Міністерство освіти і науки, молоді та спорту України
Харківський національний університет радіоелектроніки

ШЕВЧУК ОЛЕКСІЙ АНАТОЛІЙОВИЧ

УДК 004.056.5

МЕТОДИ ТА ЗАСОБИ ЕЦП З ЗАДАНИМ РІВНЕМ ЗАХИЩЕНОСТІ ТА ПІДВИЩЕНОЮ ШВИДКОДІЄЮ

05.13.21 – Системи захисту інформації

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2013

Дисертацією є рукопис.

Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки, молоді та спорту України.

Науковий керівник: доктор технічних наук, професор
Горбенко Іван Дмитрович,
завідувач кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки.

Офіційні опоненти: доктор технічних наук, професор
Краснобаєв Віктор Анатолійович,
завідувач кафедри комп'ютерної інженерії Полтавського національного технічного університу імені Юрія Кондратюка;

доктор технічних наук, доцент
Василіу Євген Вікторович,
професор кафедри автоматизованого управління технологічними процесами Одеської національної академії зв'язку ім. О.С. Попова

Захист відбудеться 12.03.2013 р. о 13 годині на засіданні спеціалізованої вченої ради К 64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

З дисертацією можна ознайомитися у бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

Автореферат розісланий 31.01.2013

Вчений секретар
спеціалізованої вченої ради І. В. Лисицька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Розвиток комп'ютерної техніки та інформаційно - телекомунікаційних систем (ІТС) сприяв створенню нових класів послуг, у тому числі дистанційних, які надаються у реальному часі. Тенденція збільшення кількості користувачів відкритих каналів зв'язку висунула нові вимоги до процесу надання таких послуг з боку захисту інформації. Для забезпечення діяльності за нових умов, в Україні було прийнято закони "Про електронний цифровий підпис", "Про захист персональних даних" та ін. Закон України "Про електронний цифровий підпис" надає правової чинності діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів та електронного цифрового підпису (ЕЦП), у відкритих середовищах.

На сьогодні розроблено й широко застосовано ряд механізмів ЕЦП, які ґрунтуються на використанні асиметричних криптографічних перетворень; стандартизовано цифрові підписи з доповненням і з відновленням повідомлення. В Україні використовується власний стандарт ЕЦП ДСТУ 4145:2002. Разом з тим, мають місце інциденти безпеки, пов'язані з використанням ЕЦП, які підтверджують необхідність, щонайменше, екстенсивного розвитку вимог до безпечних параметрів цифрових підписів, криптографічних протоколів, криптографічних функцій ґешування, процедур та регламентів тощо. Синтез та дослідження криптографічних властивостей алгоритмів ЕЦП, які відповідають визначеному міжнародними регламентами та стандартами рівню стійкості, є актуальною тематикою досліджень світової наукової спільноти.

Загальне поширення персональних комп'ютерів зумовило розвиток програмних засобів ЕЦП. Водночас, набуло розвитку зловмисне програмне забезпечення (ПЗ), у тому числі й таке, що націлене на крадіжку ключового матеріалу ЕЦП. Необхідність підвищення захищеності ключового матеріалу та розвиток шкідливого ПЗ зумовив появу апаратних засобів ЕЦП. Актуальною задачею для цього процесу стало вирішення проблемних питань, пов'язаних з обмеженнями апаратної бази, каналів зв'язку, коштів.

Серед задач, актуальних для даної тематики, можна виділити наступні. Обмеження каналів зв'язку щодо передачі та апаратних засобів щодо зберігання даних сприяє розвитку методів мінімізації обсягу даних, який займає сукупність ключового матеріалу, цифрового підпису та підписаного повідомлення. Так, стандарт цифрового підпису ДСТУ 4145:2002 не є ефективним за умови формування ЕЦП з обмеженими параметрами, проте він є перспективним, перш за все, з точки зору стійкості. Обмеження на обчислювальну здатність та просторові властивості в умовах збереження визначеного рівня стійкості – розв'язання задачі збільшення швидкодії існуючих криптографічних алгоритмів. При використанні апаратних засобів ЕЦП виникає питання щодо коректності реалізації криптографічних перетворень, яке зумовлює актуальність досліджень стійкості результатів криптографічних перетворень ЕЦП за умов відсутності автентифікації засобів ЕЦП тощо.

Для розв'язання вищезазначених задач у дисертаційній роботі досліджуються властивості ЕЦП з відновленням повідомлення, що ґрунтуються на перетвореннях у групі точок еліптичних кривих, у першу чергу відносно стандартів ISO/IEC 15946-4 та ISO/IEC 9796-3, та пропонується метод наділення аналогічними властивостями цифрового підпису, що визначається національним стандартом України ДСТУ 4145:2002.

Зв'язок роботи з науковими програмами, темами. Дисертаційну роботу виконано в рамках: держбюджетної НДР №262-1 "Розвиток, стандартизація, уніфікація, удосконалення та впровадження інфраструктури відкритих ключів, включаючи національну систему ЕЦП, на національному та міжнародному рівнях", держбюджетної НДР №237-1 "Напрями, методи та засоби удосконалення та розвитку національної інфраструктури відкритих ключів (включаючи систему електронного цифрового підпису)", госпдоговірної НДР №09-06 від 22.01.2009р. "Дослідження та розробка комбінованих інфраструктур з відкритими ключами на основі використання існуючих ІВК та системи на ідентифікаторах" (ДР №0109U002498), госпдоговірної НДР №11-06 від 01.03.2011р. "Розробка методів, комплексів та засобів ІВК для національних та міжнародних інформаційно - телекомунікаційних систем та інформаційних технологій" (ДР№0111U002634).

Мета та задачі дослідження. *Метою дисертаційної роботи* є забезпечення визначеного рівня стійкості та підвищення швидкодії апаратних засобів криптографічного захисту інформації, що реалізують національний алгоритм ЕЦП, який ґрунтується на перетвореннях у групі точок еліптичної кривої.

Відповідно до мети роботи необхідно розв'язати *наукову задачу*, яка полягає в розробці методів підвищення швидкодії основних складових алгоритмів ЕЦП із збереженням рівня захищеності в реалізаціях криптографічних засобів захисту, у тому числі апаратних.

Для досягнення мети необхідно розв'язати такі задачі:

– дослідити криптографічні властивості та стан застосування класів ЕЦП з додаванням та відновленням повідомлення, що ґрунтуються на перетвореннях у групі точок еліптичної кривої, з досвідом використання в апаратних засобах криптографічного захисту інформації;

– розробити метод удосконалення алгоритму ЕЦП ДСТУ 4145:2002 для надання властивостей відновлення повідомлення;

– розробити метод автентифікації апаратних засобів криптографічного захисту інформації, розподіл яких пов'язаний із загрозою підміни;

– розробити метод підвищення ефективності алгоритмів скалярного множення у групі точок еліптичної кривої, що може бути застосовано до схем ЕЦП, які ґрунтуються на перетвореннях у групі точок еліптичної кривої та побудовані з використанням різних алгоритмів скалярного множення, з метою збільшення швидкодії перетворення.

Об'єктом дослідження є процеси надання послуг ЕЦП із заданим рівнем захищеності та підвищеною швидкодією.

Предметом досліджень є методи та засоби здійснення й застосування ЕЦП в умовах обмежень на складність перетворень та можливості існування загроз.

Методи дослідження. Під час виконання дисертаційної роботи використовувалися такі методи: теорії складності обчислень під час оцінювання складності атак повного розкриття для перетворень типу ЕЦП, які ґрунтуються на перетвореннях у групі точок еліптичної кривої; теорії ймовірностей та математичної статистики в ході визначення криптографічної стійкості перетворень типу ЕЦП до екзистенційної підробки; криптографічного аналізу під час оцінювання складності атак повного розкриття для перетворень типу ЕЦП та аналізі властивостей схем ЕЦП з відновленням повідомлення; програмного моделювання та профілювання при реалізації процесів криптографічних перетворень, комбінаторики під час дослідження колізійних властивостей окремих елементів криптографічних перетворень; програмного моделювання паралельних процесів для аналізу стійкості запропонованого протоколу.

Використані методи розв'язання поставлених задач дозволили: застосувати такий відомий підхід, як кешування, для розв'язання задачі зменшення обчислювальної складності цифрового підпису; виявити вразливість апаратних засобів, що реалізують перетворення ЕЦП у групі точок еліптичної кривої, до підміни апаратного засобу; запропонувати метод протидії загрозі підміни засобу ЕЦП; застосувати відомий механізм відновлення повідомлень до існуючих реалізацій ЕЦП із доповненням.

Наукова новизна отриманих результатів дисертаційної роботи зумовлена теоретичним узагальненням та новим розв'язанням науково-технічної задачі, сутність якої полягає в розробці методів підвищення швидкодії основних складових алгоритмів ЕЦП із збереженням рівня захищеності в реалізаціях криптографічних засобів захисту, у тому числі апаратних.

У роботі отримано такі нові наукові результати:

1. Вперше запропоновано метод модифікації алгоритмів скалярного множення у групі точок ЕК, що використовуються для обчислення ЕЦП, який ґрунтується на частковому кешуванні множника та відповідної модифікації генератора псевдовипадкових послідовностей, що дозволяє підвищити швидкодію засобу ЕЦП.

2. Вперше запропоновано метод захисту від атаки повного розкриття за відомими результатами криптографічних перетворень, яка здійснюється за умови підміни апаратного засобу КЗІ, що ґрунтується на модифікації алгоритму автентифікації ISO/IEC 9798-2 6.1, шляхом зміни криптографічних перетворень з симетричних на перетворення з відкритим ключем, для обміну користувача з третьою довіреною стороною, що дозволяє забезпечити безпечний розподіл апаратних засобів КЗІ, які реалізують алгоритми ЕЦП, в умовах існування загрози підміни засобу криптографічного захисту.

3. Набув подальшого розвитку метод ЕЦП, визначений у Національному стандарті ДСТУ 4145:2002, який на відміну від існуючого використовує функ-

цію створення доданої збитковості замість функції ґешування повідомлення, що дозволяє зменшити обсяг ЕЦП для групи повідомлень, в залежності від характеристик повідомлення.

Практичне значення отриманих результатів полягає у наступному.

1. Збільшено швидкодію засобів ЕЦП, які ґрунтуються на перетвореннях у групі точок еліптичної кривої, від 18 до 25%.

2. Зменшено обсяг ЕЦП для групи повідомлень від Θ біт, якщо обсяг вхідного повідомлення менший, ніж 2Θ, де Θ — визначений рівень стійкості у бітах захисту.

3. Забезпечено розподіл апаратних засобів КЗІ з визначеним рівнем стійкості, які реалізують алгоритми ЕЦП, в умовах існування загрози підміни засобу криптографічного захисту.

4. Отримано програмну модель ЕЦП з відновленням повідомлення, які ґрунтуються на перетвореннях у групі точок еліптичної кривої, відповідно до стандарту ISO/IEC 9796-3.

Обґрунтованість та достовірність наукових положень, висновків та рекомендацій підтверджується їх несуперечністю з відомими положеннями теорії імовірності, абстрактної алгебри, відомими результатами, подібністю експериментальних результатів до теоретичних.

Основні результати дисертації реалізовані в системах криптографічного захисту інформації під час виконання ряду НДР та ДКР, а також використані в навчальному процесі кафедри БІТ ХНУРЕ: акт впровадження в діяльність АТ "Інститут інформаційних технологій" від 20.05.2011р.; акт впровадження в межах робіт зі створення захищених каналів у корпоративній мережі передавання даних Національної акціонерної компанії "Нафтогаз України" від 15.10.2012р.; акт впровадження в навчальний процес Харківського національного університету радіоелектроніки від 12.01.2012р.

Особистий внесок здобувача. Автор самостійно отримав наукові результати, які складають основу дисертації. Частину публікацій виконано разом з іншими вченими [5,6]. Одноосібно опубліковано за темою дисертації 4 роботи [1,2,3,4].

У статті [5] автором запропоновано та виконано аналіз ефективності та безпечності методу прискорення скалярного множення за рахунок кешування частин сесійних ключів ЕЦП. У статті [6] автором розглянуто оцінки, властивості та приклади використання ЕЦП з відновленням повідомлення.

Апробації результатів дисертації. Основні результати досліджень, які проведено в дисертаційній роботі, доповідалися на дев'яти конференціях та симпозіумах: міжнародних науково-практичних конференціях XIII-XV "Безопасность информации в информационно - телекоммуникационных системах", 2009-2012рр.; "Современные проблемы математики и её приложения в естественных науках и информационных технологиях",2011р.; "Компьютерное моделирование в наукоёмких технологиях", 2012р.; "Радиоэлектроника и молодежь в XXI веке", 2008р.; "Компьютерные науки и технологии", 2011р.

Публікації. За результатами дисертаційної роботи опубліковано 6 статей у шести наукових журналах, що входять до переліку МОНмолодьспорту, 9 доповідей та тезисів міжнародних наукових та науково-практичних конференцій.

Структура та обсяг дисертації. Дисертація складається із вступу, п'яти розділів і висновків, загальний обсяг роботи 158 с., з яких 123 с. – основного тексту, та 2 таблиці, які займають усю сторінку, містить 37 рисунків, 13 таблиць, перелік використаних джерел із 115 найменувань та 3 додатки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету та задачі дослідження, розкрито наукову та практичну значущість отриманих результатів, наведено відомості щодо впровадження результатів роботи, публікацій автора та апробацію результатів роботи.

У першому розділі дисертаційної роботи розглядається сучасний стан розвитку алгоритмів та засобів криптографічного захисту інформації (КЗІ), які забезпечують послугу ЕЦП. Розглянуто класифікацію, основні вимоги, модель загроз, вектори атаки, критерії та показники криптографічних перетворень типу ЕЦП, особливості апаратних реалізацій схем ЕЦП, сучасні вимоги до вибору ключових параметрів та відповідного рівня стійкості. Так, згідно з NIST SP 800-57, актуальним бітовим обсягом є [128;256] біт.

Проведений аналіз показав наявність таких актуальних задач: зменшення обсягу цифрового підпису повідомлення; зменшення складності обчислення цифрового підпису; перевірка безпечності реалізації цифрового підпису.

Актуальність задач зменшення обсягу та складності обчислення цифрового підпису повідомлення зумовлюються розповсюдженням компактних криптографічних засобів невеликої вартості з певними обмеженнями на обсяг даних, каналів зв'язку, живлення тощо. Прикладом перспективної технології, яка потребує розвитку та досліджень, є технологія бездротового високочастотного зв'язку малого радіусу дії (комунікація ближнього поля, NFC). Технологія використовується у таких засобах, як позначки товарів, проїзні документи та посвідчення тощо. Засоби NFC мають суттєві обмеження на канал зв'язку та обсяг інформації, яка може бути використана пристроєм. Сьогодні, під час використання таких засобів, розробники інфраструктур обмежені у використанні криптографічних примітивів. Необхідність використання нестандартизованих перевірених криптографічних перетворень призводить до впровадження слабких алгоритмів та компрометації інформаційних систем.

На погляд автора, важливими прецедентами в історії практичного використання криптографічних схем ЕЦП стали інциденти, пов'язані з компрометацією особистих ключів цифрового підпису апаратних засобів. Було використано реалізацію ECDSA з порушенням вимог до випадкових ключів сесії ЕЦП. Цей інцидент є цікавим з точки зору пошуку та виявлення уразливостей апаратних криптографічних рішень. Незважаючи на використання відомого кри-

птоалгоритму та тривіальну за сутністю атаку, факт її існування не було встановлено впродовж тривалого часу. Різні дослідники відмічають існування проблем з дослідженням реалізації криптографічних перетворень у певних фізичних пристроях. Дослідження показали, що для апаратних пристроїв, які реалізують послугу ЕЦП, існує висока ймовірність реалізації аналогічної загрози порушником. Порушник зможе здійснити загрозу повного розкриття за двома відомими результатами криптографічних перетворень, у разі використання аналогічної лазівки. Особливістю є складність детектування такого класу помилок, яка відповідає складності розв'язання задачі пошуку дискретного логарифму в групі.

За таких умов кількість сторін, яким має довіряти користувач засобів КЗІ, значно зростає. Можливим розв'язком задачі може бути використання протоколів автентифікації криптографічного засобу користувачем чи інформаційною системою. У документах, що використовуються у світовій практиці під час розробки апаратних засобів криптографічного захисту, таких як стандарти FIPS-140, вітчизняні вимоги та накази "Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису", "Про затвердження Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації" не встановлюють вимоги до автентифікації користувачем апаратного засобу. Таким чином, неможливо дослідити, що чіпи та контролери, які впроваджуються, це саме ті контролери та чіпи, які було досліджено чи очікувані.

У другому розділі розв'язується задача зменшення обсягу цифрового підпису для груп повідомлень. Під групою повідомлень розуміють деякий пакет $M = \{m_0, m_1, \ldots\}$, де $m_0, m_1, \ldots$ – деякі повідомлення, передача яких здійснюється водночас. Під обсягом цифрового підпису розуміють загальний обсяг даних, які мають бути передані для перевірки дійсності та автентичності довільного повідомлення з групи, без урахування загальносистемних параметрів.

Розглядаються такі підходи: відомий, з додаванням до групи переліку криптографічних ґеш-значень з обчисленням ЕЦП; запропонований, з використанням підписів з відновленням повідомлення. Порівняння та аналіз підходів виконується з використанням моделі каналу зв'язку з незалежними помилками.

Проаналізовано наступну залежність показника від обсягу повідомлення. Нехай P_e – ймовірність зчитування помилкового біта з каналу зв'язку, S – цифровий підпис, M – повідомлення, H – ґеш-значення повідомлення M, K_a – $L(S)$ – бітовий обсяг цифрового підпису, $L(m_j)$ – бітовий обсяг j-го повідомлення, $L(S) + \sum\limits_{j=0} L(m_j)$ – загальний бітовий обсяг даних.

Надалі наводиться аналіз окремого випадку $\forall m \in M : L(m) = L_{bm} = = \text{const}$. Спотворення довільної частини пакета призводить до неможливості відновлення будь-якого повідомлення, тому ймовірність помилкової перевірки

ЕЦП j-го повідомлення становить

$$P_E(S, M) = 1 - (1 - P_e)^{L(S)+i\,L(m_j)}. \quad (1)$$

Розглядається загальновживаний підхід до розв'язання задачі – використання переліку ґеш-значень повідомлень. Використання цифрового підпису для забезпечення автентичності та неспростовності цього переліку дозволяє зменшити ймовірність виникнення помилки. Нехай загальний обсяг даних подано як $\{M, H, S\}$, Sign – перетворення цифрового підпису, Hash – криптографічна ґеш-функція, Θ – заданий у бітах стійкості рівень захищеності, тоді $\forall m_i \in M, i \in [0, n) : h_i = \text{Hash}(m_i)$ та $S = \text{Sign}(H, K_a)$. Досліджено, що для забезпечення заданого рівня стійкості Θ, для довільного повідомлення необхідно 2Θ біт хеш-значення. Таким чином, $\forall m \in M : L(\text{Hash}(m) = const = = 2\Theta)$. Для підпису з доповненням $L(S)$ для заданого рівня стійкості визначається математичною проблемою, за якою обчислюється стійкість схеми. Так, для підписів у групі точок еліптичної кривої $L(S) = 2\Theta \times 2$. Таким чином, для неможливості відновити j-те повідомлення необхідна помилка в одному з $L(S) + L(H) + L(m_j)$ біт. Тоді $L(S) + L(H) + L(m_j) = 2\Theta \times 2 + 2i\Theta + L_{bm}$. Отже, ймовірність помилки становить

$$P_E(P_e, i, \Theta, L_{bm}) = 1 - (1 - P_e)^{2\Theta(2+i)+L_{bm}}. \quad (2)$$

Визначено, що ймовірність помилки для підходу (1) більша за (2), якщо $2\Theta(2 + i) + L_{bm} < 4\Theta + i\,L_{bm}$. Можна побачити, що це можливо за умови

$$i(L_{bm} - 2\Theta) > L_{bm},$$

тобто для $i > 1$ – тільки у випадках, коли $L_{bm} > 2\Theta$. Для підходу (2) межею є $iL_{bm} > 2\Theta$. Це означає, що метод не є придатним для використання в інформаційних системах та засобах, для яких було розглянуто актуальність задачі.

Пропонується використовувати підхід з відновленням для обчислення підпису груп невеликих повідомлень ($\sum L(m_j) < 2\Theta$). Для розв'язання задачі запропоновано використати ЕЦП з відновленням повідомлення. Цей різновид криптографічних перетворень використовує інший підхід до перевірки дійсності цифрового підпису. Так, повідомлення вважається дійсним, якщо дійсна його збитковість. Пропонується така оцінка ймовірності події $P(m)$ прийняття рішення щодо дійсності повідомлення m абонентом:

$$P(m) = \frac{\#N}{\#M}, \quad (3)$$

де M та N – множини повідомлень, причому множина $M = \{m_0, m_1, \ldots\}$ утворюється сукупністю усіх можливих дійсних повідомлень, та множина $N = = \{n_0, n_1, \ldots\}$ таких, що $\forall n \in N : n \notin M$. Кількість біт збитковості повідомлення обчислюється як $\log_2 \#N$, де $\#N$ – потужність множини. Визначен-

ня необхідного рівня стійкості криптографічних перетворень ЕЦП з відновленням повідомлення залежить від кількості збитковості підписаного повідомлення. Досліджено, що для розв'язання задачі можна використовувати ЕЦП з відновленням повідомлення, в режимі повного відновлення повідомлення. Стверджується, що для певного випадку та перетворень у групі точок еліптичної кривої, кількість біт захисту криптографічного перетворення ЕЦП від загрози екзистенційної підробки дорівнює загальній збитковості повідомлень у групі. Твердження ґрунтується на гіпотезі про складність розв'язання задачі дискретного логарифму в групі точок еліптичної кривої. Безпечність перетворення дорівнює сумі кількості біт доданої та природної збитковості всієї множини повідомлень. Таким чином, загальний обсяг підписаного повідомлення становить $2\Theta + i\, L_{bm}$ для випадку, коли загальна природна збитковість повідомлення дорівнює або більша за Θ, або $3\Theta + i\, L_{bm}$ в іншому випадку. Тоді

$$P_E(P_e, i, \Theta, L_{bm}) = 1 - (1 - P_e)^{3\Theta + i\, L_{bm}}.$$

У роботі розглянуто підхід до модифікації існуючих реалізацій криптографічних перетворень ЕЦП за національним стандартом ДСТУ 4145:2002, для надання властивості відновлення повідомлення. Запропоновано дві модифікації:

– шляхом зміни алгоритму криптографічної ґеш-суми Hash на алгоритм обчислення повідомлення для відновлення з наданою збитковістю $\delta()$, що дозволяє подати етап розрахунку r компоненти підпису як

$$r = \pi + \delta(M);$$

– шляхом зміни алгоритму створення передобчислень з використанням функції розгортання ключа KDF

$$k = rand([1, n-1]);$$
$$\Pi = \pi(kP); \Pi' = \text{KDF}(\pi(\Pi)).$$

Аналіз показує, що проблемним питанням є модифікація вже існуючих апаратних реалізацій електронних ключів. На вхід таких засобів подається значення криптографічної функції ґешування та повертається обчислене значення підпису (r, s). Для такого випадку доцільно застосовувати перший метод, що дозволить використовувати існуючі апаратні засоби електронних ключів без додаткової модифікації та оновлень.

У третьому розділі розглянуто загрозу підміни засобу криптографічного захисту інформації. Досліджено, що такі загальнопоширені вимоги до апаратних засобів КЗІ, як FIPS 140, не містять настанов щодо необхідності автентифікації апаратних засобів користувачем. Як основні загрози було розглянуто реалізації атаки універсальної підробки та повного розкриття для такої моделі порушника:

– порушника відокремлено від процесу розробки та створення засобу КЗІ;

– порушник певною мірою має фізичний доступ до засобу КЗІ ще до закінчення процесу інтеграції та безпосереднього використання засобу користувачем;

– компрометація ключової інформації за рахунок прямого доступу до елементів збереження ключової інформації не можлива, оскільки засіб КЗІ ще не пройшов етапу персоналізації;

– існує можливість заміни криптографічних алгоритмів за рахунок прямого доступу до елементів збереження алгоритмів перетворень або фізичної модифікації пристрою;

– порушник не може перехопити та втручатися у канал зв'язку з засобом;

– порушник не може використовувати фізичні канали витоку інформації для персоналізованого засобу КЗІ;

– недійсні (з помилками) результати криптографічних перетворень можуть знаходитися у відкритому доступі;

– результати криптографічних перетворень, які було отримано у помилковому стані, можуть знаходитися у відкритому доступі та призвести до компрометації ключової інформації;

– використання засобу КЗІ у відкритому середовищі не розглядається.

Було розглянуто запропоновані стандартами FIPS 140-3 заходи протидії загрозам порушника. Додатково було проаналізовано питання з комплектів PCI HSM 1.0 та 2.0. Ключовими заходами було визначено такі: наявність та застосування самотестування модуля КЗІ; повна перевірка справжності, цілісності та автентичності даних оновлення; автентифікація користувача, та впровадження розподілу доступу; впровадження відповідного рівня забезпечення фізичної цілісності засобу КЗІ; контроль фізичної цілісності модуля криптографічного захисту.

Дослідження показали, що наведених заходів недостатньо для протидії загрозі повного розкриття в певних випадках. Розглядається загроза підміни криптографічного засобу, на такий, що містить скомпрометовані секретні значення. Показано, що загроза компрометації секретного ключа персоналізованого засобу КЗІ не є актуальною. Нехай існує програмна реалізація криптографічного алгоритму $\gamma(k, m)$, де k – вхідний особистий ключ та m – вхідне повідомлення, який подано у вигляді повідомлення (тексту програми) $M_{S(k,m)}$, та його цифрового підпису $S = \text{Sign}(\text{Hash}(M_{\gamma(k,m)}), k)$. Нехай порушник може створити новий алгоритм $\gamma'(k, m) = \alpha \circ \gamma(k, m)$, де α – деякий доданок, що спотворює вхідні дані m або k, та $S' = \text{Sign}(\text{Hash}(M_{\gamma'(k,m)}), k)$. Нехай також $S = S'$. Тоді $M_{\gamma'(k,m)} = M_{\gamma(k,m)}$, та відповідно $\alpha \circ \gamma(k, m) = \gamma(k, m)$. Тоді $\forall k \in K, m \in M : \alpha \circ \gamma(k, m) = \gamma(k, m)$. Але $\alpha \circ S(k, m) \neq S(k, m)$. Таким чином, розповсюдження криптографічних засобів, що пройшли етап персоналізації, не становить певну загрозу та, навпаки, процес розповсюдження криптографічних засобів, що не пройшли етап персоналізації, має уразливості. Показано, що для засобів КЗІ, які реалізують криптографічні перетворення ЕЦП у групі точок еліптичної кривої, існує загроза компрометації незалежно від етапу

персоналізації. Дійсно, до ключа сесії K_a та особистого ключа X_a висуваються однакові вимоги. Також до сеансового ключа висуваються вимоги незв'язності та неповторюваності. Покажемо на прикладі алгоритму ЕЦП ENCR наслідки передбачуваності сесійних ключів.

Нехай порушник здійснює таку модифікацію:

$$\forall x \in X : \alpha(x) = \text{const}. \tag{4}$$

Тоді

$$\begin{array}{ll} K_a^1 = \alpha \circ \text{RNG}(); & K_a^2 = \alpha \circ \text{RNG}(); \\ \Pi = K_a^1 \times Q; & \Pi = K_a^2 \times Q; \\ r_1 = (\delta + \pi(\Pi)) \bmod n; & r_2 = (\delta + \pi(\Pi)) \bmod n; \\ s_1 = (K_a^1 - X_a \times r_1) \bmod n; & s_2 = (K_a^2 - X_a \times r_2) \bmod n; \end{array}$$

$$X_a = \frac{s_1 - s_2}{r_2 - r_1} \mod N.$$

Користувач може перевірити, чи була внесена модифікація (4) шляхом порівняння результатів перетворення цифрового підпису. Результати перетворень мають бути відмінними. Складність виявлення (4) є невеликою.

Порушник може ускладнити процес виявлення атаки так:

$$\forall x \in X : \alpha_i(x) = \alpha_{i+1}(x) + \epsilon, \tag{5}$$

де $\alpha_{i+1}(x)$ – результат $i+1$ виклику функції, $\epsilon = \text{const}$ – деяке відоме порушнику значення. Видно, що в такому випадку користувач не може перевірити, чи була внесена певна модифікація за визначеним методом. Нехай вимога щодо створення відмінних ключів сесій не виконується за (5), тоді $\forall m \in M; \forall i, j \in \mathbb{N} : \gamma_i(X_a, m) \neq \gamma_j(X_a, m)$, але порушник може компроментувати особистий ключ:

– ECNR, ECPV, ECAO, ECKNR: $X_a = (s_1 - s_2 + \epsilon)(r_2 - r_1)^{-1} \bmod n$;
– ДСТУ 4145:2002: $X_a = (s_2 - s_1 + \epsilon)(r_2 - r_1)^{-1} \bmod n$;
– ECMR: $X_a = (r_2 - r_1 + r_1 r_2 \epsilon)(r_1 s_2 - r_2 s_1)^{-1} \bmod n$.

Розглянемо можливості користувача щодо виявлення (5). Нехай необхідно визначити наявність зв'язку вигляду $f(x) = x + \epsilon$ між сеансовими ключами S^1 та S^2. Для цього користувач має розглянути гіпотезу $\epsilon = E$, де E – обране користувачем значення. Тоді, якщо $\epsilon = E$, то

$$\Pi_2 = \Pi_1 + E \times Q. \tag{6}$$

Для повної оцінки розглянемо складність реалізації атаки (5). Оскільки $\epsilon, S_{xa} \in GF(n)$, тоді складність пошуку дійсного E за методом грубої сили – $O(n)$, та дорівнює складності атаки грубої сили у випадку компрометації особистого ключа. Критерієм виконання такої гіпотези є дійсність тотожності (6), що визначена для вибраної схеми ЕЦП. Зазначимо, що для реалізації детекту-

вання (5) необхідні два послідовно отримані підписи. Також порушник може модифікувати атаку (5), використавши для обчислення сеансових ключів генератор псевдовипадкових послідовностей таким чином:

$$K_a = \text{PRNG}(\epsilon),$$

де ϵ – відомий порушнику вектор ініціалізації генератора псевдовипадкових послідовностей.

Дослідження показали, що єдиними міжнародними документами, які містять певні вимоги до процесу розповсюдження засобів КЗІ, є PCI HSM 1.0 та 2.0. Необхідно зазначити, що PCI HSM не вказує на методи забезпечення певних вимог. На нашу думку, використання криптографічних алгоритмів та примусова автентифікація засобу користувачем на етапах персоналізації є обов'язковим та невід'ємним заходом.

Дослідження показали, що довіра до виробника апаратного криптографічного засобу захисту є обов'язковою. Тому, пропонується використовувати протокол автентифікації, між користувачем засобу КЗІ, виробником засобу КЗІ та засобом КЗІ для встановлення дійсності. Аналіз посилань PCI HSM 2.0 до інших стандартів галузі криптографічного захисту показав відсутність протоколів, придатних до розв'язання задачі. Так, у разі використання симетричних протоколів виробник повинен зберігати ключову інформацію щодо усіх каналів передачі ключових носіїв, та усіх майбутніх користувачів засобів. У разі використання асиметричних протоколів необхідні додаткові ускладнення пристрою та реалізація додаткової інфраструктури. Запропоновано такий протокол автентифікації:

1) U $\rightarrow$ V: $\{D, T_{UV}\}_{PK(V)\}}$;
2) V $\rightarrow$ U: $\{\{N_V, T_{VD}\}_{K_{VD}}, \{N_V\}_{T_{VD}}\}_{T_{UV}}$;
3) U $\rightarrow$ D: $\{N_V, T_{VD}\}_{K_{VD}}$;
4) D $\rightarrow$ U: $\{N_V\}^D_{T_{VD}}$;
   U: $\{N_V\}^D_{T_{VD}} = \{N_V\}^U_{T_{VD}}$.

Запропонована модифікація механізму та криптографічного протоколу ISO/IEC 9798-2 № 6.1. дозволяє усунути певні недоліки: реалізуючи лише алгоритми симетричного шифрування у засобі КЗІ; забезпечуючи виконання вимог PCI HSM 2.0 щодо доставки засобів КЗІ за допомогою третіх служб без попередньої реєстрації та розподілу ключового матеріалу, обов'язкової реєстрації користувачів.

У четвертому розділі розглянуто метод модифікації перетворень скалярного множення, що використовуються в складі алгоритмів обчислень ЕЦП. Проаналізовано тенденцію зростання вимог до ключових параметрів ЕЦП, та відповідного нелінійного зростання складності обчислень криптографічних перетворень. Як протиріччя показана відсутність відповідного зростання обчислювальних можливостей загальнодоступних апаратних засобів.

Під час моделювання було виявлено, що операція скалярного множення в

групі точок еліптичної кривої має найбільшу складність обчислень. Так, у програмній реалізації цифрового підпису обчислення скалярного множення займає від 80% усіх обчислень. Стверджується, що підхід з оптимізацією певного алгоритму має недоліки – апаратні засоби мають різні обмеження, від яких залежить методика вибору оптимального алгоритму скалярного множення для певного пристрою. Пропонується загальний метод, який можна застосувати до різних алгоритмів скалярного множення.

Пропонується використати наступне протиріччя для зменшення складності обчислень. Нехай наявний для криптоаналітика матеріал для аналізу цифрового підпису є набір значень (r, s, M), де (r, s) – компоненти ЕЦП, та M – підписане повідомлення. Згідно з загальними схемами, у випадку ЕЦП з доповненням:

$$r = f_1(k \times G),$$
$$s = f_2(k, x_A, r),$$

де f_1, f_2 – деякі лінійні функції, k – ключ сесії, x_A – особистий ключ, G – загальносистемний параметр. Так, повне розкриття x_A можливе в результаті певних дій.

1. Атаки повного перебору (грубою силою) особистого ключа x_A. Складність атаки залежить від складності перетворень та бітового обсягу особистого ключа x_A.

2. Атака повного перебору $\epsilon = k_1 - k_2$. Складність перетворень аналогічна складності повного перебору (грубою силою) особистого ключа x_A.

3. Відновлення ключа сесії з r. Складність атаки залежить від складності зворотного перетворення $k \times G = f_1^{-1}(r)$. Для ЕЦП, що ґрунтуються на перетвореннях у групі точок еліптичної кривої, складність зворотнього перетворення дорівнює складності вирішення задачі пошуку дискретного логарифму в групі точок еліптичної кривої.

Слід зауважити, що найбільш ефективні алгоритми пошуку дискретного логарифму λ, ρ-Поларду для групи точок еліптичної кривої мають асимптотичну складність порядку $\sqrt{(n\pi/2)} \approx 1.25\sqrt{(n)}$ та використовують лише групову операцію. Метод атаки грубою силою має асимптотичну складність порядку n. Таким чином існує певне вікно між складністю атаки грубою силою та складністю розв'язання задачі дискретного логарифму. Пропонується використати наявне вікно як простір для зменшення складності обчислень.

Висуваються наступні вимоги до методів скалярного множення, до яких може бути застосовано запропонований алгоритм.

Визначимо функцію $\forall X \in GF(q) : \#X = \lfloor log_2 q \rfloor + 1$.

Визначимо пару змінних $k, k' \in GF(q)$, що отримано за допомогою деякої випадкової функції $k \leftarrow \Gamma()$.

Розглянемо модель алгоритму скалярного множення у вигляді композиції функцій кроку наступним чином. Для деякої точки ЕК $G \in E(GF(q))$, де $E(GF(q))$ – еліптична крива, визначена над $GF(q)$, визначимо алгоритм скалярного множення як композицію

$$kG = (f^w_{\#k/w} \circ f^w_{\#k/w-1} \circ \ldots \circ f^w_1)(k, G).$$

Кількість функцій, що складає композицію, становить $\#k/w$. Кожна функція

$$f^w_i(k, G) \tag{7}$$

оброблює w бітів з k та повертає деякий проміжний результат, або результат множення. Отже, функція (7) є основним кроком певного алгоритму. Слід зазначити, що набір параметрів може відрізнятися від k, G – для більшості алгоритмів скалярного множення проміжний стан має більше змінних.

Нескладно побачити, що для пари k, k' та $\xi \leq \#k/w$, де $\forall i \in [1, \xi] : \phi^w_i(k) = \phi^w_i(k')$, справедливі такі твердження:

– $f^w_\xi(k, G) = f^w_\xi(k', G)$;
– якщо $w = \text{const}$, тоді $\#\Phi^w(i, k) = w \times i$;
– якщо $\#k/w - \xi > 0$, тоді $kG \neq k'G$;
– якщо $\nu = \#k/w - \xi$, тоді відстань Геммінга $d(k, k') \leq \nu \times w$.

Для (7) має існувати

$$(k_\alpha, k_\beta, \ldots) = \phi^w_i(k), \tag{8}$$

що повертає набір бітів $(k_\alpha, k_\beta, \ldots) \in k$ таких, що $\alpha, \beta, \ldots \in [0, \#k]$.

Результат функції (8) має бути необхідним та достатнім для обчислення (7), для неї також має бути справедливе $\forall i \in [1, \#k/w] : \#\phi^w_i(k) = w$.

Наводиться наступний приклад для методу скалярного множення COMB. Визначено алгоритм відповідно до наведених функцій:

$$\begin{array}{lll} f^w_j & (k, P, A, B) := & \\ & \left| \begin{array}{lll} j = \#k/w & : & A \\ \#k/w > j > 1 & : & f^1_{\#k/w-j-1}(k, P, A + \beta, \beta), \\ & & \beta = B + \text{PR}(P, \phi^1_{\#k/w-j}(k)) \\ j = 1 & : & (P, \beta, \beta), \\ & & \beta = \infty + \text{PR}(P, \phi^1_{\#k/w}(k)) \end{array} \right. , \end{array}$$

де $\text{PR}(P, \phi^w_j(k))$ – функція, що повертає точку з таблиці передобчислень для точки P. Функція вибору операційних біт може бути подана у такому вигляді:

$$\phi^w_i(k) = \{k_{dw+i}, k_{d(w-1)+i}, \ldots, k_i\}, d = \lfloor \#k/w \rfloor.$$

Функція, що визначає усі біти, які необхідні для обчислення кроків в інтервалі $[0, i]$, може бути подана як

$$\Phi^w(i, k) = \phi^w_i(k) || \phi^w_{i-1}(k) || \ldots || \phi^w_1(k).$$

Модифікований алгоритм має такий вигляд:

1. Вхід: загальносистемний параметр G, порядковий номер обчислення N, обсяг кеша j, вікно алгоритму w, кеш (k', G').

2. Вихід: kG.

3. Обчислення:

а) якщо $N \equiv 0 \mod 2$:

1) обчислити $k \leftarrow \Gamma$, де Γ – генератор випадкових послідовностей;
2) обчислити кеш $\left(\Phi_j^w(k), f_j^w(k, G)\right)$;
3) завершити обчислення $kG \leftarrow f_{\#k}^w(k, G)$ зі стану G';
4) $N \leftarrow N + 1$.

б) інакше (якщо $N \equiv 1 \mod 2$):

1) обчислити $k \leftarrow \Gamma$, де Γ – генератор випадкових послідовностей;
2) обчислити $k'' \leftarrow \Phi_j^w(k)$;
3) завершити обчислення $kG \leftarrow f_{\#k}^w(k, G)$ зі стану (k', G');
4) $N \leftarrow N + 1$.

Досліджено, що метод є безпечним, доки $(\#k - \#\Phi^w(\xi, k)) > \sqrt{\#k}$, тобто

$$\#k - \#k^{-1} > 2^{\xi \times w}.$$

У п'ятому розділі наведено результати моделювання визначеного в третьому розділі протоколу автентифікації засобу криптографічного захисту та схем ЕЦП з відновленням повідомлення стандарту ISO/IEC 9796-3.

Для моделювання та пошуку уразливостей запропонованого протоколу використовувались засоби Casper/FDR. У процесі дослідження атак на протокол не було знайдено.

В процесі моделювання прискорення алгоритмів скалярного множення реалізовано схеми ЕЦП з відновленням повідомлення і доповненням у групі точок еліптичної кривої: ECNR, ECMR, ECAO, ECKNR, ECPV в $GF(P)$, $GF(2^m)$ для афінного, проективного та змішаного базисів. У таблиці 1 наведено окремі отримані результати вимірювань для обчислень у $GF(P)$. Як можна побачити, з наведених результатів, прискорення становить до 25% для повільного процесору Intel Atom.

Моделювання виконувалось за допомогою таких бібліотек та засобів: GCC (4.7), GMP, GF2X, NTL. Тексти програмного коду моделі доступні за адресою `http://code.google.com/p/iso-iec-9796-3/`. У таблиці 1 наведено деякі результати вимірювань у $GF(p)$, де ЦП – модель процесору A) Intel Atom N550, 1.5ГГц, 1Мб L2 кеш C) Intel Core2Duo E8500, 3Ггц, 6Мб L2 кеш; ЕЦП – схема цифрового підпису; n – порядок групи точок ЕК; Comb – результати за відомим алгоритмом Comb; ϵ – результати за модифікованим алгоритмом Comb з $i = \epsilon$ відповідно до (7).

Таблиця 1

Результати вимірювань швидкості обчислень ЕЦП (підписів/с).

ЦП	ЕЦП	$\log_2 n$	Comb	$\epsilon = 0$	$\epsilon = 1$	$\epsilon = 2$	$\epsilon = 3$	$\epsilon = 4$	$\epsilon = 7$	$\epsilon = 8$	$\epsilon = 9$	$\epsilon = 10$	$\epsilon = 11$
A	ECNR	158	1190.48	1190.48	1190.48	1190.48	1250	1250	1351.35	1428.57	-	-	-
		161	1219.51	1219.51	1219.51	1250	1282.05	1315.79	1428.57	1428.57	1515.15	-	-
		192	847.458	833.333	847.458	847.458	877.193	892.857	943.396	980.392	1000	1041.67	1063.83
	ECMR	158	1162.79	1162.79	1162.79	1190.48	1219.51	1250	1388.89	1388.89	-	-	-
		161	1190.48	1190.48	1219.51	1219.51	1250	1282.05	1388.89	1428.57	1470.59	-	-
		192	877.193	862.069	833.333	847.458	862.069	877.193	943.396	961.538	961.538	1000	1041.67
	ECAO	158	1162.79	1190.48	1162.79	1190.48	1250	1282.05	1388.89	1388.89	-	-	-
		161	1190.48	1219.51	1190.48	1250	1250	1315.79	1428.57	1428.57	1515.15	-	-
		192	877.193	877.193	847.458	847.458	862.069	877.193	943.396	980.392	980.392	1020.41	1041.67
	ECPV	158	1136.36	1162.79	1162.79	1219.51	1190.48	1250	1351.35	1388.89	-	-	-
		161	1219.51	1190.48	1190.48	1219.51	1250	1282.05	1388.89	1428.57	1470.59	-	-
		192	862.069	877.193	877.193	892.857	909.091	943.396	1000	1000	1041.67	1063.83	1086.96
	ECKNR	158	1162.79	1162.79	1190.48	1190.48	1250	1250	1351.35	1428.57	-	-	-
		161	1190.48	1219.51	1190.48	1250	1250	1315.79	1428.57	1428.57	1515.15	-	-
		192	877.193	877.193	892.857	892.857	925.926	943.396	1000	1020.41	1063.83	1063.83	1111.11
C	ECNR	158	7894.74	7500	7894.74	7894.74	8108.11	8333.33	9090.91	9090.91	-	-	-
		161	7894.74	7894.74	7894.74	7894.74	8333.33	8333.33	9090.91	9375	9677.42	-	-
		192	6666.67	6521.74	6521.74	6818.18	6818.18	6976.74	7500	7500	7894.74	7894.74	8108.11
	ECMR	158	7692.31	7500	7500	7894.74	7894.74	8108.11	8823.53	9090.91	-	-	-
		161	7692.31	7500	7894.74	7894.74	8108.11	8108.11	8823.53	9375	9375	-	-
		192	6382.98	6382.98	6521.74	6666.67	6666.67	6976.74	7142.86	7500	7692.31	7894.74	7894.74
	ECAO	158	7692.31	7500	7500	7894.74	7894.74	8108.11	8823.53	9090.91	-	-	-
		161	7692.31	7692.31	7692.31	7894.74	8108.11	8333.33	8823.53	9090.91	9677.42	-	-
		192	6382.98	6521.74	6521.74	6818.18	6818.18	6818.18	7317.07	7692.31	7692.31	7894.74	8108.11
	ECPV	158	7500	7500	7692.31	7692.31	7894.74	8108.11	8823.53	9090.91	-	-	-
		161	7692.31	7500	7692.31	7894.74	8108.11	8108.11	8823.53	9375	9375	-	-
		192	6382.98	6382.98	6521.74	6666.67	6666.67	6818.18	7317.07	7500	7692.31	7894.74	7894.74
	ECKNR	158	7692.31	7500	7500	7894.74	7894.74	8108.11	8823.53	9090.91	-	-	-
		161	7894.74	7500	7692.31	7894.74	8333.33	8108.11	8823.53	9090.91	9677.42	-	-
		192	6521.74	6382.98	6382.98	6521.74	6666.67	6818.18	7317.07	7317.07	7692.31	7692.31	8108.11

ВИСНОВКИ

Удосконалення та подальший розвиток інфраструктур відкритих ключів, у першу чергу системи ЕЦП, суттєво залежить від вирішення ряду проблемних питань, які пов'язані з підвищенням захищеності від виниклих в останні часи загроз, підвищення швидкодії, апаратної реалізації ЕЦП тощо. На сьогодні достатньо добре розроблено основні складові, що стосуються стандартизації методів, механізмів та засобів ЕЦП. В умовах розвитку та поширення апаратно - програмних, апаратних та програмних засобів КЗІ набула актуальності задача автентифікації та перевірки криптографічних пристроїв. Крім того, у зв'язку зі зменшенням складності відомих криптографічних перетворень, особливо асиметричного типу, для ряду криптографічних протоколів проблемною та актуальною задачею стало зменшення складності виконання складових ЕЦП, тобто підвищення швидкодії.

У результаті теоретичних та експериментальних досліджень, які виконано в роботі, розв'язано ряд наукових і практичних задач, які стосуються виконання ЕЦП з використанням засобів КЗІ, що забезпечують захист від їх використання несанкціонованим способом та підвищення в ряді випадків їх швидкодії.

Як основні наукові результати можна виділити такі: удосконалено метод ЕЦП, що визначений в Національному стандарті ДСТУ 4145:2002, який відрізняється від прототипу властивостями відновлення повідомлення та дозволяє ефективно підписувати групи коротких повідомлень за умов незначної модифікації існуючих засобів, що реалізують даний стандарт ЕЦП; вперше запропоновано метод захисту від атаки повного розкриття за відомими результатами криптографічних перетворень, який застосовується за умови підміни апаратного засобу КЗІ та дозволяє забезпечити безпечний розподіл апаратних засобів КЗІ, що реалізують алгоритми ЕЦП; вперше запропоновано метод модифікації алгоритмів скалярного множення у групі точок ЕК, що використовуються для обчислення ЕЦП,який дозволяє підвищити швидкодію засобу ЕЦП від 18 до 25%.

У практичному плані: запропоновано практичну модифікацію дійсного стандарту цифрового підпису України ДСТУ 4145:2002 для надання йому властивостей ЕЦП з відновленням повідомлення; практично показано, що несанкціонований доступ до засобів КЗІ дає можливість порушнику реалізовувати загрози несанкціонованого використання безпосередньо самих засобів КЗІ для виконання несанкціонованих криптографічних перетворень,наприклад, цифрового підпису, шифрування, вироблення різних видів ключів, здійснення криптографічних протоколів тощо; показано, що певні властивості загрози підміни є актуальними тільки на проміжку часу між створенням засобу КЗІ та персоналізацією модуля; запропоновано модифікацію механізму та криптографічного протоколу ISO/IEC 9798-2 № 6.1, що дозволяє практично усунути певні недоліки; практично показано, що алгоритми ЕЦП, які ґрунтуються на перетвореннях у групі точок еліптичної кривої, мають схожу обчислювальну складність,

а найбільш швидким є ECNR; встановлено експериментально, що швидкодію обчислень скалярного множення у цифровому підписі можна збільшити до 25% за рахунок кешування частин ключа сесії, причому з використанням методу в схемі обчислення цифрового підпису, збільшення швидкості, в залежності від частки скалярного множення в часі обчислення підпису, що знаходиться в діапазоні 18–24%.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Шевчук О. А. Актуальність атаки на зв'язанних ключах для апаратних реалізацій засобів КЗІ / О. А. Шевчук // Радиотехника. — 2011. — № 166. — С. 70—75.

2. Шевчук О. А. Алгоритми відновлення повідомлення ЕЦП стандарту ISO/IEC 9796-3 та екзистенціальна підробка підписів, що засновується на них / О. А. Шевчук // Прикладная радиоэлектроника. — 2011. — Т. 10, № 2. — С. 183—187.

3. Шевчук О. А. Особливості ЕЦП з відновленням повідомлення / О. А. Шевчук // Прикладная радиоэлектроника. — 2010. — Т. 9, № 3. — С. 489—492.

4. Шевчук О. А. Схеми ЕЦП для груп підписів скорочених повідомлень / О. А. Шевчук // Прикладная радиоэлектроника. — 2012. — Т. 11, № 2. — С. 240—244.

5. Шевчук О. А. Метод прискорення скалярного множення для криптографічних додатків / О. А. Шевчук, І.Д. Горбенко // Радіоелектронні і комп'ютерні системи. — 2012. — Май. — С. 86—90.

6. Шевчук О. А. Аналіз властивостей та областей застосування цифрових підписів стандарту ISO/IEC 9796-3 / О. А. Шевчук, Ю. І. Горбенко // Прикладная радиоэлектроника. — 2009. — Т. 8, № 3. — С. 304—314.

7. Шевчук А. А. Модель построения эффективных клиент-серверных решений с большой нагрузкой /А. А. Шевчук // Материалы XII Международного молодежного форума "Радиоэлектроника и молодежь в XXI веке", 2008. — Харьков: ХНУРЭ, 2008. — С. 54.

8. Шевчук А. А. Цифровые подписи с восстановлением сообщения стандарта ISO/IEC 9796-3 /А. А. Шевчук, Ю. И. Горбенко // Материалы XII Международной научно-практической конференции "Безопасность информации в информационно - телекоммуникационных системах", 19 мая 2009. — Киев: ЧП "ЕКМО", НИЦ "ТЕЗИС", НТУУ "КПИ", 2009. — С. 42.

9. Шевчук А. А. Принципы построения и применения IP шифраторов серии "КАНАЛ" /А. А. Шевчук, Ю. И. Горбенко, В. А. Бобух // Материалы XIII Международной научно-практической конференции "Безопасность информации в информационно - телекоммуникационных системах", 18 мая 2010. — Киев, 2010. — С. 37—38.

10. Шевчук А. А. Сравнительный анализ и применение ЭЦП с восстановлением /А. А. Шевчук, Ю. И. Горбенко, А. И. Пушкарев // Материалы XIII Ме-

ждународной научно-практической конференции “Безопасность информации в информационно - телекоммуникационных системах”, 18 мая 2010. — Киев, 2010. — С. 44—45.

11. Шевчук О. А. Використання відомого зв’язку між сеансовими ключами у схемах ЕЦП з відновленням повідомлення / О. А. Шевчук // Материалы XIV Международной научно-практической конференции “Безопасность информации в информационно - телекоммуникационных системах”, 17 мая 2011. — Киев, 2011. — С. 92.

12. Шевчук А. А. Схемы ЭЦП для множеств коротких сообщений / А. А. Шевчук // Материалы XV юбилейной международной научно-практической конференции “Безопасность информации в информационно - телекоммуникационных системах”, 22 мая 2012. — Киев, 2012. — С. 108.

13. Шевчук О. А. Загальна оцінка впливу функції конвертації точки на стійкість цифрового підпису до екзистенційної підробки / О. А. Шевчук // Мат. конф. “Современные проблемы математики и ее приложения в естественных науках и информационных технология”, 17 апреля 2011. — Харьков, 2011. — С. 192—193.

14. Шевчук А. А. Анализ уязвимости схем ЭЦП к атаке на связанных ключах / А. А. Шевчук, И. Д. Горбенко // Сборник трудов второй Международной научно-технической конференции “Компьютерные науки и технологии”, 3-5 октября 2011. — Белгород, 2011. — С. 411—414.

15. Шевчук О. А. Метод прискорення скалярного множення для криптографічних додатків / О. А. Шевчук // Труды научно-технической конференции с международным участием “Компьютерное моделирование в наукоемких технологиях”, 2012. — Харьков, 2012. — С. 473—474.

АНОТАЦІЯ

Шевчук О.А. Методи та засоби ЕЦП з заданим рівнем захищеності та підвищеною швидкодією. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. – Харківський національний університет радіоелектроніки, Харків, 2013.

Дисертаційна робота присвячена удосконаленню методів вироблення електронного цифрового підпису повідомлень. Вперше запропоновано метод модифікації алгоритмів скалярного множення у групі точок ЕК, що використовуються для обчислення ЕЦП, який ґрунтується на частковому кешуванні множника та відповідної модифікації генератора псевдовипадкових послідовностей і дозволяє підвищити швидкодію засобу ЕЦП. Корисний ефект досягається за рахунок дублювання частини випадкового сеансового ключа між операціями обчислення скалярного множення. Удосконалено метод ЕЦП, який визначено у Національному стандарті ДСТУ 4145:2002, та відрізняється від

прототипу зміною функції ґешування повідомлення на функцію створення доданої збитковості, що дозволяє зменшити обсяг ЕЦП для групи повідомлень, в залежності від характеристик повідомлення. Сутність удосконалення полягає у використанні повного відновлення повідомлення з цифрового підпису. Стверджується, що в такому випадку заданий рівень стійкості можна досягти з використанням меншого обсягу повідомлення. Показується сумісність цифрового підпису національного стандарту ДСТУ 4145:2002 з відомими підписами з відновленням повідомлення, які ґрунтуються на перетвореннях у групі точок еліптичної кривої. Вперше запропоновано метод захисту від атаки повного розкриття за відомими результатами криптографічних перетворень, яка здійснюється за умови підміни апаратного засобу КЗІ, що ґрунтується на модифікації алгоритму автентифікації ISO/IEC 9798-2 6.1, шляхом зміни криптографічних перетворень з симетричних на перетворення з відкритим ключем, для обміну користувача з третьою довіреною стороною, що дозволяє забезпечити безпечний розподіл апаратних засобів ЕЦП, які реалізують алгоритми ЕЦП, в умовах існування загрози підміни засобу криптографічного захисту. Досліджено уразливість апаратних засобів ЕЦП, які використовують DSA подібні схеми цифрового підпису, до підміни засобу до етапу персоналізації. Сутність запропонованого методу полягає в створенні відносин довіри з виробнком засобів ЕЦП та верифікації засобу під час персоналізації за допомогою тристороннього протоколу автентифікації.

Ключові слова: цифровий підпис, автентифікація, скалярне множення у групі точок еліптичної кривої, апаратні засоби ЕЦП.

АННОТАЦИЯ

Шевчук А.А. Методы и средства ЭЦП с заданным уровнем защищенностью и повышенным быстродействием. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – Системы защиты информации. – Харьковский национальный университет радиоэлектроники, Харьков, 2013.

Диссертационная работа посвящена улучшению методов формирования электронной цифровой подписи сообщений. Впервые предложен метод модификации алгоритмов скалярного умножения в группе точек эллиптической кривой, который используется для вычисления ЭЦП и основывается на частичном кешировании множителя и соответствующей модификации генератора псевдослучайных последовательностей, что позволяет увеличить быстродействие средства ЭЦП. Полезный эффект достигается за счет дублирования и замены части случайного ключа сессии, вместо использования случайного значения. Такая конструкция позволяет использовать кеширование промежуточных результатов, полученных во время выполнения операции скалярного умножения в группе точек эллиптической кривой. Метод сохраняет уровень стойкости за

счет ограничения на максимальный объем дублирования. Улучшен метод ЭЦП, описанный в Национальном стандарте ДСТУ 4145:2002, отличающийся от прототипа сменой функции хеширования на формирование сообщения для восстановления с дополнением. Модификация позволяет уменьшить объем цифровой подписи выполненной для группы сообщений. Предложения основывается на анализе занимаемого объема подписи. Показано, что цифровая подпись сообщения объемом меньшим, чем битовый эквивалент заданного уровня стойкости занимает больший объем чем само сообщение. Показана совместимость отдельных элементов ЭЦП с восстановлением и дополнением сообщения. Впервые предложен метод защиты от атаки полного раскрытия при условии подмены аппаратного средства ЭЦП, реализующего преобразования в группе точек эллиптической кривой. Суть атаки заключается в подмене аппаратного средства цифровой подписи на такое, которое не обеспечивает должной случайности ключа сессии, до этапа персонализации. Показано, что сложность детектирования атаки сравнима со сложностью решения задачи поиска дискретного логарифма в группе точек эллиптической кривой. Предложен протокол аутентификации.

Ключевые слова: цифровая подпись, аутентификация, скалярное умножение в группе точек эллиптической кривой, аппаратные средства ЭЦП.

ABSTRACT

Shevchuk O.A. Digital signatures with higher speed. - Manuscript. Thesis for a candidate's degree by specialty 05.13.21 - Information Security Systems. - Kharkiv National University of Radio Electronics, Kharkiv, 2013.

Dissertation work is devoted to improvement of the digital signature computation methods. Introduced new modification method for cryptographic digital signature schemes based on elliptic curves. Proposed method adds additional level of caching in suitable algorithms of scalar multiplication. Combined with modification of PRNG method can achive up to 25% of computation boost, with reduced upper level of brute force attack. Introduced modification of the digital signature method, described in the Ukrainian DSTU 4145:2002 National standard. Proposed to change the hashing subrouine to message recovery generator. Such modification allows to reduce digital signature size without modification already created hardware security modules.Introduced the method of protection against attack of full disclosure on hardware security modules, which deployed with impersonalized state. In case of successful substitution of such module attacker can compromise secret keys with several digital signatures. Introduced authentication scheme for hardware cryptographic modules.

Keywords: the digital signature, authentication, scalar multiplication in group of points of an elliptic curve, hardware security module.