УДК 681.3.06

І.Д. ГОРБЕНКО, д-р техн. наук, П.О. КРАВЧЕНКО, Л.В. МАКУТОНІНА

ОБГРУНТУВАННЯ ТА ВИБІР КРИТЕРІЇВ ТА ПОКАЗНИКІВ ОЦІНКИ КОМБІНОВАНИХ ІВК

Вступ

Як показали дослідження, побудову та розгортання інфраструктури відкритих ключів супроводжує ряд проблем. Аналіз зарубіжних публікацій показує, що деякі з недоліків можуть бути усунені за допомогою схем на ідентифікаторах, однак переваги, що надають IBE схеми, теж не дозволяють уникнути ряду суттєвих недоліків.

Перспективним напрямком вдосконалення інфраструктури відкритих ключів є об'єднання ІВК і IBE, що дозволяє створити нову схему, яка збереже переваги обох систем. Це об'єднання дозволить забезпечити захищений обмін повідомленнями між користувачами, як за допомогою сертифікатів відкритих ключів, так і без них.

Без IBE, системи PKI вимагають попереднього одержання сертифікатів перед початком захищеного інформаційного обміну. З IBE користувач може зареєструватися в системі вже після отримання повідомлення, так як ідентифікатор користувача використовується в якості ключа шифрування. Іншим проблемним питанням є проблема довіри до уповноваженого на генерацію таємних ключів. Цю проблему можна вирішувати за допомогою розподілення уповноваженого на декілька центрів генерації ключів. Дослідження у цьому напрямку вже велися, але кожне рішення мало свої обмеження [1]. Також не існує методу, що дозволяє визначити необхідну кількість центрів генерації ключів.

Практичне впровадження цих альтернативних систем в Україні передбачає розв'язання наступних завдань:

1. Розробка критеріїв порівняння систем.
2. Розробка показників оцінки стійкості і складності протоколів, що лежать в їх основі.
3. Розробка методичних рекомендацій щодо інтеграції розглянутих схем в існуючу ІВК України.

Серед переваг IBE можна виділити такі:

- в якості відкритого ключа користувача виступає відкритий ідентифікатор. Це дозволяє відмовитись від використання сертифікатів;
- не потребує реєстрації користувача до початку інформаційного обміну;
- дозволяє спростити процедуру відновлення секретного ключа;
- підтримує офф-лайн обмін (відправнику не треба перевіряти бази відкликаних сертифікатів);
- можливість інтеграції додаткових сервісів (анті-спам, перевірка на віруси, архівація);
- може використовуватися поряд з PKI.

Тобто, можна говорити, що інфраструктура IBE є більш простою та психологічно прийнятною для кінцевого користувача.

До основних недоліків IBE можна віднести:

- необхідність довіри до уповноваженого на генерацію ключів;
- необхідність використання конфіденційного каналу для передачі таємних ключів користувачу;
- недостатньо досліджений математичний апарат та стійкість криптографічних перетворень, на яких ґрунтується IBE;
- складна політика безпеки;
- складність впровадження та використання у великих (реальних) системах.

В цілому у нової архітектури досить багато недоліків, що стримує її широке використання.

Але завдяки своїй простоті (відкритий ключ є одночасно ідентифікатором користувача) IBE системи гарно підходять для використання у невеликих компаніях, де:

– потрібний захищений документообіг;

- немає коштів і потреби у використанні сертифікатів;

- є необхідність у підключенні додаткових сервісів (антиспам, антивірус тощо);

- є необхідність у контролі документообігу з боку керівництва або є довіра до уповноваженого на генерацію ключів;

- кожен співробітник має унікальний ідентифікатор.

Для такої ситуації з вищезазначених проблем жодна не буде впливати на ефективність захисту.

1. Аналіз основних робіт

Очевидно, що з того моменту, як криптографічне співтовариство усідомило недоліки і переваги традиційних схем та схем на ідентифікаторах, були зроблені спроби створити якісно нові системи, які б володіли перевагами обох схем.

Однією з перших таких спроб була робота Girault [2], який запропонував схему, в якій відкриті ключі були б само сертифіковані. Таємний ключ користувач виробляє собі сам, а відкритий ключ обчислюється уповноваженим та користувачем. Але, як показала робота Saeednia [7], ця система має недоліки, які дозволяють уповноваженому обчислити таємний ключ користувача.

В схемі Girault довірений орган обчислює відкриті ключі користувачів, зв'язані з їх ідентифікаторами, не володіючи при цьому інформацією про їх секретні ключі.

Схема складається з трьох етапів:

– встановлення параметрів – виконується довіреним органом;

– генерація ключової пари – виконується відправником;

– етап ідентифікації – на цьому етапі одержувач ідентифікує відправника, затверджуючи його відкритий ключ.

1. Етап встановлення параметрів

На етапі встановлення параметрів довірений орган обирає набір параметрів:

– ціле число n, добуток двох простих чисел p і q, таких, що $p = 2fp' + 1$, $q = 2fq' + 1$, де f, p', q' – прості числа;

– ціле число b порядку f по модулю p і q ($b^f \pmod n = 1$);

– ціле число e, взаємно просте з $p - 1$ і $q - 1$.

Далі він обчислює $h = b^e \pmod n$ та d, $e \cdot d \equiv 1 \pmod{\lambda(n)}$.

Останнім кроком довірений орган параметри n, f, b, e, h оголошує відкритими, параметр d – секретним, а p і q – відкидаються.

2. Етап генерації ключової пари

Відправник генерує секретний ключ s, обчислює $v = b^{-s} \pmod n$ та відправляє v до уповноваженого на генерацію (УГ). УГ формує ціле I, на підставі ідентифікатора відправника, та обчислює його відкритий ключ, як: $P = I^d v \pmod n$.

3. Етап ідентифікації

– відправник генерує випадкове число $r \in \{0, \ldots, f - 1\}$, обчислює $x = h^r \pmod n$, та відсилає x та (P, I) до одержувача:

– одержувач перевіряє, чи відповідає I ідентифікатору відправника, генерує випадкове число $c \in \{0, \ldots, e - 1\}$ та відсилає c до відправника:

– відправник обчислює $y = r - sc \pmod f$ та відсилає y до одержувача:

– одержувач перевіряє рівняння $h^y (P^e I)^c \pmod n = x$, якщо воно виконується, тоді відкритий ключ відправника вважається дійсним.

Таким чином, можна виділити основні кроки схеми Girault:

1) УГК формує набір відкритих параметрів n, f, b, e, h, та передає їх до А; параметр d – зберігає в секреті.

2) А генерує секретний ключ s, за допомогою якого обчислює v, відправляє v до УГК.

3) УГК, використовуючи отримане v та ціле I (по суті ідентифікатор), обчислює відкритий ключ P та відправляє його до А.

4) Потім йде автентифікація відкритого ключа користувача А користувачем В:

- А формує x, відправляє x свій ідентифікатор I та відкритий ключ P до В;
- В перевіряє дійсність ідентифікатора I, формує випадкове c та відправляє c до А;
- А за допомогою отриманого c обчислює y та відправляє його до В;
- В перевіряє рівняння $h^y (P^e I)^c \pmod n = x$, якщо воно виконується, тоді відкритий ключ А вважає дійсним.

Можна зробити висновок, що для виконання цієї схеми необхідна інтерактивна взаємодія користувачів між собою, але завдяки цьому забезпечується явна автентифікація відкритого ключа користувача А.

Shahrokh Saeednia та Rei Safavi-Naini [7] запропонували дві атаки на схему Girault, що дозволяють зловмиснику сформувати ідентифікатор, та відповідний йому відкритий ключ, без знання секретного значення довіреного органу. Перша атака можлива завдяки властивості $I^{2f} = 1 \pmod n$ ідентифікатора I. Тобто, ця атака працює для всіх ідентифікаторів I, що мають порядок $2, f$ і $2f$. Якщо даний ідентифікатор I має один із цих порядків, тоді можна обчислити відкритий ключ, пов'язаний з ним, не маючи секретного значення довіреного органу. Друга атака можлива, якщо можна знайти ідентифікатори I_1, I_2, такі, що $I_3 = I_1 I_2$, які відповідають дійсним ідентифікаторам. Атака може бути реалізована будь-якою підмножиною користувачів, які дійсно мають відкритий і закритий ключі пов'язані з їх ідентифікаторами.

В 2003 році C. Gentry [3] запропонував комбіновану схему на базі білінійних спарювань з використанням СВК.

Схема складається з чотирьох етапів:

1) setup – встановлення системних параметрів, виконується довіреним органом;

2) certification – сертифікація відкритого ключа користувача, виконується довіреним органом під час інтерактивної взаємодії з користувачем;

3) encrypt – зашифрування, виконується відправником;

4) decrypt – розшифрування, виконується одержувачем.

1. Етап встановлення системних параметрів:

На етапі встановлення параметрів довірений орган обирає набір параметрів:

- генерується груп G_1, G_2, простого порядку q, та $\hat{e} : \langle G_1, G_1, \to G_2 \rangle$ – оператор спарювання в групі точок еліптичної кривої;
- генерується базова точка $P \in G_1$;
- випадково обирається секретне значення $s_C \in Z / qZ$ та розраховується $Q = s_C P$;
- обираються дві геш-функції: $H_1 : \{0,1\}^* \to G_1$, $H_2 : G_2 \to \{0,1\}^n$, де n – довжина повідомлення.

Системними параметрами є: $params = \langle G_1, G_2, \hat{e}, n, P, Q, H_1, H_2 \rangle$, $s_C \in Z / qZ$ – секретне значення довіреного органу.

2. Етап сертифікації

- отримувач відправляє довіреному органу свої ідентифікаційні дані I, в тому числі свій відкритий ключ $s_{omp} P$;
- довірений орган перевіряє інформацію отримувача, якщо перевірка пройдена успішно, обчислює $P_{omp} = H_1(s_C P, i, I) \in G_1$ за час i;
- довірений орган формує сертифікат $Cert_{omp} = s_C P_{omp}$ і відправляє його одержувачу.

Перед початком розшифрування, отримувач повинен здійснити процедуру підписання I, на виході якої буде $s_{omp} P'_{omp}$, де $P'_{omp} = H_1(I)$, де $S_{omp} = s_C P_B + s_{omp} P'_{omp}$ – це комбі-

нований підпис для двох осіб. Відправник буде використовувати цей комбінований підпис у якості ключа розшифрування.

3. Етап зашифрування

Відправник виконує наступні дії:

1) обчислює $P'_{отр} = H_1(I) \in G_1$;

2) обчислює $P_{отр} = H_1(s_C P, i, I) \in G_1$.

3) випадково обирає $r \in Z / qZ$.

4) виробляє зашифрований текст:

$C = \left\langle rP, M \oplus H_2(g^r) \right\rangle$, де $g = \hat{e}(s_C P, P_{отр})\hat{e}(s_{отр} P, P'_{отр}) \in G_2$.

4. Етап розшифрування

1) одержувач виробляє підпис для даних I, на виході якого буде $s_{отр} P'_{отр}$, де $P'_{отр} = H_1(I)$. де $S_{отр} = s_C P_B + s_{отр} P'_{отр}$ – це комбінований підпис для двох осіб;

2) одержувач розшифровує повідомлення: $M = V \oplus H_2(\hat{e}(U, S_{отр}))$, $C = \langle U, V \rangle \in C$ – зашифрований текст.

Особливість цієї схеми полягає в використанні комбінованого підпису у якості ключа розшифрування, та у використанні сертифікату, який виробляється довіреним органом, у якості відкритого ключа. При цьому користувач власноруч генерує собі секретний ключ. Серед недоліків цієї схеми можна зазначити невизначеність механізму відновлення ключів та складність вироблення спільного підпису (необхідність попереднього з'єднання між користувачами).

Al-Riyami та Paterson [4] запропонували схему шифрування без сертифікатів (CLE – Certificateless Encryption Scheme), що реалізовується за сім етапів:

1. Встановлення системних параметрів (Setup)

Результатом цього кроку є наступні системні параметри:

$$params = \langle G_1, G_2, e, n, P, P_0, H_1, H_2, H_3, H_4 \rangle .$$

Простір зашифрованого тексту визначається як $C = G_1 \times \{0,1\}^{2n}$.

2. Розрахунок часткового секретного ключа (Partial-Private-Key-Extract)

1) $Q_A = H_1(ID_A) \in G_1^*$. де $ID_A = \{0,1\}^*$ – ідентифікатор отримувача;

2) частковий секретний ключ: $D_A = sQ_A \in G_1^*$.

Отримувач може перевірити правильність виробленого часткового секретного ключа, перевіривши рівняння: $e(D_A, P) = e(Q_A, P_0)$.

3. Встановлення секретного значення (Set-Secret-Value)

На вхід алгоритму надходять системні параметри $params$ та ідентифікатор отримувача ID_A. Алгоритм випадково обирає $x_A \in Z_q^*$, та встановлює його як секретне значення отримувача.

4. Встановлення секретного ключа (Set-Private-Key)

На вхід алгоритму надходять $params$, частковий секретний ключ отримувача D_A та секретне значення отримувача $x_A \in Z_q^*$. Алгоритм перетворює частковий секретний ключ D_A у повний секретний ключ S_A шляхом обчислення: $S_A = x_A D_A = x_A s Q_A \in G_1^*$.

5. Встановлення відкритого ключа (Set-Public-Key).

На вхід алгоритму подаються $params$, $x_A \in Z_q^*$, на виході – сформований відкритий ключ, як: $P_A = \langle X_A, Y_A \rangle$. де $X_A = x_A P$ та $Y_A = x_A P_0 = x_A s P$.

6. Зашифрування (Encrypt)

Для того, щоб зашифрувати повідомлення M, відправнику потрібно мати $ID_A = \{0,1\}^*$, $P_A = \langle X_A, Y_A \rangle$, результатом цього кроку є вироблення криптограми $C = \langle r, P.\sigma \oplus H_2(e(Q_A, Y_A)^r), M \oplus H_4(\sigma) \rangle$.

7. Розшифрування (Decrypt)

Використовуючи секретний ключ відправника S_A одержувач розшифровує повідомлення та в результаті отримує відкритий текст.

Основна ідея схем CLE полягає в особливостях формування секретного ключа користувача. Генерація секретного ключа користувача здійснюється шляхом використання двох компонент:

– перша компонента секретного ключа, або частковий секретний ключ (PPK – partial private key), генерується Ω на основі майстер-ключа;

– друга компонента – секретне значення користувача.

Користувач публікує також відкритий ключ, отриманий з секретного значення. Відправник, який хоче зашифрувати повідомлення, повинен мати лише відкритий ключ і ID одержувача, а також відкриті параметри центру генерації ключів.

Схема CLE дозволяє будь-якому користувачеві зашифрувати повідомлення для окремого одержувача, використовуючи відкриту інформацію (подібно PKI і IBE) без використання сертифікатів.

Існують і інші погляди на проблемні питання криптографії на ідентифікаторах. Наприклад, J. Callas [5] зазначає, що, по-перше, проблема анулювання сертифікатів у сучасному світі вже не стоїть гостро, і в подальшому, можливо, зовсім зникне. Це пов'язано з тим, що сьогодні можливості комп'ютерів зросли, а необмежений доступ до глобальної мережі вже не виняток, а реальність. Це зауваження деякою мірою ставить під сумнів один з найважливіших переваг IBE – відсутність сертифікатів (і відповідно off-line роботу). По-друге, використання унікальних та простих для запам'ятовування ідентифікаторів теж породжує деякі проблеми. Це, з одного боку, дає можливість зловмиснику (чи соціальному інженеру) досліджувати структуру організації, де використовують таку IBK, і отримувати інформацію про її службовців. Друга проблема полягає в тому, що отримати ідентифікатор користувача системи набагато легше (тому що він загальновідомий) і, відповідно, обчислити відкритий ключ теж дуже легко. А це вже дозволить спамерам направлено шифрувати повідомлення, будучи впевненими, що воно дійде до адресату.

J. Callas запропонував рішення, яке, на його погляд, вирішувало зазначені ним недоліки та було найбільш ефективним. Він відмовився від використання сертифікату як такого, замінивши його відповіддю (скоріш за все, підписаною) сервера.

Наведемо його схему:

1. УГК обирає таємний ключ.

2. УГК генерує IDT (цифровий відбиток ідентифікатора), використовуючи свій таємний ключ в якості простого секрету.

3. УГК обирає детермінований псевдовипадковий генератор, який ініціалізується за допомогою IDT. Цей генератор повинен видавати ключову пару (відкритий ключ, таємний ключ). Він також може бути будь-яким асиметричним криптографічним перетворенням.

Схема дійсно ставить у відповідність будь-якому ідентифікатору відповідну ключову пару та може використовувати відомі та перевірені криптопримітиви.

Процедура видачі ключів, згідно цієї схеми, буде наступна:

1) УГК виробляє IDT для кожного ID.

2) УГК ініціалізує рандомізований генератор (RNG) початковим значенням, рівним IDT.

3) УГК генерує ключову пару за допомогою RNG.

4) Якщо УГК отримує неавтентифікований запит для будь-якого ID, він повертає відкритий ключ Аліси. Це трапляється, коли Боб хоче дізнатися відкритий ключ Аліси.

5) Якщо УГК отримує автентифікований запит для будь-якого ID, він повертає таємний ключ. Це трапляється, коли Аліса хоче отримати свій таємний ключ.

Механізми автентифікації та захисту каналу зв'язку не уточнюються. По суті, від стандартної ІВК на ідентифікаторах відрізняється лише тим, що:

- користувачі виробляють відкриті ключі не самостійно, а роблять запит до уповноваженої сторони;
- можливо використовувати будь-які відомі криптопримітиви.

Проведемо аналіз переваг такої схеми. Тепер зловмисник не має можливості самостійно генерувати або визначати відкриті ключі користувачів, йому прийдеться відправляти запит на сервер. Крім того, для такої схеми можна використовувати відомі криптопримітиви, які вже пройшли перевірку часом.

Серед недоліків можна відзначити:

1) Необхідність чітко визначати та застосовувати механізми перевірки цілісності та справжності переданої інформації. Це пов'язано з тим, що відповідь УГК, навіть на запит зовнішнього користувача, повинна бути підписана (для забезпечення цілісності переданого відкритого ключа).

2) Так і не вирішена проблема відповідності єдиного відкритого ключа різним ідентифікаторам, тому що, згідно з запропонованою схемою, різним ідентифікаторам відповідають різні IDT , а тому і різні відкриті ключі.

3) Значно більше навантаження на УГК (порівняно з IBE), якщо він буде генерувати ключі навіть на неавтентифікований запит.

4) Крім того, зловмисники все рівно зможуть отримувати доступ до відкритих ключів користувачів, тому що вони мають можливість зробити неавтентифікований запит на сервер (якщо це дозволяють правила мережевого екрану).

Ця схема нагадує скоріше не ІВК на ідентифікаторах, а традиційну ІВК, де користувачі здійснюють пошук сертифіката по ключовому полю (яким, по суті, є ідентифікатор). Для великих систем цю систему недоречно використовувати, тому що вона має основний недолік PKI – необхідністю довіри до УГК.

Компанія Voltage [6] запропонувала комбінацію IBE та PKI, яка має наступну архітектуру та особливості (див. рисунок):

1. Користувач володіє сертифікатом PKI та ключами IBE (або чимось одним).
2. Сертифікати використовуються для автентифікації користувача та накладання цифрового підпису
3. Ключі IBE використовуються для шифрування.

Відповідно, змінюються етапи при зашифруванні повідомлення:

1. Користувач А отримує сертифікат відкритого ключа PKI.
2. Маючи в якості вхідних даних загальносистемні параметри та ідентифікатор одержувача В, А направлено шифрує повідомлення та підписує його на своєму таємному ключі IBE.
3. В надсилає запит до УГК на генерацію таємного ключа.
4. УГК перевіряє автентичність В, перевіряючи його сертифікат.
5. УГК генерує та надсилає В його таємний ключ.
6. В перевіряє цифровий підпис А, перевіряючи сертифікат А.
7. В розшифровує повідомлення.

Сильними сторонами такої системи, на думку компанії Voltage, буде:

1. Відмова від перевіряння відправником сертифікату одержувача (тепер це входить до обов'язків УГК).
2. Можливість взаємодії користувачів з сертифікатами та без них.
3. Можливість підключення додаткових сервісів.
4. Спрощення процедури анулювання сертифікату.

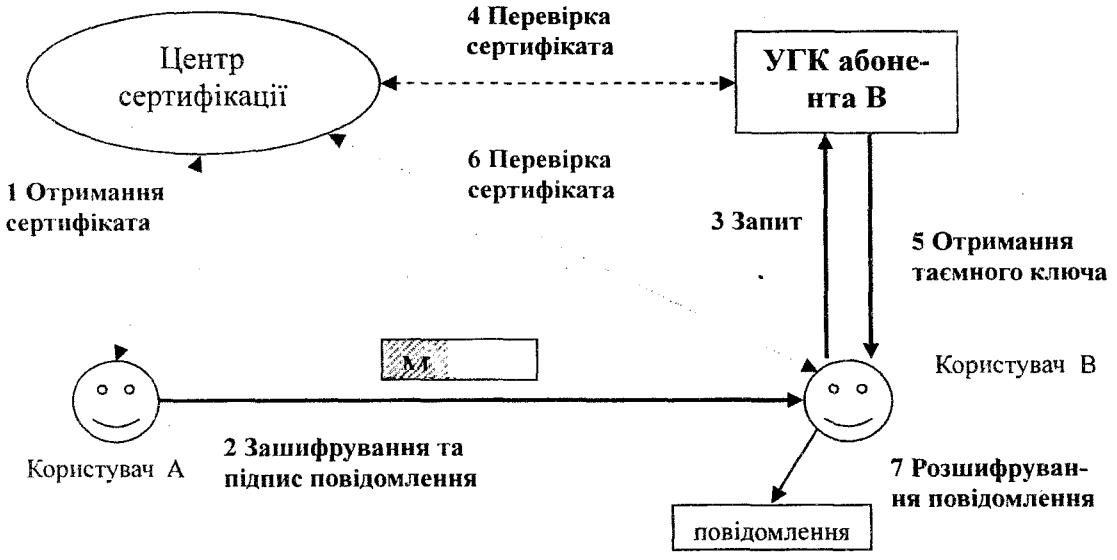

Схема взаємодії користувачів IBE+PKI Voltage

Необхідно зауважити, що:

1. Ця система може використовуватися, як надбудова над PKI.
2. Для повноцінної взаємодії користувачі повинні мати сертифікати.
3. Якщо користувачі обслуговуються різними УГК, вони мають отримувати цілісні загальні параметри цих УГК.
4. Одержувач інформації усе рівно повинен перевірити сертифікат відправника для верифікації його підпису.
5. Користувач, який не має сертифікату, може приймати повідомлення від інших користувачів, але він не має можливості підписувати повідомлення (або тільки на ключах IBE) та повинен деяким чином проходити автентифікацію на УГК. Крім того, він повинен власноруч отримувати відкриті параметри УГК одержувача.
6. УГК повинні довіряти усі користувачі, тому що він має доступ до таємних ключів.

Чим краща, ніж звичайна PKI:

1) Відправнику не потрібно перевіряти сертифікат одержувача.
2) Можна налагодити взаємодію між користувачами з сертифікатами та без.

Чим гірше:

1) УГК кожного користувача може розшифровувати повідомлення.
2) Користувачі повинні бути зареєстровані в УГК (або пройти автентифікацію, кожен раз, коли отримають ключі).

Тобто виходить, що навіть ті користувачі, які мають сертифікат, повинні довіряти УГК. Це значний недолік, що не дозволить цій системі розвиватися. Тому ця система не відповідає висунутим вимогам, що дозволяє говорити про недоречність її використання у реальному середовищі.

2. Обґрунтування та вибір критеріїв та показників оцінки комбінованих ІВК

Спочатку сформулюємо безумовні критерії оцінки комбінованої інфраструктури відкритих ключів.

1) Повинна бути реалізована модель взаємної недовіри та взаємного захисту.
2) Для захисту інформації у відритих каналах зв'язку повинні використовуватися криптопримітиви зі складністю розкриття не менше єкспоненційної (а для внутрішніх мереж – не менше субєкспоненційної).

3) Захищеність протоколів генерації та видачі ключа, що лежить в основі комбінованої ІВК, від аналітичних атак (тобто атак, що мають за мету порушити нормальний хід протоколу і скривдити цілі безпеки).

Також, для більш детального аналізу наведених схем, пропонуються наступні умовні критерії:

1. Рівень довіри до ІВК (згідно Girault).
2. Необхідність використання сертифікатів.
3. Порядок генерації відкритого ключа.
4. Порядок генерації таємного ключа.
5. Необхідність взаємодії між користувачами у реальному часі.
6. Необхідність взаємодії з сервером у реальному часі.
7. Кількість проходів / взаємодій між користувачами та сервером.
8. Автентифікація відкритого ключа.

Згідно з наведеними критеріями було проведено порівняльний аналіз наведених гібридних схем, результати якого увійшли у таблицю.

Схема / Критерій	Girault	Gentry	Al-Riyami, Paterson	J. Callas	Voltage
1	2	3	3	1	1
2	-	+	-	- (підпис)	+/-
3	УГК	УГК	користувач	УГК	УГК
4	користувач	відправник одержувач	спільно з УГК	УГК	УГК / користувач
5	+	+	-	-	+
6	+	+	-	+	+
7	5	5	3	1	7
8	відправника	+	-	-	+

Висновки

Перспективним напрямком вдосконалення інфраструктури відкритих ключів є об'єднання ІВК і ІВЕ, що дозволяє створити нові схеми, які збережуть переваги обох систем.

Пропонується порівняння комбінованих інфраструктур здійснювати на основі використання інтегрального безумовного та інтегрального умовного критеріїв. При цьому інтегральні критерії можна обчислювати на основі часткових критеріїв.

Запропоновані безумовні критерії забезпечують вибір інфраструктури, яка буде безпечною з точки зору криптографічної стійкості, формальної стійкості криптографічних протоколів, та буде реалізовувати модель взаємної недовіри та взаємного захисту. За наведеними умовними критеріями можна провести порівняння та вибрати схему, що буде найбільш підходити до конкретного випадку.

Список літератури: 1. *Бондаренко М.Ф., Горбенко І.Д., Мелецький О.П., Кравченко П.О.* Аналіз та перспективи сучасних протоколів видання та генерації ключів для інфраструктури на базі ідентифікаторів // Прикладная радиоэлектроника. – 2007. – Т. 6, №3. – С. 356-362. 2. *M. Girault:* Self-Certified Public Keys // Eurocrypt. – 1991: 490-497 3. *S. Al-Riyami, K. Paterson.* Certificateless public key cryptography. – 2003. 3. *C. Gentry.* Certificate-based encryption and the certificate revocation problem. 2003. 4. *K. Paterson.* Cryptography from pairings: a snapshot of current research. 2002. 5. *J. Callas* Identity-Based Encryption with Conventional Public-Key Infrastructure. PGP Corporation Palo Alto, California, USA, 2005. 6. *Voltage* Security. Identity-Based Encryption and PKI Making Security Work. 2005. 7. *S Saeednia, R. Safavi-Naini,* On the security of Girault's identification scheme // 1998 International Workshop on Practice and Theory in Public Key Cryptography (PKC'98). – 1998. – P 114-118.

Харківський національний університет радіоелектроніки

Надійшла до редколегії 12.08.2011