УДК 681.323

П.О. КРАВЧЕНКО

УДОСКОНАЛЕНИЙ МЕТОД ГЕНЕРАЦІЇ ТА ВИДАЧІ КЛЮЧІВ ДЛЯ КОМБІНОВАНИХ ІНФРАСТРУКТУР ВІДКРИТИХ КЛЮЧІВ

Описується удосконалений метод генерації таємного ключа для комбінованої інфраструктури відкритих ключів, який відрізняється паралельними запитами користувача до розподіленого уповноваженого на генерацію ключів та формуванням особистого ключа користувачем, що дозволяє збільшити показники доступності для розподіленого уповноваженого на генерацію ключів.

Вступ

Однією з альтертатив інфраструктурі відкритих ключів (ІВК) на базі X.509 є ІВК на базі ідентифікаторів та комбіновані ІВК, що поєнують переваги обох інфраструктур. Однак одним з важливих проблемних питань, яке потребує рішення, є низька криптоживучість такої ІВК. Це пояснюється тим, що при компрометації майстер-ключа ІВК на ідентифікаторах зловмисник може обчислити усі особисті ключі користувачів. Для вирішення цього проблемного питання застосовують криптоживучі ІВК на ідентифікаторах, що характеризуються розподіленим уповноваженим на генерацію ключів (УГК). Майстер-ключ розподіляється між декількома серверами за деяким алгоритмом, що дозволяє відновити його тільки у разі участі необхідної кількості серверів. Архітектура криптоживучої комбінованої ІВК наведена на рис. 1.

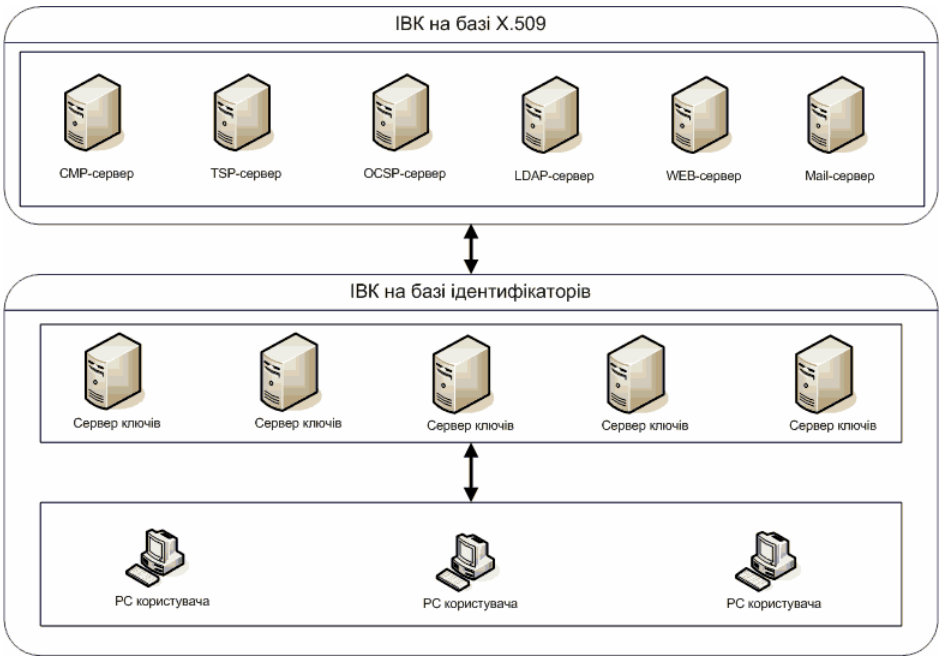

Рис. 1. Архітектура криптоживучої комбінованої ІВК

Для генерації особистого ключа користувача у криптоживучій комбінованій ІВК застосовують методи генерації та видачі ключів. Наведемо вимоги, яким повинні задовільняти протоколи, що є реалізацією таких методів:

– експоненційна складність атаки “груба сила” зі сторони уповноваженого на генерацію ключів;

– неможливість обчислення особистого ключа меншою, ніж порогова, кількістю серверів;

– відсутність автентифікованого та конфіденційного каналу зв’язку;

– забезпечення доступності розподіленого уповноваженого на генерацію ключів.

Ціль – розробка удосконаленого методу генерації та видачі ключів для комбінованої ІВК, який би задовольняв висунутим вимогам.

Об'єкт дослідження – процеси криптографічних перетворень у ІВК при реалізації процесів генерації ключів.

Предмет дослідження – метод генерації та видачі особистих ключів користувачів для криптоживучої комбінованої ІВК.

1. Існуючі рішення відносно генерації та видачі ключів

Розглянемо протоколи, що не потребують конфіденційного каналу зв'язку між користувачем та розподіленим уповноваженим на генерацію ключів.

У роботі [1] Lee запропонував протокол, який дозволяв виробляти особистий ключ без необхідності у конфіденційному каналі звязку. Користувачу необхідно реєструватися тільки у одному з множини розподілених УГК. При подальших дослідженнях Gangishetti [2] знайшов серйозні вразливості такого протоколу, на основі яких були проведені успішні атаки. Також Chunxiang [3] показав, що центр генерації може успішно провести атаку, яка дозволить йому отримати особистий ключ будь-якого користувача.

Протокол Kumar [4] використовує ідею, запропоновану Lee, але в ньому використана схема, що дозволяє генерувати особистий ключ користувача t серверам з n (t<n), але процесом генерації керує єдиний уповноважений на генерацію ключів. Суттєвим недоліком цього протоколу є те, що УГК може імітувати користувача при умові компрометації хоча б одного з серверів генерації [5].

Протокол Мелецького використовує схожу на Lee схему (рис. 2), але стійкий до усіх відомих атак. Недоліком такого протоколу є те, що у разі виведення з ладу хоча б одного сервера уся система перестане функціонувати.

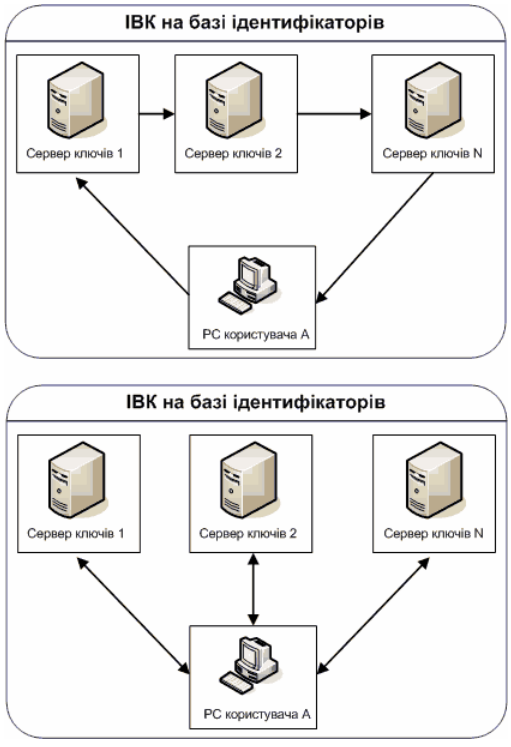

Рис. 2. Схема методу генерації ключів Lee, Мелецького

Відзначимо, що даний недолік властивий усім наведеним протоколам, тому що особистий ключ користувача виробляє уповноважений на генерацію ключів, і його доступність критична для роботи системи.

2. Удосконалений метод генерації та видачі ключів

Відзначимо, що основними відмінностями удосконаленого методу є паралельні запити до уповноважених на генерацію ключів та формування особистого ключа користувачем самостійно (рис. 3).

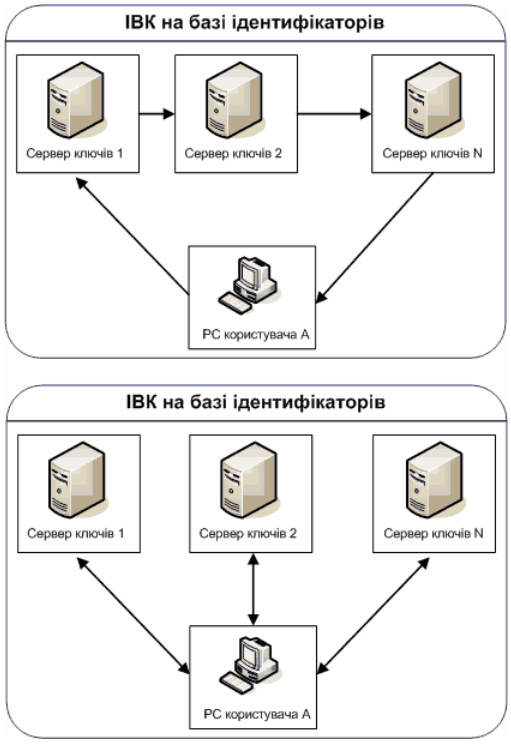

Рис. 3. Схема удосконаленого методу генерації ключів

Удосконалений метод генерації ключів характеризується такими етапами.

Етап 1. Ініціалізація. Здійснюється у такій послідовності:

– налаштування та установка параметрів серверів генерації;

– налаштування забезпечення користувача та реєстрація його в системі;

– виконання протоколу та вироблення по необхідності ключів.

Налаштування та системна установка усіх УГК виконується так:

Усі n УГК разом обирають просте число q, дві групи G_1, G_2 порядку q_i та білінійне відображення Вейля або Тейта $e : G_1 \times G_1 \to G_2$ та генератор групи $P \in G_1$. Далі обираються криптографічні геш-функції $H_1 : \{0,1\}^* \to G_1$ та $H_2 : G_2 \to \{0,1\}^l$ для деякого l.

Генерується майстер-ключ системи $S < p$, де p – просте число, порядок групи точок ЕК. Будується многочлен $a_{n-1}x_i^{\left\lfloor \frac{n+1}{2} \right\rfloor - 1} + ... + a_1 x_i + S = 0$. Згідно зі схемою Лагранжа, обчислюються частки s_i ключа для кожного сервера генерації. Кожен сервер генерації обчислює його відкритий ключ $P_i = s_i P$. Таким чином, будь-які $\left\lfloor \frac{n+1}{2} \right\rfloor$ з n УГК.

Обчислюється загальносистемний відкритий ключ $Y_N = SP$. Номери k_i кожного сервера запам'ятовуються.

Отже, публікуються або є доступними для усіх користувачів такі загальносистемні параметри: $Params = \{G_1, G_2, e, H_1, H_2, P, P_0, P_1, ...P_n, k_1, k_2, k_n, Y_N\}$.

Етап 2. Реєстрація користувача. Користувач обирає відкритий ідентифікатор ID, обчислює відповідний відкритий ключ Q_{ID} та виробляє довгостроковий секрет x. Далі користувач проходить реєстрацію на кожному сервері генерації та надає йому шляхом, що забезпечує цілісність, параметр xQ_{ID}, xP_i. Центр генерації перевіряє його правильність за допомогою обчислення та перевірки умов: $e(xQ_{ID}, P_i) = e(Q_{ID}, xP_i)$ та зберігає дані, отримані від користувача у власній базі даних. Як результат, користувачу видається доказ реєстрації у вигляді $prf_{ID} = s_i H(ID \| xQ_{ID})$.

Користувач перевіряє доказ реєстрації за допомогою рівності $e(prf_{ID}, P) = e(H(ID \| xQ_{ID}), P_i)$. При позитивному результаті процедура реєстрації вважається успішною.

Етап 3. Паралельний запит часткових ключів користувачем. Користувач здійснює запит до кожного ЦГ, надсилаючи йому кортеж $\{ID, x^{-1}P\}$.

Отримавши кортеж, ЦГ вибирає зі своєї БД xQ_{ID}, яке відповідає даному ID, та перевіряє справжність отриманої інформації: $e(x^{-1}P, xQ_{ID}) = e(P, Q_{ID})$. Якщо кортеж справжній, то ЦГ множить значення xQ_{ID} на свій таємний ключ s_i та надсилає повідомлення $\{ID, s_i xQ_{ID}\}$ користувачу.

Етап 4. Вироблення та перевірка особистого ключа користувачем. Користувач, отримавши $t \geq k$ відповідей, обирає з них будь-які k, множить кожне на x^{-1} та отримує кортеж $(s_0 Q_{ID}, s_1 Q_{ID}, s_N Q_{ID})$. Користувач будує систему рівнянь:

$$\begin{cases} a_{n-1}k_i^{n-1} + ... + a_1 k_i + a_0 = s_i Q_{ID} \pmod p, \\ a_{n-1}k_j^{n-1} + ... + a_1 k_j + a_0 = s_j Q_{ID} \pmod p, \\ a_{n-1}k_t^{n-1} + ... + a_1 k_t + a_0 = s_t Q_{ID} \pmod p, \end{cases} \quad (1)$$

де s_i, s_j, s_t – особисті ключі серверів генерації, до яких звертався користувач; $a_0 = S$ – таємний ключ системи (що був розподілений серверами генерації).

Користувач будує многочлен Лагранжа:

$$F(x) = \sum_i l_i(x) y_i \pmod p,$$

тут $l_i(x) = \prod \frac{x - x_j}{x_i - x_i} \pmod p$.

Користовач виконує підстановку значень k_i замість x_i, розв'язує систему (1) та отримує коєфіцієнт многочлена $a_{n-1}Q_{ID}, ... a_1 Q_{ID}, a_0 Q_{ID}$. Коєфіцієнт $a_0 Q_{ID} = SQ_{ID}$ буде таємним ключем користувача.

Користувач перевіряє справжність отриманого особистого ключа SQ_{ID} за допомогою рівності $e(SQ_{ID}, P) = e(Q_{ID}, P_{sys})$. При позитивному результаті перевірки він приймає отриманий ключ як особистий.

3. Обчислення показників стійкоті та доступності

Стійкість протоколу базується на інтерполяційній формулі Лагранжа, а також залежить від довжини модуля перетворень P і довжин S_i -х часток секрету. Розглянемо можливі атаки на схему Шаміра. Основною задачею атак є визначення загального секрету $S = a_0$. Величину a_0 можна визначити безпосередньо або через приватні секрети $f(l_i), ..., f(l_k)$. Якщо $a_0 = S$ і формується довіреною стороною випадково, то складність атаки типу "груба сила" за визначенням a_0 можна оцінити через імовірність P_0 її здійснення:

$$P_0 = \frac{1}{p-2} \approx \frac{1}{p} = p^{-1}. \quad (2)$$

Складність атаки "груба сила" за визначенням a_0 через $f(i_1), ..., f(i_k) \in GF(p)$ можна оцінити як

$$P_f = \left(\frac{1}{(p-1)^k} \right) = (p-1)^{-k} \approx p^{-k}. \quad (3)$$

Попередні порівняння (2) і (3) показують, що краща є атака за безпосереднім визначенням a_0. Складність цієї атаки залежить тільки від величини модуля p. Якщо p – відкритий загальносистемний параметр, відомий криптоаналітику, то складність атаки можна визначити також через безпечний час:

$$T_б = \frac{I_0}{\zeta K} \approx \frac{p}{\zeta K}, \qquad (4)$$

де $I_0 \approx p$ – число спроб підбору значення a_0 з імовірністю 1; ζ – продуктивність криптоаналітичної системи; $K = 3{,}1 \cdot 10^7$ с/рік – кількість секунд у році.

Доведемо твердження.

Твердження. Припустимо, що майстер-ключ S розподілений між n об'єктами, з яких $\left\lfloor \frac{n+1}{2} \right\rfloor$ мають змогу відтворити ключ, тобто використовується порогова схема Лагранжа $(\left\lfloor \frac{n+1}{2} \right\rfloor, n)$. Приймемо, що ймовірність успішної атаки на відмову в обслуговуванні на об'єкт дорівнює p та що усі атаки на об'єкти незалежні. Тоді ймовірність P ненадання послуги доступність $\left\lfloor \frac{n+1}{2} \right\rfloor$ об'єктами оцінюється, відповідно для базового та удосконаленого методу, співвідношеннями $P = 1 - (1-p)^n$ та $P = \sum_{k=\left\lfloor \frac{n+1}{2} \right\rfloor}^{n} C_n^k \cdot p^k \cdot (1-p)^{n-k}$.

Доведення. Для випадку базового методу обчислимо ймовірність неуспішності атаки $P_{неусп}$. Очевидно, що $P_{неусп} = (1-p)$. Враховуючи, що атаки на усі n обєктів незалежні, отримаємо ймовірність неуспішності атаки на n обєктів як $P^n{}_{неусп} = (1-p)^n$. Тоді ймовірність успішної атаки хоча б на один з n обєктів дорівнює $P = 1 - (1-p)^n$. Для удосконаленого методу використаємо формулу Бернуллі та розрахуємо ймовірність виведення з ладу $\left\lfloor \frac{n+1}{2} \right\rfloor, \left\lfloor \frac{n+1}{2} \right\rfloor + 1, .. n$ серверів. Ймовірність виведення з ладу $\left\lfloor \frac{n+1}{2} \right\rfloor$ серверів дорівнює $P_{неусп} = C_n^{\left\lfloor \frac{n+1}{2} \right\rfloor} \cdot p^{\left\lfloor \frac{n+1}{2} \right\rfloor} \cdot (1-p)^{\left(n - \left\lfloor \frac{n+1}{2} \right\rfloor\right)}$. Тоді ймовірність ненадання послуги доступність буде визначатися співвідношенням $P = \sum_{k=\left\lfloor \frac{n+1}{2} \right\rfloor}^{n} C_n^k \cdot p^k \cdot (1-p)^{n-k}$.

Показники доступності та конфіденційності для ймовірності $P = 0.1$ успішної атаки на відмову в обслуговуванні та ймовірності компрометації $P = 0.0001$ системи наведені у таблиці. За прототип візьмемо метод Мелецького.

Прототип			**Удосконалений метод**		
Кількість серверів	Ймовірність виходу з ладу	Ймовірність компрометації	Кількість серверів	Ймовірність виходу з ладу	Ймовірність компрометації
2	0.19	1.00E-008	2	0.19	1.00E-008
3	0.27	1.00E-012	3	0.028	1.00E-008
4	0.34	1.00E-016	4	0.0523	1.00E-012
5	0.41	1.00E-020	5	0.0085	1.00E-012

На рис. 4 наведено графік залежності ймовірності виходу з ладу системи від ймовірності успішності атаки на відмову в обслуговуванні для 5 серверів відповідно для базового (верхній) та удосконаленого (нижній) методу.

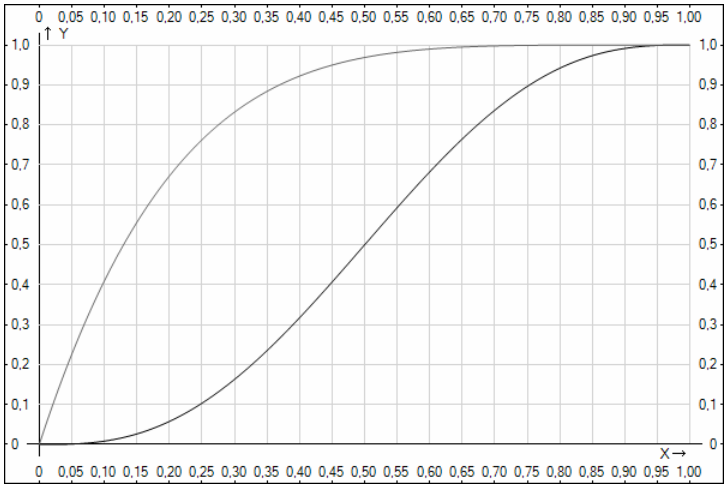

Рис. 4. Схема удосконаленого методу генерації ключів

Висновки

Наукова новизна представлена методом генерації таємного ключа для комбінованої інфраструктури відкритих ключів, який відрізняється паралельними запитами користувача до розподіленого уповноваженого на генерацію ключів та формуванням особистого ключа користувачем, що дозволяє збільшити показники доступності для розподіленого уповноваженого на генерацію ключів.

Практична значущість полягає у можливості побудови криптоживучої комбінованої ІВК, що відповідає вимогам наданню послуги доступність.

Зазначимо, що основними недоліками системи є збільшення її компонентів для досягнення тієї ж ймовірності компрометації. Проте рішення про застосування такої системи буде прийнято згідно з вимогами, що пред'являються до неї.

Перелік літератури: **1**. *Lee B., Boyd C., Dawson E., Kim K., Yang J., Yoo S.* Secure key issuing in ID-based cryptography, ACS Conferences in Research and Practice in Information Technology 32. 2004. P. 69-74. **2**. *Gangishetti R., Choudary Gorantla M., Lal Das M., Saxena A*. Cryptoanalysis of key issuing protocols in ID-based cryptosystems, IMSCCS, 2006. P. 8-12. **3**. *Chunxiang X., Junhui Z., Zhiguang Q.* A note on secure key issuing in ID-based cryptography. Technical report, 2005, http://eprint.iacr.org/2005/180.pdf. 4 p. **4**. *Kumar K.P., Shailaja G., Saxena A*. Secure and efficient threshold key issuing protocol for ID-based cryptosystems. IACR Cryptology ePrint Archive, 2006, 10 p. **5**. *Горбенко І.Д.* Удосконалений протокол вироблення ключів з асиметричними криптографічними перетвореннями зі спарюванням точок еліптичних кривих на базі ідентифікаторів / І.Д. Горбенко, П.О. Кравченко, О.П. Мелецький // Радиотехника. Харьков, 2006. Вып. 147. С.99-106.

Надійшла до редколегії 27.08.2011

Кравченко Павло Олександрович, аспірант каф. БІТ ХНУРЕ. Наукові інтереси: інфраструктури відкритих ключів. Адреса: Україна, 61166, Харків, пр. Леніна, 14, тел: 702-18-07, E-mail: kravchenkopo@gmail.com.