МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Коваленко Богдан Анатолійович

УДК 004.056.55

Методи побудови та оцінки стійкості клептографічних механізмів у гібридних криптосистемах

Спеціальність: 05.13.21 – Системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2020

Дисертацією є рукопис.

Робота виконана в Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського».

Науковий керівник:	доктор технічних наук, старший науковий співробітник **Кудін Антон Михайлович**, професор кафедри математичних методів захисту інформації Фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
Офіційні опоненти:	доктор технічних наук, професор **Шелест Михайло Євгенович**,професор кафедри математичного моделювання Національного університету «Чернігівська політехніка».
	доктор технічних наук, старший науковий співробітник **Чевардін Владислав Євгенович**, начальник кафедри захисту інформації та кіберзахисту Військового інституту телекомунікацій та інформатизації ім. Героїв Крут.

Захист відбудеться 17 вересня 2020 р. о 15-00 на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, м. Київ, просп. Любомира Гузара 1, ауд. 11-111.

З дисертацією можна ознайомитись у бібліотеці Національного авіаційного університету за адресою: 03058, м. Київ, просп. Любомира Гузара 1.

Автореферат розісланий 17 серпня 2020 р.

Учений секретар спеціалізованої
вченої ради Д 26.062.17
д.т.н., доцент Гнатюк С.О.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. З огляду на широке розповсюдження використання гібридних криптосистем у інформаційно-телекомунікаційних системах, особливої гостроти набувають задачі захисту даних криптосистем на всіх рівнях життєвого циклу: на етапі проектування, реалізації, розгортання та використання. Однією з характеристик сучасних криптосистем є розповсюдження їх використання в тому числі і в пристроях, які не відповідають стандартам з безпеки реалізації, що породжує нові вектори атак, зокрема клептографічних атак, наприклад, з модифікацією реалізації криптосистеми на кінцевому пристрої. Такі типи атак є особливо небезпечними, враховуючи той факт, що жертва зловмисника, будучи частиною певної захищеної системи (електронного документообігу, платіжної системи, секретного зв'язку тощо), може нести загрозу також для не скомпрометованих учасників системи (наприклад, витік спільних секретних даних). Можливими напрямками вирішення цієї проблеми є побудова криптосистем, стійких до різних типів клептографічних атак; розробка критеріїв наявності (відсутності) клептографічних закладок у примітивах; синтез криптографічних систем та криптопримітивів з закладками з метою розширення множини шаблонів проектування закладок для дослідження методів виявлення та протидії.

Клептографія вивчає методи синтезу та аналізу каналів прихованого витоку секрету (embedded trapdoor, subliminal channel) на базі криптосистем, що дозволяють особі, що впровадила канал (Розробник), отримати певну чутливу інформацію криптосистеми.

Клептографія, як напрямок інформаційної безпеки, тісно пов'язана як з криптологією так і зі стеганографією, що можна відобразити схемою (див. Рис. 1).

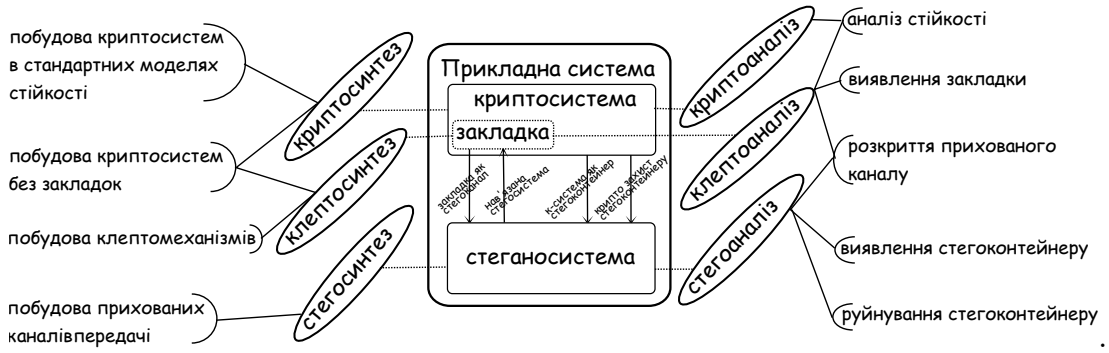

Рис. 1. Зв'язок між клептографією, криптологією та стеганографією

На даний момент, основним напрямом клептографічної діяльності є синтез криптосистем та примітивів із закладками, що має практичне значення. Проте методи захисту від клептографічних атак наразі зводяться до традиційного криптоаналізу потенційно вразливих систем, до певних інтуїтивних рекомендацій (яких далеко не завжди дотримуються) щодо процесу розробки та до базових

заходів захисту програмно-апаратних комплексів. Одна з найвідоміших формально описаних клептографічних систем є SETUP (Secretly Embedded Trapdoor with Universal Protection), який був запропонований А. Яном та М. Юном у 1996 році та дозволяє організувати непомітну передачу секретного ключа криптосистем на базі RSA та задачі дискретного логарифму. Не зважаючи на широку та давню відомість цих методів, спроби протидії SETUP зводяться переважно до контролю цілісності реалізацій, що може бути не завжди ефективно. Серед вітчизняних та постсовєтських авторів, найближчими до клептографічної тематики є роботи Шелеста М.Є, Задіраки В.К., Прогонова Д.О., Мельникова Ю.Н., Жукова О.Е., Міщенка В.О., проте ці роботи здебільшого сфокусовані на проблемах стеганографії і лише поверхнево – клептографії. Відсутність системного підходу до побудови криптосистем стійких до клептографічних атак та методів оцінки систем щодо наявності закладок призводить до ризиків інформаційної безпеки, які підвищуються з ростом розповсюдженості криптосистем та довіри до розробника криптосистеми.

Таким чином, видається доцільним створення методів побудови криптосистем та криптопримітивів з доведеної стійкістю до клептографічних атак, а також створення науково обґрунтованих підходів до оцінки ризиків наявності закладок у примітивах на етапі розробки та конкурсних відборів що і є основою досліджень даної роботи.

Зв'язок роботи з науковими програмами, планами, темами. Робота над дисертацією проводилася в рамках науково-дослідних проектів «Корифена» (номер держреєстрації 0118U001653) на замовлення Служби зовнішньої розвідки України, «Родоліт» (номер держреєстрації 0111U007473) на замовлення Служби безпеки України та Національного банку України, що підкріплено двома актами впровадження.

Мета та задачі досліджень. Метою дисертаційної роботи є підвищення рівня захищеності гібридних криптосистем проти клептографічних атак, що передбачає побудову методів виявлення та синтезу клептографічних механізмів в гібридних криптосистемах.

Для досягнення поставленої мети необхідно вирішити такі задачі:

1. Провести аналіз відомих методів побудови клептографічних механізмів.
2. Формалізувати клас протоколів типу «запит-відповідь» у клептографічному контексті.
3. Розробити критерії відсутності клептографічної модифікації реалізації протоколу та побудувати протоколи з доведеною відсутністю клептографічних закладок.
4. Розробити методи побудови клептографічних лазівок геш-функцій з метою визначення загальних принципів впровадження клептографічних лазівок в криптографічні примітиви.
5. Розробити метод виявлення клептографічних лазівок в криптопримітивах.

Об'єкт дослідження: процес клептографічної модифікації реалізацій криптосистем.

Предмет дослідження: методи побудови криптосистем з доведеною неможливістю непомітного вбудовування клептографічної закладки у дану криптосистему.

Методи досліджень. Основу дисертаційних досліджень складають теоретичні дослідження. Для аналізу існуючих методів побудови клептомеханізмів застосовувалися методи абстрактної алгебри, теорії складності обчислень та методів математичної логіки. Для отримання достатніх умов відсутності каналу, а також для зведення стійкості функції стиснення гешу до складності задачі дискретного логарифмування використовувалися методи теорії складності обчислень, теорії алгоритмів та методи лінійної алгебри.

Наукова новизна одержаних результатів. Підсумком розв'язання зазначених задач є такі нові наукові результати, що висуваються на захист:

1. Вперше запропоновано математичну модель для протоколів типу «запит-відповідь» у клептографічному сенсі, яка за рахунок використання моделі практичної нерозрізненості та базових властивостей клептографічного каналу витоку для оцінки стійкості протоколу дозволяє формалізувати клептографічну лазівку у широкому класі криптографічних протоколів.
2. Вперше отримані достатні умови неможливості непомітної клептографічної модифікації криптосистеми, які за рахунок сформульованої теореми та її наслідку дозволяють проектувати протоколи, що є стійкими до побудови каналу непомітного витоку.
3. Вперше розроблено метод побудови функції гешування з клептографічним механізмом, який за рахунок використання перетворення на базі задачі дискретного логарифмування в одній із стандартних конструкцій функції стиснення, що стійкі до колізій, та схемі Меркла-Дамгарда, дозволяє Розробнику ефективно відновлювати частину повідомлення за відомим геш-кодом.
4. Вперше запропонована метрика «клептографічного потенціалу» як кількість інформації Розробника, що передається у структуру примітиву, яка за рахунок оцінювання надлишковості параметрів у структурі криптографічного примітиву дозволяє порівнювати різні криптопримітиви за ризиком наявності клептографічного механізму в них.
5. Вдосконалено загальну класифікацію вразливостей реалізацій криптосистем Б. Шнаєра, яка за рахунок порівняння за рядом критеріїв, а саме, за закритістю реалізації, за деструктивністю, за рівнем побудови та за способом впровадження, дозволяє систематизувати існуючі клептографічні механізми.
6. Отримано подальший розвиток методу Пренеля побудови шифру на основі схеми Фейстеля з вбудованими диференційними шляхами високої ймовірності. За рахунок застосування його в основі функції стиснення геш-функції, дозволяє будувати новий тип закладок, що дозволяє Розробнику отримувати обчислювальну перевагу у спеціальних режимах роботи функції гешування (наприклад, у застосуванні в протоколах консенсусу технології блокчейн).

Практичне значення одержаних результатів.

1. Запропоновані модифікації алгоритмів базових протоколів генерації nonce та узгодження ключа Діффі-Хеллмана, які є доведено стійкими до клептографічної модифікації реалізації що дозволяє підвищити рівень захищеності криптосистеми за припущення часткової компрометації одного з учасників.
2. Запропоновані алгоритм та програмна реалізація мовою Python3 функції стиснення, що може бути використана у конструкції Меркла-Дамгарда та містить клептографічний механізм, дозволяє розробнику практично відновлювати повідомлення (за додаткових умов) за відомим геш-кодом.
3. Для лазівки у блокчейн протоколах консенсусу Proof-of-Work отримані оцінки переваги Розробника для різної кількості контрольованих бітів та ймовірності допоміжних диференційних шляхів, що демонструє необхідність подальших досліджень безпеки блокчейн систем у клептографічному контексті.
4. Для ряду примітивів (геш-функцій та алгоритмів симетричного шифрування) були отримані оцінки клептографічної надлишковості. Розрахунки показали, що серед розглянутих алгоритмів найбільша клептографічна надлишковість у російського стандарту геш-функції ГОСТ Р 34.11-2012 («Стрибог») – 12582.19 біт (тобто за даною метрикою, алгоритм має найбільший ризик наявності клептографічного механізму). Натомість, найменша клептографічна надлишковість спостерігається в стандарті блокового шифрування AES – 32.

Особистий внесок здобувача. У [6, 7] автором запропонована модель протоколу типу «запит-відповідь» з вбудованим каналом витоку секрету, сформульована та доведена теорема про достатні умови відсутності каналу витоку у протоколі та запропоновані деякі базові протоколи стійкі до побудови SETUP; в [2] автором проаналізована можливість переносу методів диференційного аналізу блокових шифрів на функції гешування, які мають у структурі блоковий фейстелівський шифр, що дозволяє будувати клептографічні лазівки спеціального виду; у роботі [3] автором запропоновано удосконалений метод автоматичного пошуку множин диференційних шляхів великої ймовірності у геш-функціях для пошуку клептографічних лазівок, що базуються на множинах таємних диференційних шляхів; у роботі [1] автором досліджені спеціальні режими роботи геш-функцій, що можуть вести до нових типів клептографічних лазівок; в статті [4] досліджуються можливості побудови лазівки в геш-функціях.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідались на всеукраїнських конференціях та семінарах: XIII Всеукраїнська науково-практична конференція студентів, м. Київ, 21-23 травня 2015 р. [8];X Міжнародна науково-практична конференція, м. Івано-Франківськ, 27-29 травня 2015 р. [9]; семінар «Проблеми сучасної криптології», 21 квітня 2016 р.; семінар «Методи обчислювальної математики та математичне моделювання процесів в неоднорідних середовищах», 26 лютого 2019 р; конференція «High Performance Computing», Київ, 22-23 жовтня 2018 р.; міжнародна конференція

«Стан та удосконалення безпеки інформаційно-телекомунікаційних систем», Миколаїв, 19-21 червня 2019 р. [11]; міжнародна конференція «Development of modern technologies and scientific potential of the world», Лондон, 29 червня 2019 р. [10]; міжнародна конференція «20th Central European Conference on Cryptology», Загреб, 24-26 червня 2020 р. [12].

Публікації. Основні результати дисертаційної роботи опубліковано в 12 роботах [1-12], з них 1 – у виданні, що входить в наукометричну базу SCOPUS, 5 – в інші наукометричні бази, 1 – електронний журнал Міжнародної асоціації криптографічних досліджень (IACR).

Структура роботи та її обсяг. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, 4 розділів, загальних висновків, 2 додатків, списку використаних джерел, і має 107 сторінок основного тексту, 11 рисунків, 7 таблиць, 4 сторінки додатків. Список використаних джерел містить 90 найменувань і займає 10 сторінки. Загальний обсяг дисертаційної роботи – 131 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми, сформульовано мету та задачі досліджень, відображено наукову новизну і практичну значимість отриманих результатів, впровадження отриманих результатів та їх апробація.

У першому розділі проводиться огляд сучасного стану клептографічних досліджень, відомих методів та прецедентів використання клептографічних схем.

Наводяться такі приклади криптопримітивів: алгоритм симетричного шифрування DES (структура якого послаблена, ймовірно, для надання можливості АНБ США проводити практичне дешифрування та відновлення ключа), генератор псевдовипадкової послідовності DualEC DRGB (якщо параметри алгоритму згенеровані залежними між собою, то розробник, який знає цю залежність, може ефективно прогнозувати вихід генератора), потенційні закладки у російських стандартах гешування ГОСТ Р 34.11-2012 та шифрування ГОСТ Р 34.12-2015 (ряд робіт вказують на неясність принципів генерації констант та їхню надлишковість, що наводить на підозри про наявність закладок), закладки у структурі еліптичної кривої та канали витоку секрету на базі задач RSA та дискретного логарифмування.

У другому розділі розроблено теоретичні основи захисту криптосистем від клептографічних атак.

На базі проведеного аналізу удосконалено класифікацію Шнаєра клептографічних примітивів за декількома критеріями (див. табл. 1). Автор використовує поняття практичної нерозрізненості для формалізації клептографічної лазівки, оскільки вони є практичними односторонніми функціями, що загалом не підпадають під модель теоретико-інформаційної чи обчислювальної складності.

Таблиця 1

Класифікація клептографічних механізмів

Класифікація	Тип клептомеханізму	Приклади
За закритістю реалізації	відкриті стандартизовані реалізації	програмні бібліотеки, схемотехнічні описи, специфікації алгоритмів
	закриті реалізації	пропрієтарні програмні продукти з обфускацією програмного коду та потоків даних
	апаратні реалізації	криптографічні мікроконтролери, апаратні криптомодулі
За наслідками аналізу	недеструктивні (з можливістю подальшого використання)	аналіз програмних компонент, маскованих апаратних компонент, логічний аналіз специфікацій тощо
	деструктивні (без можливості подальшого використання)	аналіз криптографічних контролерів, вбудованої EEPROM-пам'яті тощо
За рівнем побудови	модифікація готових криптосистем	додавання каналу витоку в реалізацію системи, наприклад, атака BEAST протоколу TLS1.0 і нижче
	побудова нових криптоалгоритмів з вбудованими закладками	приклади ймовірно таких алгоритмів: DES, DualEC DRGB
За способом впровадження	модифікація працюючих криптосистем на стороні користувача	через троянські програми, використання вразливостей веб інтерфейсу та інші кібератаки
	відкрите розповсюдження клептографічних модифікацій реалізацій алгоритмів	наприклад, у вигляді програмних компонентів
	розповсюдження пропрієтарних закритих криптосистем у вигляді апаратних модулів	
	лобіювання стандартизації клептографічних криптосистем, нав'язування їхнього використання через правові механізми, корпоративні політики чи маркетингові кампанії	

Визначення 1. (Практичний класифікатор ансамблів) Нехай існує два ансамблі $E = \{e_1, e_2, ...\}$ та $E' = \{e'_1, e'_2, ...\}$, $e_i, e'_i \in S$, де S – скінчена множина. Додатково заданий часовий поріг t, максимальний час, що відпускається на виконання алгоритму (наприклад, $t = 2^{80}$).

Класифікатором ансамблів називатимемо ймовірнісний розпізнавальний алгоритм A_t, обмежений часом роботи t, що для вектору довжини l, $\vec{\nu} \in E^l \cup E'^l$,

повертає значення:

$$\begin{cases} A_t(E, \vec{\nu}) = 1 & \Leftrightarrow \vec{\nu} \in E^l \\ A_t(E', \vec{\nu}) = 1 & \Leftrightarrow \vec{\nu} \in E'^l \end{cases}.$$

Також визначимо перевагу (advantage) практичного класифікатора у розпізнаванні ансамблів як $Adv_{A_t}(E, E', l) = |P\{A_t(E, \vec{\nu}) = 1\} - P\{A_t(E', \vec{\nu}) = 1\}|$, де $\vec{\nu} \in E^l \cup E'^l$ – випадковий вектор довжини l.

Визначення 2. (Практична нерозрізненість) Два ансамблі E та E' називаються практично нерозрізнені (practical indistinguishable) для заданого параметру безпеки t, якщо максимальна перевага у розпізнаванні для всіх практичних класифікаторів (визначення 1) буде незначною відносно параметра безпеки: $Adv(E, E') = \max_{l,A_t}\{Adv_{A_t}(E, E', l)\} < \varepsilon(t)$, де $\varepsilon(t)$ – порогове значення для «незначної» ймовірності (наприклад, $\varepsilon(t) = 2^{-40}$ при $t = 2^{80}$).

Надалі, для практично нерозрізнених множин E та E' використовуватимемо позначення $E \simeq_t E'$.

Визначення 3. (Протокол «запит-відповідь», формальна модель) Протоколом типу «запит-відповідь» називатимемо кортеж $\langle D_t, V, U, A_t\rangle$, де:
$D_t : V \times U \to \{0, 1\}$ – ймовірнісний алгоритм, обмежений часом роботи t, що перевіряє відповідь оракула на відповідність протоколу. Кожну коректну пару запит-відповідь алгоритм розпізнає з ймовірністю 1, тобто є алгоритмом типу Монте-Карло
V – множина запитів сторони Bob, U – множина відповідей оракула Alice
$A_t : V \to U$ – рандомізований алгоритм оракула Alice без витоку секрету: $\forall v \in V : D_t(A_t(v)) = 1$

Визначення 4. (Канал витоку на базі протоколу «запит-відповідь», формальна модель) Протоколом типу «запит-відповідь» з каналом витоку називатимемо кортеж з моделі протоколу «запит-відповідь» (визначення 3) $\langle D_t, V, U, A_t, R_t^\omega, A_t^\omega\rangle$ з додатковими параметрами R_t^ω та A_t^ω (канал витоку), де D_t, V, U, A_t мають той же сенс, що і в базовій моделі:
$A_t^\omega : V \times \{0, 1\} \to U$ – рандомізований алгоритм оракула Alice з витоком секрету:

$$\forall v \in V, s \in \{0, 1\} : D_t(A_t^\omega(v, s)) = 1,$$

$v \overset{rand}{\in} V, s \in \{0, 1\} : P\{R_t^\omega(v, A_t^\omega(v, s)) = s\} > 1/2 + \varepsilon(t)$
$R_t^\omega : V \times U \to \{0, 1\}$ – ймовірнісний алгоритм, що декодує повідомлення, передане стороною Alice, на основі секрету ω.

Додатково накладаються умови секретності та непомітності каналу: множини

$$H = \{\langle v, u\rangle | v \in V, u \in U : u = A_t(v)\},$$

$$H_0 = \{\langle v, u\rangle | v \in V, u \in U : u = A_t^\omega(v, 1)\},$$
$$H_1 = \{\langle v, u\rangle | v \in V, u \in U : u = A_t^\omega(v, 0)\}$$

є попарно практично нерозрізненими: $H \simeq_t H_0 \simeq_t H_1$ (відношення $\simeq_t$ введене у визначені 2).

Також додається припущення про відсутність інформації для розробника з виходу алгоритму A_t: $|P\{R_t^\omega(v, A_t(v)) = 0\} - P\{R_t^\omega(v, A_t(v)) = 1\}| < \varepsilon(t)$.

Розроблена модель необхідна в подальшому для вирішення головної проблеми: побудови криптопротоколу з доведеною відсутністю каналів витоку.

Визначення 5. (рівність рандомізованих алгоритмів) Рандомізовані алгоритми $A_t, A'_t : \mathfrak{L}_1 \to \mathfrak{L}_2$, обмежені часом роботи t називатимемо однаковими $(A_t = A'_t)$, якщо $P\{A_t(l) \neq A'_t(l)\} < \varepsilon(t)$, $l \overset{rand}{\in} \mathfrak{L}_1$. Далі позначатимемо рівність та нерівність алгоритмів відповідно знаками $'='$ та $'\neq'$.

В роботі сформульована та доведена теорема про необхідну умову наявності каналу витоку в моделі протоколу типу «запит-відповідь» (визначення 4).

Теорема 1. (Необхідна умова наявності каналу витоку) Якщо в протоколі типу «запит-відповідь» існує канал витоку, то $\exists A_t, A'_t : V \to U$, $A'_t \neq A_t$, що $P\{D_t(v, A_t(v)) = 1\} > 1 - \varepsilon(t)$ і $P\{D_t(v, A'_t(v)) = 1\} > 1 - \varepsilon(t)$

В роботі сформульовано важливий наслідок теореми – достатні умови відсутності каналу витоку.

Наслідок. Нехай $\exists A_t, \forall v \in V : P\{D_t(v, A_t(v)) = 1\} = 1$ і

$$\forall A'_t : A'_t \neq A_t, P\{D_t(v, A'_t(v)) = 1\} = \sigma < 1 - \varepsilon(t) v \overset{rand}{\in} V$$

(нерівність $'\neq'$ згідно з визначенням 5). Тоді в протоколі неможливо побудувати канал непомітного витоку секрету. Більш того, у випадку передачі повідомлення секретним каналом, ймовірність виявлення факту цього складатиме $P \geq 1 - \sigma$.

У даному розділі також вводиться метрика «клептографічного потенціалу» для оцінки потенційної можливості наявності лазівки у криптопримітиві. множина усіх можливих алгоритмів криптопримітивів, при чому якщо $\phi(A) < \phi(B), A, B \in \mathbb{A}$, то «ризики» наявності клептомеханізму у примітиві B є вищими, тобто дана функція є метрикою «клептографічного потенціалу» криптосистеми.

Нехай, даний криптопримітив $Prim$ є функцією виду $Prim : Par \to Out$, де Par – простір вхідних параметрів (відкритий текст, ключі, стартові вектори тощо), Out – простір виходів потенційного алгоритму. Визначимо також множину всіх можливих функцій $\mathbb{F} = Par^{Out}, Prim \in \mathbb{F}$ та множину заборонених функцій $\hat{\mathbb{F}} \in \mathbb{F} : Prim \notin \hat{\mathbb{F}}$ (в контексті побудови криптопримітиву, заборонені функції – класи алгоритмів, які виключаються на етапі оцінки кандидата і раніше – алгоритми із слабкими криптографічними властивостями, вразливі до відомих типів теоретичних та практичних атак). Припустимо, Розробник володіє методом (алгоритмом), який реалізує ін'єктивну функцію, що на основі власного секрету Розробника з множини секретів Ω повертає алгоритм криптопримітиву з закладкою:

$$TrapGen_{Prim} : \Omega \to \mathbb{F}_{Prim} \backslash \hat{\mathbb{F}}_{Prim}.$$

Тепер визначимо власне клептографічний потенціал Розробника.

Визначення 6. (Клептографічний потенціал). Для криптографічного примітиву $Prim$, вимоги до вигляду та властивостей якого задають множину

функцій $R_{Prim} = \mathbb{F}_{Prim} \backslash \hat{\mathbb{F}}_{Prim}$, називатимемо клептографічним потенціалом кількість інформації, що закладена розробником у структуру примітиву, тобто:

$$\phi(Prim) = H(R_{Prim}) - H(R_{Prim}|D) \leq \log_2(|R_{Prim}|),$$

де $H(R_{Prim})$ – безумовна ентропія структури примітиву, $H(R_{Prim}|D)$ – ентропія структури примітиву за умови ініціалізації розробником. Вважатимемо, що розподіл для безумовних ймовірностей є рівномірним, що відповідає максимальній невизначеності.

Оцінити клептографічний потенціал за визначенням 6 є практично складною задачею через нетривіальність обмежень на множини допустимих функцій. Більш практичним є поняття «клептографічної надлишковості», яке вводиться далі.

Визначення 7. (Клептографічна надлишковість). Клептографічною надлишковістю криптопримітиву $Prim$ із класу альтернативних алгоритмів, заданого відношенням $R^{\simeq}_{Prim}$ називатимемо кількість інформації, що може бути закладена Розробником у структуру примітиву через вибір представника із класу альтернативних алгоритмів:

$$\rho_{\simeq}(Prim) = H(R^{\simeq}_{Prim}) - H(R^{\simeq}_{Prim}|D) \leq \log_2(|R^{\simeq}_{Prim}|).$$

В роботі сформальована та доведена теорема про те, що клептографічна надлишковість є оцінкою знизу клептографічного потенціалу.

Теорема 2. Клептографічна надлишковість (визначення 7) є оцінкою знизу для клептографічного потенціалу (визначення 6):

$$\phi(Prim) \geq \rho_{\simeq}(Prim).$$

Відношення еквівалентності, від якого залежить значення клептографічної надлишковості, може обиратися різними способами.

В роботі наведені базові правила, що можуть визначати відношення еквівалентності криптопримітивів. Правила можуть зберігати еквівалентність алгоритмів, наприклад, при зміні раундових констант на довільні інші, заміні блоків підстановки, стартових векторів тощо (зі збереженням заданих криптографічних властивостей примітиву).

Стосовно визначення строгого порядку на множині, головна вимога до впорядкування – Розробник конкретного примітива не повинен впливати на визначення порядку, тобто метод вибору порядку має бути заздалегідь узгоджений між учасниками.

В роботі розроблена базова схема процесу зменшення клептографічних ризиків гібридної криптосистеми (див. Рис. 2).

Компонентами даної схеми є база відомих клептографічних механізмів, база відомих криптографічних примітивів та протоколів та власне цільова гібридна криптосистема. Основа схеми – неперервна взаємодія паралельних процесів (блоків), кожен з яких відповідає за свою підзадачу. Компонентами схеми

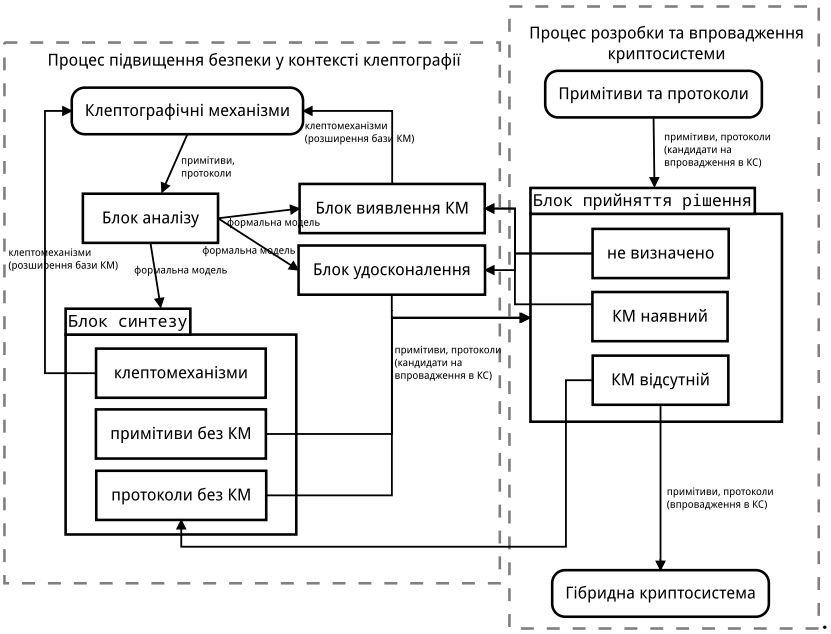

Рис. 2. Схема процесу зменшення клептографічних ризиків гібридної криптосистеми

є блоки аналізу (аналіз клептографічних механізмів, класифікація, побудова формальної моделі), синтезу (побудова криптосистем з клептомеханізмами та з доведеною відсутністю закладок), виявлення клептомеханізмів (детектування та клептоаналіз), удосконалення (модифікація базової криптосистеми до криптосистеми вільної від клептомеханізмів).

У третьому розділі представляються розроблені автором методи побудови криптосистем з доведеною відсутністю каналів витоку секрету. Ключовим принципом роботи методів є те, що жоден з абонентів системи не використовує в протоколах внутрішні джерела випадковості, а всі псевдовипадкові послідовності генеруються на базі публічних унікальних значень (лічильників) з механізмами доведення оригінальності (відсутності модифікацій). Це дозволяє забезпечити виконання достатніх умов, що є умовами наслідку теореми 1 про відсутність каналу непомітного витоку секрету.

В роботі пропонуються два базові протоколи для демонстрації методу: протокол генерації випадкового запиту nonce (що використовується у багатьох протоколах, зокрема протоколах аутентифікації) та протокол узгодження секретного ключа на базі задачі Діффі-Хеллмана.

Базова схема протоколу випадкового запиту nonce.

Вихідні дані: абоненти Alice та Bob.

Кроки роботи протоколу:

1. Alice генерує унікальний одноразовий запит nonce та відправляє Bob.
2. Bob посилає відповідь «запит прийняв».

Якщо ця послідовність випадкова та має довжину r бітів, Розробник, що модифікує систему, може використовувати r бітів як стегоконтейнер для

подальшого витоку, наприклад, секретного ключа. Тож задачею нової схеми є унеможливлення зробити це непомітно.

Модифікація протоколу генерації nonce з викриттям стегоконтейнеру.

Вихідні дані:

1. Абоненти Alice та Bob.
2. Асиметрична криптосистема з простором K секретних ключів та простором Q публічних.
3. $Sign : K \times \{0,1\}^* \to B$ – функція генерації цифрового підпису без рандомізатору, B – простір підписів.
4. $Verify : Q \times \{0,1\}^* \times B \to \{0,1\}$ – функція перевірки цифрового підпису.
5. пара асиметричних ключів абонента $(k_A, p_A), k_A \in K, p_A \in Q$.
6. $\psi : \{0,1\}^* \to \{0,1\}^*$, $\psi_0 : Time \to \{0,1\}^*$ алгоритми генерації нового значення та ініціалізації лічильника.

Кроки роботи протоколу:

1. Абонент Alice обчислює наступне значення лічильника $ctr_i = \psi(ctr_{i-1})$. Якщо попереднього значення не існує, можливе його створення, наприклад, на основі мітки часу $ctr_0 = \psi_0(time)$.
2. Абонент Alice обчислює $nonce = Sign(k_A, ctr_i)$ та передає значення $ctr_i|nonce$.
3. Bob перевіряє факт того, що не були задіяні власні джерела ентропії: $Verify(p_A, ctr_i, nonce) = 1$, $ctr_i = \psi(ctr_{i-1})$.

Формалізація протоколу:

Визначення 8. (Протокол генерації випадкового запиту з викриттям стегоконтейнеру) Припустимо, абонент є оракулом Alice, сторона Bob займається викриттям каналу витоку.

Протоколом генерації випадкового запиту з викриттям стегоконтейнера назвемо кортеж $\langle D_t, V, U, A_t \rangle$ моделі протоколу типу «запит-відповідь» (визначення 3), де:
V – множина можливих значень лічильника,
U – множина можливих значень виходу абоненту,
$A_t \equiv Sign(k_A, v)$, $v \in V$ – алгоритм абонента,
$D_t \equiv Verify(p_A, v, u)$, $u \in U$.

В роботі була сформульована та доведена теорема про стійкість до атаки SETUP вдосконаленого протоколу генерації nonce.

Теорема 3. Нехай справедливе припущення: $\forall v \in V$, $\forall A_t : A_t(k_A, v) \neq Sign(k_A, v)$, $P\{Verify(p_A, v, A_t(k_A, v)) = 1\} < \varepsilon(t)$ (тобто, практично неможливо створити пару різних підписів одного повідомлення).
Тоді у протоколі передачі випадкової послідовності (визначення 8) відсутній канал непомітного витоку секрету.

Також у рамках роботи запропоновано протокол узгодження ключа, що захищений від атаки побудови SETUP.

Для ілюстрації побудови каналу без витоку, використаємо як базовий однопрохідний протокол Діффі-Хеллмана.

Базовий протокол Діффі-Хелмана.

Вихідні дані:

1. Абоненти Alice та Bob.
2. Асиметрична криптосистема для алгоритму Діффі-Хеллмана: G – генератор,K, Q – простір закритих та відкритих ключів $'\cdot' : K \times Q \to Q$ – функція узгодження (піднесення до степеню).
3. Пара асиметричних ключів абонента Alice $(k_A, p_A), k_A \in K, p_A \in Q$.
4. Пара асиметричних ключів абонента Bob $(k_B, p_B), k_B \in K, p_B \in Q$.

Кроки роботи протоколу:

1. Абонент Alice генерує сесійний секретний ключ $x \overset{rand}{\in} K$
2. Alice відправляє відкритий сесійний ключ: $X = x \cdot G$, $W \to$ Bob.
3. Alice обчислює симетричний (спільний) ключ каналу: $s = x \cdot p_B$.
4. Bob обчислює спільний симетричний ключ каналу: $s = k_B \cdot X$.

Розглянемо протокол встановлення захищеного каналу зв'язку між абонентами Alice та Bob за модифікованим протоколом Діффі-Хелмана, що дозволяє генерувати випадковий сесійний ключ каналу без можливості побудови прихованого каналу витоку SETUP.

Модифікований протокол Діффі-Хелмана.

Вихідні дані:

1. Асиметрична криптосистема (для цифровиго підпису) з простором $\tilde{K}$ секретних ключів та простором $\tilde{Q}$ публічних.
2. Асиметрична криптосистема для алгоритму Діффі-Хеллмана: G – генератор,K, Q – простір закритих та відкритих ключів $'\cdot' : K \times Q \to Q$ – функція узгодження (піднесення до степеню).
3. Симетричний шифр (E, D) з простором ключів S, та бієктивними функціями $E : S \times B \to B$, $D : \forall s \in S, \forall b \in B, D_s(E_s(b)) = b$.
4. $Sign : \tilde{K} \times \{0,1\}^* \to B$ – функція генерації цифрового підпису без рандомізатору, B – простір підписів.
5. $Verify : \tilde{Q} \times \{0,1\}^* \times B \to \{0,1\}$ – функція перевірки цифрового підпису.
6. Пара асиметричних ключів абонента Alice $(k_A, p_A), k_A \in \tilde{K}, p_A \in \tilde{Q}$.
7. Пара асиметричних ключів абонента Bob $(k_B, p_B), k_B \in K, p_B \in Q$.
8. Криптографічно сильні функції хешування $h1 : B \to K$, $h2 : Q \to S$.
9. $\psi : \{0,1\}^* \to \{0,1\}^*$, $\psi_0 : Time \to \{0,1\}^*$ алгоритми генерації нового значення та ініціалізації лічильника.

Кроки роботи протоколу:

1. Абонент Alice обчислює наступне значення лічильника $ctr_i = \psi(ctr_{i-1})$. Якщо попереднього значення не існує, можливе його створення, наприклад, на основі мітки часу $ctr_0 = \psi_0(time)$.
2. Alice:
   - Генерує сесійний секретний ключ $q = Sign(k_A, ctr_i|'Alice'|'Bob')$.
   - Симетричний ключ каналу: $s = h2(h1(q) \cdot p_B)$.
   - Відправляє відкритий сесійний ключ, лічильник та ідентифікатори

абонентів: $W = h1(q) \cdot G, (W, ctr_i, 'Alice', 'Bob') \rightarrow$ Bob.

3. Bob обчислює спільний симетричний ключ каналу: $s = h2(k_B \cdot W)$.
4. Alice відправляє свій секретний сесійний ключ закритим каналом: $E_s(q) \rightarrow Bob$.
5. Bob розшифровує ключ q. Перевіряє, чи дійсно цей ключ згенерований на основі публічної послідовності:
   - Перевірка $ctr_i = \psi(ctr_{i-1})$. Якщо ні – лічильник не обчислений узгодженим алгоритмом, підозра на канал витоку, роз'єднання.
   - Перевірка $h1(q) \cdot G = W$. Якщо ні – ключ недійсний, з'єднання розривається.
   - Перевірка $Verify(p_A, ctr_i|'Alice'|'Bob', q) = 1$. Якщо ні, то сесійний секретний ключ згенеровано не на основі відкритого лічильника, підозра на канал витоку, роз'єднання.

Формалізація протоколу:

Визначення 9. (Протокол узгодження спільного ключа без каналу непомітного витоку секрету) Протоколом узгодження спільного сесійного ключа без каналу непомітного витоку секрету назвемо кортеж $\langle D_t, V, U, A_t \rangle$ моделі протоколу типу «запит-відповідь», де:
V – множина можливих значень лічильника,
U – множина можливих значень виходу Alice,
$A_t \equiv h1(q) \times G)|e$ – алгоритм абонента Alice, $q = Sign(k_A, v), e = E_s(q)$, $v \in V$,
$D_t(v, u) \equiv Verify(p_A, v, getq(u)) * \mathbb{I}(getp(u) = h1(D_{gets(u)}(gete(u))) \cdot G$, $u \in U$, де функції $getq, getp, gets, gete$ обчислюються таким чином:
$getp(u) = h1(q) \cdot G$; $gete(u) = e$;
$gets(u) = h2(k_B \cdot getp(u))$; $getq(u) = D_{gets(u)}(gete(u))$.

Сформульована та доведена теорема про стійкість вдосконаленого протоколу Діффі-Хеллмана до атаки SETUP.

Теорема 4. Нехай справедливі припущення:

1. $\forall v \in V$, $\forall A_t : A_t(k_A, v) \neq Sign(k_A, v)$, $P\{Verify(p_A, v, A_t(k_A, v)) = 1\} < \varepsilon(t)$ (тобто, практично неможливо створити пару різних підписів одного повідомлення).
2. Функції $getq, getp, gets, gete$ обчислюються за час, яким можна знехтувати.

Тоді в удосконаленому протоколі Діффі-Хеллмана (визначення 9) відсутній канал непомітного витоку секрету.

Науковим результатом є модифікації базових протоколів з доведеною відсутністю SETUP. Це означає, що для даних схем неможливо побудувати атаку SETUP, що запропонована Янгом і Юнгом.

Розроблені методи можливості побудови клептографічного механізму для криптопримітивів, зокрема у геш-функціях, та пропонується метод побудови геш-функції з клептомеханізмом, що дозволяє розробнику відновлювати (за певних умов) прообраз функції стиснення за наявним геш-кодом.

Задача побудови функції гешування з лазівкою була сформульована таким

чином: побудувати функцію стиснення функції хешування, що використовує конструкцію Меркла-Дамгарда і в основі функції стиснення – одна з відомих схем побудови функції стиснення на основі симетричного шифру (в даному випадку, конструкція $f17(v,m) \equiv E_m(v) \oplus m$).

Визначення 10. (базове перетворення на основі проблеми дискретного логарифмування) Нехай задана циклічна група $\langle G, + \rangle$ з генератором порядку $g : ord(g) = n$. Для групи можна визначити операцію «$\cdot$», $w \cdot a = \underbrace{a + a + ... + a}_{w}$.

Також задається параметр розміру блоку $k \geq 2$.

Базовим перетворенням називатимемо функцію на $T_k : G^k \times Z_n^k \to Z_n^k$:

$$T_k(\vec{v}, \vec{x}) = \vec{\eta} \circ \begin{bmatrix} x_0 & x_1 & ... & x_{k-1} \\ x_1 & x_2 & ... & x_0 \\ ... & ... & ... & ... \\ x_{k-1} & x_0 & ... & x_{k-2} \end{bmatrix} \times \begin{bmatrix} v_0 \\ v_1 \\ ... \\ v_{k-1} \end{bmatrix},$$

де $\vec{v} \in G^k, \vec{x} = Z_n^k$, $\vec{\eta} = \langle \underbrace{\eta, ..., \eta}_{k} \rangle$, $\eta : G \to \xi, \xi \subset Z_n$ – бієктивне відображення, причому η та η^{-1} можуть бути реалізовані ефективним алгоритмом.

На базі даного перетворення та конструкції f_{17} була побудована функція стиснення.

Визначення 11. (Функція стиснення на базі перетворення T_k)
Функцією стиснення на базі перетворення T_k називатимемо функцію:

$$F(\vec{v}, \vec{m}) = T_k(\vec{v}, \vec{m}) \boxplus \vec{m}, \tag{1}$$

де $\vec{v} \in G^k, \vec{m} \in Z_n^k$, операція '$\boxplus$' – покомпонентне додавання у Z_n^k.

Запропонована функція (визначення 11) має вигляд стандартної конструкції f_{17}. Також, була сформульована та доведена теорема про стійкість даної конструкції.

Теорема 5. Для $\forall k \geq 2, G, Z_n$ конструкція функції стиснення (визначення 11) з базовим перетворенням $T_k : G \times Z_n \to Z_n$: дозволяє непомітно передати розробнику, який обрав та зафіксував $\vec{v}$, фрагмент m_r блоку повідомлення $\vec{m}$ за умови знання $\{m_i\}, i = 0..k-1, i \neq r$ та розкладу $\vec{v} = \langle s_0 \cdot g, ..., s_{k-1} \cdot g \rangle$. При цьому складність задачі відновлення m_r, без знання секрету розробника, зводиться до задачі дискретного логарифмування над $\langle G, + \rangle$.

В результаті дослідження можливості побудови геш-функції з лазівкою розроблений метод побудови такої функції стиснення, яка дозволяє Розробнику ефективно відновлювати повідомлення за умови, що воно частково відоме (наприклад, як у випадку гешування короткого паролю).

Метод побудови геш-функції з закладкою.

Вихідні дані: циклічна група $\langle G, + \rangle$ з генератором g, параметр розміру блоку k, секрет розробника $\vec{s} \in Z_n^k$.
Результат: функція стиснення $F(\vec{v}, \vec{m})$, що дозволяє, знаючи секрет $\vec{s} \in Z_n$ та частини блоку повідомлення $\{m_i\}_{i \neq r}$ відновити частину m_r.
Кроки методу:

1. Формування стартового вектора геш-функції: $\vec{v} = \langle s_0 \cdot g, .., s_{k-1} \cdot g \rangle$.
2. Побудова перетворення T_k (визначення 10) на основі параметру k.
3. Побудова функції стиснення F (визначення 11) на основі перетворення T_k та стартового вектора $\vec{v}$.

Згідно з теоремою 5 дана конструкція дозволяє непомітно передати розробнику частину повідомлення m_r, якщо він володіє секретом $\vec{s} \in Z_n$ та частин блоку повідомлення $\{m_i\}_{i \neq r}$.

Окрім методу побудови геш-функції із лазівкою на базі необоротньої функції також пропонується використання методу Пренеля побудови фейстелівських S-блоків із прихованим диференційним шляхом високої ймовірності для побудови геш-функції з лазівкою спеціального виду, що надає Розробнику перевагу за участі в PoW консенсусі технології блокчейн.

Припустимо, що Розробник має множину диференціальних шляхів, що дають йому можливість контролювати m з n бітів складності з ймовірністю p_{dev} (мається на увазі, що обравши довільне повідомлення M Розробник накладає на нього один з диференційних шляхів, що з ймовірністю p_{dev} інвертує контрольовану сукупність біт геш-коду). Тепер задача Розробника – слідувати такій схемі перебору повідомлень, щоб збільшити ймовірність появи перших n нулів відносно ідеального випадку $p = 2^{-n}$.

Розробник виконує такі кроки для оптимізації перебору:

1. Обирає множину диференціальних шляхів $\{\delta_i\}_{i=1..2^m}$ з ймовірностями відповідно $\{p_i\}_{i=1..2^m}$, що дозволяють інвертувати будь яку комбінацію з m бітів.
2. Генерує початкове повідомлення (випадковим чином) таке, що решта $n - m$ неконтрольовані біти були нульовими.
3. Застосовує необхідний диференціальний шлях з $\{\delta_i\}_{i=1..2^m}$ так, щоб контрольовані m бітів стали нульовими. Ймовірність успішного застосування диференційного шляху буде:

$$p_{dev} = 2^{-m} \sum_{i=1}^{2^m} p_i.$$

4. У випадку, якщо геш-код модифікованого повідомлення містить усі n старших біт нульовими – завершує роботу (складність гешу досягнуто). В іншому випадку – переходить до кроку 2. Остаточна ймовірність того, що усі n старших біт нульові буде:

$$P_{success} = 2^{m-n} \left(2^{-m} + \left(1 - 2^{-m}\right) \left(p_{dev} + (1 - p_{dev})2^{-n}\right)\right).$$

Необхідно врахувати, що час перебору збільшиться (при нульових n-m бітах потрібно додатково проводити операцію гешування). Тому, середній час досягнення складності блоку складатиме:

$$L_{dev} = \frac{1}{P_{success}(1 - 2^{m-n} + 2^{-n})}.$$

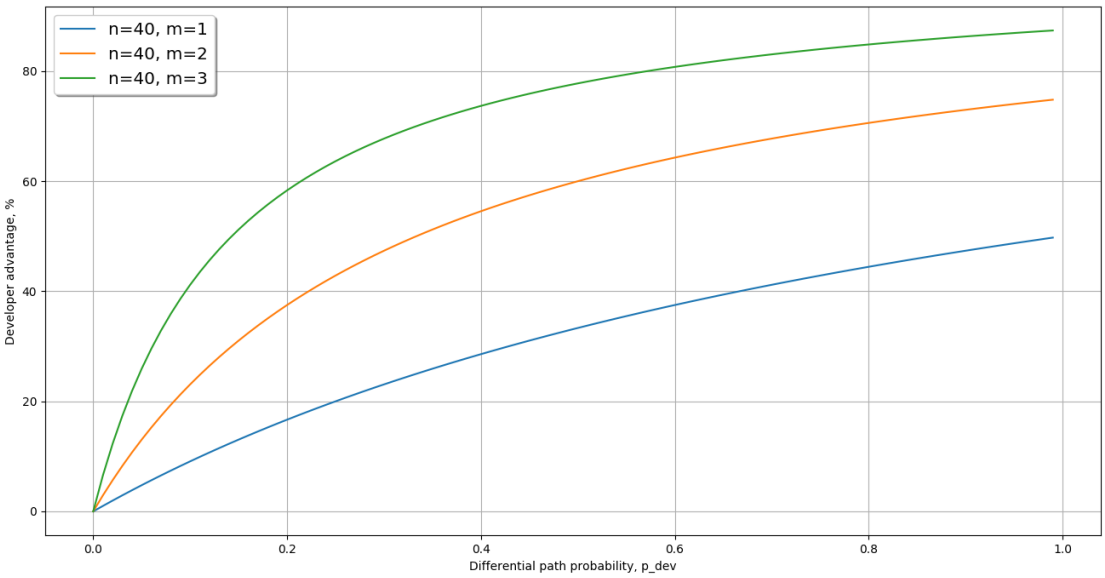

Рис. 3. Залежність переваги розробника від середньої ймовірності диференційного шляху p_{dev}

Таким чином, отримуємо перевагу Розробника в обчислені геш-функції:

$$\eta = (L_{dev} - 2^n) \cdot 2^{-n} \cdot 100\%. \tag{2}$$

У четвертому розділі запропонована методика порівняння ефективності (переваги розробника) при використанні клептографічної лазівки у геш-функції консенсусу. Ефективність застосування методу можна оцінити за формулою (2). Покажемо перевагу Розробника для різних значень кількості контрольованих бітів та середньої ймовірності диференційного шляху p_{dev} (складність блоку взята фіксовано $n = 40$, приблизно така поточна складність блоку Bitcoin).

З рис. 3 видно, що з ростом середньої ймовірності диференційних шляхів, що використовуються для контролю m бітів геш-коду росте і перевага Розробника, досягаючи максимуму при $p_{dev} = 1$.

З отриманих розрахунків видно, що підхід до клептографічної модифікації геш-функції алгоритму консенсусу технології блокчейн дійсно може надавати суттєву перевагу Розробнику у змаганнях потужностей Proof-of-Work. При цьому, така модифікація не виявляється іншими учасниками системи, що не володіють секретом Розробника.

Також у даному розділі отримані результати порівняння клептографічної надлишковості деяких криптографічних примітивів (див. Таблиця 2).

Одержані результати демонструють різні можливості щодо побудови клептографічного механізму для різних криптопримітивах. Найбільше ризиковий з обраних алгоритмів є російський стандарт геш-функції «Стрибог» – 12582.19 біт. Така кількість інформації необґрунтовано обраних констант наводить на підозру

Таблиця 2
Клептографічна надлишковість різних симетричних клептографічних примітивів

Примітив	Конструкція	Джерела надлишковості	Клептографічна надлишковість
AES	SP-мережа	процедури SubBytes та MixColumns	32 біт
SHA-256	схема Фейстеля незбалансована	нелінійні функції блоку підстановки	78 біт
ГОСТ 28147-89	схема Фейстеля	S-блок	512 біт
ГОСТ Р 34.12-2015 «Кузнєчік»	SP-мережа	S-блок та лінійне перетворення	2176 біт
ДСТУ 7624:2014 «Калина»	SP-мережа	чотири S-блоки	8192 біт
ГОСТ Р 34.11-2012 «Стрибог»	SP-мережа	S-блок, байтова перестановка, лінійне перетворення $V^8 \to V^8$, раундові константи	12582.19 біт

про можливість існування лазівки розробника. Натомість, для стандарту блокового шифрування AES знайдено лише 32 біти надлишкової інформації у структурі, що потенційно задається секретом Розробника, тож можна припустити, що лазівка відсутня або ж алгоритм є вразливим.

ВИСНОВКИ

В роботі розв'язані наукові задачі побудови та дослідження моделей клептографічних механізмів та визначення методів побудови криптосистем з доведеною відсутністю клептографічних каналів витоку.

У процесі виконання дисертаційної роботи були отримані такі вагомі результати:

1. Вперше запропоновано математичну модель для протоколів типу «запит-відповідь» у клептографічному сенсі, в результаті чого отримана можливість строгої оцінки клептографічної стійкості протоколів, що зводяться до протоколів типу «запит-відповідь».
2. Вперше отримані достатні умови неможливості непомітної клептографічної модифікації криптосистеми, в результаті чого отримана можливість строгого доведення відсутності клептографічної модифікації у криптографічних протоколах.
3. Вперше розроблено метод побудови функції гешування з клептографічним механізмом, в результаті чого можливе створення геш-функції з лазівкою, що дозволяє Розробнику частково відновлювати повідомлення за відомим геш-кодом.

4. Вперше запропонована метрика «клептографічного потенціалу», в результаті чого отримана можливість порівнювати клептографічні примітиви за ризиком наявності у них закладок.
5. Отримані значення клептографічної надлишковості для відомих криптопримітивів, наприклад, в стандарті блокового шифрування AES клептографічний потенціал можна зменшити на 32 біти, а у російської геш-функції ГОСТ Р 34.11-2012 («Стрибог») – на 12582.19 бітів.
6. Удосконалено загальну класифікацію клептографічних систем Шнаєра, в результаті чого отримані вектори клептографічних атак на криптографічні системи та примітиви.
7. Удосконалено базові протоколи запиту nonce та узгодження ключа Діффі-Хеллмана, в результаті чого отримана база для побудови криптографічних протоколів зі строго доведенною відсутністю клептографічного каналу витоку.
8. Отримано подальший розвиток методу Пренеля побудови шифру для побудови клептографічної функції гешування, в результаті чого, у випадку використання такої функції у протоколах PoW консенсусу блокчейн перевага Розробника підвищується до 50% порівняно зі звичайним учасником.
9. Для лазівки у блокчейн протоколах консенсусу Proof-of-Work отримані оцінки переваги Розробника для різної кількості контрольованих бітів та ймовірності допоміжних диференційних шляхів. У випадку контролю лише одного біта, перевага Розробника може сягати 50%.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Коваленко Б.А., Кудін А.М., Швидченко І.В., «Технологія блокчейн: питання аналізу та синтезу», Кібернетика та системний аналіз, т.55, №3, с.165-173, 2019.

2. Коваленко Б.А., Кудін А.М., «Диференційний аналіз функцій хешування та блокових шифрів: узагальнений підхід», Безпека інформації, т.21, №2, с.159–164,2015.

3. Коваленко Б.А., Кудін А.М., «Алгоритмічні аспекти пошуку прообразів геш-функцій на прикладі MD5», Захист інформації, т.17, №3, с.205-210, 2015.

4. Коваленко Б.А., Кудін А.М. «Побудова клептографічних механізмів у функціях гешування», Захист інформації, т.21, №2, с.121-128, 2019.

5. Кудін А.М., Ковальчук Л.В., Коваленко Б.А., «Теоретичні засади та застосування блокчейн-технологій: імплементація нових протоколів консенсусу та краудсорсінг обчислень», Математичне та комп'ютерне моделювання, №19, с.62-68, 2019.

6. Коваленко Б.А., «Побудова криптографічних протоколів вільних від клептографічних модифікацій», Безпека інформації, т.25, №2, с.122-126, 2019.

7. Kovalenko B. Kleptography trapdoor free cryptographic protocols [Електронний ресурс] / B. Kovalenko, A. Kudin // Cryptology ePrint Archive. – 2018. – Режим доступу до ресурсу: https://eprint.iacr.org/2018/989.

8. Коваленко, Б. А. Побудова клептографічних модифікацій функцій хешування / Б. А. Коваленко, А. М. Кудін // Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», м. Київ, 21-23 травня 2015. – Київ : НТУУ «КПІ». – 2015. – с. 122-124.

9. Коваленко Б.А., Кудін А.М., «Диференційний аналіз функцій хешування та блокових шифрів: узагальнений підхід»: матеріали п'ятої міжнар. наук.-практ. конф., 27-29 травня 2015 /М-во освіти і науки України, Прикарпатський національ. університ. ім. Василя Стефаника, Вінницький націон. тех. університ.– Івано-Франківськ: с.154-157.

10. Коваленко Б.А., «Побудова криптографічних примітивів без клептографічних лазівок»: зб. наук. праць за матеріалами міжнар. наук.-практ. конф., 29 липня 2019 р./ ГО «Європейська наукова платформа»'. – Лондон: т.3, с.97-102.

11. Коваленко Б.А., Кудін А.М. «Побудова криптографічних протоколів, захищених від побудови SETUP»: збір. тез наук. допов. конф. «Стан та удосконалення безпеки інформаційно-телекомунікаційних систем» 19-21 червня 2019 р./М-во освіти і науки України, ДССЗІ України [та ін.].–Миколаїв: с.23-24.

12. Kovalenko B., Kudin A., «Evaluation and minimization of kleptography risks in cryptographic algorithms»: збір. тез наук. допов. конф. «20th Central European Conference on Cryptology» 24-26 червня 2020 р. –Загреб: с.37-38.

АНОТАЦІЯ

Коваленко Б.А. Методи побудови та оцінки стійкості клептографічних механізмів у гібридних криптосистемах. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.13.21 «Системи захисту інформації». – Національний авіаційний університет, Міністерство освіти і науки України, Київ, 2020.

У дисертації розв'язано актуальну наукову задачу розробки методу побудови криптосистем з доведеною відсутністю клептографічної модифікації. Запропоновано загальну класифікацію клептографічних систем, вперше запропоновано формалізацію для протоколів типу «запит-відповідь» у

клептографічному сенсі, вперше отримані достатні умови неможливості непомітної клептографічної модифікації криптосистеми, продемонстровано метод побудови функції гешування з клептографічним механізмом. Отримані нові наукові результати дозволяють розширити аналіз існуючих та нових криптосистем та примітивів відносно атак зі сторони розробника або зловмисної модифікації реалізації криптосистем. Головним практичним результатом є можливість на практиці будувати нові криптопротоколи з доведеною стійкістю до атак зловмисної модифікації з побудовою каналу витоку секрету та підвищення рівня захищеності криптографічних систем.

Ключові слова: клептографія, протокол типу «запит-відповідь», практична стійкість, SETUP, канал непомітного витоку секрету, обчислювальна стійкість.

ABSTRACT

Kovalenko B. Methods of kleptographic mechanisms implementation and security estimation in hybrid cryptosystems. – Manuscript.

PhD dissertation, specialty 05.13.21 – Information Security Systems. – National Aviation University, Kyiv, 2020

There is science actual problem solved in the dissertation, namely the problem of creation approaches and methods for proven kleptographic modification free cryptosystem. General classification of kleptographic systems has been suggested, firstly formal model over "challenge-response" protocols in kleptographic sense has been suggested, firstly sufficient conditions of impossibility of kleptographic modifications have been obtained, the new method of implementation hash function with kleptographic mechanism has been demonstrated. These science results allow to improve analysis process of both released and being developed cryptographic systems to increase level of resistance against malicious modification. The main practical result is a capability of development of new cryptographic protocols with proved resistance against cleptographic attacks and improving security level of cryptographic systems.

The dissertation consists of introduction, four sections, conclusion and list of used sources.

The introduction substantiates topic's actuality, formulates goals and tasks of research, the scientific novelty and the practical significance of the results.

In the first section is overview of current state of kleptographic research, known methods and use cases of kleptographic schemes. Firstly, it's demonstrated one of the most famous usage – symmetric encryption algorithm DES, which is designed with weakened structure to allow National Security Agency to perform practical cryptoanalysis using its huge computational resources and unknown cryptoanalysis method (namely, linear cryptoanalysis). Further, it's described modern example – random number generator DualEC DRGB, which was standardized in 2006 and it's a cryptographicaly secure RNG only if the development follows standard. However, if algorithm's parameters have relation, that is known by somebody, relation's owner is

able to forecast output in practice. Next examples are russian hash function GOST P34-11-2012 and block ciphers GOST P34-12-2015 that are suspected to be designed with kleptographic trapdoor. Finally, it's demonstrated kleptographic trapdoors based on asymmetric primitives: elliptic curves, RSA and Discrete Logarithm Problem.

The second section devoted to the theory of kleptographic trapdoors. It started from classification of kleptographic mechanisms. Further, it's introduced formal model of practical distinguisher to precise security metrics. After, formal model of "challenge-response" protocol type is introduced with kleptographic extension of this model. The main scientific result of this section are sufficient conditions of SETUP free protocol. It allows to develop protocols without kleptographic trapdoors. The last result of the section is new kleptographic metric called "kleptographic potential". This metric may be used for evaluation of risks of kleptographic trapdoor existence in cryptographic primitive and it may be used in crypto primitive's design stage and for filtering of suspicious candidates on crypto competitions.

The 3-rd section demonstrates sufficient conditions applying: two basic SETUP free protocols are designed – enhanced nonce generation protocol and enhanced 1-round Diffie-Hellman key agreement protocol. The main idea is usage of non randomized digital signature that is used to generate public random values that can't be disclosed before publication but can be verified for non randomness. Theorems about absence of SETUP are formulated and proved. Also, there are two methods for hash function trapdoor development. One of them uses special transformation based on Discrete Logarithm Problem and allows Developer to recover part of message from known hash digest. Another method is Preneell's method for generation trapdoored Feistel's cipher which is applied to hash function basic cipher and gives Developer advantage in special use cases, here it's blockchain Proof-of-Work consensus protocol. Thus, Developer, who knows secret in the hash function design, is able to guess message with special formatted hash digest (e.g., digest has some amount of "zero" most significant bits) with greater probability that for ideal hash function. At the and of section, it's described improved method of Stevens's algorithm for differential paths generation to perform extensive search for trapdoored hash functions.

The fourth section presents evaluation of efficient (Developer's advantage) for trapdoored hash function in blockchain PoW consensus protocols. The efficiency depends on number of handled bits and probability of differential paths. Evaluations shows that even if Developer handles only on bit of digest prefix, his advantage may be up to 50%. Also, there is evaluation of kleptographic potential for some famous cryptographic primitives: symmetric encryption algorithms (AES, GOST 28147-89, GOST R 34.12.2015, DSTU 7624:2014) and hash functions (SHA-256, GOST R 34.11-2012). It turned out that the least kleptographic potential is in AES algorithm, so it has the minimal (from considered ones) risk of existence of kleptographic trapdoor (kleptographic redundancy is 32). In other side, russian hash function standard GOST R 34.11.2012 ("Stribog") has the highest risks (kleptographic redundancy is 12582.19).

Key words: kleptography, "challenge-response" protocol, practical resistance, SETUP, subliminal channel, computational complexity