

МОДИФІКАЦІЇ КОДІВ РІДА-СОЛОМОНА ДЛЯ ПІДВИЩЕННЯ НАДІЙНОСТІ ТА ЗАХИСТУ QR-КОДІВ

Вінницький національний технічний університет

Анотація

У даній роботі досліджено вплив кодів Ріда-Соломона на надійність та безпеку QR-кодів. Розглянуто основні загрози, пов'язані з фізичними пошкодженнями та навмисними атаками, зокрема підміною та модифікацією QR-кодів. Проаналізовано можливості підвищення ефективності корекції помилок шляхом модифікації кодів Ріда-Соломона, використання розширених полів Галуа, поліноміальних перевірок, криптографічних методів та алгоритмів машинного навчання. Запропоновано підходи для підвищення стійкості QR-кодів до маніпуляцій, зокрема впровадження адаптивного кодування та механізмів автентифікації даних.

Ключові слова: QR-коди, коди Ріда-Соломона, корекція помилок, захист даних, криптографія, модифікація кодів, поля Галуа, машинне навчання.

Abstract

This paper examines the impact of Reed-Solomon codes on the reliability and security of QR codes. The main threats associated with physical damage and deliberate attacks, such as substitution and modification of QR codes, are considered. The possibilities of improving error correction efficiency through the modification of Reed-Solomon codes, the use of extended Galois fields, polynomial checks, cryptographic methods, and machine learning algorithms are analyzed. Approaches to enhancing QR code resistance to manipulations are proposed, including the implementation of adaptive encoding and data authentication mechanisms.

Keywords: QR codes, Reed-Solomon codes, error correction, data protection, cryptography, code modification, Galois fields, machine learning.

Вступ

Коди швидкого реагування, які зазвичай називають QR-кодами, є чудовим способом передачі інформації [1]. Незважаючи на їх неймовірну зручність у використанні існує проблема, що може впливати на безпеку QR-кодів, а саме можливість розрізняти фізичні ушкодження (як-от подряпини, забруднення та викривлення друку) та навмисні атаки (підробка або модифікація даних). Часто в різного роду фішингових атаках та для розповсюдження вірусів використовуються підроблені QR-коди. Це обумовлено тим фактом, що в той час як звичайні методи виправлення помилок дозволяють відновлення певних даних, вони абсолютно безсилі проти навмисних модифікацій. Тому, з урахуванням вищезазначеного, тема цієї роботи, як підвищити надійність QR-кодів за допомогою кодів Ріда-Соломона та інших сучасних технологій, є актуальною.

Метою дослідження є аналіз впливу кодів Ріда-Соломона на надійність і безпеку QR-кодів, оцінка їхньої ефективності у виправленні помилок та виявленні можливих загроз, а також розробка оптимальних підходів для підвищення стійкості QR-кодів до фізичних пошкоджень і навмисних атак.

Об'єктом дослідження є процес корекції помилок у QR-кодах та методи забезпечення їхнього захисту від навмисних маніпуляцій.

Предметом дослідження є методи і засоби застосування кодів Ріда-Соломона для підвищення надійності QR-кодів, використання розширених полів Галуа, криптографічних методів та алгоритмів машинного навчання для виявлення та запобігання маніпуляціям.

Головною задачею є пошук методів, що сприятимуть підвищенню стійкості QR-кодів до фізичних пошкоджень і навмисних атак шляхом використання кодів Ріда-Соломона, адаптивного кодування та механізмів автентифікації даних.

Аналіз предметної області та дослідження більш оптимальних методів

Хоча QR-коди широко використовуються в різних сферах, вони все ж обмежені до того що може вплинути на ефективність і безпеку технології QR-кодів. Основний ризик полягає у фізичному спотворенні, що може призвести до повної або часткової втрати даних, а також є небезпека навмисних атак, коли зломисник модифікує QR-код для перенаправлення на шкідливий ресурс замість першоджерела. Вбудовані механізми корекції помилок, що суттєво покращують здатність відновлення QR-кодів для втраченої інформації, проте ці коди не в змозі виявляти навмисні зміни, які зазвичай залишаються в межах рівня корекції. Це створює потенційні загрози, для здійснення хакерських атак, коли правильний код все ще може бути прочитаний пристроєм, проте вже містить шкідливі дані.

Метод Ріда-Соломона, який використовується в QR-кодах, працює подібно до виправлення помилок парності, він додає додаткові біти до даних, щоб виправити помилки. Найнижчий рівень корекції L відновлює до 7% втрачених даних, рівень M збільшує цей показник до 15%, середній рівень Q дозволяє виправити до 25%, а найвищий рівень H забезпечує максимальний захист, компенсуючи до 30% пошкодженої інформації (див. рисунок 1) [2]. Вищий рівень корекції робить QR-код більш витривалим до фізичних пошкоджень, але водночас зменшує обсяг основних даних, які можна закодувати.

Version	Size	Error Correction Level	Storable Bytes
1	21x21	L	17
		M	14
		Q	11
		H	7
2	25x25	L	32
		M	26
		Q	20
		H	14
3	29x29	L	53
		M	42
		Q	32
		H	24

Рисунок 1 – Місткість QR-кода в залежності від його версії, розміру та рівня виправлення помилок

Незважаючи на неабияку ефективність кодів Ріда-Соломона для виправлення випадкових помилок, вони не можуть відрізнити шахрайське втручання від інших випадкових пошкоджень. Використовуючи різні методи кодування дану вразливість можна виправити. Нижче наведено декілька способів покращення кодів Ріда-Соломона для підвищення їх безпеки:

1. Розширені поля Галуа.

Стандартні коди Ріда-Соломона GF(256) (2^8) обмежені полями Галуа у восьмому степені, але їх можна адаптувати до розширених полів GF(2^m), таких як GF(2^{10}) або GF(2^{12}), це підвищить здатність корекції помилок та зробить QR-код стійким до маніпуляцій [3]. Інша техніка полягає у використанні нестандартних примітивних поліномів для генерації коду. Оскільки класичні коди Ріда-Соломона використовують фіксовані примітивні поліноми, саме тому їх доволі легко передбачити. Змінивши спосіб генерування цих поліномів (наприклад, використавши псевдовипадкові коефіцієнти), зломисникам буде набагато складніше модифікувати код.

2. Поліноміальні перевірки для аутентифікації.

Іншим методом вирішення даної проблеми є використання поліноміальних перевірок. Це означає, що частина символу QR буде виділена для контрольних символів, а їхню верифікацію буде здійснено на зовнішньому сервері/базі даних або додатковому алгоритмі. Крім того також можливе динамічне кодування, що генеруватиме QR-код щоразу з унікальними параметрами, такими як позначка часу або унікальний ідентифікатор сеансу тощо. Це допоможе перевірити актуальність QR-коду та знизить ймовірність підробки чи повторного використання.

3. Інтегрована криптографія для виявлення змін.

Для запобігання підробці також можна скористатися криптографічними методами, такими як хешування та цифрові підписи тощо. Наприклад, згенерувавши унікальний підпис, що представляє QR-код використовуючи стійку хеш-функцію SHA-256. При зчитуванні даних

згенероване хеш значення може бути порівняне з хешем отриманих даних. Можливий також більш складний спосіб – а саме електронний цифровий підпис (EDS), у якому дані з QR-коду підписуються за допомогою асиметричного шифрування (RSA, ECC). Пристрій для зчитування може перевіряти цей підпис, якщо він не співпадає з очікуваним, QR-код є підробленим або зміненим.

4. Машинне навчання для аналізу змін QR-коду.

Оскільки шахраї та хакери, що змінюють QR-коди повинні залишатися в межах допустимого рівня корекції, щоб сканери могли відновити змінені дані, то для протидії цьому можна використати машинне навчання [4]. Застосовуючи алгоритми машинного навчання для аналізу структури QR-коду та виявлення аномалій також можна покращити безпеку QR-кодів. Якщо навчити нейронні мережі розпізнавати різницю між випадковими пошкодженнями та штучними змінам, то можна буде виявляти підроблені QR-коди та попереджати користувачів про небезпеку.

Висновки

В ході дослідження було розглянуто основні вразливості QR-кодів, пов'язані з неможливістю розпізнавання різниці між фізичними пошкодженнями і навмисними атаками. Було проаналізовано додаткові механізми захисту, а саме використання розширених полів Галуа та нестандартних примітивних поліномів, досліджено методи поліноміальної перевірки та динамічного кодування і розглянуто можливості застосування криптографічних технологій, таких як хешування та цифрові підписи, і використання алгоритмів машинного навчання, для забезпечення надійного захисту QR-кодів від фальсифікації.

Запропонований підхід є інноваційним, оскільки поєднує традиційні методи корекції помилок із сучасними криптографічними технологіями та алгоритмами штучного інтелекту. Використання розроблених методів дозволить значно підвищити безпеку QR-кодів, не лише зменшуючи ризики, пов'язані з випадковими пошкодженнями, а й ефективно протидіючи навмисним атакам та шахрайству.

Отже, впровадження комплексного підходу до захисту QR-кодів, що включає корекцію помилок, криптографічні механізми та алгоритми машинного навчання, є доцільним та необхідним для підвищення їхньої стійкості та безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. CS Field Guide. QR Codes. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.csfieldguide.org.nz/en/chapters/coding-error-control/qr-codes/> (дата звернення: 20.03.2025).
2. QR Code Fusion. QR Codes and Reed-Solomon Codes. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.qrcodefusion.com/codes/qr/reed-solomon> (дата звернення: 20.03.2025).
3. ResearchGate. Reliability on QR Codes and Reed-Solomon codes. [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/382108603_Reliability_on_QR_Codes_and_Reed-Solomon_codes (дата звернення: 20.03.2025).
4. QR Code using ML kit in Android [Електронний ресурс] – Режим доступу до ресурсу: <https://medium.com/@myofficework000/qr-code-using-ml-kit-in-android-78564f02fb5c> (дата звернення: 20.03.2025).

Сидорук Анна Олександрівна – студентка групи 4ПІ-216, факультет інформаційних технологій та комп'ютерної інженерії

рії, Вінницький національний технічний університет, м. Вінниця, e-mail: alanamiae.sid@gmail.com.

Романюк Оксана Володимирівна – кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: romaniukoksanav@gmail.com.

Anna Sydoruk – student of group 4PI-21b, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: alanamiae.sid@gmail.com.

Oksana Romaniuk – Ph.D., Associate Professor of Software Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: romaniukoksanav@gmail.com.