УДК 623.746.4-519:004.056.55: 004.274

С.Я. Гільгурт, д.т.н.
(Національний авіаційний університет, Україна)
І.І. Яблоков
(Донецький національний технічний університет, Україна)

Реалізація на ПЛІС посилених алгоритмів шифрування каналу зв'язку з БПЛА

Проаналізовані можливі підходи до підвищення стійкості алгоритмів шифрування в каналах зв'язку з БПЛА. Проаналізовані можливості та переваги використання ПЛІС для їх реалізації. Розглянуто структурну схему операційного блоку шифропроцесора. З розглянутих підходів до посилення шифрування більш прийнятним виявилися алгоритми динамічної модифікації.

Однією з актуальних напрямів вдосконалення технологій керування сучасними БПЛА є підвищення надійності каналу зв'язку літального апарату з наземною базовою станцією. Крім застосування засобів радіоелектронної боротьби зловмисник може перехоплювати управління БПЛА шляхом втручання в процесс обміну інформацією в цьому каналі. Теоретично проблема вразливості каналів передачі даних може бути вирішена одним із наступних трьох способів: застосування автономних БПЛА, використання супутникових ретрансляторів, закриття лінії зв'язку криптографічних засобів [1]. В більшості практичних застосувань найбільш прийнятним є останній з перерахованих варіантів.

Завдання закриття каналу зв'язку з БПЛА висуває суворі та суперечливі вимоги до бортової апаратури. Високу швидкодію, надійність шифрування та масогабаритні показники особливо складно забезпечити при підвищених вимогах до пропускної спроможності каналу та невеликий масі БПЛА. Бортове обладнання зазвичай має суттєві обмеження щодо обчислювальних можливостей та енергоспоживання [2]. Традиційні мікроконтролерні рішення не здатні ефективно здійснювати складні криптографічні операції, необхідні для реалізації звичайних схем шифрування [3]. З іншого боку, складні умови використання, особливо для мілітарних застосувань, вимагають більш стійкого закриття інформації. Тому набувають актуальності апаратні рішення з використанням програмованих інтегральних логічних схем (ПЛІС), насамперед – типу Field Programmable Gate Array (FPGA) [4]. Сучасні вироби програмованої логіки дозволяють забезпечити високу продуктивність при незначному споживанні електроенергії, додаючи при цьому безпрецедентну гнучкість, особливо корисну для реалізації посилених алгоритмів закриття інформації.

В даному дослідженні відомі шляхи до підвищення стійкості алгоритмів шифрування проаналізовані на предмет застосування в захищених каналах зв'язку з БПЛА.

Питання розкриття зловмисником секретної інформації залежить головним чином від наявності у нього ресурсів двох видів: обчислювальних і часових. Звідси випливають шляхи підвищення ступеня захищеності інформації, які спрямовані, відповідно, на збільшення ресурсноємності задачі розкриття та

на скорочення часу, що надається зловмисникові. Найбільш очевидними способами їх реалізації є: комбінування (повторне застосування) алгоритмів шифрування та динамічна модифікація (зміна алгоритму шифрування в часі).

Сутність методу комбінування посилення захисту полягає в тому, що вихідний текст зашифровується кілька разів. Інакше кажучи, виконується кілька послідовних кроків, кожному з яких здійснюється процедура криптографічного перетворення. При цьому результати попереднього кроку є вхідними для наступного кроку.

Одним із варіантів комбінування (і найпростішим методом для реалізації) є багаторазове шифрування. У цьому випадку на кожному кроці використовується той самий алгоритм з різними ключами. Доведено, що для широкого класу блокових симетричних шифрів з ключовим простором меншим, ніж простір повідомлень, розумне збільшення кількості кроків покращує якість шифрування [5].

Каскадний підхід передбачає використання різних алгоритмів щокроку. Теоретичні дослідження щодо підвищення безпеки даного підходу досі продовжуються. Хоча ще в 90-х роках було доведено, що якщо всі ключі, що використовуються на різних кроках, незалежні, то складність злому послідовності алгоритмів, принаймні, не нижче за складність злому першого з застосовуваних алгоритмів [6].

Інший напрямок посилення криптографічних методів, динамічна модифікація, передбачає зміну алгоритму шифрування в часі. При використанні цього напрямку виникають питання, пов'язані із синхронізацією процесів зашифрування у відправника та розшифрування у отримувача.

Найбільшою мірою реалізувати переваги методів посилення дозволяють гібридні алгоритми, що поєднують комбінування з динамічною модифікацією. Можливі три способи такого поєднання: динамічне багаторазове посилення, динамічне каскадне посилення та динамічне каскадне посилення різновидами.

При динамічному багаторазовому посиленні на кожному кроці шифрування відкритий текст перетворюється по тому самому алгоритму, але при наступному сеансі цей алгоритм змінюється. При динамічному каскадному підході, на відміну попереднього, на кожному кроці використовуються різні алгоритми, які також міняються на різних сеансах обміну даними. При динамічному каскадному посиленні різновидами на кожному кроці використовуються різні різновиду одного й того ж алгоритму, але на наступних сеансах змінюється їх порядок.

Динамічний комбінований вид посилення пред'являє до шифратора високі вимоги щодо продуктивності та гнучкості. Як було сказано вище, ні програмне рішення, ні апаратне не задовольняють обом цим вимогам. Шифратори, реалізовані на уніфікованих обчислювачах продуктивніше програмних шифраторів, водночас є гнучкими, на відміну апаратних.

Найбільш поширеними алгоритмами шифрування є алгоритми блокового симетричного шифрування (БСШ). Більшість сучасних блокових алгоритмів працюють схожим чином: над вихідним текстом виконується якесь перетворення за участю ключа шифрування, яке повторюється певне число разів

(раундів). На основі даної схожості в можна сформувати узагальнену структуру процесора блокового симетричного шифрування на базі ПЛІС (рис. 1) [7].

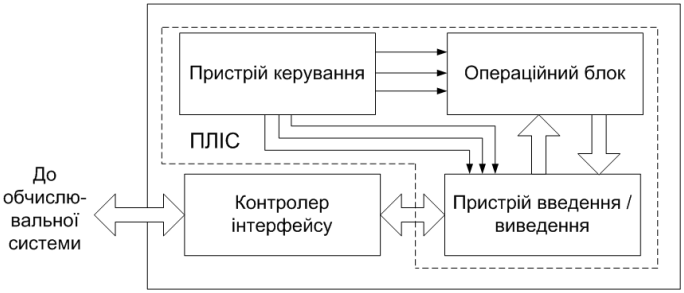

Рис. 1. Узагальнена структурна схема шифропроцесора

В цій схемі пристрій введення/виведення передає в операційний блок режими роботи, ключ, а також вхідний блок даних. В результаті обробки даних пристрій вводу/виводу приймає зашифрований блок даних. Роботою операційного блоку та обчислювальним процесом в цілому керує пристрій керування. Всі згадані модулі синтезуються в складі мікросхеми ПЛІС.

Завдяки згаданої вище подібності алгоритмів БСШ їх реалізація, так само як і реалізація методів посиленого шифрування може здійснюватися операційним блоком, що має структуру, наведену на рис. 2.

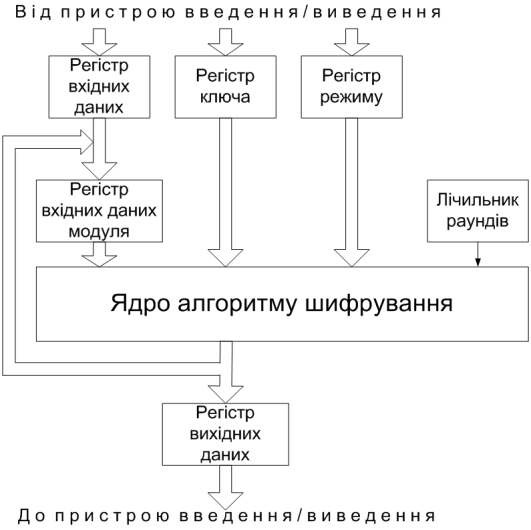

Рис. 2. Структурна схема операційного блоку

На вхід операційного блоку з пристрою введення/виведення поступають значення режиму роботи шифратора, ключа, а також вхідний блок даних. Далі ця інформація та вміст лічильника раундів, який контролюється пристроєм керування, поступає на вхід модуля ядра алгоритму шифрування, де виконується власне перетворення. Оброблений блок даних розміщується у регістр вихідних даних і передається в пристрій введення/виведення.

В термінах цифрової техніки ядра алгоритму шифрування є комбінаційною схемою, яка не містить тригерів, регістрів та інших елементів пам'яті. Отже, при його синтезі розробнику не доводиться вирішувати традиційно складні для розробників систем на ПЛІС питання тактування, синхронізації, часового планування тощо.

Оскільки в БСШ інформація обробляється блоками – фрагментами даних довжиною в кілька байтів, особливістю їх застосування для закриття каналів послідовної передачі даних, таких як RS-232, є той факт, що дані, які приймаються по послідовному каналу, необхідно зберегти в буферному запам'ятовуючому пристрої, а після обробки криптоалгоритмом знову перетворити в послідовну форму. Як наслідок, до тракту передачі інформації схемою шифрування вноситься затримка, яка залежить від заданого алгоритму, швидкодії шифруючого пристрою і обраної швидкості комунікаційного каналу.

Повна затримка, що виникає в результаті виконання процедури закриття інформації при передачі даних в один бік, включаючи операції зашифрування та розшифрування, у разі використання довільного алгоритму БСШ визначається за такою формулою [1]:

$$T_п = 2 \cdot (2 \cdot (N_б \cdot (N_п + N_с) \cdot T_с) + T_ш),$$

де $N_б$ – кількість байтів у блоці для заданого алгоритму БСШ; $N_п$ – кількість корисних (інформаційних) бітів у комунікаційному пакеті; $N_с$ – кількість службових бітів у комунікаційному пакеті (стартовий, стоповий, біт парності); $T_с$ – період тактової частоти, обернено пропорційний обраній швидкості передачі; $T_ш$ – час зашифрування/розшифрування (однаковий у випадку БСШ).

При використанні протоколу RS-232 з параметрами: вісім інформаційних бітів, однин стартовий, один стоповий, без контролю парності, швидкість передачі 9600 біт/сек та алгоритму шифрування ГОСТ 28147-89 (розмір блоку 8 байтів) величина повної затримки при передачі інформації в один бік дорівнює:

$$T_п = 2 \cdot (2 \cdot (8 \cdot 10 \cdot 1/9600) + T_ш) = 2 \cdot (0{,}0167 + T_ш).$$

Отже, навіть якщо час шифрування буде зневажливо малим, невід'ємна затримка в комунікаційному каналі для заданої швидкості і обраного алгоритму складатиме не менше 33 мс. Застосування алгоритму AES призведе до вдвічі більшої затримки, оскільки довжина блоку для нього дорівнює 16 байтам. Використання таких методів посиленого шифрування, як багаторазове та каскадне шифрування кратно збільшує час Тш. Відтак більш придатними для використання в каналах зв'язку з БПЛА є методи динамічної модифікації.

Висновки

Проведений в даному дослідженні аналіз свідчить про перспективність використання ПЛІС для закриття інформації в тракті обміну даних між базовою станцією та БПЛА. З розглянутих підходів до посилення шифрування більш прийнятним виявилися алгоритми динамічної модифікації, що базуються на зміні алгоритму шифрування в процесі обміну даними.

Список літератури

1. Давиденко А.Н. Анализ вопросов закрытия информационного канала связи с беспилотным летательным аппаратом / А.Н. Давиденко, С.Я. Гильгурт, А.С. Потенко, А.К. Евдина // Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2014. – Вип. 71. – С. 70-76.
2. Nyangaresi V.O. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges / V.O. Nyangaresi, A. Ibrahim, Z.A. Abduljabbar, M.A. Hussain, M.A. Al Sibahee, Z.A. Hussien, M.J.J. Ghrabat // Proceedings of the 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 9–10 December 2021. – P. 1–6.
3. Nyangaresi V.O. A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles / V.O. Nyangaresi, H.M. Jasim, K.A.-A. Mutlaq, Z.A. Abduljabbar, J. Ma, I.Q. Abduljaleel, D.G. Honi // Electronics, 2023. – vol. 12. – no. 17: 3688.
4. Hilgurt S.Ya. A Survey on Hardware Solutions for Signature-Based Security Systems / S.Ya. Hilgurt // Information Technologies: Theoretical and Applied Problems (ITTAP-2021): Proceedings of the 1st International Workshop, Ternopil, Ukraine, 16 – 18 Nov. 2021. – Ternopil: Faculty of Computer Information Systems and Software Engineering, 2021. – P. 6-23.
5. Gazi P. Cascade Encryption Revisited / P. Gazi, U.M. Maurer // ASIACRYPT 2009, LNCS 5912, 2009. – P. 37-51.
6. Maurer U.M. Cascade ciphers: The importance of being first. / U.M. Maurer, J.L. Massey // Journal of Cryptology, vol. 6, № 1, 1993. – P. 55–61.
7. Гіранова А.К. Підхід до розробки реконфігуровних процесорів, що реалізують симетричні алгоритми закриття інформації / А.К. Гіранова // Сучасні комп'ютерні системи та мережі розробка та використання: матеріали 5-ї Міжнародної науково-технічної конференції ACSN-2011 – Львів: НВФ «Українські технології», 2011. – С. 183-184.