УДК 681.3.06

НАПРЯМКИ ВДОСКОНАЛЕННЯ СИСТЕМ АСИМЕТРИЧНОЇ КРИПТОГРАФІЇ В УКРАЇНІ

В.І. ДОЛГОВ, Ю.М. ІЩЕНКО

Наводяться результати аналізу напрямків вдосконалення систем асиметричної криптографії в Україні. Формулюються задачі практичного впровадження цих альтернативних систем в Україні.

The results of analysing directions of improving asymmetric cryptography systems in Ukraine are provided. The problems of practical implementation of these alternative systems in Ukraine are formulated.

ВСТУП

Законодавством України («Закон про ЕЦП») в якості базової архітектури легітимних систем асиметричної криптографії визначена ієрархічна модель інфраструктури відкритих ключів (PKI-Public Key Infrastructure). Здавалося б, PKI є ідеальним механізмом для забезпечення шифрування та надання послуг електронного цифрового підпису, але, як показує аналіз досвіду технологічно розвинутих країн, побудову та розгортання інфраструктури відкритих ключів супроводжує ряд проблем. Відповідні труднощі виникають і у впровадженні PKI в Україні. Робота присвячена аналізу існуючих систем асиметричної криптографії й визначенню перспективних напрямків їх практичного впровадження в Україні.

1. СХЕМА ШИФРУВАННЯ НА ІДЕНТИФІКАТОРАХ

Інфраструктура відкритих ключів (IBK) є сукупністю програмно-апаратних та організаційно-технічних засобів, які дозволяють використовувати в системах захисту інформації криптографію з відкритими ключами [1]. Основними функціями IBK є: створення сертифікатів відкритих ключів, які виконують функцію зв'язку ключа шифрування з ідентифікаційними даними користувача (власника ключа), забезпечення умов їх зберігання, резервного копіювання, відновлення і депонування, ведення списку відкликаних сертифікатів тощо . У якості основних переваг інфраструктури відкритих ключів можна відзначити:

– підтримку механізму електронного цифрового підпису;

– строгу автентифікацію сторін (відправника та одержувача).

Основними недоліками PKI є:

– необхідність реєстрації користувачів перед початком зв'язку;

– ризик витоку критичної інформації з каталогу сертифікатів;

– необхідність перевірки користувачами статусу сертифікату перед його застосуванням (шляхом звернення до списку відкликаних сертифікатів чи до сервера онлайнової перевірки статусу сертифіката);

– складність (фінансова та часова) процедури відновлення ключів;

– складність забезпечення додаткових послуг (анти-спам, анти-вірус, архівація).

Більшість із зазначених недоліків IBK усунено у схемі шифрування на ідентифікаторах (IBE-Identity-Based Encryption), концепцію якої запропонував A. Shamir ще у 1984 році [4]. У якості приклада розглянемо одну з найпоширеніших схем на ідентифікаторах, схему Boneh-Franklina [5], основна ідея якої полягає у відображенні ідентифікаційної інформації в точку на еліптичній кривій, а відповідний секретний ключ обчислюється помноженням відображеної точки на головний ключ. Схема реалізується наступним чином:

Установка системних параметрів (Setup). Третя довірена сторона (ТДС) виконує такі кроки:

1. ТДС генерує $\langle G_1, G_2, e\rangle$, де G_1 та G_2 є групами деякого простого порядку q, $e:\langle G_1, G_2, \to G_2\rangle$ – оператор спарювання в групі точок еліптичної кривої.

2. Випадковим шляхом обирається базова точка $P \in G_1$.

3. Випадково, з групи Z_p обирається параметр s та розраховується $P_{pub} \to [s]P$.

4. Обираються дві криптографічні геш-функції: $F:\{0,1\}^* \to G_1$ та $H:G_2 \to \{0,1\}^n$.

У цьому прикладі простором вихідних повідомлень M є множина $\{0,1\}^n$.

ТДС зберігає число s в якості секретного ключа системи (головного ключа) і оголошує відкриті системні параметри:

$$params = \langle G_1, G_2, e, n, P, P_{pub}, F, H\rangle .$$

Розрахунок секретного ключа (*Private-Key-Extraction*).

На вхід алгоритму надходить ідентифікатор отримувача $ID = \{0,1\}^*$. Виконавши фізичну ідентифікацію отримувача та переконавшись в унікальності його ідентифікатора ID, ТДС виконує такі кроки.

1. Обчислює $Q_{ID} = F(ID_{ID}) \in G_1$, що є відкритим ключем отримувача.

2. Обчислює секретний ключ отримувача $d_{ID} \leftarrow [s]Q_{ID}$.

Шифрування (*Encrypt*). Для того, щоб зашифрувати повідомлення M, відправнику потрібно обчислити $Q_{ID} = F(ID_{ID})$, системні параметри,

отримати випадкове число $r \in Z_p$ та виконати такі кроки:

1. Обчислити параметр:

$$g_{ID} \leftarrow e\left(Q_{ID}, [r]P_{pub}\right) \in G_2 .$$

2. Отримати шифртекст:

$$C \leftarrow \left([r]P, M \oplus H\left(g_{ID}\right)\right).$$

Розшифрування (*Decrypt*). Вважаємо, що $C = \langle U, V \rangle \in C$ – зашифрований, за допомогою відкритого ключа отримувача ID, текст. Для розшифрування, використовуючи свій секретний ключ $d_{ID} \in G_1$, отримувач повинен обчислити величину $V \oplus H(e(d_{ID}, U))$.

Значення, до якого отримувач застосовує функцію гешування H у ході розшифрування, фактично є величиною g_{ID}, тобто саме тим числом, до якого відправник застосовував функцію гешування H під час шифрування, отже:

$$V \oplus H(e(d_{ID}, U)) = M \oplus H(g_{ID}) \oplus H(g_{ID}) = M ,$$

оскільки побітова операція XOR є зворотною сама собі.

Відмінною рисою схем шифрування на ідентифікаторах є те, що в якості ключа шифрування використовується ідентифікатор користувача. Секретні ключі обчислює третя довірена сторона. Відмова від сертифікатів дозволяє говорити про такі переваги IBE схем [6,7]:

– не потрібна підтримка каталогу сертифікатів, що виключає ризик витоку через нього критичної інформації;

– не потрібно попередньо реєструвати користувачів у системі;

– можливість оффлайн роботи, тому що користувачам не потрібно працювати зі списками відкликаних сертифікатів або з сервером он-лайнової перевірки статусу сертифіката;

– забезпечення автоматичного відновлення ключів;

– більш проста інтеграція додаткових механізмів захисту.

Поряд з розглянутими перевагами, з'являються і недоліки:

– загроза розшифрування повідомлень третьою довіреною стороною, що може бути небажано для учасників інформаційного обміну;

– виникає проблема організації захищеного каналу для передачі секретних ключів від третьої довіреної сторони до користувачів.

2. СХЕМА ШИФРУВАННЯ НА БАЗІ СЕРТИФІКАТІВ (CBE)

C. Gentry у 2003 році [8] зробив спробу об'єднання переваг PKI та IBE схем, запропонувавши схему шифрування на базі сертифікатів (CBE-Certificate-Based Encryption), як у PKI, але з використанням ідентифікаторів, як в IBE.

Схема реалізується наступним чином:

Установка системних параметрів (*Setup*).

1. Центр сертифікації (ЦС) генерує G_1, G_2, що є групами деякого простого порядку q, та $\hat{e}: \langle G_1, G_1, \rightarrow G_2 \rangle$ – оператор спарювання в групі точок еліптичної кривої.

2. Випадково генерується базова точка $P \in G_1$.

3. Випадково обирається секретне значення $s_C \in Z / qZ$ та розраховується $Q = s_C P$.

4. Обираються дві криптографічні геш-функції: $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : G_2 \rightarrow \{0,1\}^n$ для деякого n, де n – довжина повідомлення.

Системними параметрами є:

$$params = \langle G_1, G_2, \hat{e}, n, P, Q, H_1, H_2 \rangle .$$

Секретне значення центру сертифікації $s_C \in Z / qZ$.

ЦС використовує ці параметри для формування сертифікатів відкритих ключів. Припустимо, що пара секретний ключ/відкритий ключ отримувача є $(s_{\text{отр}}, s_{\text{отр}}P)$, де $s_{\text{отр}}P$ обчислюється з урахуванням параметрів центру сертифікації. ЦС формує сертифікат для отримувача наступним чином:

Сертифікація (Certification).

Позначимо інформацію отримувача як *R`info*.

1. Отримувач відправляє інформацію *R`info* до центру сертифікації, яка включає його відкритий ключ $s_{\text{отр}}P$, та інші необхідні ідентифікаційні дані, наприклад ім'я отримувача.

2. ЦС перевіряє інформацію отримувача.

3. Якщо перевірка пройдена успішно, ЦС обчислює $P_{\text{отр}} = H_1(s_C P, i, R`info) \in G_1$ за час i.

4. ЦС формує сертифікат $Cert_{\text{отр}} = s_C P_{\text{отр}}$ і відправляє його отримувачу.

Перед початком розшифрування, отримувач повинен здійснити процедуру підписання *R`info*, на виході якої буде $s_{\text{отр}} P'_{\text{отр}}$, де $P'_{\text{отр}} = H_1(R`info)$. Зауважимо, що $S_{\text{отр}} = s_C P_B + s_{\text{отр}} P'_{\text{отр}}$ є комбінованим підписом для двох осіб, як визначено у [9,10]. Відправник буде використовувати цей комбінований підпис у якості ключа розшифрування.

Шифрування (*Encrypt*). Для того, щоб зашифрувати повідомлення M, відправник (за допомогою *R`info*) повинен:

1. Обчислити $P'_{\text{отр}} = H_1(R`info) \in G_1$.

2. Обчислити $P_{\text{отр}} = H_1(s_C P, i, R`info) \in G_1$.

3. Випадково обрати $r \in Z / qZ$.

4. Отримати шифртекст: $C = \left[rP, M \oplus H_2(g^r) \right]$, де $g = \hat{e}(s_C P, P_{\text{отр}}) \hat{e}(s_{\text{отр}} P, P'_{\text{отр}}) \in G_2$.

Розшифрування (*Decrypt*). Вважаємо, що $C = \langle U, V \rangle \in C$ – зашифрований текст. Для того, щоб розшифрувати $[U, V]$, отримувач повинен обчислити: $M = V \oplus H_2(\hat{e}(U, S_{\text{отр}}))$.

Розглянута схема дозволяє уникнути проблеми довіри до третьої довіреної сторони, до того ж, немає необхідності використовувати захищений канал для отримання секретного ключа користувачів, адже користувач сам генерує свій секретний ключ. Але схема має недолік, пов'язаний з

тим, що використання схеми з сертифікатами не дає змоги використати всі переваги схем на ідентифікаторах. Так, існує проблема з відновленням ключів, яка пов'язана з використанням сертифікатів [11].

3. СХЕМА ШИФРУВАННЯ БЕЗ СЕРТИФІКАТІВ (CLE)

Альтернативною схемою шифрування, яка могла б об'єднати переваги, і усунути недоліки PKI та IBE схем є схема шифрування без сертифікатів (CLE – Certificateless Encryption Scheme), основна ідея якої була викладена у роботі авторів Al-Riyami та Peterson [12].

Схема шифрування без сертифікатів (CLE) реалізовується за 7 етапів.

Установка системних параметрів (*Setup*).Алгоритм виконується за наступні кроки:

1. Нехай Ω – генератор системних параметрів. Ω генерує $\langle G_1, G_2, e\rangle$, де G_1 та G_2 є групами деякого простого порядку q, $e:\langle G_1, G_2, \rightarrow G_2\rangle$ – оператор спарювання в групі точок еліптичної кривої.

2. Випадковим шляхом обирається базова точка $P \in G_1$.

3. Випадково, з групи Z_q^* обирається параметр s та розраховується $P_0 = sP$.

4. Обираються чотири криптографічні геш-функції: $H_1 : \{0,1\}^n \rightarrow G_1^*$, $H_2 : G_2 \rightarrow \{0,1\}^n$, $H_3 : \{0,1\}^n \times \{0,1\}^n \rightarrow Z_q^*$, $H_4 : \{0,1\}^n \rightarrow \{0,1\}^n$, де n – довжина повідомлення.

Системними параметрами є:

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

Простір шифртексту визначається як:

$$C = G_1 \times \{0,1\}^{2n} .$$

Розрахунок часткового секретного ключа (*Partial-Private-Key-Extract*). На вхід алгоритму надходить ідентифікатор А (отримувача) $ID_A = \{0,1\}^*$. Алгоритм обчислює:

1. $Q_A = H_1(ID_A) \in G_1^*$.

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

Важливо відмітити, що отримувач може перевірити правильність роботи алгоритму *Розрахунок часткового секретного ключа* шляхом перевірки рівності $e(D_A, P) = e(Q_A, P_0)$.

Установка 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.

Установка 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:

$$S_A = x_A D_A = x_A s Q_A \in G_1^* .$$

Установка 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 $Y_A = x_A P_0 = x_A sP$.

Шифрування (*Encrypt*). Для того, щоб зашифрувати повідомлення M, відправнику потрібно мати $ID_A = \{0,1\}^*$, $P_A = \langle X_A, Y_A\rangle$ та виконати наступні кроки:

1. Перевірити, що $X_A, Y_A \in G_1^*$ шляхом перевірки рівності $e(X_A, P_0) = e(Y_A, P)$. Якщо ні – зупинити шифрування.

2. Обчислити $Q_A = H_1(ID_A) \in G_1^*$.

3. Випадково обрати $\sigma \in \{0,1\}^n$.

4. Встановити $r = H_3(\sigma, M)$.

5. Отримати шифртекст:

$C = \langle r, P.\sigma \oplus H_2(e(Q_A, Y_A)^r), M \oplus H_4(\sigma)\rangle$.

Розшифрування (*Decrypt*). Вважаємо, що $C = \langle U, V, W\rangle \in \Psi$ – зашифрований текст. Для розшифрування використовуємо секретний ключ відправника S_A:

1. Обчислюємо $V \oplus H_2(e(S_A, U)) = \sigma'$.

2. Обчислюємо $W \oplus H_4(\sigma') = M'$.

3. Встановлюємо $r' = H_3(\sigma', M')$ та перевіряємо рівність $U = r'P$. Нерівність значить помилку у розшифруванні.

4. Отримуємо M' як розшифрований C.

Якщо C є результатом правильного шифрування повідомлення M, легко побачити, що у результаті розшифрування C, отримуємо $M' = M$.

У цій схемі усувається основний недолік IBE схем, який полягає в необхідності надання ключа третій стороні, але без необхідності використання сертифікатів (як у PKI). Також, завдяки відсутності сертифікатів, вирішується проблема з відновленням ключів.

Основна ідея схем CLE полягає в особливостях формування секретного ключа користувача [13]. Як було визначено вище, генерація секретного ключа користувача здійснюється шляхом обчислення і наступного з'єднання 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. Таким чином, схема CLE дозволяє будь-якому користувачеві зашифрувати повідомлення для окремого одержувача, використовуючи відкриту інформацію (подібно PKI і IBE). Однак на відміну від традиційної PKI схеми, це досягається без необхідності використання сертифікатів. І що найголовніше, розподіл секрету між центром генерації ключів і користувачем в процесі формування секретного ключа, виключає можливість розшифрування всіх повідомлень у системі центром генерації ключів (основний недолік IBE систем) [14].

ВИСНОВКИ

Як було зазначено, 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 IBK 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, Таким чином, відправник може підписувати повідомлення будь-яким користувачам, навіть тим, що знаходяться в офф-лайні.

У якості прикладів таких «об'єднаних» схем розглянуті схеми CLE та CBE. Математичний апарат цих схем базується на спарюваннях в групі точок еліптичних кривих, завдяки чому стійкість схем ґрунтується на класичній задачі складності вирішення проблеми дискретного логарифму в групі точок еліптичної кривої, тобто є достатньо високою [4,5,9,11,13].

Слід однак відзначити, що практичне впровадження цих альтернативних систем в Україні передбачає розв'язання наступних завдань:

– розробка критеріїв порівняння систем;

– розробка показників оцінки їх стійкості і складності;

– розробка методичних рекомендацій щодо інтеграції розглянутих схем в існуючу IBK України.

Література.

[1] ITU-T (International Telecommunications Union) Recommendation X.509: Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. 2000

[2] *Горбенко І.Д., Онопрієнко В.В. та ін.* Стан та проблемні питання створення та розвитку Національної IBK. Прикладна радіоелектроніка. Том. 5 №1 2006. С. 41-51

[3] *Горбатов В.С., Полянская О.Ю.* Основы технологии PKI. – М.: Горячая линия – Телеком, 2004 – 246с.

[4] *A. Shamir,* Identity-based Cryptosystems and Signature Schemes, Proceedings of CRYPTO `84, LNCS 196, pages 47-53, Springer-Verlag, 1984.

[5] *D. Boneh and M. Franklin,* Identity-based Encryption from the Weil pairing, Proceedings of CRYPTO 2001, LNCS 2139, pages 213-229, Springer-Verlag, 2001.

[6] *F. Hess,* Efficient Identity Based Signature Schemes Based on Pairings, Selected Areas in Cryptography - Proceedings of SAC 2002, LNCS 2595, pages 310-324, Springer- Verlag, 2002.

[7] *J. Baek, J. Newmarch, R. Safavi-Naini and W. Susilo,* A Survey of Identity-Based Cryptography, Proc. of the 10th Annual Conference for Australian Unix Users Group (AUUG 2004), pp. 95-102, 2004

[8] *C. Gentry,* Certificate-Based Encryption and the Certification Revocation Problem, Proceedings of EUROCRYPT 2003, LNCS 2656, Springer-Verlag 2003, pages 272-293.

[9] *D. Galindo, P. Morillo, and C. Rafols,* Improved certificate-based encryption in the standard model, Journal of Systems and Software, vol. 81(7), pp. 1218-1226, 2008.

[10] *Y. Lu and J. Li,* A general and secure certificate-based encryption construction, In 3rd ChinaGrid Annual Conference, China, pp. 182-189, 2008.

[11] *Yang Lu and Jiguo Li,* Constructing Efficient Certificate-based Encryption with Paring, Journal of computers, vol. 4, no. 1, January 2009

[12] *S.S. Al-Riyami, K. G. Peterson.:* Certificateless public key cryptography. In: C.S. Laih (ed.) Advances in Cryptology – Asiacrypt 2003, Lecture Notes in Computer Science, vol. 2894, pp. 452-473. Springer-Verlag 2003.

[13] *A. W. Dent, B. Libert and K. G. Paterson.* Certificateless Encryption Schemes Strongly Secure in the Standard Model. In R. Cramer, editor, Public Key Cryptography -PKC 2008, volume 4939 of Lecture Notes in Computer Science, Springer-Verlag, pp. 344-359, 2008.

[14] *A. W. Dent.* A Survey of Certificateless Encryption Schemes and Security Models. International Journal of Information Security, vol. 7, no. 5, pp. 349-377, 2008.

Надійшла до редколегії 14.09.2009

Долгов Віктор Іванович, доктор технічних наук, професор, професор кафедри «Безпеки інформаційних технологій» ХНУРЕ. Область наукових інтересів: криптографія, криптоаналіз.

Іщенко Юлія Михайлівна, аспірант кафедри «Безпеки інформаційних технологій» ХНУРЕ. Область наукових інтересів: інфраструктура відкритих ключів, системи електронного цифрового підпису