УДК 681.3.06

Результати порівняльного аналізу стандартів криптосистем наідентифікаторах IEEE P1636.3, RFC 5091, RFC 5408

П. О. Кравченко, Л. В. Макутоніна
Харківський національний університет радіоелектроніки, Україна

У даній статті представлений загальний опис та порівняльна характеристика стандартів криптосистем на ідентифікаторах, таких, як RFC 5091, RFC 5408 та IEEE P1636.3™/D1 в області форматів даних і загальної інфраструктури передачі даних в IBE системах. У стандарті RFC 5408 описується архітектура безпеки, необхідні структури даних для криптосистем на ідентифікаторах. Стандарти RFC 5091 і IEEE P1636.3™/D1 описують системи відкритого ключа на ідентифікаторах, засновані на білінійних спарюваннях.

Ключові слова: *криптографія відкритого ключа, криптографія на ідентифікаторах, шифрування, засноване на спарюваннях, криптосистема BF, криптосистема BB1.*

В данной статье представлено общее описание и сравнительная характеристика стандартов криптосистем на идентификаторах, таких, как RFC 5091, RFC 5408 и IEEE P1636.3™/d1 в области форматов данных и общей инфраструктуры передачи данных в IBE системах. В стандарте RFC 5408 описывается архитектура безопасности, необходимые структуры данных для криптосистем на идентификаторах. Стандарты RFC 5091 и IEEE P1636.3™/d1 описывают системы открытого ключа на идентификаторах, основанные на билинейных спариваниях.

Ключевые слова: *криптография открытого ключа, криптография на идентификаторах, шифрование, основанное на спариваниях, криптосистема BF, криптосистема BB1.*

In this article general description and comparative description of standards of identity-based cryptosystems, such, as RFC 5091, RFC 5408 and IEEE P1636.3™/d1 in area of layouts of data and general infrastructure of communication of data in IBE systems. Architecture of safety is described in the standard of RFC 5408, necessary structures of data for identity-based cryptosystems. The standards of RFC 5091 and IEEE P1636.3™/d1 are described by the identity-based public-key systems based on bilinear pairings.

Key words: *public-key cryptography, identity-based encryption, pairing-based encryption, cryptosystem BF, cryptosystem BB1.*

1. Загальні відомості та актуальність теми

Шифрування, засноване на ідентифікаторах, – новий напрям в криптографії, який вирішує одну з головних проблем в інфраструктурі відкритих ключів – скріплення інформації про певного користувача з ключовими даними. У напрямі криптографії на ідентифікаторах в Україні на даний момент не було випущено жодного стандарту чи технічної специфікації. Даний напрям є новим та перспективним для України, і вимагає подальшого аналізу, оскільки з розвитком криптографії потрібно підвищувати рівень безпечності відкритих ключових даних, надавати послуги справжності, доступності, неспростовності, цілісності, тобто усі послуги безпеки інформації, що стосуються секретних ключових даних, окрім конфіденційності.

Метою цієї статті є визначення стану стандартизації криптографічних систем на ідентифікаторах та порівняльний аналіз з наступної розробкою рекомендацій відносно їх застосування.

Криптографія, заснована на ідентифікаторах (IBE) є технологією кодування відкритого ключа, яка дозволяє відкритому ключу бути обчисленим за допомогою ідентифікатора і набору з відкритих математичних параметрів. При цьому враховується відповідний секретний ключ, який буде обчислений за допомогою ідентифікатора, ряду відкритих математичних параметрів, і секретного значення всього домену. Відкритий ключ IBE може бути обчислений будь-ким, у кого є необхідні відкриті параметри; майстер ключ необхідний, для обчислення секретного ключа IBE, обчислення можуть бути виконані тільки сервером, якому довіряють, і який має цей секрет.

Характеристика систем IBE, яка відрізняється їх від інших інфраструктур відкритих ключів тим, що відкриті параметри отримуються користувачем один раз, шифрування можливе без подальшого з'єднання з сервером під час періоду дії відкритих параметрів. Стандартна IBK вимагає наявність підключення користувача до мережі (наприклад, для перевірки статуса сертифіката).

Для реалізації IBE-протоколу обміну повідомленнями необхідні наступні компоненти системи:

1). PKG - Private-key Generator - генератор секретного ключа. PKG містить майстер ключ, який використовується для генерації секретних ключів сеансу IBE. PKG приймає запит користувача на секретний ключ, проводить автентифікацію користувача, і якщо автентифікація пройшла успішно, повертає секретний ключ сеансу IBE.

2). PPS - Public Parameter Server – сервер відкритих параметрів. IBE відкриті параметри включають криптографічні параметри, до яких забезпечений відкритий доступ. Розподіляє, із забезпеченням безпеки, відкриті параметри та інформацію про користувачів системи для PKG. Схема взаємодії основних елементів IBE-систем представлена на Рис. 1.

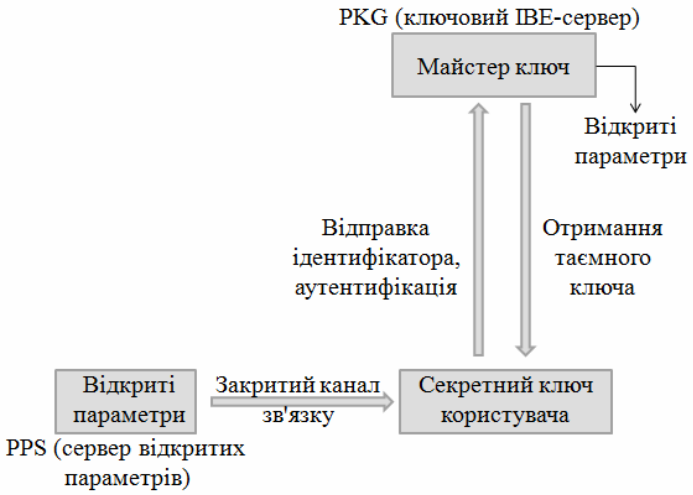

Рис. 1. Схема взаємодії базових елементів IBE-систем

2. Відправлення та одержання IBE-зашифрованого повідомлення

У стандартах RFC 5408 [1] і RFC 5091 [2], для відправки IBE-зашифрованого повідомлення користувач повинен виконати наступні кроки:

1). Отримати відкриті параметри. Як тільки користувач отримав відкриті параметри, він може виконати операцію шифрування IBE. Відкриті параметри можуть бути доступними на PPS. URI або IRI, з якого користувачі отримують IBE відкриті параметри повинні бути перевірені на достовірність. У всіх розглянутих стандартах механізми автентифікації не приводяться, дана тема потребує подальшого опрацьовування і аналізу. Крок 1 показаний нижче на Рис. 2.

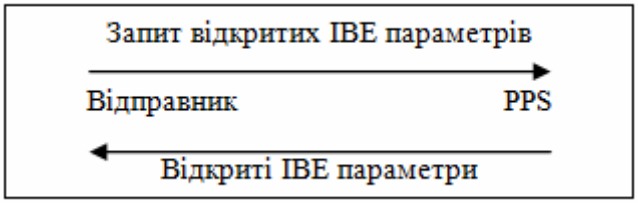

Рис. 2. Запит IBE відкритих параметрів

2). Створити і послати IBE-зашифроване повідомлення. Для того щоб зашифрувати повідомлення відправник вибирає ключ шифрування вмісту, далі – CEK (content-encryption key), та використовує його для шифрування повідомлення, потім шифрує CEK на відкритому IBE ключі одержувача. Окрім відкритих параметрів, також необхідний ідентифікатор одержувача, форма якого визначена відкритими параметрами.

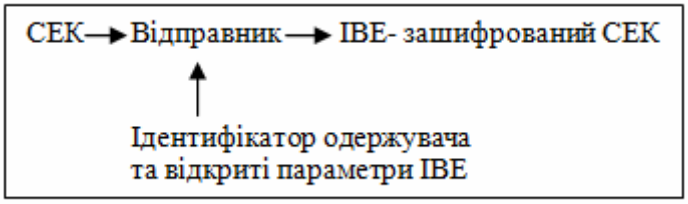

Рис.3. Використання алгоритму відкритого ключа IBE, для шифрування

Щоб прочитати IBE-зашифроване повідомлення, одержувач такого повідомлення аналізує його на наявність URI, потім отримує відкриті параметри IBE. У стандартах RFC 5091 і RFC 5408, для отримання IBE-зашифрованого повідомлення користувач повинен виконати наступні кроки:

1). Отримати відкриті параметри, які дозволяють унікально створити відкриті і секретні ключі. Відкриті параметри надаються сервером PPS по безпечному протоколу. Користувач повинен перевірити, що відповідне ім'я в свідоцтві сервера відповідає URI PPS.

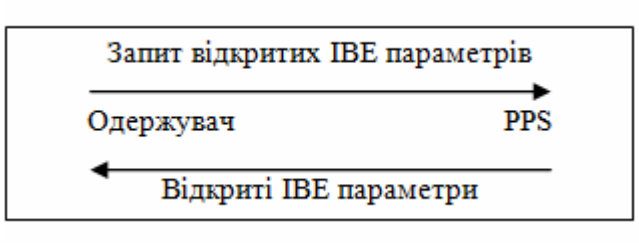

Рис.4. Запит IBE відкритих параметрів

2). Отримати секретний ключ IBE. Окрім IBE відкритих параметрів, одержувач повинен отримати секретний ключ, відповідний відкритому ключу, який використовував відправник. Секретний ключ надаються PKG по безпечному протоколу.

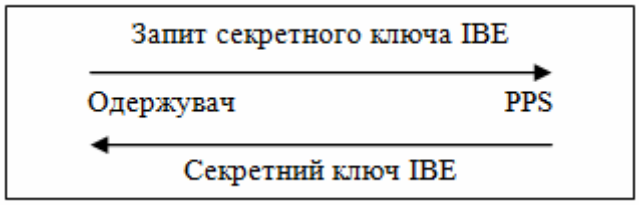

Рис. 5. Отримання секретного ключа IBE

3). Розшифрувати IBE-зашифроване повідомлення. Після отримання необхідного секретного ключа IBE, одержувач використовує цей секретний ключ IBE і передані відкриті параметри IBE для розшифровки СЕК. Ця операція показана нижче на Рис. 6.

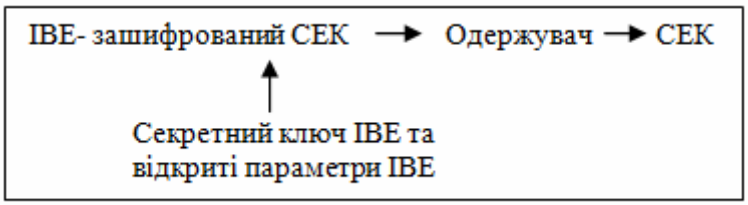

Рис. 6. Використання алгоритму відкритого ключа IBE, для декодування

Далі одержувач використовує СЕК, для розшифрування зашифрованого змісту повідомлення.

3. Короткий опис і аналіз форматів даних системи IBE запропонованих в RFC 5408

У RFC 5408 визначається, як компонент системи IBE може відновити відкриті параметри. Клієнт, під час передачі або отримання, повинен виконувати конфігурацію цих параметрів вручну, наприклад, через редагування файлу конфігурації. Однак, для спрощення конфігурації, клієнт повинен також надіслати запит відкритого параметра URI/IRI [5,6], що описаний в RFC 5408, для вибору відкритих параметрів заснований на конфігурації URI/IRI. Це

особливо корисно для інтеграції між системами IBE. Визначаючи єдиний URI/IRI, клієнт може проводити конфігурацію, для вибору всіх відповідних параметрів віддаленого PKG. Ці відкриті параметри можуть використовуватися, для шифрування повідомлення одержувачами, які засвідчують особу і відновлюють секретні ключі даного PKG.

Усі структури і типи даних зберігаються в об'єднаному модулі ASN.1.

Структура IBEIdentityInfo використовується для передачі ідентифікатора одержувача (є зашифрованою).

Структура uriPPSOID містить поля, що заповнюються одержувачем або відправником, містить відкриті параметри.

Структура IBESysParams містить відкриті параметри IBE.

IBEPublicParameters – структура, що містить відкриті параметри, відповідні алгоритмам IBE, які підтримують PKG.

Відповідно до стандарту 5408 у стандартному реєстраційному дереві повинні реєструватися три типи носіїв:

- The application/ibe-pp-data MIME type – тип носія, який передає відкриті параметри, необхідні для операцій криптографічної системи;
- The application/ibe-key-request+xml MIME type – тип носія, який містить рекомендації по автентифікації, клієнт може використовувати ці рекомендації, для формування запиту ключа, який містить додаткові дані автентифікації;
- The application/ibe-pkg-reply+xml MIME type – тип носія, за допомогою якого по захищеному протоколу передається секретний ключ IBE. Перед передачею користувач перевіряє свідоцтво сервера.

Формат відповіді сервера PKG

У стандарті 5408 визначені наступні формати відповіді сервера PKG:

IBE100 KEY_FOLLOWS – містить структуру IBEPrivateKeyReply. При правильному запиті повертає секретний ключ – структуру privateKey.

IBE101 RESERVED – код відповіді, що відповідає за функціональну сумісність нових версій протоколу. Якщо в тілі повідомлення міститься яка або інформація, то користувач повинен відмовитися від отриманих даних.

IBE201 FOLLOW_ENROLL_URI – містить елемент <ibe:location>, який визначає URI механізм автентифікації, містить сертифікат автентифікації, який надалі використовує користувач в <ibe:authData> елементі запиту ключа.

IBE300 SYSTEM_ERROR – вказує на внутрішню помилку сервера.

IBE301 INVALID_REQUEST – містить інформацію, яка може допомогти діагностувати помилку.

IBE303 CLIENT_OBSOLETE – даний код відповіді вказує, що сервер нездібний правильно обробити запит, оскільки версія запиту вже не підтримується сервером.

IBE304 AUTHORIZATION DENIED – даний код відповіді вказує, що сервер отримав ключовий запит, але сертифікат автентифікації був заблокований.

Якщо користувач отримав IBE300, IBE301, IBE303, чи IBE304 код відповіді, він повинен перервати запит ключа і відмовитися від будь-яких даних, включених в тіло відповіді.

4. Короткий опис та аналіз стандарту IEEE P1636.3™/d1-2008

Стандарт визначає загальні методи криптографії на відкритому ключі, основані на ідентифікаторах, які використовують спарювання, включаючи математичні примітиви секретних ключів, шифрування на відкритому ключі, цифрові підписи, і схеми шифрування, засновані на цих примітивах [7]. Даний стандарт також визначає алгоритми використовуваних геш-функцій, зв'язані параметри шифрування, відкриті ключі і секретні ключі.

Стандарт P1363-3 приводить довідкову інформацію для специфікацій безлічі методик, криптографії відкритого ключа, заснованої на спарюваннях, з яких прикладки можуть вибрати і цей стандарт визначає структуру цих методик, яка дозволяє вибрати відповідну методику, для певної прикладки.

Криптографія, заснована на спарюваннях, допускає інші компактніші версії традиційних криптографічних методів, такі як короткі схеми підписів, або методики управління ключем, які можуть відобразити вибраний із прикладки рядок ідентифікатора до відкритого ключа.

Різні типи криптографічних методик можуть бути абстрактно розглянуті згідно наступної загальної моделі з трьох рівнів:

- Примітиви – базові математичні операції, які засновані на задачах теоретико-числової складності. Примітиви не призначені, тільки для досягнення безпечності, але вони служать базовими блоками для схем.
- Схеми – колекція зв'язаних операцій, що комбінують примітиви і додаткові методи (Розділ 4.4 стандарту P1363-3). Схеми можуть забезпечити безпечність теоретичної складності, яка збільшується, коли вони відповідним чином застосовуються в протоколах.
- Протоколи – послідовності операцій, які будуть виконані декількома сторонами, для досягнення деякої заданої безпечності. Протоколи можуть досягти заданого рівня безпечності, якщо вини коректно здійснені.

Загальна структура примітивів описана в Розділах 5, 6,7 P1363-3; специфікація схем визначена в Розділі 8 P1363-3. Даний стандарт не визначає протоколи, вони є специфічними для кожної окремої прикладки і не розглядаються в даному стандарті. Проте, методики, визначені в цьому стандарті, є ключовими компонентами для створення різних криптографічних протоколів. Крім того, Додаток D стандарту P1363-3 описує, які методики можуть використовуватися в протоколах, для досягнення певних атрибутів безпеки.

5. Порівняльний аналіз методів генерації ключових даних і параметрів

В описаних стандартах використовується криптографія відкритого ключа на ідентифікаторах. Загальним приведених стандартів є застосування алгоритмів Boneh-Franklin и Boneh-Boyen. У стандартах RFC 5091, RFC 5408, IEEE P1636.3™/D1 обов'язковою вимогою є підтвердження достовірності відправника і одержувача повідомлення, генератора секретного ключа і сервера відкритих параметрів. Механізми автентифікації не приводяться в стандартах RFC 5091, RFC 5408, IEEE P1636.3™/D1, проте обов'язкові до застосування, оскільки системи на відкритому ключі будуються на моделі взаємної недовіри.

У стандарті RFC 5408-2009 приводиться загальний опис алгоритмів Boneh-Franklin і Boneh-Boyen, приведені протоколи обміну інформацією в IBE-схемах, описані використовувані в даних протоколах структури і типи даних.

Стандарт RFC 5091-2007 використовує математику в групі точок еліптичної кривої. Як відкриті параметри має характеристики кривої, дві точки на ЕК, номер версії алгоритму. У алгоритмі BB1 до наведених елементам додається результат спарювання двох точок *P_1, P_2 – v*. На відміну від стандарту RFC 5091-2007, стандарт IEEE P1636.3™/D1-2008 використовує математику і в полі (алгоритми BB1-IBE и BB1-KEM) и в групі точок ЕК (алгоритм BF-IBE).

Стандарт P1636.3™/D1-2008, на відміну від стандарту RFC 5091-2007, в якому використовується одна геш-функція SHA, може використовуватися декілька геш-функцій. В алгоритмі BB1-KEM використовується дві геш-функції – IHF-SHA і SHF-SHA. Алгоритм BB1-IBE аналогічний алгоритму BB1-KEM, основна відмінність – використовується три геш-функції – дві IHF1-SHA і SHF1-SHA.

Майстер ключ алгоритму BF стандарту RFC 5091-2007 представляє ціле число *s*, а для алгоритму BB1 – три цілі числа - *alpha, beta, gamma*. В алгоритмі BF-IBE стандарту IEEE P1636.3™/D1-2008 майстер ключ – елемент поля кінцевого поля *s*, а в алгоритмі BB1-KEM і BB1-IBE – три елементи - s_1, s_2, s_3.

Відкритий ключ у всіх алгоритмах розглянутих стандартів обчислюється, як геш-функція від ідентифікатора і відкритих параметрів.

Алгоритм BF генерації секретних ключів сеансу стандарту RFC 5091-2007 використовує геш-функцію від отриманих відкритих параметрів і ідентифікатора, на виході має точку на ЕК *S_ id*. Ключ сеансу в алгоритмі BB1, також як і в алгоритмі BF стандарту RFC 5091-2007, обчислюється за допомогою геш-функції від отриманих відкритих параметрів і ідентифікатора, на виході на відміну від BF має дві точки на ЕК - *D_0* и *D_1*. В стандарті IEEE P1636.3™/D1-2008, також, як і в стандарті RFC 5091-2007, для витягання секретного ключа сеансу використовується ключ сервера, відкриті параметри, ідентифікатор. Ключ сеансу для алгоритму BF-IBE – точка ЕК - K_{ID}, а для алгоритмів BB1-KEM и BB1-IBE – два значення в полі - $K_{0,ID}$ і $K_{1,ID}$.

6. Висновки

Практичне застосування інфраструктур відкритого ключа на сертифікатах виявила ряд недоліків та проблемних питань. Серед них необхідно виділити значну вартість, психологічну неприйнятність, недостатній рівень уніфікації тощо. Вказані недоліки можуть бути видалені при застосуванні криптосистем на ідентифікаторах. Основоположним принципом таких систем є те, що в якості відритого ключа асиметричної пари, причому незалежно від методу перетворення, використовується відкриті дані користувача, наприклад e-mail, почтова адреса тощо.

Проведені дослідження та порівняльний аналіз показали, що наведені стандарти визначають формати даних та модель генерації та передачі параметрів, ключів та повідомлень між сервером та користувачами, протоколи взаємодії, у тому числі вироблення та узгодження ключів, шифрування та електронного цифрового підпису та інші. Проаналізовані стандарти не вирішують проблему безпечної передачі ключових даних та параметрів, вони

лише вимагають від реальних систем такого функціоналу. Тобто можна сказати, що проаналізовані стандарти не вирішують проблем, що властиві системам на базі ідентифікаторів (довіри до УГК та безпечного отримання відкритих параметрів та ключів). Тому необхідно проводити подальші дослідження щодо вирішення зазначених проблем.

ЛІТЕРАТУРА

1. Martin, M. Schertler, G. Appenzeller, "Identity-Based Encryption Architecture and Supporting Data Structures", RFC 5408, January 2009.
2. X. Boyen, L. Martin, "Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", RFC 5091, December 2007.
3. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Proc. of CRYPTO 01, LNCS 2139, pp. 213-229, 2001.
4. D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," In Proc. of EUROCRYPT 04, LNCS 3027, pp. 223-238, 2004.
5. Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.
6. Duerst, M. and M. Suignard, "Internationalized Resource Identifiers (IRIs)", RFC 3987, January 2005.
7. Hoes Lane, "Draft Standard for Identity-based Public-key Cryptography Using Pairings", IEEE P1636.3™/D1, April 2008.

Надійшла - 23.04.2010.