УДК 681.3.06:519.248.681

УДОСКОНАЛЕННЯ ПРОТОКОЛУ НУЛЬОВИХ ЗНАНЬ, ЗАСНОВАНОГО НА ДИСКРЕТНИХ ЛОГАРИФМАХ

І.В. ОЛЕШКО

В роботі запропоновано удосконалену версію протоколу нульових знань, заснованого на дискретних логарифмах – протокол нульових знань з використанням еліптичної кривої. За допомогою методу аналізу ієрархій було проведено порівняльний аналіз двох протоколів: існуючого протоколу на дискретних логарифмах та його удосконаленої версії. Доведено, що кращим протоколом є протокол нульових знань з використанням еліптичної кривої.

Ключові слова: протокол нульових знань, дискретний логарифм, еліптична крива, механізм автентифікації, Пред'явник, сертифікат, метод аналізу ієрархій.

ВСТУП

До механізмів і протоколів нульових знань висуваються суворі вимоги в частині забезпечення їх безпечності з необхідним рівнем гарантій. Сьогодні знайшов застосування протокол нульових знань, що базується на перетвореннях в скінченому полі [1]. Захищеність такого протоколу від атаки "повне розкриття " носить субекспоненційний характер. У зв'язку з цим, відповідно до вимог FIPS 186-3 [2], для забезпечення навіть мінімального рівня захищеності від атаки "повне розкриття", необхідно встановити модуль перетворення не менше 2^{2048} . Таке збільшення модуля викликає зменшення швидкодії і необхідність збільшення потужності засобів обчислення.

Розв'язання цього протиріччя, на наш погляд, можна досягти на основі використання механізму, що розглянутий вище, у групі точок еліптичної кривої. Метою цієї статті є обґрунтування та удосконалення криптографічного протоколу нульових знань на основі його реалізації у групі точок еліптичної кривої. Вказана мета досягається на основі розв'язання таких задач:

1. Аналіз рівня безпечності протоколу нульових знань на дискретному логарифмі, що наведено в стандарті [1].

2. Визначення та вирішення основних етапів та задач з удосконалення протоколу на основі застосування замість дискретного логарифму перетворення у групі точок еліптичної кривої.

3. Обґрунтування та вибір критеріїв, виконання порівняльного аналізу та розробка рекомендацій із застосування удосконаленого протоколу нульових знань.

1. МЕХАНІЗМ, ЗАСНОВАНИЙ НА СЕРТИФІКАТАХ З ВИКОРИСТАННЯМ ДИСКРЕТНИХ ЛОГАРИФМІВ

З метою використання цього механізму групами об'єктів, мають бути виконані такі кроки [1]:

а) кожен об'єкт, який має намір діяти або як пред'явник або як перевіряючий, повинен мати засоби генерації випадкових чисел;

б) усі об'єкти, що входять до складу визначеної групи, мають узгодити три позитивних цілих числа p, q та g. Ціле число p має бути простим числом, q має бути обрано таким способом, щоб воно було простим числом та одночасно було множником $p-1$. А число g має бути обрано так, щоб воно було елементом порядку q за модулем p, таким, що задовольняє вимоги:

$$g^q \bmod p = 1, \quad (1)$$

$$g \neq 1. \quad (2)$$

Значення p та q мають бути такі, що для заданого довільного цілого числа $i(1 \le i \le q)$, знаходження цілого числа j (якщо таке існує) такого, що $g^j \bmod p = i$ має бути обчислювально неможливо;

в) усі об'єкти групи мають дійти до згоди щодо того, яка функція хешування використовуватиметься;

г) кожен об'єкт, який має намір діяти як пред'явник, має бути забезпечений асиметричною ключовою парою;

д) кожен об'єкт, який має намір діяти як перевіряючий, має бути забезпечений засобами обчислення довірених копій відкритих ключів перевірки для об'єктів, чия ідентичність перевіряється.

Кожен об'єкт, який має намір діяти як пред'явник у цьому механізмі, має бути забезпечений асиметричною ключовою парою (y_E, z_x), де z_X (особистий ключ) має бути цілим числом, таким, що задовольняє нерівності $0 \le z_X \le q$. Відповідне значення відкритого ключа перевірки y_X має дорівнювати $g^{z_x} \bmod p$.

Нижче наведено обміни, які необхідно здійснювати в ході виконання односпрямованого механізму автентифікації між Пред'явником А та Перевіряючим В, для того щоб В мав змогу впевнитися в тому, що об'єкт А є тим за кого він себе видає.

Механізм автентифікації наведено на рис. 1. Цифри у дужках позначають відповідні кроки обміну, які описано нижче.

Форма першого маркера ($TokenAB_1$), що надсилається пред'явником перевіряючому або

$TokenAB_1 = W$, або $TokenAB_1 = h(W \| Text)$. W — це доказ, h — функція гешування, а $Text$ це необов'язкове текстове поле. Якщо це текстове поле непусте, то об'єкт B повинен мати засоби для того, щоб отримати це значення; це може потребувати від об'єкта A надіслати все або частину текстового поля разом із маркером $TokenAB_1$.

Форма другого маркера ($TokenAB_2$), що надсилається пред'явником перевіряючому: $TokenAB_2 = D$, де D — це відповідь.

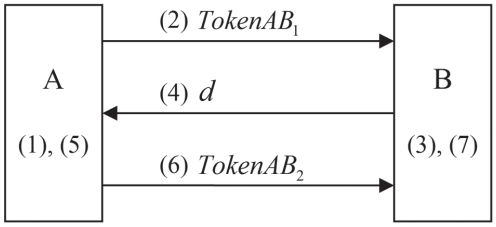

Рис. 1. Механізми, засновані на дискретних логарифмах

1) Об'єкт A обирає випадкове число r, з огляду на те, що r має бути цілим числом, яке задовольняє нерівності $1 \le r \le q$. Це число зберігається в таємниці об'єктом A. Об'єкт A обчислює доказ W:

$$W = g^r \bmod p. \quad (3)$$

2) Об'єкт A надсилає $TokenAB_1$ об'єкту B. Маркер $TokenAB_1$ має бути рівним або W або $h(W \| Text)$.

3) Отримавши маркер $TokenAB_1$, об'єкт B має випадковим чином обрати ціле число d (запит), значення якого має задовольняти нерівності $0 \le d \le q$.

4) Об'єкт B надсилає запит d об'єкту A.

5) Отримавши запит d, об'єкт A повинен обчислити відповідь D з (секретного) значення r та особистого ключа z_A об'єкта A за такою формулою:

$$D = r - dz_A \bmod q. \quad (4)$$

6) Об'єкт A надсилає маркер $TokenAB_2$ об'єкту B.

7) Отримавши відповідь D, об'єкт B має виконати такі розрахунки:

а) об'єкт B перевіряє, що $0 < D < q$. І якщо це не так, то об'єкт B бракує об'єкт A;

б) об'єкт B обчислює значення W' за такою формулою:

$$W' = (y_A)^d g^D \bmod p. \quad (5)$$

г) якщо W було надіслано при першому обміні процедури, то об'єкт B перевіряє, що обчислене значення $W' = W$. Якщо $h(W \| Text)$ було надіслано при першому обміні процедури, то об'єкт B перевіряє, що обчислене значення $h(W' \| Text) = h(W \| Text)$, яке надіслано при першому обміні процедури. Якщо перевірка завершилася успішно, вважається, що уся ця ітерація завершена успішно. В інших випадках об'єкт B бракує об'єкт A.

2. АНАЛІЗ ІСНУЮЧОГО ПРОТОКОЛУ АВТЕНТИФІКАЦІЇ, ЗАСНОВАНОГО НА СЕРТИФІКАТАХ З ВИКОРИСТАННЯМ ДИСКРЕТНИХ ЛОГАРИФМІВ

Проведемо аналіз одного з протоколу нульових знань, заснованого на сертифікатах з використанням дискретних логарифмів. Складність криптографічного алгоритму залежить від довжини ключа, що використовується, а, отже, і від кількості різних, можливих ключів. Складність криптоаналізу алгоритму, заснованого на дискретних логарифмах, обчислюється за формулою [3]:

$$I_{дл} = e^{\delta(\ln p)^{\nu}(\ln\ln p)^{1-\nu}}. \quad (6)$$

Сучасні обчислювальні потужності, а також алгоритм криптоаналізу дозволяють використовувати в цій формулі такі значення для δ і ν: $\delta = 2.06$, $\nu = 1/3$.

Припустимо, що даний протокол заснований на перетвореннях у групі точок еліптичної кривої. Складність криптоаналізу для такого протоколу обчислюватиметься за такою формулою :

$$I_{ек} \approx \sqrt{-2n\ln(1 - P_к)}, \quad (7)$$

де n — порядок базової точки, $P_к$ — імовірність колізії.

У подальших розрахунках приймемо, що $P_к = 0.99$, тоді:

$$I_{ек0,99} \approx \sqrt{-2n\ln 10^{-2}} = \sqrt{4\ln 10 n} \approx 3.03\sqrt{n}. \quad (8)$$

Також проведемо розрахунок безпечного часу $t_б$. Безпечним часом називається кількість часу, необхідне для розкриття алгоритму із заздалегідь заданою ймовірністю успіху. $t_б$ розраховується за формулою [4]:

$$t_б = \frac{N_{кл}}{\gamma \cdot k} P_у, \quad (9)$$

де $N_{кл} = I$; к $\approx 3{,}1 * 10^7$ (с), кількість секунд у році; $P_у$ — імовірність успіху. У подальших розрахунках $P_у = 1$, тобто 100%; γ — кількість операцій в секунду, які виконуються системою криптоаналітика для заданого алгоритму. Для операцій, які виконуються в полях та кільцях $\gamma = 10^{12}$, а для операцій у групі точок еліптичної кривої — $\gamma = 10^{10}$.

Розрахуємо значення стійкості I та безпечного часу $t_б$, для алгоритмів, що базуються на перетвореннях у полях та кільцях та у групі точок еліптичної кривої (ЕК). Розрахуємо ці значення для таких довжин ключа: 2^{128}, 2^{256}, 2^{512}, 2^{1024}.

Таблиця 1

Порівняння I та t_1, в залежності від довжини ключа

Довжина ключа	2^{128}		2^{256}	
	I	$t_б$	I	$t_б$
Поля та кільця	$7.1*10^{10}$	$2.3*10^{-9}$	$1.4*10^{15}$	$0.45*10^{-4}$
Еліптична крива	$5.6*10^{19}$	$1.2*10^{2}$	$1.03*10^{39}$	$3.3*10^{21}$

Таблиця 2

Порівняння I та t_1, в залежності від довжини ключа

Довжина ключа	2^{512}		2^{1024}	
	I	$t_б$	I	$t_б$
Поля та кільця	$4.4*10^{20}$	14	$9.5*10^{27}$	$3.07*10^{8}$
Еліптична крива	$3.5*10^{77}$	$1.1*10^{60}$	$4.06*10^{154}$	$1.3*10^{137}$

При порівнянні цих двох алгоритмів, спостерігається збільшення часу необхідного для розкриття ключа при збереженні його довжини для алгоритму, що базується на перетвореннях у групі точок еліптичної кривої, або з іншого боку, $t_б$ залишається колишнім, а довжина ключа значно зменшується. Тому пропозицією з удосконалення протоколу автентифікації, заснованого на сертифікатах з використанням дискретних логарифмів, буде переклад його на ЕК.

3. УДОСКОНАЛЕННЯ ПРОТОКОЛУ АВТЕНТИФІКАЦІЇ НА ДИСКРЕТНИХ ЛОГАРИФМАХ

Для переводу даного протоколу на еліптичні криві за основу був взятий алгоритм електронного цифрового підпису EC-GDSA, описаний в [5]. В результаті, у протоколі нульових знань, заснованому на дискретних логарифмах, описаному вище, необхідно зробити такі зміни:

- замінити випадкове число *r*, яке задовольняє нерівності $1 \le r \le q$ на випадкове ціле число k в інтервалі $\{1,...,n-1\}$;
- замінити доказ W на r, яке обчислюється за формулою $r = \pi(k \cdot G) \bmod n$, де G — це порядок базової точки;
- замінити ціле число d (запит), значення якого має задовольняти нерівності $0 \le d \le q$ на e, яке в свою чергу має задовольняти нерівності $1 \le e \le n$;
- замість асиметричної ключової пари (y_X, z_X), де z_X — таємний ключ, необхідно використовувати іншу ключову пару d_A, Q_A, де d_A — це секретний ключ, а відкритий ключ генерується за формулою $Q_A = d_A^{-1} \cdot G$.

Далі для наочності наведена таблиця порівняння, у першій колонці кроки алгоритму без змін, як у стандарті [1], а в другій — кроки алгоритму після переведення його на еліптичну криву.

Для перевірки нового алгоритму автентифікації нульових знань була розроблена програмна реалізація. Як криптографічна бібліотека була використана бібліотека Crypto + + ® Library 5.2.1. Параметри полів і еліптичної кривої для нового алгоритму були такі:

$$f(x) = x^{191} + x^9 + 1$$

$$y^2 + xy = x^3 + ax^2 + b$$

n: 4000000000000000000000004A20E90C39067C893BBB9A5h

a: 2866537B676752636A68F56554E12640276B649EF7526267h

b: 2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185ECh

G(x, y) = (36B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0Dh, 65BE73433B3F95E332932E70EA245CA2418EA0EF98018FBh)

Таблиця 3

Порівняння алгоритмів автентифікації

Протокол з використанням дискретних логарифмів	Протокол з використанням еліптичної кривої
1) Пред'явник генерує випадкове ціле число r, яке задовольняє нерівності $1 \le r \le q$. Дане число зберігається в таємниці. Пред'явник обчислює W: $W = g^r \bmod p$;	1)) Пред'явник генерує випадкове ціле число k, яке знаходиться в інтервалі $\{1,...,n-1\}$. Дане число зберігається в таємниці. Пред'явник обчислює r: $r = \pi(k \cdot G)$;
2) Пред'явник відсилає Перевіряючому маркер $TokenAB_1 = W$;	2) Пред'явник відсилає Перевіряючому $r = \pi(k \cdot G)$;
3) Перевіряючий генерує число d, $0 \le d \le q$;	3) Перевіряючий генерує число e, значення якого повинно задовольняти нерівності $1 \le e \le n$;
4) Перевіряючий відправляє число d Пред'явнику;	4) Перевіряючий відправляє число e Пред'явнику;
5) Пред'явник повинен обчислити відповідь D на основі r та власного ключа z_A за формулою: $D = r - dz_A \bmod q$;	5) Пред'явник повинен обчислити відповідь S на основі k та власного ключа d_A за формулою: $S = (kr - e)d_A \bmod n$;
6) Пред'явник відправляє маркер $TokenAB_2 = D$ Перевіряючому;	6) Пред'явник відправляє S Перевіряючому;
7) Перевіряючий перевіряє, чи належить D до інтервалу $0 < D < q$, обчислює значення W' за формулою: $W' = (y_A)^d g^D \bmod p$ та перевіряє W=W'. Якщо перевірка закінчилась успішно, то вважається, що вся ітерація завершилась успішно. В іншому випадку Перевіряючий ігнорує Пред'явника.	7) Отримавши відповідь S, Перевіряючий обчислює значення r' за формулою: $r' = \pi((SQ_A + eG)r^{-1})$; та перевіряє $r = r'$. Якщо перевірка закінчилась успішно, то вважається, що вся ітерація завершилась успішно. В іншому випадку Перевіряючий ігнорує Пред'явника.

4. СУТНІСТЬ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ

У методі аналізу ієрархій елементи завдання порівнюються попарно відносно їхнього впливу («ваги», або «інтенсивності») на загальну для них характеристику [6]. Парні порівняння елементів призводять до матричної форми таблиці.

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

Рис. 2. Порівняння елементів методом аналізу ієрархій

Ця матриця має властивість зворотної симетричності, тобто $a_{ji} = 1/a_{ij}$. Вона складається для порівняння відносної важливості критеріїв на другому рівні стосовно загальної мети на першому рівні, на третьому рівні стосовно критеріїв другого рівня і т. д. [7].

Заповнення квадратних матриць парних порівнянь виконується за таким правилом. Якщо елемент E_1 переважає над елементом E_2, то клітинка матриці, що відповідає перетинанню елементу E_1 (рядка) й елементу E_2 (стовпця), заповнюється цілим числом (від 1 до 9), а клітинка, що відповідає перетинанню рядка E_2 й стовпця E_1, заповнюється зворотним йому числом. Якщо елемент E_2 переважає над E_1, то ціле число ставиться в клітинку, що відповідає рядку E_2 й стовпцю E_1, а дріб ставиться в клітинку, що відповідає рядку E_1 й стовпцю E_2. Якщо елементи E_1 й E_2 мають однакову вагу, то в обох позиціях матриці ставляться одиниці.

Наведемо приклад формування матриці парних порівнянь. Нехай $E_1, E_2, ..., E_n$ – множина із n елементів , а $\nu_1, \nu_2, ... \nu_n$ – відповідно їхні ваги, або інтенсивності. Порівняємо попарно ваги, або інтенсивності всіх елементів множини щодо загальної для них властивості або мети. У цьому випадку матриця парних порівнянь $[E]$ матиме вигляд, як наведено на рисунку 3.

$[E] =$

	E_1	E_2	...	E_n
E_1	ν_1 / ν_1	ν_1 / ν_2	...	ν_1 / ν_n
E_2	ν_2 / ν_1	ν_2 / ν_2	...	ν_2 / ν_n
...	...	...	...	...
E_n	ν_n / ν_1	ν_n / ν_2	...	ν_n / ν_n

Рис. 3. Матриця парних порівнянь

При здійсненні попарних порівнянь необхідно відповісти на одне з питань: який із двох елементів, що порівнюються, важливіший, який більше ймовірний та який кращий. Отримані судження виражаються в цілих числах з урахуванням дев'ятибальної шкали (табл. 4) [7].

В ході використання зазначеної шкали, порівнюючи два об'єкти після досягнення мети, розташованої на вищестоящому рівні ієрархії, необхідно поставити у відповідність цьому порівнянню число 1, 3, 5, 7, 9 або зворотне йому значення. Числа 2, 4, 6, 8 і їх зворотні величини використовуються для полегшення компромісів між дещо відмінними від основних чисел судженнями. У тих випадках, коли складно розрізнити скільки проміжних градацій від абсолютного до слабкої переваги або цього не потрібно в конкретному завданні, може використовуватися шкала з меншим числом градацій. Найменше така шкала може мати дві оцінки: 1 — об'єкти рівнозначні; 2 — перевага одного об'єкта над іншим.

Таблиця 4

Шкала відносин (ступені значущості елементів)

Ступінь значущості	Визначення	Пояснення
1	Однакова значущість	Дві дії вносять однаковий вклад у досягнення мети
3	Деяка перевага значущості однієї дії над іншою (слабка значущість)	Існують аргументи на користь переваги однієї з дій, але ці аргументи недостатньо переконливі
5	Істотна або сильна значущість	Існують надійні дані або логічні судження для того, щоб показати перевагу однієї з дій
7	Очевидна або дуже сильна значущість	Переконливе свідчення на користь однієї дії над іншою
9	Абсолютна значущість	Свідчення на користь переваги однієї дії над іншою переконливі в максимальному ступені
2,4,6,8	Проміжні значення між двома сусідніми судженнями	Ситуація, коли необхідне компромісне рішення
Зворотні величини наведених вище величин	Якщо дії *i* при порівнянні з дією *j* приписується одне з вказаних вище ненульових чисел, то дії *j* при порівнянні з дією *i* приписується зворотне значення	Якщо узгодженість була визначена при одержанні N числових значень для створення матриці

Із групи матриць попарних порівнянь ми формуємо набір локальних пріоритетів, які виражають відносний вплив множини елементів нижнього рівня на елемент рівня, що примикає зверху. Для цього необхідно обчислити множину власних векторів для кожної матриці, які після нормалізації стають векторами пріоритетів. Найбільш точним способом для обчислення власного вектора є метод обчислення геометричного середнього шляхом перемножування всіх елементів у кожному рядку з наступним добуванням кореня n-го ступеня, де n — кількість елементів у рядку.

$$q_j^{(r-1)} = \sqrt[n]{(v_j^{(r)} / v_1^{(r)}) \times (v_j^{(r)} / v_2^{(r)}) \times \cdots \times (v_j^{(r)} / v_n^{(r)})}\ , \quad (10)$$

де r — рівень ієрархії, для матриці якого виконується розрахунок, n — кількість елементів у рядку, j — порядковий номер рядка.

Отриманий у такий спосіб стовпець нормалізується діленням кожного числа на суму всіх чисел.

$$\gamma_j^{(r-1)} = \frac{q_j^{(r-1)}}{\sum_{i=1}^{t_r} q_i^{(r-1)}}\ . \quad (11)$$

Матриця попарних порівнянь може бути узгодженою і не узгодженою. У загальному випадку, під узгодженістю мається на увазі те, що за наявності основного масиву необроблених даних всі інші дані логічно можуть бути отримані з основного масиву. Для проведення парних порівнянь n об'єктів або дій, які представлені в даних хоча б один раз, потрібно n-1 суджень про парні порівняння. З них можна вивести всі інші судження, використовуючи таке відношення: якщо об'єкт A_1 в 3 рази перевершує об'єкт A_2 і в 6 разів перевершує A_3, то $A_1 = 3A_2$ і $A_1 = 6A_3$. Отже, $3A_2 = 6A_3$, або $A_2 = 2A_3$ і $A_3 = 1/2A_2$. Якщо чисельне значення судження в позиції (2, 3) відрізняється від 2, то матриця буде неузгодженою. Це трапляється часто і не є проблемою.

Відомо, що узгодженість матриці еквівалентна вимозі рівності її максимального власного значення $\lambda_{max} = n$. Можна також оцінити відхилення від узгодженості за формулою $(\lambda_{max} - n) / (n - 1)$. Ця величина називається індексом узгодженості (ІУ). Зауважимо, що нерівність $\lambda_{max} \geq n$ завжди правильна. Наскільки погана узгодженість для певного завдання, можна оцінити шляхом порівняння отриманого нами значення ІУ з її значенням з випадково вибраних суджень і відповідних зворотних величин матриці того ж розміру. Ця величина має назву випадковий індекс (ВІ) [7]. У Національній лабораторії Окриджа згенерували середні ВІ для матриць порядку від 1 до 15 на базі 100 випадкових вибірок. Їх значення наведено в таблиці.

Таблиця 5

Значення ВІ для різних порядків матриці

Розмір матриці	1	2	3	4	5	6	7
ВІ	0	0	0,58	0,9	1,12	1,24	1,32

Продовження таблиці 5

8	9	10	11	12	13	14	15
1,41	1,45	1,49	1,51	1,48	1,56	1,57	1,59

Відношення ІУ до ВІ для матриці того самого порядку називається відношенням узгодженості (ВУ). Значення ВУ, менше, ніж 0,1 вважатимемо прийнятним. Для знаходження λ_{max} необхідно виконати такі кроки:

- Помножити матрицю порівнянь на оцінку вектора рішення. Отримаємо новий вектор.
- Розділити перший компонент цього вектора на першу компоненту оцінки вектора рішення, другу компоненту нового вектора на другу компоненту оцінки вектора рішення і т. д. Визначимо ще один вектор.
- Розділити суму компонент останнього вектора на число компонент. Таким чином знайдемо наближення до числа λ_{max}.

Обчислення значень ІУ та ВУ виконується за формулами, наведеними вище.

5. ПОРІВНЯННЯ ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ МЕТОДОМ АНАЛІЗУ ІЄРАРХІЙ

Протоколи автентифікації оцінюватимемо за такими критеріями [8]:

1. Автентифікація суб'єкта;
2. Автентифікація ключа;
3. Вид автентифікації суб'єкта;
4. Вид автентифікації ключа;
5. Наявність підтвердження ключа;
6. Новизна ключів;
7. Керування ключовими даними;
8. Захист від атак типу «повтор раніше переданого»;
9. Число обмінів повідомленнями;
10. Складність обчислень;
11. Можливість використання попередніх обчислень;
12. Вимоги до третьої сторони;
13. Криптографічна стійкість ключа;
14. Складність реалізації атак «повне розкриття»;
15. Вид неспростовності.

Порівняємо протоколи автентифікації за вище наведеними критеріями (табл. 6).

Таблиця 6

Порівняння протоколів автентифікації

	Протоколи / Критерії	Протокол, заснований на сертифікатах з використанням дискретних логарифмів	Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК
1	Автентифікація суб'єкта	Суб'єкт А для суб'єкта В	Суб'єкт А для суб'єкта В
2	Автентифікація ключа	Явна від А до В	Явна від А до В
3	Вид автентифікації суб'єкта	Однобічна абонента А до В	Однобічна абонента А до В
4	Вид автентифікації ключа	Однобічна автентифікація ключа абонента А	Однобічна автентифікація ключа абонента А
5	Наявність підтвердження ключа	Підтвердження ключа абонента А, Z_A	Підтвердження ключа абонента А, d_A
6	Новизна ключів	Немає новизни ключів	Немає новизни ключів

Продовження таблиці 6

7	Керування ключовими даними	На розсуд сторін протоколу	На розсуд сторін протоколу
8	Захист від атак типу «повтор раніше переданого повідомлення»	Здійснюється за рахунок випадкового числа r й випадкового цілого числа d	Здійснюється за рахунок випадкового числа r й випадкового цілого числа d
9	Число обмінів повідомленнями	3	3
10	Складність обчислень	1 операція секретного перетворення, 1 операція відкритого перетворення	1 операція секретного перетворення, 1 операція відкритого перетворення
11	Можливість використання попередніх обчислень	Немає	Немає
12	Вимоги до 3-ї сторони	Сторони протоколу самі вирішують, хто виготовляє пару ключів і якщо це третя сторона, то вона генерує відкритий та секретний ключ	Сторони протоколу самі вирішують, хто виготовляє пару ключів і якщо це третя сторона, то вона генерує відкритий та секретний ключ
13	Криптостійкість ключа	Забезпечується криптостійкість Y_A за відсутності компрометації секретної інформації акредитації Z_A	Забезпечується криптостійкість Y_A за відсутності компрометації секретної інформації акредитації d_A
14	Складність реалізації атак «повне розкриття»	Субекспоненційна	Експоненційна
15	Неспростовність	Неспростовність об'єкта А здійснюється за рахунок Z_A	Неспростовність об'єкта А здійснюється за рахунок d_A

Для того, щоб обрати кращий протокол автентифікації, зробимо процедуру декомпозиції та побудуємо дерево цілей. Для цього розіб'ємо 15 критеріїв, що характеризують протокол на 3 підгрупи:

1. Критерії, які стосуються ключа:
   - автентифікація ключа;
   - вид автентифікації ключа;
   - підтвердження ключа;
   - новизна ключа;
   - керування ключовими даними;
   - криптостійкість ключа.
2. Загальні вимоги:
   - автентифікація суб'єкта;
   - вид автентифікації суб'єкта;
   - число обмінів повідомленнями;
   - складність обчислень;
   - можливість використання попередніх обчислень;
   - вимоги до 3-ї сторони.
3. Показник захищеності:
   - захист від атак типу «повтор раніше переданого повідомлення»;
   - складність реалізації атак «повне розкриття»;
   - неспростовність.

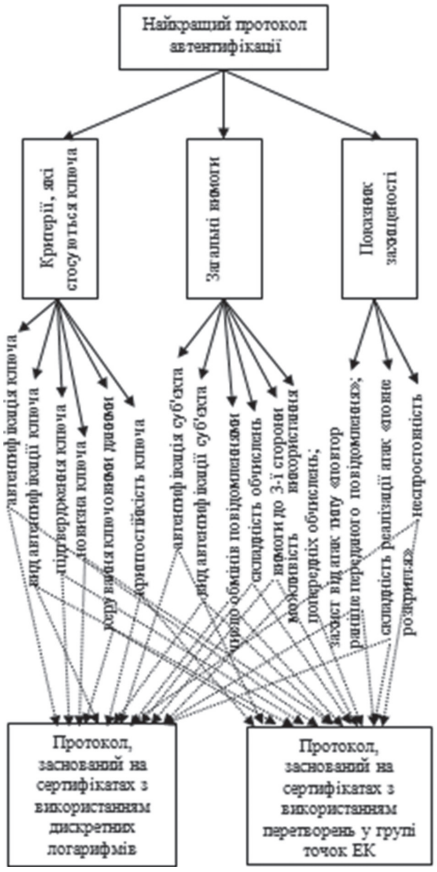

Рис. 4. Схема методу аналізу ієрархій

Далі наводяться матриці попарних порівнянь для кожного рівня ієрархії.

Таблиця 7

Матриця попарних порівнянь 1-го рівня

Вибір кращого протоколу	Критерії, які стосуються ключа	Загальні вимоги	Показник захищеності	q	γ
Критерії, які стосуються ключа	1	1/3	1/7	0,362	0.081
Загальні вимоги	3	1	1/5	0.843	0.188
Показник захищеності	7	5	1	3.271	0.731

$\lambda_{max} = 3.066$ ІУ=0,033 ВУ= 0,057

Таблиця 8

Матриця попарних порівнянь
2-го рівня, 1-ї групи критеріїв

Критерії, які стосуються ключа	Автентифікація ключа	Вид автентифікації ключа	Підтвердження ключа	Новизна ключа	Керування ключовими даними	Крипостійкість ключа	q	γ
Автентифікація ключа	1	1	1/3	1/3	1/4	1/9	0.382	0.040
Вид автентифкації ключа	1	1	1/3	1/3	1/4	1/9	0.382	0.040
Підтвердження ключа	3	3	1	1/2	1/3	1/8	0.757	0.078
Новизна ключа	3	3	2	1	3	1/5	1.487	0.154
Керування ключовими даними	4	4	3	1/3	1	1/9	1.101	0.114
Крипостійкість ключа	9	9	8	5	9	1	5.548	0.575

λ_{max} =6,5 ІУ= 0,1 ВУ= 0,08

Таблиця 9

Матриця попарних порівнянь
2-го рівня, 2-ї групи критеріїв

Загальні вимоги	Автентифікація суб'єкта	Вид автентифікації суб'єкта	Число обмінів повідомленнями	Складність обчислень	Вимоги до 3-ї сторони	Використання попередніх	q	γ
Автентифікація суб'єкта	1	2	1/2	1/4	4	1/5	0,765	0,085
Вид автентифікації суб'єкта	1/2	1	1/3	1/6	4	1/7	0,501	0,056
Число обмінів повідомленнями	2	3	1	1/5	3	1/6	0,918	0,102
Складність обчислень	4	6	5	1	6	1/3	2,493	0,277
Вимоги до 3-ї сторони	1/4	1/4	1/3	1/6	1	1/7	0,281	0,031
Використання попередніх обчислень	5	7	6	3	7	1	4,049	0,449

λ_{max} =6.537 ІУ=0.107 ВУ= 0.087

Таблиця 10

Матриця попарних порівнянь 2-го рівня,
3-ї групи критеріїв

Показник захищеності	Захист від атак типу повтор раніше	Складність реалізації атак «повне розкриття»	Неспростовність	q	γ
Захист від атак типу «повтор раніше переданого повідомлення»	1	1/4	2	0,794	0,219
Складність реалізації атак «повне розкриття»	4	1	3	2,289	0,63
Неспростовність	1/2	1/3	1	0,55	0,151

λ_{max} =3.109 ІУ= 0.055 ВУ= 0.094

Таблиця 11

Матриця попарних порівнянь
3-го рівня, 1-ї групи критеріїв

Автентифікація ключа	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 12

Матриця попарних порівнянь
3-го рівня, 2-ї групи критеріїв

Вид автентифікації ключа	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 13

Матриця попарних порівнянь
3-го рівня, 3-ї групи критеріїв

Підтвердження ключа	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 14

Матриця попарних порівнянь
3-го рівня, 4-ї групи критеріїв

Новизна ключа	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 15

Матриця попарних порівнянь
3-го рівня, 5-ї групи критеріїв

Керування ключовими даними	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 16

Матриця попарних порівнянь
3-го рівня, 6-ї групи критеріїв

Криптостійкість ключа	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1/4	0,5	0,2
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	4	1	2	0,8

Таблиця 17

Матриця попарних порівнянь
3-го рівня, 7-ї групи критеріїв

Автентифікація суб'єкта	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 18

Матриця попарних порівнянь
3-го рівня, 8-ї групи критеріїв

Вид автентифікації суб'єкта	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 19

Матриця попарних порівнянь
3-го рівня, 9-ї групи критеріїв

Число обмінів повідомленнями	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 20

Матриця попарних порівнянь
3-го рівня, 10-ї групи критеріїв

Складність обчислень	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1/5	0,447	0,167
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	5	1	2,236	0,833

Таблиця 21

Матриця попарних порівнянь
3-го рівня, 11-ї групи критеріїв

Вимоги до 3-ї сторони	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 22

Матриця попарних порівнянь
3-го рівня, 12-ї групи критеріїв

Можливість використання попередніх обчислень	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 23

Матриця попарних порівнянь
3-го рівня, 13-ї групи критеріїв

Захист від атак типу «повтор раніше переданого повідомлення»	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Таблиця 24

Матриця попарних порівнянь
3-го рівня, 14-ї групи критеріїв

складність реалізації атак «повне розкриття»	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1/7	0,378	0,125
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	7	1	2,646	0,875

Таблиця 25

Матриця попарних порівнянь
3-го рівня, 15-ї групи критеріїв

Неспростовність	Протокол з використанням дискретних логарифмів	Протокол на ЕК	q	γ
Протокол, заснований на сертифікатах з використанням дискретних логарифмів	1	1	1	0.5
Протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК	1	1	1	0.5

Розглянемо матриці впливу різних рівнів.

Внесок підцілей першого рівня в основну мету:

$$Y^{1,0}{}_1 = \begin{pmatrix} 0{,}081 \\ 0{,}188 \\ 0{,}731 \end{pmatrix}.$$

Внесок підцілей другого рівня в підцілі першого рівня виглядає так:

$$Y^{2,1}{}_1 = \begin{pmatrix} 0{,}04 \\ 0{,}04 \\ 0{,}078 \\ 0{,}154 \\ 0{,}114 \\ 0{,}575 \end{pmatrix};\ Y^{2,1}{}_2 = \begin{pmatrix} 0{,}085 \\ 0{,}056 \\ 0{,}102 \\ 0{,}277 \\ 0{,}031 \\ 0{,}449 \end{pmatrix};\ Y^{2,1}{}_3 = \begin{pmatrix} 0{,}219 \\ 0{,}63 \\ 0{,}151 \end{pmatrix}.$$

Внесок підцілей третього рівня в підцілі другого рівня виглядає так:

$$Y^{3,2}_{1-6} = \begin{pmatrix} 0{,}5\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}2 \\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}8 \end{pmatrix}$$

$$Y^{3,2}_{7-12} = \begin{pmatrix} 0{,}5\ 0{,}5\ 0{,}5\ 0{,}167\ 0{,}5\ 0{,}5 \\ 0{,}5\ 0{,}5\ 0{,}5\ 0{,}833\ 0{,}5\ 0{,}5 \end{pmatrix}$$

$$Y^{3,2}_{13-15} = \begin{pmatrix} 0{,}5\ \ 0{,}125\ 0{,}5 \\ 0{,}5\ 0{,}875\ 0{,}5 \end{pmatrix}$$

$$Y^{3,1}_1 = Y^{2,1}_1 * Y^{3,2}_{1-6} =$$

$$= \begin{pmatrix} 0{,}328 \\ 0{,}673 \end{pmatrix}\ Y^{3,1}_2 = Y^{2,1}_2 * Y^{3,2}_{7-12} = \begin{pmatrix} 0{,}408 \\ 0{,}592 \end{pmatrix}$$

$$Y^{3,1}_3 = Y^{2,1}_3 * Y^{3,2}_{13-15} = \begin{pmatrix} 0{,}264 \\ 0{,}736 \end{pmatrix}$$

Результуючий вектор значущості розраховується так:

$$Y^{3,0}_1 = Y^{1,0}_1 * Y^{1,1}_{1-3} = \begin{pmatrix} 0{,}081 \\ 0{,}188 \\ 0{,}731 \end{pmatrix} * \begin{pmatrix} 0{,}328\ 0{,}408\ 0{,}264 \\ 0{,}673\ 0{,}592\ 0{,}736 \end{pmatrix} =$$

$$= \begin{pmatrix} 0{,}296 \\ 0{,}704 \end{pmatrix}.$$

Виходячи із отриманих нами даних, можна зробити висновок про те, що найкращим протоколом автентифікації (із порівнюваних) є протокол, заснований на сертифікатах з використанням перетворень у групі точок ЕК.

ВИСНОВКИ

Забезпечення безпеки інформаційної системи є одним з найважливіших завдань в ході її експлуатації, оскільки від збереження конфіденційності, цілісності і доступності інформаційних ресурсів багато в чому залежить швидкість прийняття рішень, ефективність і надійність роботи. Зараз для будь-якої компанії, чи особи, яким необхідно захищати дані, як ніколи важлива безпека та перевірка автентичності. На сьогодні існує багато протоколів автентифікації. Важливим є завдання пошуку найкращого протоколу. Однією із вразливостей протоколу простої автентифікації є те, що після того, як Пред'явник передасть свій пароль Перевіряючому, останній може використовувати його та видавати себе за Пред'явника. Протоколи суворої автентифікації мають кращу стійкість, проте їх вразливість полягає в тому, що Пред'явник зобов'язаний продемонструвати знання секретного ключа, хай навіть і одноразово; при цьому передана інформація не може бути безпосередньо використана Перевіряючим, проте деяка її частина допоможе отримати додаткову інформацію про секрет Пред'явника. Наприклад, Перевіряючий має можливість так сформувати запити, щоб відповіді, які передавались, аналізувалися на предмет вмісту додаткової інформації.

Протоколи з нульовими знаннями були розроблені спеціально для вирішення даної

проблеми. Вони дозволяють встановити істинність твердження і при цьому не передавати будь-якої додаткової інформації про саме твердження.

В роботі запропоновано удосконалений протокол нульових знань, заснований на сертифікатах з використанням перетворень у групі точок ЕК. Проведено порівняльний аналіз методом аналізу ієрархій удосконаленого протоколу із протоколом, заснованим на сертифікатах з використанням дискретних логарифмів. Після проведення порівняльного аналізу і отримання результуючого вектора значущості, доведено, що удосконалений протокол має кращі властивості безпеки.

Література

[1] ISO/IEC 9798-5. Методи захисту. Автентифікація об'єктів. Частина 5: Протоколи, що використовують методи які грунтуються на нульових знаннях.

[2] FIPS PUB 186-3. Digital Signature Standard. – USA, 2009. – 130 p.

[3] Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах / І.Д. Горбенко, Т.О. Гріненко // Навч. посібник. Ч.1. Криптографічний захист інформації – Харків: ХНУРЕ, 2004. – 368 с.

[4] Балагура Д.С. Методы оценки сложности криптоанализа для криптографических приложений в группе точек эллиптической кривой, учитывающие вероятность коллизий / Д.С. Балагура, Ю.И. Горбенко // Радиотехника: Всеукр. межвед. научн.-техн. сб. — 2005. Вып. 142. — С. 205–213.

[5] ISO/IEC 15946-2. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 2: Електронні цифрові підписи.

[6] Андрейчиков А.В. Анализ, синтез, планирование решений в экономике / А.В Андрейчиков, О.Н Андрейчикова // М.: Финансы и статистика, 2002. – 386 с.

[7] Саати Т. Принятие решений. Метод анализа иерархий: пер. с англ. М.: Радио и связь, 1989. – 316 с.

[8] ISO/IEC 9798-1. Information technology – Security techniques – Entity authentication – Part1: General.

Надійшла до редколегії 15.05.2013

Олешко Інна Вікторівна, аспірант кафедри БІТ ХНУРЕ. Наукові інтереси: електронна паспортна система, біометрична автентифікація.

УДК 681.3.06:519.248.681

Усовершенствование протокола нулевых знаний, основанного на дискретных логарифмах / И.В. Олешко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 363–372.

В работе предложена усовершенствованная версия протокола нулевых знаний, основанного на дискретных логарифмах — протокол нулевых знаний с использованием эллиптической кривой. С помощью метода анализа иерархий был проведен сравнительный анализ двух протоколов: существующего протокола на дискретных логарифмах и его усовершенствованной версии. Доказано, что лучшим протоколом является протокол нулевых знаний с использованием эллиптической кривой.

Ключевые слова: протокол нулевых знаний, дискретный логарифм, эллиптическая кривая, механизм аутентификации, Инициатор, сертификат, метод анализа иерархий.

Табл.: 25. Ил.: 4. Библиогр.: 8 назв.

UDC 681.3.06:519.248.681

Improving of zero-knowledge protocol based on discrete logarithms / I.V. Oleshko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 363–372.

The paper presents an improved version of an zero-knowledge protocol based on discrete logarithms — a zero-knowledge protocol using an elliptic curve. A comparative analysis of two protocols has been performed with the help of hierarchy analysis method: the discrete logarithms-based existing algorithm and its improved version. It is proved that the best protocol is the zero knowledge protocol using an elliptic curve.

Keywords: zero-knowledge protocol, discrete logarithm, elliptic curve, authentication mechanism, claimant, certificate, hierarchy analytic method.

Tab.: 25. Fig.: 4. Ref.: 8 items.