УДК 511.512

О.С. Петренко[1], О.Є. Петренко[2]

[1] *Харківський університет Повітряних Сил імені Івана Кожедуба, Харків*
[2] *Харківський інститут банківської справи Університету банківської справи Національного банку України, Харків*

ПРОПОЗИЦІЇ ЩОДО ЗАСТОСУВАННЯ АСИМЕТРИЧНОГО ШИФРУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ В КАНАЛАХ ПЕРЕДАВАННЯ КОМАНДНИХ ТА ТЕЛЕМЕТРИЧНИХ ДАНИХ МІЖ БПЛА ТА ОПЕРАТОРОМ

Проведено аналіз проблем, пов'язаних, головним чином, з безпекою експлуатації безпілотних літальних апаратів, а саме, проблем забезпечення інформаційної безпеки. Запропоновано використання алгоритмів шифрування даних та направленого шифрування для забезпечення криптографічного захисту в каналах передавання командних та телеметричних даних між БПЛА та наземним пунктом управління з метою вирішення проблем інформаційної небезпеки безпілотних авіаційних систем, а саме запобігання перехопленню даних, що передаються з борту БПЛА третьою стороною та запобігання незаконному вторгненню в канал зв'язку між БПЛА і оператором з метою атаки на органи управління БПЛА для захоплення літального апарату.

Ключові слова: *безпілотний літальний апарат, канал передавання даних, криптографічний захист, кореляційні атаки, направлене шифрування, алгоритм RSA, еліптичні криві.*

Вступ

Постановка проблеми. Досягнення сучасної науки і техніки в області авіабудування, обчислювальної техніки, радіоелектроніки і систем керування створили основу для реалізації програм і проектів розробки безпілотних літальних апаратів (БПЛА) різноманітного цільового призначення. За останні роки значно підвищився інтерес до БПЛА в більшості розвинутих держав, над їх створенням у даний час працюють десятки фірм, виконуючі державні програми з створення БПЛА нового покоління.

Це обумовлено багатьма чинниками і, насамперед, тим, що в умовах сучасних і майбутніх війн зростають втрати дорогої авіаційної техніки і особового складу в зв'язку з високим розвитком засобів ППО. Застосування БПЛА дозволяє більш ефективно та оперативно вирішувати задачі розвідки і РЕБ, цілевказання і коригування вогню, бойового керування і зв'язку, метеорологічної, радіаційної, хімічної і біологічної розвідки, без ризику для особового складу, в інтересах командування різноманітних рівнів видів збройних сил.

Однак разом з цим при використанні БПЛА виникає ряд серйозних проблем, пов'язаних, головним чином, з безпекою їх експлуатації в частості, проблем забезпечення інформаційної безпеки.

Вперше про проблему незаконного вторгнення в канал зв'язку між БПЛА і оператором заговорили в 2008 році, коли стало відомо, що повстанці в Іраку та Афганістані можуть перехоплювати данні з БПЛА. Це стало можливим з причини того, що на БПЛА RQ/MQ1 Predator и MQ9 Reaper використовуються нешифровані канали зв'язку.

Зневага захистом каналів передавання даних також може призвести до несанкціонованого втручання противника в канал управління БПЛА та до захоплення апарату. Наприклад, 4 грудня 2012 року іракські джерела ЗМІ повідомили про здійснення посадки на сході Ірану американського БПЛА RQ 170 Sentinel засобами радіоелектронної боротьби. Після цього були оприлюднені відео докази цього інциденту. В даному випадку було здійснене втручання в незахищений канал управління БПЛА.

З наведених прикладів витікає необхідність забезпечення належного криптографічного захисту каналів передавання даних між літальними апаратами та наземними пунктами управління (НПУ).

Аналіз останніх досліджень і публікацій показує, що проблемам інформаційного обміну між БПЛА та пунктами управління приділяється досить велика увага.

Наприклад в [1] розглянуті вимоги, що пред'являються в збройних силах країн НАТО до радіоліній передавання інформації з борта БПЛА.

В [2] проведений аналіз технічних засобів реалізації цих вимог.

Також питання загальновійськової стандартизації БПЛА та проблем незаконного втручання в канал зв'язку між БПЛА та оператором розглядаються в роботі [3].

Розробці програмно-моделюючого комплексу шифру, що забезпечує швидкісне поточне крипто-

графічне перетворення широкополосних сигналів, які формуються цифровими відеокамерами на борту БПЛА присвячена публікація [4].

Однак, слід зазначити, що існує декілька видів атак щодо стійкості схем потокового шифрування широкополосних сигналів.

Відповідно [5] найбільш "сильними" стосовно потокових шифрів, що представлені в роботі [4], є кореляційні атаки (Correlations Attacks).

Таким чином, статистичний аналіз шифрованих даних в зоні застосування БПЛА у сукупності з заздалегідь отриманими відомостями про структуру повідомлень з борта БПЛА, надають змогу противнику провести відповідну кореляційну атаку та визначивши ключ шифрування отримувати дані з БПЛА та втручатися в канал управління.

Метою статті є розробка пропозиції щодо застосування асиметричного, а саме направленого шифрування, для забезпечення криптографічного захисту в каналах передавання командних та телеметричних даних між БПЛА та наземними пунктами управління.

Виклад основного матеріалу

Усунути недоліки застосування програмно-моделюючого комплексу шифру, що запропонований в роботі [4], можливо шляхом використання схеми направленого шифрування. Сутність схем направленого шифрування полягає в тому, що інформація шифрується на відкритому ключі отримувача, а розшифровується на таємному ключі отримувача.

Реалізують вказані схеми використовуючи алгоритм RSA [5] та алгоритми, що базуються на перетвореннях в групах точок еліптичних кривих. Алгоритм RSA є одним з найвідоміших алгоритмів, який застосовує перетворення над кільцем класу лишків по модулю простого числа.

Але слід зазначити, що складність цього алгоритму базується на розв'язанні задачі факторизації модуля перетворення.

Забезпечити стійкість алгоритму RSA, в сучасних умовах можливо лише шляхом збільшення довжини ключа.

Наприклад, для забезпечення прийнятної стійкості порядку 10^{24} елементарних операцій при використанні алгоритму RSA необхідно використовували ключі розміром не менше 1024 біт, краще 2048 біт [5], що в свою чергу потребує великих обсягів обчислень та відповідно великого часу на шифрування та дешифрування.

Альтернативою алгоритму RSA є алгоритми, які базуються на перетвореннях в групах точок еліптичних кривих, які дозволяють забезпечувати прийнятну стійкість, використовуючи менші довжини параметрів.

Так, згідно формул, наведених в [5], складність перетворення для криптоаналізу RSA при використанні модуля, розмірність якого дорівнює 2048 біт, еквівалентна складності перетворення в групах точок еліптичних кривих, порядки базових точок яких дорівнюють 256 біт. Зручна апаратна та програмна реалізація перетворень в групах точок еліптичних кривих існує над розширенням поля характеристики два $GF(2^n)$.

З метою більш детального пояснення сутності даних алгоритмів, розглянемо використання направленого шифрування в групі точок еліптичних кривих для передачі даних з борта БПЛА.

Для застосування алгоритму направленого шифрування використаємо рівняння еліптичної кривої E над полем $GF(2^n)$, яка згідно роботи [6] має такий вигляд:

$$y^2 + xy \equiv x^3 + ax^2 + b \bmod\left(f(x), 2\right), \qquad (1)$$

де x, y – змінні, a і b елементи поля $GF(2^n)$ – коефіцієнти рівняння еліптичної кривої, f(x) – незведений поліном ступеню n, який породжує поле $GF(2^n)$.

Від значення параметру a залежить вид кривої, від значення параметра b залежить кількість точок кривої.

Здійснення направленого шифрування розпочинається з побудови загальносистемних параметрів для криптографічних перетворень в групах точок еліптичних кривих.

В загальному випадку процес побудови загальносистемних параметрів для криптографічних перетворень в групах точок еліптичних кривих передбачає виконання таких дій:

- вибір поля;
- вибір випадковим чином коефіцієнтів еліптичної кривої, із елементів обраного поля;
- обчисленні порядку еліптичної кривої;
- перевірки придатності даної кривої для використання в криптографічних додатках;
- вибору базової точки та обчисленні її порядку;
- перевірки придатності використання базової точки для здійснення криптографічних перетворень.

Але існує і другий спосіб отримати загальносистемні параметри, це скористатися державним стандартом ДСТУ 4145-2002 [7], в якому наведені еліптичні криві визначені над розширенням поля характеристики два для ступеня розширення від 163 до 431, що придатні до застосування в криптографічних перетвореннях.

Схематично порядок шифрування та передавання пакетів телеметричних даних з борту безпілотного літального апарата оператору представлено на рис. 1.

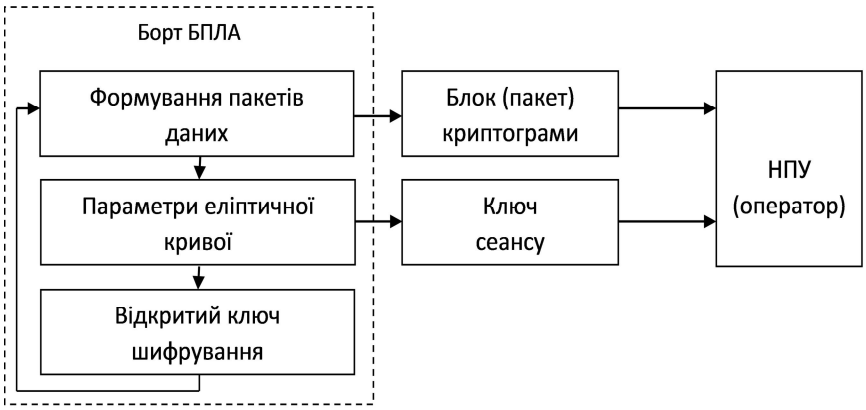

Рис. 1. Схема шифрування та передавання пакетів телеметричних даних з борту БПЛА оператору

Формалізація даної схеми полягає у наступному. Для реалізації криптографічного направленого шифрування в групі точок еліптичної кривої необхідно згенерувати пару ключів (d, Q), де d – таємний ключ борта БПЛА, який є випадковим та Q – відкритий ключ борта БПЛА, що обчислюється за правилом:

$$Q \equiv dG \bmod\left(f(x), 2^n\right), \qquad (2)$$

де G – базова точка на еліптичній кривій, f(x) – незведений поліном ступеню n.

Для здійснення направленого шифрування пакети даних M розбивають на блоки M_i, довжини яких менше модуля перетворення та для опису блоку криптограм C використовують наступне перетворення:

$$C \equiv M_i + kQ \bmod\left(f(x), 2^n\right), \qquad (3)$$

де M_i – блоки інформації, k – таємний ключ сеансу.

Також обчислюють відкритий ключ сеансу:

$$C_1 \equiv kG \bmod\left(f(x), 2^n\right), \qquad (4)$$

де G – базова точка на еліптичній кривій порядку n.

Далі БПЛА відправляє два блоки даних сеансовий ключ C_1, та зашифроване повідомлення C оператору.

Розшифрування оператором зашифрованого повідомлення здійснюється в три ітерації:

а) використовуючи таємний ключ d обчислюють значення $dC_1 = dkG \bmod\left(f(x), 2\right)$, яке є точкою еліптичної кривої (1);

б) розшифрування криптограми C, яка передано з борту БПЛА здійснюють за правилом:

$$C - dC_1 \equiv M_i + kQ - dkG \bmod\left(f(x), 2\right) \equiv M_i; \qquad (5)$$

в) однозначність перетворення перевіряється при підстановці в (5) замість Q, його виразу з порівняння (2).

Таким чином, може бути вирішена перша проблема інформаційної небезпеки безпілотних авіаційних систем (БАС), а саме перехоплення даних, що передаються з борту БПЛА третьою стороною.

Але слід відзначити, що існує також друга проблема інформаційної небезпеки безпілотних авіаційних систем, а саме проблема незаконного вторгнення в канал зв'язку між БПЛА і оператором з метою атаки на органи управління БПЛА для захоплення літального апарату. Дана проблема особливо актуальна для БАС військового та подвійного призначення.

Розглянутий алгоритм направленого шифрування дозволяє захистити дані, які передаються з борту БПЛА, але не вирішує проблемне питання втручання противника в канал управління БПЛА та захоплення апарату. Вирішити питання захисту від захоплення можливо за допомогою використання класичної схеми шифрування даних. Згідно з цією схемою, шифрування команд управління польотом БПЛА здійснює оператор, використовуючи свій таємний ключ, а апаратура на борту БПЛА розшифровує команди оператора за допомогою відкритого ключа оператора. Алгоритм реалізації даної операції реалізований з застосуванням протоколу Мессі-Омурі [8], з тією різницею, що дві ключові пари формує оператор, із них він застосовує три, а один знаходиться на борту БПЛА. Алгоритм шифрування команд управління передбачає:

а) оператор, застосовуючи рівняння еліптичної кривої (1), знаходить базову точку G та її порядок m;

б) за допомогою отриманих даних оператор формує дві ключові пари, а саме таємний ключ оператора k_o, який є взаємно простим з порядком базової точки та відкритий ключ q_o за правилом:

$$q_o \equiv k_0^{-1} \bmod\left(f(x), 2^n\right); \qquad (6)$$

в) відкритий ключ БПЛА $q_б$ та таємний ключ $k_б$ оператор знаходить також як в б);

г) оператор розміщує команди управління (повідомлення M) у вигляді точки еліптичної кривої $P_м$;

д) формування зашифрованого повідомлення здійснюється в три етапи.

Перший етап. Оператор формує криптограму Y_0 за правилом:

$$Y_0 \equiv k_o P_M \bmod\left(f(x), 2^n\right). \quad (7)$$

Другий етап. Застосовуючи таємний ключ БПЛА $k_б$, оператор формує криптограму

$$Y_b \equiv k_b Y_0 \equiv k_b k_o P_M \bmod\left(f(x), 2^n\right). \quad (8)$$

Третій етап. Оператор формує зашифроване повідомлення $C \equiv q_o Y_b \bmod\left(f(x), 2^n\right)$ та передає його на борт БПЛА.

Розшифрування команд здійснюється на борту БПЛА за допомогою відкритого ключа БПЛА $k_б$ за такою формулою:

$$P_M \equiv q_b C \bmod\left(f(x), 2^n\right). \quad (9)$$

Висновки

Проведений аналіз проблем, пов'язаних з безпекою експлуатації безпілотних літальних апаратів, показав, що не зважаючи на велику увагу в галузі стандартизації каналів зв'язку та структури даних, що передаються з БПЛА, та форматів команд управління від оператора, існує ряд проблем, пов'язаних з інформаційною безпекою цих каналів передавання даних. Головними з них є небезпека перехоплення даних, що передаються з борту БПЛА та небезпека втручання в канал управління БПЛА.

Показано, що для кожної з наведених проблем потрібно використовувати різні методи криптографічного захисту та відповідні алгоритми.

Таким чином, запропоновані для застосування алгоритми шифрування даних та направленого шифрування дозволяють створити надійний та захищений зв'язок між літальними апаратами та НПУ для запобігання несанкціонованого управління БПЛА сторонніми особами та порушення конфіденційності інформації, яка передається з борта БПЛА.

Список літератури

1. Слюсар В. Передача данных с борта БПЛА: стандарты НАТО / В. Слюсар // ЭЛЕКТРОНИКА: НТБ. – 2010. – № 3. – С. 80-86.

2. Слюсар В. Радиолинии связи с БПЛА: Примеры реализации / В. Слюсар // ЭЛЕКТРОНИКА: НТБ. – 2010. – № 5.– С. 56-60.

3. [Електронний ресурс]. – Режим доступу до ресурсу: https://airlebedev.wordpress.com/2011/10/06 безопасность-передачи-данных-с-бпла/.

4. Белецкий А.А. Программно-моделирующий комплекс криптографических AES-подобных примитивов нелинейной подстановки / А.А. Белецкий, А.В. Максименко, Д.А. Навроцкий, А.Д. Свердлова, А.И. Семенюк // Захист інформації. – 2014. – Т 16, № 3. – С. 184-191.

5. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування [Текст] / І.Д. Горбенко, Ю.І. Горбенко. – Х.: Форт, 2012. – 880 с. – ISBN 978-617-630-005-2.

6. Silverman J.H. The arifmetic of Elliptic Curve / J.H. Silverman. – GTM 106, Springer – Verlag, New York, 1986. – 868 p.

7. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка ДСТУ 4145-2002 – [Чинний від 2003-07-01]. – К.: Держстандарт України, 2003. – 31 с.

8. Koblitz N. Course in number theory and cryptography / N. Koblitz. – Springer – Verlag. New–York, 1993 – 179 p.

Надійшла до редколегії 5.05.2015

Рецензент: д-р техн. наук проф. О.І. Сухаревський, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ПРЕДЛОЖЕНИЯ ПО ПРИМЕНЕНИЮ АСИММЕТРИЧЕСКОГО ШИФРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ В КАНАЛАХ ПЕРЕДАЧИ КОМАНДНЫХ И ТЕЛЕМЕТРИЧЕСКИХ ДАННЫХ МЕЖДУ БПЛА И ОПЕРАТОРОМ

А.С. Петренко, О.Е. Петренко

Проведен анализ проблем, связанных, главным образом, с безопасностью эксплуатации беспилотных летательных аппаратов, а именно, проблем обеспечения информационной безопасности. Предложено использование алгоритмов шифрования данных и направленного шифрования для обеспечения криптографической защиты в каналах передачи командных и телеметрических данных между БПЛА и наземным пунктом управления с целью решения проблем информационной безопасности бесплотных авиационных систем, а именно предотвращения перехвата данных, передаваемых с борта БПЛА третьей стороной и предотвращения незаконного вторжения в канал связи между БПЛА и оператором с целью атаки на органы управления БПЛА для захвата летательного аппарата.

Ключевые слова: *бесплотный летательный аппарат, канал передачи данных, криптографическая защита, корреляционные атаки, направленное шифрование, алгоритм RSA, эллиптические кривые.*

PROPOSALS FOR THE USE OF ASYMMETRIC ENCRYPTION TO ENSURE CRYPTOGRAPHIC PROTECTION OF THE TRANSMISSION CHANNELS OF COMMAND AND TELEMETRY DATA BETWEEN THE UAV AND THE OPERATOR

A.S. Petrenko, O.E. Petrenko

The analysis of the problems associated mainly with the safe operation of unmanned aerial vehicles, namely, the problems of information security. Proposed the use of data encryption algorithms and directional encryption to ensure cryptographic protection of the transmission channels of command and telemetry data between UAVs and ground control to address the issues of information security ethereal aircraft systems, namely to prevent interception of data transmitted from the board of the UAV by a third party and prevent illegal invasion of the communication channel between the UAV and the operator in order to attack on the controls to capture the UAV aircraft.

Keywords: *disembodied aircraft data link, cryptographic protection, correlation attacks aimed encryption algorithm RSA, elliptic curves.*