Підвищення ефективності шифрування керуючого трафіку БПЛА засобами модифікованого блокового методу

Журавська І.М.[1], Мусієнко М.П.[2], Румянков Д.І.[3]

[1] Доц., к.т.н., доцент каф. інформаційних технологій і програмних систем, Чорноморський державний університет імені Петра Могили, вул. 68 Десантників, 10, м. Миколаїв, Україна, dzhin@meta.ua
[2] Проф., д.т.н., декан ф-ту комп'ютерних наук, Чорноморський державний університет імені Петра Могили
вул. 68 Десантників, 10, м. Миколаїв, Україна, musienko2001@ukr.net
[3]Бакалаврант інтелектуальних інформаційних систем, Чорноморський державний університет імені Петра Могили, вул. 68 Десантників, 10, м. Миколаїв, Україна, dzhimasan@gmail.com

***Анотація* – Обґрунтовано застосування методу блокового шифрування на основі операції XOR для підвищення криптостійкості при скороченні часу шифрування керуючих повідомлень до безпілотних літальних апаратів (БПЛА). Виконання внутрішнього шифрування кожного блоку даних виконується в чотири раунди. Таким чином створюється залежність результату шифрування від значення байтів на кожному раунді, що підвищує криптостійкість системи й не витрачає обчислювальних ресурсів. Визначено кількісні характеристики шифрування й дешифрування з використанням запропонованого методу, обґрунтовано можливість як програмної, так і апаратної реалізації зазначеного шифрування, що надасть можливість підвищити швидкість захищеного обміну інформацією з БПЛА. Визначено напрямки та прикладні задачі ефективного застосування розробленого методу.**

Ключові слова: блоковий метод шифрування, операція XOR, керуючий трафік БПЛА.

Improving traffic control UAV encryption means of the modified block method

Zhuravska I.M. [1], Musiyenko M.P. [2], Rumiankov D.I.[3]

[1]Assoc. Prof., PhD, Department of Information Technologies and Software Systems, Petro Mohyla Black Sea State University, 68 Desantnykiv str., 10, Mykolaiv, Ukraine, dzhin@meta.ua
[2] Prof., DrSc, Dean of the Computer Science Faculty, Petro Mohyla Black Sea State University
68 Desantnykiv str., 10, Mykolaiv, Ukraine, musienko2001@ukr.net
[3]BSc Student, Department of Intelligent Information Systems, Petro Mohyla Black Sea State University, 68 Desantnykiv str., 10, Mykolaiv, Ukraine, dzhimasan@gmail.com

***Abstract* – Application of the block encryption method based on XOR operations is substantiated to improve the cryptographically strong of encrypted control messages while reducing time to the unmanned aerial vehicle (UAV). Implementation the internal encrypt of each data block is carried out in four rounds. This creates a dependency on encrypted results from byte values in each round, that increases the cryptographically strong of system and simultaneously does not waste computing resources. The quantitative characteristics of encryption and decryption using the proposed method are defined. A possibility both software and hardware implementation of this encryption will allow to increase speed of protected information exchange with UAV. Directions and applied problems of effective usage of the developed method are described.**

Keywords: block encryption method, XOR operation, managing UAV traffic.

Вступ

Трудомісткі та складні обчислення, що потребують серйозних програмних та апаратних ресурсів для шифрування трафіку, не можуть бути застосовані до безпілотних літальних апаратів (БПЛА), тому що це привело б до встановлення на борт БПЛА додаткових обчислювальних плат та зменшило масу корисного навантаження останніх.

Це призводить до того, що у деяких випадках власники БПЛА зовсім відмовляються від шифрування, тому що зазначені вище затримки можуть привести до несвоєчасного отримання літальним апаратом керуючого сигналу, й останній може бути втраченим через зіткнення з перепоною.

Зазначений підхід дозволяє створювати полегшені мікро- та міні-БПЛА ближнього радіусу дії, але підвищує ризик втрати такого БПЛА через перехват керування останнім сторонніми особами [1]. Крім того, відео, яке передається з БПЛА до центру керування (абонента) у незашифрованому вигляді може бути підмінено шляхом атаки «людина посередині», внаслідок чого власник БПЛА отримає недостовірну інформацію про об'єкт моніторингу.

Існуючи методи шифрування не забезпечують необхідну швидкодію тими обчислювальними ресурсами, які маються на борту малогабаритних БПЛА.

Зважаючи на те, що підвищувати вагу такого БПЛА шляхом модернізації обчислювальної плати недоцільно, треба докласти зусиль щодо спрощення методу шифрування без підвищення вразливості застосованого методу.

Реалізація механізмів безпеки одночасним забезпеченням конфіденційності та цілісності повідомлення найбільш ефективно здійснюється на теперішній час із застосуванням криптографічного алгоритму симетричного блокового перетворення. Але в більшості блокових стандартів (у т. ч. й у новому ДСТУ 7624:2014 на базі шифру «Калина») не розглядалася задача компактної апаратної реалізації та мінімального енергоспоживання, при одночасному забезпеченні припустимого рівня криптографічної стійкості [2].

Тому вітчизняні криптографи докладають зусиль для вирішення описаних задач шляхом використання елементарних функцій, які достатньо економно використовують обчислювані потужності пристроїв [3]. Зазначена мета також може бути досягнена за рахунок впровадження в блоковий метод шифрування простої операції XOR, але з усуненням такого її недоліку, як лінійність.

Застосовані операції повинні бути виконані за один такт процесора та можуть мати як програмну, так і апаратну імплементацію, у т. ч. на пристроях з обмеженими можливостями (нп., мікроконтролери).

Модифікація класичного блокового методу, яка пропонується, базується на виконанні великої кількості первинних операцій розкладення байтів на блоки даних та їх перемішування (транспозиція) між собою. Для зменшення кількості затрат обчислювальних ресурсів, блоки утворюються довжиною в 4 байти. Таке створення модульності дає змогу рівномірно розподілити обсяг даних між апаратними частинами, які виконують обрахунки.

Авторами розвивається напрямок дослідження та розробки методів і засобів шифрування трафіку БПЛА шляхом вирішення задач оптимізаційного характер, саме виходячи з розрахунків відносно можливостей обчислювальних ресурсів апаратної частини та визначення основних характеристик раундів на базі застосування математичного апарату додавання «по модулю 2» та перестановки байтів місцями.

Основи блокового методу шифруування

Блоковий метод шифрування, заснований на використанні маловитратних операцій, які можна виконувати за один такт процесору дозволяє зменшити час виконання створення шифрованих даних, які в кінцевій меті повинні бути прийняті на стороні БПЛА, тим самим забезпечити швидкий обмін актуальними даними.

Використання в середині раундів операції XOR між кожним байтом реалізує математичну процедуру виконання домішування сторонніх даних й створення так званого «білого шуму». Згідно залежності відбувається пов’язання байтів між собою й висувається вимога до збереження відповідного зворотного порядку для отримання першутвореної інформації.

На рис. 1 наведено схему внутрішньоблокового шифрування запропонованого методу.

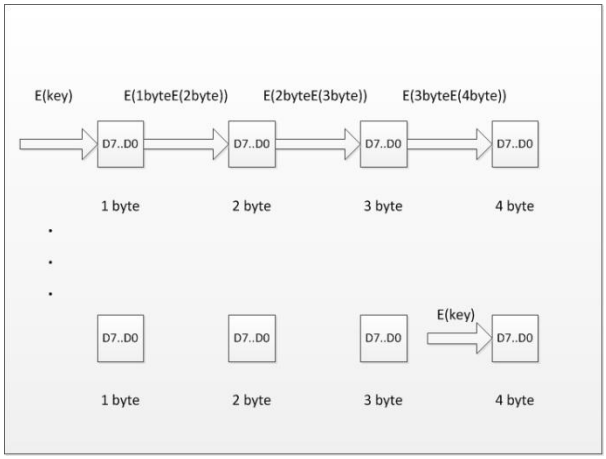

Рисунок 1 – Схема внутрішньоблокового шифрування

Для реалізації методу внутришньоблокового шифрування необхідно застосовувати операцію XOR до кожного наступного символу. Такі перетворення відзначаються простотою технічної реалізації та забезпечують утворення відповідної залежності між невеликими частинами даними. Описаний підхід надає можливість розпаралелювання розрахунків між обчислювальними ресурсами. Всередині кожного такого блоку виконується етапні перетворення (спотворення) інформації.

Тобто, використовуючи операцію XOR, ми кожного разу змінюємо значення від відповідної позиції, яка залежить від поточного значення ітерації. Наприклад, починаємо від першого символу даних й далі за ланцюгом переходимо до наступного. А ось вже в кінці загального циклу подаємо значення ключа лише на останній байт блоку. Таким чином, кожен байт блоку зберігає свою частину ключа, без якої дізнатися достовірну інформацію майже неможливо.

Реалізація блокового шифрування з раундовими функціями

Використання всередині кожного блоку чотирьох раундів зв’язку байтів засобами бінарної операції надає загальноутвореній закодованій інформації належної криптостійкості при простій технічній та програмній реалізації.

Запропоновано нові методи утворення раундів без використання складних математичних обчислень множення, обрахунку кореня та зведення числа в ступінь, а лише на основі операції XOR, яка виконує домішування до загальної послідовності окремих значень, що вводять залежність

для розшифрування та не збільшують час виконання методу.

В табл. 1 наведено результати обрахунків часу на виконання кодування/декодування інформації відповідної довжини.

Таблиця 1 – Середній час тестів для криптографічних перетворень

Вид тестування	**Результати**
Швидкість виконання шифрування (сек)	0.253 с (500 байтів)
Швидкість виконання дешифрування (сек)	0.259 с (500 байтів)
Частотність (%)	12% (500 байтів)
Актуальність переданої інформації	1 година
Криптостійкість	5 днів

Як показують наведені в таблиці результати, запропонований метод швидко виконує операції шифрування та дешифрування інформації. За рахунок розбиття на блоки ми отримуємо унікальність значень байтів для кожного блоку на основі циклічних повторів використання операції XOR до кожного байту відповідного блоку. Це дозволяє отримати послідовності байтів, які містять у собі «білий шум» разом з чистою інформацією.

Запропоновані методи досліджені до загального вигляду криптосистеми даного пакету статистичних тестів. Нижче наведена структура програмного забезпечення (рис. 2), яке використовує зазначений метод в роботі. В середині ПЗ організована наступна структура: «парсер», обробник з'єднання, криптографічний модуль (відповідає за кодування/декодування даних).

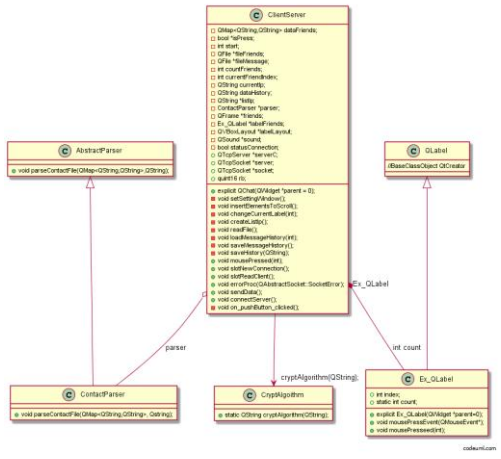

Рисунок 2 – UML-діаграма класів

Механізм взаємодії між модулями всередині ПЗ наступний: є вхідні параметри на модулі сервера (той що приймає), які надсилаються до модулю дешифратора, що використовує зазначений метод. Після того, як робота криптографічного модуля завершена, дані передаються до «парсеру», який приводить отриману інформацію до нормального за структурою виду. Модуль клієнта насилає дані від одного пристрою. Після цього цикл виконання повторюється.

ВИСНОВКИ

Завдяки модифікації методу блокового шифрування на основі простих обчислювальних операцій перестановок, зміщенням та використання бінарної операції XOR, отримані високі показники криптостійкості системи до злому та збалансованість між виконанням кодування/декодування інформації. Запропоновані підходи щодо вирішення питання оптимізації затрат обчислювальних ресурсів на основі операції XOR з реалізацією всередині блокового стандарту шифрування спрощеної раундової функції, при простій технічній реалізації та невисокій вартості виробництва, дозволяють зекономити ресурси, якими володіє електронне обладнання БПЛА. Результати проведених досліджень визначають ефективність та практичну значимість використання запропонованих методів для досягнення належної швидкості обміну закодованими даними та надання їй відповідної криптостійкості.

Метод блокового шифрування з маловитратними (відносно обчислювальних ресурсів) операціями дозволяє здійснювати швидкий обмін даними при малій вимогливості до обчислювальної потужності електроніки, що дозволило віднести його до методу з підвищеної оптимізацією з боку апаратної частини. Простота технічної реалізації та покращення криптостійкості системи загалом, внаслідок використання запропонованих методів перемішування, розбиття на блоки байтів й утворення зв'язку між ними всередині кожного з блоків, визначають ефективність застосування методу блокового шифрування в системах як з великими обчислювальними можливостями, так і з обмеженими, забезпечуючи в той же час належну надійність щодо захисту даних, що передаються до БПЛА.

ЛІТЕРАТУРА REFERENCES

[1] Сашников, Т. К. К вопросу обеспечения информационной безопасности беспилотных авиационных систем с летательными аппаратами малого и лёгкого класса в специализированных АСУ / Т. К. Сашников // T-Comm – Телекоммуникации и Транспорт. – 2013. № 6. – Режим доступа : http://cyberleninka.ru/article/n/k-voprosu-obespecheniya-informatsionnoy-bezopasnosti-bespilotnyh-aviatsionnyh-sistem-s-letatelnymi-apparatami-malogo-i-lyogkogo-klassa. – Загл. с экрана.

[2] Олійников, Р. В. Принципи побудови і основні властивості нового національного стандарту блокового шифрування України / Р. В. Олійников, І. Д. Горбенко, О. В. Казіміров // Захист інформації. – 2015 (04-06). – Т. 17, №2. – С. 142–157.

[3] Лужецький, В. А. Використання операції множення за модулем в симетричних блокових шифрах / В. А. Лужецький, О. В. Дмитришин. – Системи обробки інформації. – 2010. – № 5(86). – С. 9–14.