УДК 004.056(477)

Назарій СТАДНІК

Західноукраїнський національний університет

РОЗРОБКА АЛГОРИТМІВ ЦИФРОВОГО ПІДПИСУ З ВИКОРИСТАННЯМ СУЧАСНИХ ГЕШ-ФУНКЦІЙ

Вступ. У сучасному світі цифрових технологій забезпечення автентичності та цілісності електронних документів стає все більш критичним завданням. Цифровий підпис є одним з найважливіших криптографічних механізмів, який дозволяє вирішити ці проблеми, надаючи можливість верифікувати походження документа та гарантувати його незмінність. Особливу роль у створенні надійних цифрових підписів відіграють геш-функції, які забезпечують формування унікального відбитка документа та є невід'ємною частиною процесу підписання.

Мета: полягає у теоретичному обґрунтуванні та аналізі існуючих алгоритмів цифрового підпису, що використовують сучасні криптографічні геш функції.

1. Принцип роботи цифрового підпису на основі геш-функції

У сучасному світі інформаційних технологій забезпечення безпеки електронного документообігу є критично важливим завданням. Цифровий підпис (ЦП) став невід'ємною частиною сучасних систем захисту інформації, забезпечуючи аутентифікацію, цілісність та неспростовність електронних документів. Особливу роль у функціонуванні систем цифрового підпису відіграють криптографічні геш-функції, які забезпечують формування унікального цифрового відбитка документа. Розуміння принципів роботи цифрового підпису на основі геш-функцій є fundamental для розробки та впровадження надійних систем електронного документообігу [1].

Основою будь-якої системи ЦП є криптографічні перетворення, що базуються на математичних властивостях геш-функцій. Геш-функція представляє собою математичний алгоритм, який перетворює вхідні дані довільної довжини у вихідний бітовий рядок фіксованої довжини.

На рисуноку 1 зображено загальну схему формування геш-значення документа, де продемонстровано процес перетворення вхідного повідомлення у геш-код фіксованої довжини. Важливими властивостями криптографічних геш-функцій є однонаправленість (неможливість відновлення вхідного повідомлення за його геш-значенням) та відсутність колізій (складність знаходження різних повідомлень з однаковим геш-значенням) [2].

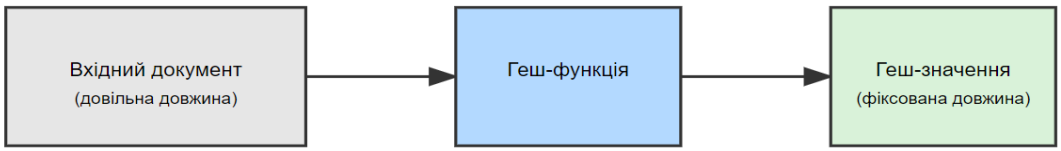

Рисунок 1 - Схема формування геш-значення документа.

Процес формування ЦП включає кілька етапів криптографічних перетворень. Спочатку для вхідного документа обчислюється його геш-значення

за допомогою криптографічної геш-функції. Отримане геш-значення потім шифрується за допомогою особистого ключа підписувача, формуючи власне цифровий підпис. Важливо відзначити, що розмір цифрового підпису залишається постійним незалежно від розміру вхідного документа, що є однією з ключових переваг використання геш-функцій у схемах цифрового підпису [3].

Сучасні системи ЦП використовують різні криптографічні геш-функції, серед яких найбільш поширеними є SHA-2 та SHA-3. На рисунку 2 представлено порівняльний аналіз продуктивності різних геш-функцій при обробці документів різного розміру. Графік демонструє залежність часу обчислення геш-значення від розміру вхідних даних для різних алгоритмів.

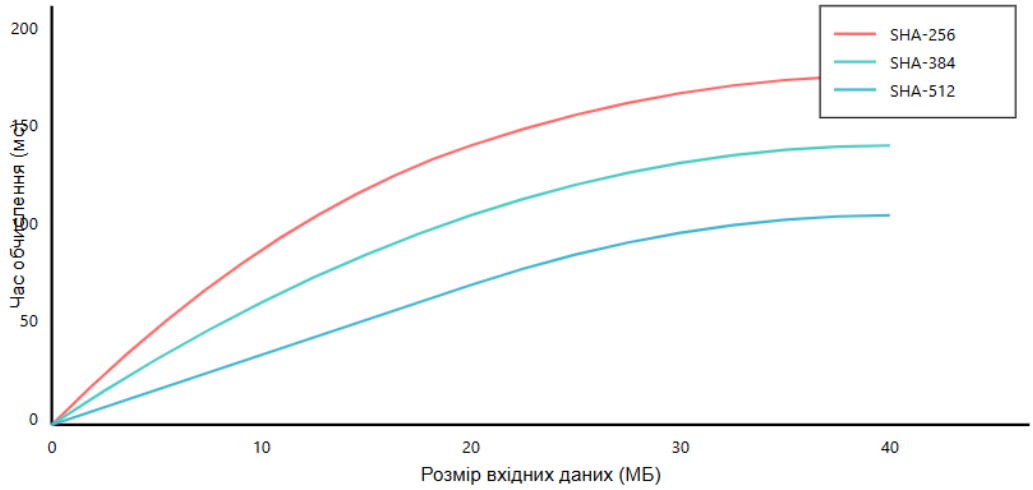

Рисунок 2 - Порівняльний аналіз продуктивності різних геш-функцій

Безпека системи ЦП значною мірою залежить від криптографічної стійкості використовуваної геш-функції. Сучасні геш-функції повинні забезпечувати стійкість до різних видів криптографічних атак, включаючи пошук прообразів, пошук колізій та пошук другого прообразу. Важливим аспектом є також забезпечення лавинного ефекту, коли навіть незначна зміна вхідного повідомлення призводить до суттєвої зміни його геш-значення [4].

При виборі геш-функції для системи ЦП необхідно враховувати кілька ключових факторів. По-перше, це криптографічна стійкість - геш-функція повинна забезпечувати достатній рівень захисту від відомих типів атак. По-друге, це продуктивність - геш-функція повинна ефективно обробляти великі обсяги даних. По-третє, це вимоги до обчислювальних ресурсів - важливо враховувати обмеження конкретної системи щодо пам'яті та процесорного часу [5].

Особливу увагу слід приділити процесу верифікації ЦП. На рисунку 3 показано схему перевірки ЦП, де продемонстровано процес порівняння обчисленого геш-значення документа з розшифрованим значенням ЦП.

В процесі верифікації ЦП відбувається розшифрування підпису за допомогою відкритого ключа підписувача та порівняння отриманого значення з геш-значенням документа, обчисленим при перевірці. Якщо ці значення співпадають, це підтверджує, що документ не був змінений після підписання та що підпис був створений власником відповідного закритого ключа [6].

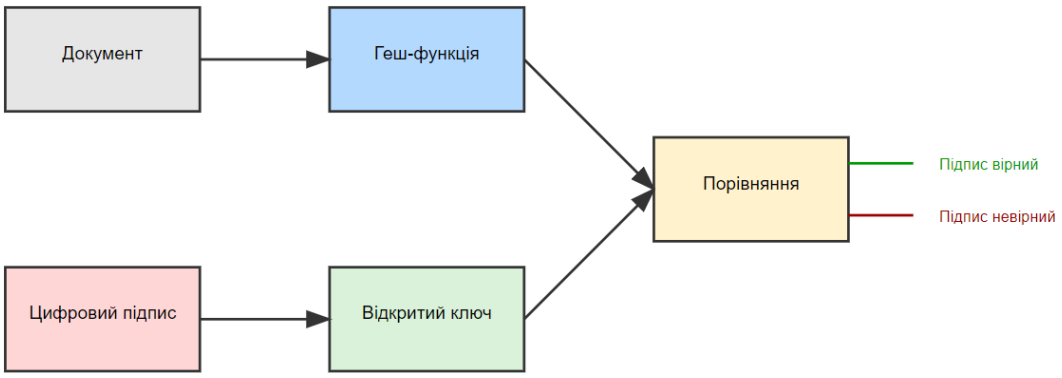

Рисунок 3 - Схема перевірки ЦП

Важливим аспектом функціонування систем ЦП є управління ключами. Закритий ключ, який використовується для створення підпису, повинен надійно зберігатися та бути доступним тільки авторизованим користувачам. Відкритий ключ, необхідний для перевірки підпису, повинен бути доступний всім учасникам системи електронного документообігу. При цьому важливо забезпечити достовірність відкритих ключів, що зазвичай досягається за допомогою сертифікатів відкритих ключів, виданих довіреними центрами сертифікації [7].

З розвитком квантових обчислень особливої актуальності набуває питання постквантової криптографії. Хоча сучасні геш-функції вважаються відносно стійкими до квантових атак, ведеться активна розробка нових алгоритмів, що забезпечують безпеку в умовах наявності квантових комп'ютерів. Це стосується як самих геш-функцій, так і алгоритмів асиметричного шифрування, що використовуються в схемах цифрового підпису.

Практичне застосування цифрових підписів на основі геш-функцій охоплює широкий спектр галузей. У фінансовому секторі вони використовуються для забезпечення безпеки електронних платежів та документообігу. В державному управлінні ЦП забезпечують юридичну значимість електронних документів. У корпоративному середовищі вони є невід'ємною частиною систем електронного документообігу та забезпечення інформаційної безпеки [8].

Важливим аспектом використання ЦП є їх відповідність законодавчим вимогам та міжнародним стандартам. Різні країни мають власні нормативні акти, що регулюють використання електронних підписів, але загальною тенденцією є гармонізація національних стандартів з міжнародними нормами. Це сприяє розвитку транскордонного електронного документообігу та підвищенню довіри до систем ЦП.

Інтеграція систем ЦП в існуючі інформаційні системи вимагає ретельного планування та врахування специфіки конкретного середовища. Важливо забезпечити зручність використання для кінцевих користувачів при збереженні необхідного рівня безпеки. Це включає розробку зрозумілих інтерфейсів, автоматизацію рутинних операцій та впровадження механізмів відновлення у випадку втрати ключів [9].

Особлива увага при впровадженні систем ЦП приділяється питанням масштабованості та продуктивності. З ростом обсягів електронного документообігу система повинна забезпечувати ефективну обробку великої кількості документів без втрати продуктивності. Це досягається за рахунок

оптимізації алгоритмів, використання апаратного прискорення та правильного вибору параметрів системи [10].

У контексті мобільних та хмарних обчислень з'являються нові виклики та можливості для систем ЦП. Необхідно забезпечити надійну роботу на мобільних пристроях з обмеженими ресурсами, а також вирішити питання безпечного зберігання ключів у хмарному середовищі. Розвиваються технології віддаленого підпису, коли закритий ключ зберігається на захищеному сервері, а підписання відбувається після надійної автентифікації користувача.

Перспективними напрямками розвитку систем ЦП є впровадження групових та кільцевих підписів, які забезпечують додаткові властивості анонімності та конфіденційності. Також активно досліджуються можливості використання блокчейн-технологій для створення розподілених систем управління ЦП та забезпечення довгострокового зберігання підписаних документів.

ЦП на основі геш-функцій є фундаментальною технологією забезпечення безпеки електронного документообігу. Постійний розвиток криптографічних алгоритмів, вдосконалення механізмів управління ключами та адаптація до нових технологічних викликів забезпечують актуальність та ефективність цього механізму захисту інформації. Подальший розвиток систем ЦП буде спрямований на підвищення рівня безпеки, покращення зручності використання та розширення функціональних можливостей відповідно до зростаючих потреб цифрового суспільства.

Іншим важливим аспектом є інтеграція систем цифрового підпису з існуючими інформаційними системами та платформами. Це дозволяє безперешкодно обмінюватися документами між різними учасниками процесу, особливо державними установами, компаніями та приватними особами. Удосконалення API і створення стандартів взаємодії між різними системами не тільки підвищує ефективність електронного документообігу, а й допомагає знизити ризики, пов'язані з ручним введенням даних і помилками, які можуть виникнути в результат.

Не менш важливим є питання правового регулювання та стандартизації цифрових підписів на міжнародному рівні. Успішне впровадження системи цифрового підпису, чіткої правової бази, що визначає стан електронних документів і підписів, а також розробка і впровадження міжнародних стандартів, таких як eIDAS, в Європейському Союзі для їх визнання в різних юрисдикціях стануть важливим кроком на шляху інтеграції цифрових підписів в глобальний електронний документообіг, сприяючи до розвитку електронної комерції і зниження адміністративних бар'єрів.

Висновок. Розвиток та впровадження систем цифрового підпису на основі геш-функцій є ключовим фактором забезпечення безпеки сучасного електронного документообігу. Проведений аналіз показав, що ефективність таких систем базується на математичних властивостях криптографічних геш-функцій, які забезпечують унікальність та незмінність цифрового відбитка документа. Використання сучасних алгоритмів гешування у поєднанні з асиметричною криптографією дозволяє створювати надійні механізми підтвердження

автентичності та цілісності електронних документів.

Особливу увагу в дослідженні було приділено аналізу різних аспектів функціонування систем цифрового підпису, включаючи процеси формування та верифікації підпису, управління ключами, забезпечення відповідності законодавчим вимогам та міжнародним стандартам. Виявлено, що ефективність системи цифрового підпису значною мірою залежить від правильного вибору криптографічних алгоритмів та їх параметрів, а також від реалізації належних механізмів захисту ключової інформації. Важливим фактором є також забезпечення зручності використання системи при збереженні необхідного рівня безпеки.

Результати дослідження вказують на перспективність подальшого розвитку систем цифрового підпису в напрямку впровадження постквантових алгоритмів, розвитку технологій віддаленого підпису та інтеграції з новими технологічними платформами. Особливого значення набуває адаптація систем цифрового підпису до умов мобільних та хмарних обчислень, а також розробка механізмів, що забезпечують додаткові властивості конфіденційності та анонімності. Подальший розвиток цієї технології буде визначатися як еволюцією криптографічних методів, так і зростаючими потребами цифрового суспільства в надійних механізмах забезпечення довіри в електронному середовищі.

Перелік використаних джерел.

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis: Wiley, 2020. 1232 p.

2. Boneh D., Shoup V. A Graduate Course in Applied Cryptography. Stanford University, 2023. URL: https://crypto.stanford.edu/~dabo/cryptobook/

3. Kumar S., Singh M. Hash Function Applications in Digital Signature: A Comprehensive Review. Journal of Information Security and Applications, 2021. Vol. 58. P. 102715.

4. Goldwasser S., Bellare M. Lecture Notes on Cryptography. MIT Laboratory for Computer Science, 2022. 289 p.

5. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. Chapman and Hall/CRC, 2020. 667 p.

6. Preneel B. Cryptographic Hash Functions: Theory and Practice. International Journal of Information Security, 2021. Vol. 20(2). P. 159-182.

7. Rivest R., Shamir A., Adleman L. Digital Signatures and Public-Key Cryptosystems: Twenty Years Later. Cryptography and Security: Selected Papers. 2022. P. 211-228.

8. Smart N. Cryptography Made Simple. 2nd ed. Springer International Publishing, 2021. 483 p.

9. Wang X., Yu H. How to Break SHA-1: Security Analysis and Practical Implementations. IEEE Transactions on Information Forensics and Security, 2023. Vol. 16. P. 3489-3504.

10. Zheng Y., Matsumoto T. Practical Applications of Digital Signatures in Cloud Computing. Cloud Computing Security: Advanced Topics, 2022. P. 145-167.