УДК 681.3.06

РЕЗУЛЬТАТИ АНАЛІЗУ КРИПТОСИСТЕМ НА ІДЕНТИФІКАТОРАХ, АНАЛІЗ ДОКУМЕНТІВ IEEE P1636.3, RFC 5091, RFC 5408

М.Ф. БОНДАРЕНКО, П.О. КРАВЧЕНКО, Л.В. МАКУТОНІНА

У даній статті представлений загальний опис та характеристика документів криптографічних систем 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 документі RFC 5408 наводиться архітектура безпеки, необхідні структури даних для криптосистем на ідентифікаторах. Документи RFC 5091 і IEEE P1636.3™/D1 описують системи відкритого ключа на ідентифікаторах, засновані на білінійних спарюваннях.

Ключові слова: інфраструктура відкритих ключів, криптосистеми на ідентифікатори.

ВСТУП

Підтримка інфраструктури відкритих ключів PKI (Public Key Infrastructure) є дуже складним завданням. Зараз надійність багатьох запропонованих систем шифрування з відкритим ключем багато в чому залежить від сертифікату відкритого ключа. Але використання сертифікатів породжує ряд труднощів: проблема анулювання сертифікатів до закінчення терміну дії, передача великої кількості інформації, юридичні складнощі, великі грошові витрати. Проблему PKI можуть розв'язати криптосистеми на основі ідентифікаційних даних.

Спочатку схема шифрування на основі ідентифікаційних даних була запропонована в 1984 році Шаміром з метою спростити сертифікаційну систему. При використанні шифрування на основі ідентифікаційних даних користувачам не треба обмінюватися своїми відкритими ключами. Відкритий ключ користувача легко обчислюється з ідентифікаційних даних користувача. Тільки на етапі розшифрування потрібні послуги центру генерації ключів (Private Key Generator PKG) для того, щоб згенерувати системні параметри і секретний ключ користувача. PKG, використовуючи ідентифікаційні дані, які загальновідомі і представлені в стандартизованому вигляді, обчислює секретний ключ і передає його користувачеві. Хоча така схема породжує деякі складнощі: PKG знає секретні ключі, що в деяких застосуваннях може бути серйозною проблемою; для отримання секретного ключа користувачеві потрібно автентифікацію у PKG; для передачі секретного ключа від PKG користувачеві потрібний захищений канал.

З моменту появи цієї ідеї в 1984 році до недавнього часу побудова схеми зашифрування на основі ідентифікаційних даних залишалася відкритою проблемою. Ситуація змінилася в 2001 році з появою статті Боне-Франкліна (Boneh, Franklin). Боне і Франклін представили схему шифрування на основі ідентифікаційних даних, що використовує властивості білінійних перетворень на еліптичних кривих, яка стала першою повністю функціональною схемою шифрування на основі ідентифікаційних даних.

Раніше білінійні спарювання, а саме спарювання Вейля і спарювання Тейта, використовувалися в криптографії для реалізації MOV атак та FR атак відповідно. Ці атаки засновані на зведенні задачі дискретного логарифмування на еліптичних кривих до задачі дискретного логарифмування в кінцевому полі. Тільки після появи статті Боне-Франкліна білінійні спарювання стали використовуватися не в цілях криптографічного аналізу, а для побудови нових криптографічних протоколів.

Розробка криптографічних систем, заснованих на ідентифікаційних даних та білінійних спарюваннях, є дуже перспективною. З кожним роком росте кількість таких протоколів, що представляються на міжнародних конференціях. Зокрема діє робоча група IEEE P1363.3: Identity-Based Public Key Cryptography, очолювана William Whyte, Terence Spies, що займається розробкою стандарту криптографії на основі ідентифікаційних даних,що використовує білінійні спарювання.

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

Криптографія, заснована на ідентифікаторах (IBE), є технологією шифрування відкритого ключа, яка дозволяє відкритому ключу бути обчисленим за допомогою ідентифікатора і набору відкритих математичних параметрів. При цьому враховується відповідний секретний ключ, який буде обчислений за допомогою ідентифікатора, ряду відкритих математичних параметрів, і секретного значення – головного ключа всього домену, – майстер ключа. Відкритий ключ IBE може бути обчислений будь-ким, у кого є необхідні відкриті параметри; майстер ключ необхідний, для обчислення секретного ключа сеансу 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, зашифрування можливе без подальшого з'єднання з сервером під час періоду

дії відкритих параметрів. Традиційна ІВК вимагає наявність підключення користувача до мережі (наприклад, для перевірки статусу сертифіката).

Для реалізації ІВЕ-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 ІВЕ. PKG приймає запит користувача на секретний ключ, проводить автентифікацію користувача, і якщо автентифікація пройшла успішно, повертає секретний ключ сеансу ІВЕ.

2) PPS – Public Parameter Server – сервер відкритих параметрів. ІВЕ 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 ІВЕ-систем представлена на рис.

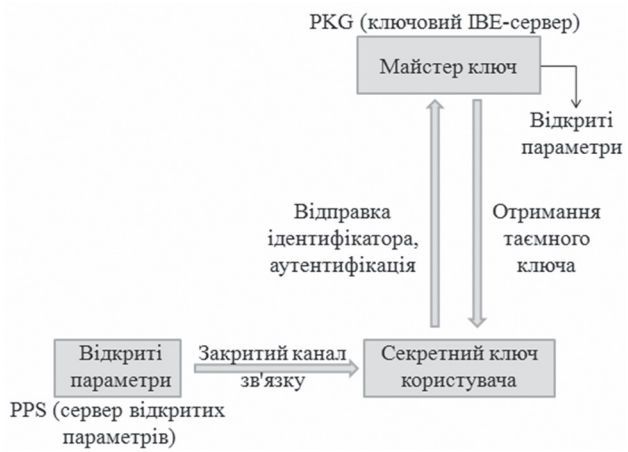

Схема взаємодії базових елементів ІВЕ-систем

1. ВІДПРАВЛЕННЯ ТА ОДЕРЖАННЯ ІВЕ-ЗАШИФРОВАНОГО ПОВІДОМЛЕННЯ

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

1) Отримати відкриті параметри. Як тільки користувач отримав відкриті параметри, він може виконати операцію зашифрування ІВЕ. Відкриті параметри можуть бути доступними на PPS. URI або IRI, з якого користувачі отримують ІВЕ відкриті параметри повинні бути перевірені на достовірність. У всіх розглянутих документах механізми автентифікації не наводяться, дана тема потребує подальшого опрацьовування і аналізу.

2) Створити і послати ІВЕ-зашифроване повідомлення. Для того щоб зашифрувати повідомлення відправник обчислює сеансовий ключ шифрування, далі – CEK (content-encryption key), та використовує його для зашифрування повідомлення, потім зашифровує CEK на відкритому ІВЕ ключі одержувача. Окрім відкритих параметрів, також необхідний ідентифікатор одержувача, форма якого визначена відкритими параметрами. Коли даний ідентифікатор співпадає з ідентифікатором повідомлення, посланого до цього, тоді не потрібна ніяка додаткова інформація від користувача для відправки зашифрованого повідомлення, яка знадобилася б для відправки незашифрованого повідомлення, і це є однією з переваг систем, заснованих на ІВЕ.

Щоб прочитати ІВЕ-зашифроване повідомлення, одержувач такого повідомлення аналізує його на наявність URI, потім отримує відкриті параметри ІВЕ.

У документах RFC 5408 [1] та RFC 5091 [2], для отримання ІВЕ-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;

2) отримати секретний ключ ІВЕ. Окрім ІВЕ відкритих параметрів, одержувач повинен отримати секретний ключ, відповідний відкритому ключу, який використовував відправник. Одержувач ІВЕ-зашифрованого повідомлення надає PKG відкритий ключ ІВЕ, який використовується для зашифрування повідомлення і автентифікації повідомлення, і робить запит на секретний ключ, який відповідає відкритому ключу ІВЕ. Секретний ключ надаються PKG по безпечному протоколу;

3) розшифрувати ІВЕ-зашифроване повідомлення. Після отримання необхідного секретного ключа ІВЕ, одержувач використовує цей секретний ключ ІВЕ і передані відкриті параметри ІВЕ для розшифрування CEK.

Далі одержувач використовує CEK, для розшифрування зашифрованого змісту повідомлення.

2. АНАЛІЗ КРИПТОСИСТЕМ НА ІДЕНТИФІКАТОРАХ

Криптосистеми ІВЕ формують таку основу для безпечного середовища обміну повідомленнями, яка відокремлює автентифікацію від шифрування, а також підтримує широкий діапазон джерел автентифікації, для забезпечення ідентифікації користувачів. Розділення автентифікації та шифрування – вкрай необхідна перевага, оскільки дана властивість ІВЕ систем дає можливість організаціям використовувати існуючі механізми (наприклад, каталоги, портали), для підтвердження достовірності користувачів. Дана властивість також дає можливість організаціям використовувати різні ідентифікаційні резерви, для автентифікації різних типів користувачів як відповідних. Далі, можливо, по потребі динамічно коректувати використовуваний механізм автентифікації; наприклад, якщо стосунки з користувачем стають формальнішими, користувач може перейти з використовуваного механізму автентифікації на надійніший механізм автентифікації.

Оскільки секретні ключі в системах ІВЕ генеруються за запитом, відновлення ключа в системах

IBE є тривіальне. Дана можливість дуже спрощує адміністративне розшифрування даних і допускає просту інтеграцію з граничними службами.

Переваги IBE:

1. Забезпечує просту, зручну у використанні процедуру шифрування (відправники потребують лише ідентифікатор одержувача).

2. Дані криптосистеми не вимагають призначеної для користувача попередньої реєстрації для відправників або одержувачів.

3. Підтримка гнучких механізмів автентифікації (не потрібне використання сертифікатів для автентифікації і підпису).

4. Можливий обмін повідомленнями між користувачами з сертифікатами і користувачами, що не мають сертифікатів.

5. Забезпечує автоматичне відновлення ключа.

6. Легка інтеграція з граничними службами передачі повідомлень (службами антиспаму, антивірусного захисту, архівації).

7. Підтримка роботи «off-line» (відправники не потребують перевірки будь-якого з ресурсів, наприклад CRLs або OCSP).

8. Невисока складність обчислень.

По запиту мережевого сканера антивірусу, антиспаму, або іншої прикладки безпеки системи (наприклад, при обміні політиками повідомленнями), можлива генерація сервером PKG на льоту необхідного секретного ключа, для перегляду вмісту повідомлення даних прикладок. Без здатності генерувати і відновити ключі зашифрування за запитом, секретні ключі користувачів мають зберігатися у спеціальному сховищі, потребують надійного захисту, вони мають бути заархівовані, для можливості роботи прикладок з текстом зашифрованих повідомлень.

На відміну від звичайної інфраструктури відкритих ключів, системи IBE не вимагають складної перевірки, попередньої реєстрації або відкликання сертифікатів. Ще одна перевага систем IBE перед системами PKI, – відсутність відкликаних списків сертифікатів та інших списків сертифікатів. Немає по суті жодної потреби в сертифікатах. Замість цього відкритий ключ користувача генерується з його ідентифікатора. Система IBE не вимагає, щоб уповноважений на сертифікацію виробив, засвідчив, або зберіг індивідуальні відкриті ключі.

Єдина інформація, яку надовго зберігає сервер PKG IBE, є «майстер ключ» – по суті велике випадкове число, яке використовується для генерації ключів сеансу користувачів і системних параметрів сервера.

Одна з найважчих проблем для системи PKI, – відкликання сертифікатів, якщо секретний ключ, на якому підписаний сертифікат скомпрометований, або якщо сертифікат потрібно заблокувати. У документі RFC 5408, який описує формати даних IBE-систем, дана проблема вирішується досить просто – в структурі «IBESysParams» (структура, що містить відкриті параметри) включені поле «validity», в якому вказаний період дії відкритих параметрів. Після виділення даного періоду відкриті параметри, а, отже, і відкриті і секретні ключі генеруються заново. Період дії може бути заданий адміністратором безпеки.

Стійкість алгоритмів IBE базується на розв'язанні задачі дискретного логарифму, а також на рішенні задачі білінійної проблеми Диффі-Гелмана.

Переваги IBE протоколів очевидні: такі протоколи роблять непотрібною інфраструктуру відкритих ключів. Замість неї необхідно підтримувати PKG, що значно простіше. Зокрема, якщо всі клієнти використовують один і той же PKG, то вони можуть безпечно спілкуватися і при цьому їм не потрібно шукати відкриті ключі в мережі.

Проте IBE системи мають ряд недоліків:

1. PKG знає секретний ключ одержувача, що в деяких застосуваннях може бути серйозною проблемою. Цей недолік можливо усунути, якщо застосовувати схеми розподілу таємниці, наприклад, зберігати майстер ключ по частинам на різних серверах PKG.

2. PKG повинен провести автентифікацію користувача (як і в системах з Центрами сертифікації).

3. Для передачі секретного ключа від PKG до користувача, що його отримує, необхідний захищений канал.

4. Одержувач публікує свої PKG відкриті параметри і відправнику необхідно отримати ці параметри, перш ніж відправляти одержувачу зашифрований лист.

Описані схеми шифрування дозволяють значно знизити загальну складність протоколів обміну ключами.

3. СТАНДАРТИЗАЦІЯ КРИПТОГРАФІЧНИХ СИСТЕМ НА ІДЕНТИФІКАТОРАХ

Керівним стандартом в галузі криптографічних систем на ідентифікаторах є проект стандарту IEEE P1363.3 [7] – Draft Standard for Identity-based Public-key Cryptography Using Pairings – Проект стандарту для криптографічних систем з відкритим ключем, заснованих на ідентифікаторах, що використовує спарювання. Проект стандарту 2008 року IEEE P1363.3 – стандарт, призначений для локальних мереж 802.1 – 802.12, розроблений робочими групами проекту 802 Інституту Інженерів по Електротехніці та Радіоелектроніки (IEEE).

Також, технічними специфікаціями, для реалізації схем криптографічних систем на ідентифікаторах є документи RFC 5408-2009 та RFC 5091-2007.

RFC 5408 – Identity-Based Encryption Architecture and Supporting Data Structures – Архітектура та підтримуючі структури даних, для криптографічних систем на ідентифікаторах. Документ RFC 5408-2009 [1] описує архітектуру безпеки, потрібну для здійснення шифрування, заснованого на ідентифікаторах. Описує протокол шифрування ключа, що використовує ідентифікатор, як відкритий ключ. Визначає структури даних, які

можуть бути використані, для здійснення такого протокола.

RFC 5091 [2] – Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems – Стандарт криптографічних систем на ідентифікаторах: Реалізація схем BF та BB1 на суперсингулярній еліптичній кривій. Документ RFC 5091 надає набір специфікацій для реалізації IBE систем шифрування, заснованих на білінійних спарюваннях. Описані дві криптосистеми: система IBE, запропонована Boneh і Franklin (BF), і система IBE, запропонована Boneh і Boyen (BB1). Приведені безпечні і практичні виконання для кожної системи, що охоплюють основні алгоритми IBE, з рівнем безпечності, що зазвичай досягається у гібридних схемах.

4. КОРОТКИЙ ОПИС IBE СХЕМ, ПРИВЕДЕНИХ У ДОКУМЕНТІ RFC 5091-2007

Обчислення і відкритих, і секретних ключів в системі IBE відносно RFC 5091-2007 може відбуватися за потребою, і є результатом своєчасного створення і відкритих, і секретних ключів. Це контрастує з іншими криптосистемами на відкритих ключах, в яких ключі генеруються псевдовипадково і розподіляються перед встановленням відкритого з'єднання, і в яких секретні ключі розшифрування повинні бути надійно архівовані, щоб можна було скористатися їх копіями, у випадку, якщо вони втрачені або зруйновані. Здатність обчислити одержувачем відкритий ключ зокрема позбавляє від необхідності відправника і одержувача взаємодіяти один з одним, або безпосередньо, або через проксі-сервер, такий як директивний сервер, перш ніж послати безпечні повідомлення.

Криптографічна система Boneh-Franklin (BF)

Криптографічна система BF в документі RFC 5091-2007 основана на шифруванні в групі точок еліптичної кривої, та складається з трьох наступних алгоритмів:

• алгоритм BFsetup – виробляє майстер ключ і генерує відкриті параметри; має дві версії Bfsetup і Bfsetup1, обидві версії випадково вибирають майстер ключ і зв'язані відкриті параметри; результуючий майстер ключ і відкриті параметри окремо зашифровуються;

• алгоритм BFderivePubl – утворює відкритий ключ з ідентифікатора користувача і дійсних відкритих параметрів, за допомогою приведених нижче геш-функцій у вигляді точки ЄК;

• алгоритм BFextractPriv – утворює секретний ключ сеансу з ряду дійсних відкритих параметрів і відповідного майстер ключа, результат роботи алгоритму – точка ЕК.

Криптографічна система Boneh-Boyen (BB1)

Криптографічна система BB1 в документі RFC 5091-2007 також основана на шифруванні в групі точок еліптичної кривої, та складається з трьох наступних алгоритмів:

• алгоритм BBsetup – виробляє майстер ключ і генерує відкриті параметри; випадково вибирається набір головних ключів і зв'язаних відкритих параметрів. Вхід і вихід алгоритму аналогічний BF;

• алгоритм BBderivePubl – утворює відкритий ключ з ідентифікатора користувача і дійсних відкритих параметрів, за допомогою приведених нижче геш-функцій у вигляді цілого числа;

• алгоритм BBextractPriv – утворює секретний ключ сеансу з ідентифікатора, ряду дійсних відкритих параметрів і відповідного майстер ключа, вихід алгоритму – дві точки ЄК.

Геш-функції та параметри безпечності, наведені в RFC 5091-2007.

Параметр *n* відповідає довжині модуля в бітах, як і у класичних криптографічних системах відкритого ключа типу Діфі-Гелмана або RSA.

Таблиця 1

Визначення залежних параметрів безпеки *n_p*, *n_q* і відповідних геш-функцій

n	*n_p*	*n_q*	*hashfcn*
1024	512	160	SHA-1
2048	1024	224	SHA-224
3072	1536	256	SHA-256
7680	3840	384	SHA-384
15360	7680	512	SHA-512

5. КОРОТКИЙ ОПИС І АНАЛІЗ ФОРМАТІВ ДАНИХ СИСТЕМИ IBE ЗАПРОПОНОВАНИХ В RFC 5408

У RFC 5408 визначається, як саме відновлюються відкриті параметри у системах IBE. Клієнт, під час передачі або отримання, повинен виконувати конфігурацію цих параметрів вручну, наприклад, через редагування файлу конфігурації. Для спрощення конфігурації, клієнт повинен також надіслати запит відкритого параметра URI/IRI [5,6], що описаний в RFC 5408, для вибору відкритих параметрів, заснованих на конфігурації URI/IRI. Це особливо корисно для інтеграції між системами IBE. Ці відкриті параметри можуть використовуватися, для розшифрування повідомлення одержувачами, вони 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 документу RFC 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 документі RFC 5408 визначені наступні формати відповіді сервера PKG:

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

IBE101 RESERVED – поле, що відповідає за функціональну сумісність нових версій протоколу. Якщо в ньому міститься інформація, то користувач повинен відмовитися від отриманих даних.

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

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.

6. КОРОТКИЙ ОПИС ТА АНАЛІЗ ПРОЕКТУ СТАНДАРТУ IEEE P1636.3-2008

Стандарт визначає загальні криптографічні методи з відкритим ключем, засновані 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 різноманітних протоколів 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 ключами, які можуть відобразити вибраний із прикладки ідентифікатор у відкритий ключ.

Структура криптографічних методик, заснованих на спарюваннях, подібна визначеній в IEEE 1363a, де важко здійсненна теоретико-числова задача використовуються як підстава для криптографічних схем, які включені в протоколи. Заснована на спарюваннях криптографія використовується по-різному, але зв'язана з набором завдань, які, імовірно, є, в обчислювальному відношенні, нездійсненними у відповідних розмірах. Ці проблеми, типові варіанти білінійної задачі Diffie-Hellman (BDH), викладеної в 1363a.

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.

Примітиви, використані в стандарті P1363-3

Примітиви, визначені в стандарті P1363-3:

• примітиви, засновані на спаровуваннях Діфі-Гелмана, у рандомізованих і нерандомізованих формулюваннях;

• примітиви, засновані на сліпих комутативних спаровуваннях;

• примітиви, засновані на спаровуваннях геш-функції параметрів домену.

У кожного з цих примітивних типів є чотири складові:

• генерація;

• перевірка згенерованого значення;

• зашифрування;

• розшифрування.

Примітиви в цьому стандарті представляються як математичні операції, і використовуються як стандартні блоки для повних схем. Виконання примітивного підпису може повернути щось схоже на підпис, навіть якщо на його вході не було дійсного секретного ключа, або ж виконання може також відхилити вхідні дані. Користувач примітиву повинен дати гарантію того, що вхідні значення задовольняють обмеженням або повинен включати релевантні перевірки. Наприклад, користувач може використовувати релевантний ключ і методи ратифікації параметра домену.

Специфікація примітиву складається з наступної інформації:

• вхід до примітиву;

• припущення про вхід, приведені в описі операції, виступаючої примітивом;

• вихід примітиву;

• операція, виконана примітивом, виражена рядом кроків;

• рекомендації області відповідності, що описують мінімальний набір входів, для яких виконання повинне проходити відповідно до примітиву, що рекомендується (див. Додаток В P1363-3).

Формат входів, виходів і процедури виконання примітивів, не розглядаються у цьому стандарті. Див. Додаток Е P1363-3 для отримання додаткової інформації про формати входу і виходу.

Схеми, запропоновані стандартом P1363-3

Типи схем, визначені стандартом P1363-3:

• шифрування, засноване на ідентифікаторах;

• інкапсуляція ключа, заснована на ідентифікаторах;

• підписи, засновані на ідентифікаторах.

Мета цих схем полягає в створенні захищеного каналу зв'язку між декількома сторонами, з імовірно присутніми, одним або декількома уповноваженими на генерацію. Дані схеми дозволяють відправнику перетворювати ідентифікатор одержувача, ряд ключових параметрів сервера, у відкритий ключ. Відкритий ключ може використовуватися для шифрування або отримання симетричного ключа. Одержувач повинен потім зробити запит на секретний ключ від уповноваженого на генерацію.

Схеми в даному стандарті представляються в загальній формі, заснованій на певних примітивах і додаткових методах шифрування повідомлення. Схеми також включають операції управлінням ключа, такі як вибір секретного ключа або отримання відкритого ключа іншої сторони. Для належної безпеки сторона повинна бути упевнена в цілісності та справжності ключа власника та відкритих параметрів.

У специфікацію схеми входить наступна інформація:

• опції схеми, такі як альтернативи для примітивів і додаткові методи;

• одна або більш операцій, залежно від схеми, виражені у ряді кроків;

• рекомендації області відповідності для реалізації відповідної схеми (див. Додаток В [7]).

Протоколи, наведені у проекті стандарту P1363.3

У IEEE P1363.3 наведені два криптографічних примітиви, які по своєї суті є протоколами встановлення ключа, це два протоколи встановлення ключа, що засновані на спарюваннях – схема Ванга та схема SCK (Smart-Chen-Kudla).

Дані протоколи дозволяють встановити відкриті та секретні ключі користувачам, для подальшого використання цих ключових даних в схемах шифрування повідомлень.

Опис геш-функцій, які використовуються в IEEE P1636.3

Стандартом IEEE P1636.3 рекомендовано до застосування три типа геш-функцій:

• геш-функція до цілого числа – IHF1-SHA;

• геш-функція до рядка – SHF1-SHA;

• геш-функція до точки на кривій – PHF1-SHA.

Функція IHF1-SHA використовує сім'ю SHA-1 та SHA-2 геш-функцій, для перетворення рядка до цілого числа. Інші геш-функції можуть бути сконструйовані за потребою за допомогою використання IHF1-SHA.

Таблиця 2

Визначення параметра захисту і відповідної геш-функції

Параметр безпечності, *t*	Використовувана геш-функція, *H*
80	SHA-1
112	SHA-224
128	SHA-256
192	SHA-384
256	SHA-512

ВИСНОВОК

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.

В даній роботі підлягали аналізу такі документи, як RFC 5091, RFC 5408, IEEE P1636.3. Загальним у розглянутих документах є застосування алгоритмів Boneh-Franklin и Boneh-Boyen. У документах RFC 5091, RFC 5408, IEEE P1636.3 обов'язковою вимогою є підтвердження достовірності відправника і одержувача повідомлення, генератора секретного ключа і сервера відкритих параметрів. Механізми автентифікації не приводяться в документах RFC 5091, RFC 5408, IEEE P1636.3, проте обов'язкові до застосування.

У документі RFC 5408 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.

Документ RFC 5091 використовує математику в групі точок еліптичної кривої. Як відкриті параметри має характеристики кривої, дві точки на EK, номер версії алгоритму.

У проекті стандарту IEEE P1636.3 описані три алгоритми шифрування, засновані ідентифікаторах, що використовують спарювання точок EK – це алгоритми BB1-IBE, BB1-KEM та алгоритм BF-IBE.

В даному стандарті приводиться наступна загальна модель побудови IBE-схем, заснованих на спарюваннях точок EK:

1) Примітиви – базові математичні операції (примітиви, засновані на спарюваннях Діфі-Гелмана; примітиви, засновані на сліпих комутативних спарюваннях и т. п.).

2) Схеми – зв'язані операції, що комбінують примітиви та додаткові методи (шифрування, інкапсуляція ключа та підписи, засновані на ідентифікаторах).

3) Протоколи – послідовності операцій, які виконуються декількома сторонами, для досягнення деякого заданого рівня безпечності.

З погляду застосування, примітиви можуть бути реалізовані на нижньому рівні (наприклад, реалізовані в межах апаратних або програмних модулів), схеми можуть бути реалізовані на середньому рівні (наприклад, реалізовані в межах криптографічних бібліотек сервісу), і протоколи можуть бути розглянуті як реалізація вищого рівня (наприклад, реалізовані в межах повних наборів застосувань).

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

Відкритий ключ у всіх алгоритмах розглянутих документах обчислюється за допомогою функції гешування від ідентифікатора і відкритих параметрів.

Проведені дослідження та порівняльний аналіз показали, що описані документи дозволяють реалізувати криптоперетворення на ідентифікаторах, забезпечують необхідний рівень стійкості у випадку застосування перетворень на еліптичній кривій. Запропоновані функції гешування є стійкими до визначення прообразу, другого прообразу, а також є стійкими до колізій. При використанні алгоритмів, що визначені в стандартах забезпечується необхідний рівень таких послуг, як конфіденційність та неспростовність. Розглянуті документи можуть бути гармонізовані в Україні та прийняті у якості технічних специфікацій.

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 до редколегії 15.06.2010.

Бондаренко Михайло Федорович, член-кореспондент НАН України, Лауреат державної премії України, доктор технічних наук, професор, ректор Харківського національного университету радіоелектроніки.

Макутоніна Лідія Вікторівна, студент групи ІБ-06-2 ХНУРЕ. Область наукових інтересів: асиметричні криптосистеми, криптографічні системи на ідентифікаторах.

Кравченко Павло Олександрович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: асиметричні криптосистеми, криптографічні системи на ідентифікаторах.

УДК 681.3.06

Результаты анализа криптосистем на идентификаторах, анализ документов IEEE P1636.3, RFC 5091, RFC 5408/ М.Ф. Бондаренко, П.О.Кравченко, Л.В. Макутонина // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 394–400.

Приведены результаты классификации и сравнительного анализа криптографических систем на идентификаторах, а также краткое описание основных стандартов криптографических систем на идентификаторах, которые рекомендуется принять в Украине в виде технических спецификаций.

Ключевые слова: инфраструктура открытых ключей, криптосистемы на идентификаторах.

Табл. 2. Ил.1. Библиогр.: 7 назв.

UDC 681.3.06

Results of analyzing the identity-based encryption, analysis of documents IEEE P1636.3, RFC 5091, RFC 5408 / M.F. Bondarenko, P.O. Kravchenko, L.V. Makutonina// Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 394-400.

The results of classification and comparative analysis of identity-based encryption are presented. A brief description of basic standards of the identity-based encryption which are recommended to be accepted in Ukraine as technical specifications, is given.

Key words: PKI, identify-based cryptosystem.

Tab. 2. Fig. 1. Ref.: 7 items.