паролів, формованих від особистих ключів, але й самих ключів.

Проте застосування біометричних даних як джерело ключової інформації має ряд складнощів:

– біометричні дані складно багаторазово чітко відтворити;

– біометричні дані можуть змінюватися з часом і залежать від фізичного та емоційного стану їх власника;

– проблема зміни ключів – самі по собі біометричні дані у разі компрометації більше не можуть бути використані;

– при сучасному розвитку апаратних та програмних ресурсів, біометричні дані можуть бути перехоплені та відтворені зловмисником, наприклад, зображення райдужної оболонки ока може бути просто зафіксовано камерою зловмисника.

У даній роботі розглянуто три види біометричних криптосистем. Визначено, що найбільш перспективним напрямом досліджень, з точки зору криптографічної стійкості, є біометричні криптосистеми з генерацією ключа.

Література

[1] *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування: монографія. –Харків: «Форт», 2012. – 870 с.

[2] *Есин В.І., Кузнецов О.О., Сорока Л.С.* Безпека інформаційних систем і технологій. – Харків: ХНУ ім. В.Н. Каразіна, 2013. – 632 с.

[3] *Горбенко Ю.І.* Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. – Харків: «Форт», 2015. – 960 с.

[4] *A. K. Jain, R. Bolle, S. Pankanti.* Biometrics: personal identification in networked society, 1999, Vol. 1, 434 p.

[5] *U. Uludag, S. Pankanti, S. Prabhakar, A. Jain.* Biometric Cryptosystems: Issues and Challenges, Proceedings of the IEEE, June 2004, Vol. 92, NO. 6.

[6] *Anil K. Jain, Arun Ross.* An Introduction to Biometric Recognition. IEEE Transactions on circuits and systems for video technology, 2004, Vol. 14, NO. 1. pp. 4–20.

[7] *A. Juels, M. Sudan.* A fuzzy vault scheme. Des. Codes Cryptography, 2006, Vol. 38, NO. 2, pp. 237–257

[8] *Juels A.* fuzzy commitment scheme / A. Juels, M. Wattenberg. 6th ACM Conference on Computer Communications and Security, Singapore, 1999, pp. 28-36

[9] *X. Boyen* Reusable cryptographic fuzzy extractors / X. Boyen. 11th ACM Conference on Computer and Communications Security, USA, 2004, pp. 82–91.

[10] *Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith.* Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM Journal on Computing, 2008, Vol. 38, No. 1, pp. 97–139

[11] *G. Davida, Y. Frankel, B. Matt.* On the relation of error correction and cryptography to an off-line biometric identification scheme. Proceedings of Workshop on Coding and Cryptography, Paris, France, 1999, pp. 129–138.

[12] *R. Sashank Singhvi, S. P. Venkatachalam, P. M. Kannan, V. Palanisamy.* Cryptography key generation using biometrics. International Conference on Control, Automation, Communication and Energy Conservation (INCACEC), 2009, pp. 1–6.

Надійшла до редколегії 15.12.2018

Луценко Марія Сергіївна, науковий співробітник ПАТ «ІІТ», здобувач кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Галузь наукових інтересів – біометрична криптографія, блокові симетричні шифри.

Кузнецов Олександр Олександрович, доктор технічних наук, професор, заступник головного конструктора ПАТ «ІІТ», професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна. Галузь наукових інтересів – криптографія та автентифікація, алгебраїчна теорія кодів, обробка, передача та захист інформації.

Прокопович-Ткаченко Дмитро Ігоревич, кандидат технічних наук, завідувач кафедри кібербезпеки Університету митної справи та фінансів. Заступник Голови Державної служби спеціального зв'язку та захисту інформації України (2013 – 2014 р.). Галузь наукових інтересів – інформаційна та кібербезпека держави, біометрична криптографія, автентифікація та безпека безпроводових мереж.

Звєрєв Володимир Павлович, кандидат технічних наук, старший науковий співробітник, Помічник Голови Національної поліції України, Голова Державної служби спеціального зв'язку та захисту інформації України (2014 – 2015 р.). Галузь наукових інтересів – інформаційна та кібернетична безпека держави.

Уварова Анна Олександрівна, провідний інженер Конструкторського бюро «Південне» ім. М. К. Янгеля», здобувач кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Галузь наукових інтересів – біометрична криптографія, блокові симетричні шифри.

УДК 004.056.55

Луценко М. С. **Сравнительный анализ биометрических криптосистем** / М. С. Луценко, А. А. Кузнецов, Д. И. Прокопович-Ткаченко, В. П. Зверев, А. А. Уварова // Прикладная радиоэлектроника: научно-техн. журнал. – 2018. – Том 17, №. 3, 4. – С. 182–191.

Исследуются существующие биометрические криптографические системы, предназначенные, в частности для формирования надежных и безопасных псевдослучайных последовательностей (т.н. криптографических ключей, паролей, кодов доступа и т.д.). Проводится сравнительный анализ различных видов биометрических криптосистем (с освобождением ключа; со связыванием ключа, с генерацией ключа), определяются их преимущества и недостатки. Приводятся конкретные схемы и вычислительные алгоритмы использования биометрических образов для формирования криптографических ключей, обосновываются перспективные направления дальнейших исследований.

Ключевые слова: биометрические образы, кодовые криптосистемы, генерация криптографических ключей

Табл.: 03. Ил.: 11. Библиогр.: 12 наим.

UDC 004.056.55

Lutsenko M. **Comparative analysis of biometric cryptosystems** / M. Lutsenko, A. Kuznetsov, D. Prokopovych-Tkachenko, V. Zvieriev, A. Uvarova // Applied Radio Electronics: Sci. Journ. – 2018. – Vol. 17, № 3, 4. – P. 182–191.

Existing biometric cryptographic systems, intended, in particular, for formation of reliable and secure pseudo-random sequences (so-called cryptographic keys, passwords, access codes, etc.) are investigated. A comparative analysis of various types of biometric cryptosystems (with the release of the key; with the binding of the key, with the generation of the key) is carried out; their advantages and disadvantages are determined. Specific schemes and computational algorithms for the use of biometric images for forming cryptographic keys are given, promising areas for further research are justified.

Keywords: biometric images, code cryptosystems, generation of cryptographic keys.

Tab. 3. Fig. 11. Ref.: 12 items.