ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

Гальченко Андрій Віталійович

УДК 004.056.55 (004.032.24, 004.627, 004.75)

ДИСЕРТАЦІЯ
Інструментальні засоби криптографічних систем на базі заперечуваного шифрування

122 – Комп’ютерні науки
12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ А.В. Гальченко

Науковий керівник:
Чопоров Сергій Вікторович
доктор технічних наук, професор

Запоріжжя – 2021

АНОТАЦІЯ

Гальченко А.В. Інструментальні засоби криптографічних систем на базі заперечуваного шифрування. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 - Комп'ютерні науки. Запорізький національний університет Міністерства освіти і науки України, Запоріжжя, 2021.

Об'єктом дослідження є механізми перетворення даних, які використовуються в сучасних засобах криптографічного захисту інформації, зокрема механізми заперечуваного шифрування.

Предметом дослідження є способи і методи ефективного перетворення даних, які не призводять до появи змін у вихідних алгоритмах заперечуваного шифрування.

Метою роботи є збільшення швидкості перетворення даних, яке лежить в основі існуючих алгоритмів заперечуваного шифрування даних, шляхом розробки способів ефективної організації обчислень.

У **вступі** обґрунтовано актуальність теми дисертаційної роботи, зазначено зв'язок роботи з науково-технічними проектами, сформульовано мету і завдання дослідження, визначено об'єкт, предмет та методи дослідження, показано наукову новизну та практичне значення отриманих результатів, наведено інформацію про практичне використання доробку, особистий внесок здобувача, апробацію результатів дослідження та їх висвітлення у наукових публікаціях. Приводяться відомості щодо структури та обсягу дисертаційної роботи.

У **розділі 1** виконано аналіз відкритих джерел і встановлено, що захист електронної інформації – це одна з актуальних проблем в галузі інформаційної безпеки, яка тісно пов'язана зі станом розвитку та впровадженням засобів машинної обробки даних та фактично залежить від нього. Визначено, що для

захисту електронної інформації використовують різноманітні пристрої та методи, зокрема програмні. Однак програмні методи набули більш широкого застосування. Тому розвиток засобів програмного захисту даних та засобів, які лежать в їх основі, є одним з пріоритетних напрямів у галузях інформаційних технологій та інформаційної безпеки. Зазначено, що в основі програмних методів захисту лежить використання криптографічних та стеганографічних методів захисту даних. Їх використання дозволяє приховати факт наявності та існування інформації у контексті з метою попередження неконтрольованого розповсюдження інформації, її несанкціонованої зміни (втрати), захисту чутливої інформації від зловживань третіми особами. В даному розділі акцентовано увагу на тому, що саме контекст інформації має найбільшу цінність для користувача та сторонніх осіб і може бути використаний для незаконного збагачення третіх осіб, нанесення шкоди фізичному та психічному стану користувачів, завдання репутаційних збитків юридичним особам, тощо. Зазначено, що поява атак, які ґрунтуються на застосуванні примусу до користувачів інформаційних систем, призводить до зменшення рівня захисту механізмів класичної криптографії та стеганографії, оскільки надійність їх захисту ґрунтується лише на обчислювальній стійкості алгоритмів перетворення даних. До того ж гарантований ними рівень захисту залежить від дотримання користувачами вимог організаційної безпеки. Окрім того, можливість використання засобів захисту в окремих випадках обмежена відповідно до вимог законодавства. Тому розвиток перспективних напрямів програмного захисту даних, зокрема криптографії, позбавлених вказаних недоліків є актуальною проблемою в теперішній час. Аналіз існуючих алгоритмів перетворення даних дозволив виділити найбільш перспективні напрями розвитку криптографії: багаторівневе перетворення даних, комутативні схеми шифрування, імплементація гомоморфних механізмів захисту даних, заперечуване шифрування, квантові перетворення та подібні до них. Однак зазначено, що практичне застосування отримали лише багаторівневе шифрування та квантові перетворення, оскільки їх реалізації

ґрунтуються на використанні існуючих методів і технологій передачі, обробки та перетворення даних з високою продуктивністю. Разом з тим встановлено, що комутативне, гомоморфне та заперечуване шифрування також досить перспективні, але не отримали практичного застосування в сучасних автоматизованих системах, оскільки їх використання потребує значних обчислювальних ресурсів. Враховуючи це, розробка ефективних методів обчислень, які лежать в основі вказаних засобів, зокрема заперечуваного шифрування, стала основною метою роботи.

У **розділі 2** наведено опис розробленої блокової моделі перетворення даних, використання якої дозволяє досягти швидкості необхідної для виконання криптографічних перетворень, покладених в основу алгоритмів заперечуваного шифрування. Зазначено, що вказана модель стала фундаментом для розробок у подальших розділах. В її основі лежить комбінація елементів симетричної криптографії та криптографічних перетворень з відкритим ключем. Результатом застосування даного підходу стали збільшення розміру вихідних даних і зростання швидкості криптографічних перетворень. У порівнянні з існуючими рішеннями, використання запропонованої моделі дозволило збільшити швидкість перетворень та виключити необхідність внесення змін у вихідні алгоритми заперечуваного шифрування. Останнє є суттєвою в порівнянні з існуючими рішеннями. Вказане дозволило, попередньо, вирішити проблему не створюючи додаткових вразливостей у структурі вихідних алгоритмів заперечуваного шифрування, у порівнянні з існуючими аналогами. Також у контексті вивчення елементів симетричної криптографії розглянуто можливість використання режимів шифрування. Для цього були розроблені адаптивні схеми режимів перетворення даних призначені для застосування в алгоритмах заперечуваного шифрування. Однак аналіз їх структури дозволив встановити, що для вихідних алгоритмів заперечуваного шифрування на практиці доцільною є імплементація саме режимів ECB і CBC, оскільки їх механізми дозволяють захисти саме дані. Окрім того, експериментами встановлено, що показники сумарної швидкодії вихідної моделі в значній мірі

залежать від апаратного забезпечення кінцевих пристроїв. В результаті експериментів визначено, що при виконанні криптографічних перетворень вихідної моделі на базі процесорів AMD x64 Family 16 Model 6 Stepping 3 та Intel x64 Family 6 Model 142 Stepping 10 різниця в швидкості склала до 7 разів.

У **розділі 3** виконано подальший аналіз структури алгоритмів заперечуваного шифрування, результати якого продемонстрували, що перетворення вказаних алгоритмів ґрунтуються на вирішенні великої кількості складних задач за одиницю машинного часу. При цьому вирішення власне складних задач за рахунок розпаралелення обчислень ускладнене через лінійність обчислювальних алгоритмів (зокрема алгоритму Тоннелі-Шенкса та подібних до нього). Для вирішення цієї проблеми удосконалено вихідну модель перетворення даних за допомогою паралельних обчислень. Зазначається, що базова модель є обгорткою над алгоритмами заперечуваного шифрування, тому зміни в її структурі не впливають на них і роблять можливим використання паралельних обчислень. Даний підхід дозволив скоротити час виконання криптографічних перетворень до 4 раз. В ході аналізу отриманого показника прискорення встановлено, що ефективність використання паралельних обчислень в алгоритмах заперечуваного шифрування досить низька у зв’язку зі значною часткою паралельно виконуваних операцій з даними. Для отримання більш високого показника прискорення розроблено механізм попередньої обробки вихідних даних, який ґрунтується на використанні принципу «розділяй та володарюй». Використання даного принципу в структурі удосконаленої моделі дозволило збільшити сумарну ефективність від використання паралельних обчислень до 8 разів, за незначну кількість часу. При цьому визначено, що подальше вдосконалення моделі, в напрямі паралельних обчислень, можливе лише за можливості збільшення обчислювальних потужностей автоматизованої системи (головна проблема для застосування алгоритмів заперечуваного шифрування).

У **розділі 4** зазначено, що швидкість криптографічних перетворень в алгоритмах заперечуваного шифрування залежить від розміру вихідних даних,

розміру та кількості блоків з даними. Управління вказаними характеристиками у попередньому розділі дозволило позитивно вплинути на кінцеву продуктивність моделі. В зв’язку з цим розроблено адаптивний механізм кодування даних, який ґрунтується на: прогнозуванні коефіцієнту компресії файлів з даними; управлінні рівнем компресії даних; компресії/декомпресії даних за допомогою алгоритмів кодування LZMA2 і Deflate. Його імплементація у вихідну та паралельні моделі дозволила скоротити розмір вихідних даних до 16 разів і збільшити швидкість криптографічних перетворень до 6 разів. При цьому встановлено, що кодування даних може бути використане для підготовки лише окремих типів даних. Тому ефективність використання даного механізму обмежена.

У **розділі 5** зазначено, що можливість збільшення швидкості криптографічних перетворень на кінцевих пристроях обмежена обчислювальними потужностями локальних пристроїв. Акцентовано увагу на тому, що не усі кінцеві пристрої мають однаково високі обчислювальні потужності, у зв’язку з чим сумарна швидкість перетворення даних для кожного кінцевого пристрою буде відрізнятися. Для отримання більш стабільних показників швидкодії та можливості перетворення файлів з даними більшого розміру розроблено розподілену модель заперечуваного перетворення даних, в основу якої покладено метод статичного балансування навантаження. За результатами проведених експериментів визначено, що запропоноване рішення дозволило збільшити сумарну швидкість перетворення даних у пропорції 1.5 рази/вузол.

Ключові слова: алгоритм Тонеллі-Шенкса, багаторівневе шифрування, блокове шифрування, гібридні алгоритми, гомоморфне шифрування, заперечуване шифрування, квантове шифрування, кодування даних, комутативне шифрування, паралельні обчислення, розділяй і володарюй, розподілені обчислення, симетричне шифрування, шифрування з відкритим ключем.

ABSTRACT

Halchenko A.V Cryptography systems' tools based on the deniable encryption. – PhD Thesis. Manuscript.

Thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy. Study program: 122 - Computer Science. Zaporizhzhia National University of the Ministry of Education and Science of Ukraine, Zaporizhzhia, 2021

Object of research: the modern cryptography systems' data processing tools applied in deniable encryption schemes.

Subject of research: effective data processing methods and approaches that does not threat the original deniable encryption schemes.

The goal of this thesis is to increase the data processing speed for applying the existed deniable encryption algorithms, by developing well-organized calculation methods.

The **Introduction** substantiates the topicality of the thesis, outlines its relationship to scientific and technical research projects. It formulates the research goal and objectives, specifies the object, subject, and methods of research, and highlights the scientific novelty and practical value of the obtained results. It sketches out how the research results were used in practical cases. Further, it summarizes the personal contribution of the applicant, and presents how the approbation and publication of the contributed results were done. Finally, the Introduction provides the quantitative information about the structure of the thesis.

Chapter 1 reviews the top issue in the information security industry, which depends on the information technologies development. It determined that a plenty of methods applied to protect the electronic information (hardware, software, etc.). The special software applying is more widespread. Information security software and same tools improvement is one of the most important approaches for information technology and information security, both. It's also determined that data protection tools have become more widespread in various human activities. They are based on the cryptography and steganography methods. It allows hiding the data and its context, preventing data from uncontrolled access and unauthorized changes, the third party

abusing. It admits that the data context is the most valuable for users and offenders. Not only that, but it can be used to illegally enrich, harm the physical and mental condition of users, inflict reputational damages on legal entities, etc. It's highlighted that classical cryptography and steganography safety is based on the protection schemes computational stability. But the users' bad faith for organizational security requirements makes it more compliance. It determines that some laws restrict cryptography and steganography methods applying. Therefore, the specified software development with the progressive protection schemes is an urgent issue nowadays. It's found that the most advanced cybersecurity approaches are multi-level encryption, commutative encryption schemes, homomorphic mechanisms' implementation, deniable encryption, quantum transformations, etc. However, multi-level encryption and quantum transformations become widespread. They are based on the common transferring, processing and high-performance encryption technologies. But commutative, homomorphic and deniable encryption have not become usage in modern automated systems. They require significant computational resources. That's why efficient computational methods and core tools development has become the main goal of the paper.

In **Chapter 2**, we developed the new computational scheme. It's based on the symmetric and public key cryptography combination and used to improve the basic deniable encryption algorithms. This approach has become to the original data size and data processing speed increasing. The suggested model allowed increasing transformations speed and eliminate changes of the original deniable encryption algorithms comparing to the existed solutions. Symmetric cryptography modes have been investigated. As a result, the common encryption modes have been transformed and become specialized for the deniable encryption algorithms applying. However, their analysis appears that the ECB and CBC modes can be applied. These modes provide the data protection immediately. Besides, it's found that suggested computational model performance depends on the workstations' capacity. Some experiments have been carried with the AMD x64 Family 16 Model 6 Stepping 3 and

Intel x64 Family 6 Model 142 Stepping 10 processors. The summary performance rate value equals to 1:7.

Chapter 3 focuses on the second deniable encryption algorithms investigation. It determined that the base model consists of plenty of complex tasks. It reduces the general capacity of the model. But these tasks cannot be calculated with parallel computing mechanisms (the Tunnel-Shanks algorithm, etc.). That's why the basic computing model has been improved. This approach provides a wrapper for the deniable encryption algorithms, which does not affect the computing model. The summary performance rate value equals to 1:4. The parallel computing model low performance is highlighted. The parallel computing usage becomes to the model general performance growing. But the parallel data operations significant rate equals to 100-120%. It becomes to reduce the model total performance. However, the basic computing model has been advanced with the data pre-processor applying. This method is based on the "divide and conquer" concept. This solution became to the model efficient to 8 times. It determined that the further development requires more advanced automated systems' capacity (the main issue of the deniable encryption algorithms applying).

Chapter 4 establishes that both models' performance depends on the original data length and quantity of data blocks. These variables' management allows influences the summary model performance. An adaptive data encoding mechanism has been developed for this task. It's based on the files' compression ratio forecasting, data compression management, LZMA2 and Deflate encoding algorithms applying. Its usage has become to the original data size reducing (up to 16 times), model performance increasing (up to 6 times). It's established that the suggested solution can be applied to several data types only. That's why its usage is restricted.

In **Chapter 5** found that some local computing technologies have been investigated and applied. It allowed to increase the deniable encryption algorithms performance on the end clients. But it's found that clients had the different capacity, because of hardware restrictions. The distributed encryption model with the static load balancing

developed. It determined that the suggested model allowed large data sets processing. The total data processing speed has been increased up to the 1.5 times / node rate.
Keywords: Tonelli-Shanks algorithm, multilevel encryption, block encryption, hybrid algorithms, homomorphic encryption, deniable encryption, quantum encryption, data encoding, commutative encryption, parallel computation, divide and conquer method, distributed encryption, distributed computing.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. **Гальченко А.В.**, Козіна Г.Л. Модифікація алгоритму заперечуваного шифрування Менга. *Радіоелектроніка. Інформатика. Управління.* 2016. № 2. С. 77-86. (**Web of Science**)
2. **Гальченко А.В.** Захист персональних даних з використанням алгоритмів неоднозначного шифрування. *Вісник ЗНУ.* 2017. № 2. С. 19-32.
3. **Гальченко А.В.**, Чопоров С. В. Заперечуване шифрування на основі застосування підходу гібридних криптографічних систем. *Радіоелектроніка. Інформатика. Управління.* 2019. № 1. С. 178-191. (**Web of Science**)
4. **Galchenko A.**, Choporov S. Block cipher modes in the deniable encryption. *Вісник ЗНУ.* 2019. № 1. С. 146-153.
5. **Гальченко А.В.**, Чопоров С.В. Кодування даних в алгоритмах заперечуваного шифрування. *Прикладні питання математичного моделювання.* 2020. Т. 3, № 2 (1). С. 72-79.
6. **Гальченко А.В.**, Чопоров С.В. Реалізація заперечуваного шифрування на базі розподілених обчислень. *Вісник ЗНУ.* 2020. № 1. С. 128-138.
7. **Гальченко А.В.**, Чопоров С. В. Використання методу розділяй та володарюй в алгоритмах заперечуваного шифрування. *Кібербезпека: освіта, наука, техніка.* 2020. Т. 2, № 10. С. 29-44.

Праці, які засвідчують апробацію матеріалів дисертації:

8. Козіна Г.Л., **Гальченко А.В.** Дослідження властивостей алгоритмів заперечуваного шифрування. *Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікації та інформаційних технологій*: зб. тез доп. VIII Міжнародної науково-практичної конференції, м. Запоріжжя, 21-23 верес. 2016 р. Запоріжжя, 2016. С. 238-240.
9. **Гальченко А.В.** Перспективи використання заперечуваного шифрування в галузі авіаперевезень. *АВІА 2017*: зб. тез доп. XIII Міжнародної

науково-технічної конференції, м. Київ, 19–21 квіт. 2017 р. Київ, 2017. С. 24–28.

10. **Гальченко А.В.**, Чопоров С.В. Зменшення ефективності криптографічних засобів захисту інформації. *Актуальні проблеми математики та інформатики*: зб. тез доп. 8 Всеукраїнської регіональної наукової конференції молодих дослідників, м. Запоріжжя, 27-28 квіт. 2017 р. Запоріжжя, 2017. С. 21-23.
11. **Гальченко А.В.**, Чопоров С.В. Мережева Модель Заперечуваного Шифрування. *ICT 2019*: зб. тез доп. 8 Міжнародної науково-технічної конференції, м. Харків, 9-14 верес. 2019 р. Харків, 2019. С. 239-242.
12. **Гальченко А.В.**, Чопоров С.В. Розподілені обчислення та заперечуване шифрування даних. *МКММ 2020*: зб. тез доп. 21 Міжнародної конференції з математичного моделювання, 14-18 верес. 2020. Херсон, 2020. С. 79.
13. **Гальченко А. В.**, Чопоров С. В. Моніторинг використання не ліцензованого програмного забезпечення. *ICT 2020*: зб. тез доп. 9 Міжнародної науково-технічної конференції, м. Харків, 17-20 лист. 2020 р. Харків, 2020. С. 182-185.