

ГІБРИДНИЙ МЕТОД НАПРАВЛЕНОГО ШИФРУВАННЯ, ЯКИЙ БАЗУЄТЬСЯ НА ІДЕНТИФІКАТОРАХ І АЛГЕБРАЇЧНИХ РЕШІТКАХ

Вступ

Впровадження систем електронного документообігу та електронного цифрового підпису в цілому, а також застосування акредитованого центру сертифікації ключів «Інфраструктура відкритих ключів» (АЦСК «ІВК»), виявили ряд проблемних питань і протиріч відносно асиметричних криптографічних систем на базі сертифікатів, реалізованих відповідно до стандарту X.509, стосовно впровадження та стандартизації даних систем, основні з яких стосуються недосконалості системи управління ключовими даними [1]. Тому, активно ведуться роботи щодо впровадження альтернативних криптографічних систем з відкритими ключами, а саме систем, в основі яких лежить шифрування на ідентифікаторах. Так, об'єднаним технічним комітетом Міжнародної організації із стандартизації і Міжнародної електротехнічної комісії ведеться робота щодо створення міжнародного стандарту ISO/IEC 18033-5 – Шифри, що засновані на ідентифікаторах, який знаходиться на стадії публікації, яка планується на листопад 2015 року.

Більшість існуючих схем, які базуються на ідентифікаторах, використовують математику білінійних відображень точок на еліптичних кривих. Складність даних перетворень базується на вирішенні задачі дискретного логарифму в групі точок еліптичної кривої, та знаходиться в межах між субекспоненційною і експоненційною [2]. Також математичний апарат на білінійних відображеннях вимагає вагомих затрат відносно складності реалізації даних криптоперетворень, що тягне за собою суттєве погіршення швидкісних показників.

Альтернативою математиці спарювань точок є математика, що використовує перетворення у фактор-кільцях – алгебраїчні решітки [3]. Криптографічні перетворення, засновані на цій математиці, мають лінійну складність обчислень, яка забезпечує прийнятну швидкодію. Криптографічна стійкість таких алгоритмів ґрунтується на складності вирішення задачі знаходження найкоротшого вектора у заданій решітці та її різновидах [4]. На сьогодні не існує алгоритмів, які б знаходили найкоротший вектор зі складністю, меншу за експоненційну. Більш дослідженою за всі криптосистеми на алгебраїчних решітках вважається NTRU-криптосистема, і вона ж є єдиним натеper стандартизованим методом, заснованим на фактор-кільцях [5]. Тому запропонований гібридний метод було розроблено на базі NTRU-методу у фактор-кільцях.

Мета статті – удосконалення та розробка нового методу криптографічних перетворень, що засновані на ідентифікаторах та алгебраїчних решітках для підвищення швидкодії криптографічних перетворень на ідентифікаторах, та забезпечення експоненціального рівня криптографічної стійкості.

Математична модель пропонованого гібридного методу

Пропонується математична модель гібридного методу направленої шифрування на ідентифікаторах, побудована на основі криптосистеми NTRU. Відмінність полягає у генеруванні ключових даних. Замість відкритого ключа користувача використовується заданий користувачем ідентифікатор, який за допомогою спеціальної функції відображення відображається у елемент алгебраїчної решітки [6]. Секретний ключ користувача, на відміну від класичного NTRU методу, виробляється за допомогою відповідного ідентифікатора і майстер-ключа системи. Стійкість одержаної математичної моделі базується на складності вирішення задачі пошуку найкоротшого вектора в решітці (SVP-задача) та є експоненційною.

Математична модель гібридного методу шифрування представлена у табл. 1.

Таблиця 1

	Зашифрування	Розшифрування
Вхідні дані	Відкрите повідомлення m , ідентифікатор користувача ID .	Зашифроване повідомлення c , ідентифікатор користувача ID , майстер- ключ F_{msk} .
Вихідні дані	Зашифроване повідомлення c .	Зашифроване повідомлення m .
Основна операція	Зашифрування: $c \leftarrow h_{ID}b + m$.	Розшифрування $m \leftarrow F_{ID}c$.

Гібридний метод направлено шифрування на ідентифікаторах та алгебраїчних решітках

На основі запропонованої математичної моделі розроблено модифікований метод направлено шифрування на ідентифікаторах та алгебраїчних решітках, стійкість якого є експоненційною та заснованою на вирішенні задачі пошуку найкоротшого вектора в решітці [6]. Основні компоненти, що використовує запропонований гібридний метод шифрування на ідентифікаторах та алгебраїчних решітках:

- майстер-ключ F_{msk} ;
- ідентифікатор користувача ID ;
- секретний ключ користувача F_{ID} ;
- відкритий ключ користувача h_{ID} ;
- сліпий поліном b , випадкова компонента, використовується при зашифруванні для захисту від атаки за обраними зашифрованими текстами;
- випадкова компонента g .

Гібридний метод направлено шифрування на ідентифікаторах та алгебраїчних решітках представляється наступним чином:

1. Генерується майстер-ключ F_{msk} , який складається зі N поліномів f_i секретних ключів: $F_{msk} \in \{f_i \mid f_0, \dots, f_{N-1}\}$, із числом 1, -1 і 0, що знаходиться у заданому інтервалі та відповідає обраному рівню захищеності.

2. Ідентифікатор користувача представляється у вигляді N бітового рядка, використовуючи функцію гешування: $H(ID)$.

3. Секретний ключ користувача обчислюється шляхом множення ненульових бітів даного ідентифікатора ID_i із відповідними поліномами f_i майстер-ключа F , тобто якщо

$$ID_i = 1: F_{ID} \leftarrow \left(\left(\prod_{i=0}^{N-1} f_i \right) \bmod p \right) p + 1.$$

4. Відкритий ключ обчислюються так: $h_{ID} = (F_{ID}^{-1} \cdot g \cdot p) \bmod q$, де F_{ID}^{-1} – зворотній елемент; g – поліном, тимчасова випадкова компонента; $p = 3$.

5. Операція зашифрування здійснюється так: $c = (b \cdot h_{ID} + m) \bmod q$.

6. Операція розшифрування здійснюється так: $m = F_{ID} \cdot c$.

Правильність виконання даного криптографічного перетворення можна перевірити так:

$$\begin{aligned} m &= F_{ID} \cdot c = F_{ID} \cdot (b \cdot h_{ID} + m) = F_{ID} \cdot (b \cdot (F_{ID}^{-1} \cdot g \cdot p) + m) = \\ &= F_{ID} \cdot b \cdot F_{ID}^{-1} \cdot g \cdot p + F_{ID} \cdot m = \\ &= b \cdot g \cdot p + \left(\left(\prod_{i=0}^{N-1} f_i \right) \bmod p \right) p + 1 \cdot m \bmod p = m. \end{aligned}$$

Швидкісні та просторові показники роботи гібридного методу

Пропонований гібридний метод на ідентифікаторах має основні переваги криптосистем на алгебраїчних решітках, але, на жаль, має і недолік, властивий цим системам, а саме – збільшення розміру зашифрованих текстів. Коефіцієнт зростання зашифрованого тексту в залежності від обраних параметрів надано у табл. 2. В даній таблиці також визначається рівень захищеності для визначених довжин ступеню поліному N . Довжина зашифрованого тексту у бітах обчислювалась за формулою: $l_c = N \log_2 q$.

Таблиця 2

Рівень захищеності	Ступінь поліному кільця, N	Максимальна довжина вхідного повідомлення, l_m , біт	Довжина шифротексту, l_c , біт	Коефіцієнт зростання розміру шифротекста, $k_{m \rightarrow c}$
112	401	480	4411	9.1895
112	541	688	5951	8.6497
112	659	864	7249	8.3900
128	449	536	4939	9.2145
128	613	776	6743	8.6894
128	761	1000	8371	8.3710
192	677	808	7447	9.2165
192	887	1128	9757	8.6498
192	1087_1	1360	11957	8.7919
256	1087_2	1424	11957	8.3967
256	1171	1488	12881	8.6565
256	1499	1976	16489	8.3446

При виконанні роботи реалізованого методу використовувався великий модуль $q = 2048$. При одержанні швидкісних показників розробленої програмної моделі гібридного методу шифрування, наведених у табл. 3, виконувалося 50 генерувань ключових даних та 10000 операцій зашифрування/розшифрування для кожного набору параметрів та обчислювалося усереднене значення часу виконання цих операцій.

Таблиця 3

Ступінь поліному кільця, N	Кількість генерацій ключових даних, од/с	Кількість операцій зашифрування, од/с	Кількість операцій розшифрування, од/с	Швидкість зашифрування, Мбіт/с	Швидкість розшифрування, Мбіт/с
401	15.4188	6967.3243	7657.6308	3.3443	33.7778
541	4.2413	10090.8575	11206.9177	6.9425	66.6923
659	3.0191	9823.0132	2778.2307	8.4870	20.1393
449	6.7132	5033.4905	6248.5969	2.6979	30.8618
613	3.4030	8479.7662	9278.6489	6.5802	62.5659
761	2.1193	8167.6245	2221.3485	8.1676	18.5949
677	2.9366	3890.1118	4083.8548	3.1432	30.4124
887	1.1992	5011.5006	5351.9093	5.6529	52.2185
1087_1	14.7003	4855.5538	5156.2409	6.6035	61.6531
1087_2	14.7002	3115.0124	3226.9298	4.4357	38.5843
1171	11.9373	3053.0802	3176.2735	4.5429	40.9135
1499	7.3374	2970.6264	3083.5112	5.8699	50.8440

Швидкодія реалізованого гібридного методу направлено шифрування на ідентифікаторах і алгебраїчних решітках порівнювалась зі швидкодією реалізованого стандартного методу Боне – Франкліна (BF) направлено шифрування на ідентифікаторах, що заснований на білінійних відображеннях.

В ході оцінки були отримані результати, наведені в табл.3, які свідчать про те, що використання моделі алгебраїчних криптографічних перетворень дозволило покращити швидкісні показники шифрування на ідентифікаторах на 2-3 порядки [6].

Запропоновану модель модифікованого методу направленого шифрування було розроблено за допомогою мови програмування C; результати, наведені в табл. 3, отримано на ПЕОМ з такими технічними характеристиками:

- процесор Intel Core i5 3570K 3.4GHz, який працював на частоті 3.6GHz;
- оперативна пам'ять 16 Gb RAM, з частотою 1600 MHz;
- операційна система Windows 7 x64 Professional;
- середовище розробки Microsoft Visual Studio Express 2012.

Таблиця 4

Рівень захищеності	Гібридний метод			Класичний метод Боне – Франкліна				
	Ступінь поліному кільця, N	Швидкість зашифрування, Мбіт/с	Швидкість розшифрування, Мбіт/с	Порядок підгрупи групи точок ЕК, біт	Порядок розширення скінченого поля, біт	Швидкість зашифрування, Мбіт/с	Швидкість розшифрування, Мбіт/с	Кількість генерацій ключових даних, од/с
112	541	6.9425	66.6923	224	2048	0.671	1.55	1.4285
128	613	6.5802	62.5659	256	4096	0.224	0.624	0.5001
192	887	5.6529	52.2185	384	6144	0.035	0.105	0.0731
256	1499	5.8699	50.8440	512	8192	0.016	0.05	0.0347

Тобто, з даних табл. 4 можна зробити висновок, що швидкісні показники гібридного методу є приблизно однаковими для різних наборів параметрів і суттєво не залежать від обраного розміру алгебраїчної решітки, тоді як швидкісні показники методів на білінійних відображеннях залежать від обраного порядку точок над еліптичною кривою і погіршуються зі зростанням даного порядку.

Висновки

В даній статті наведено математичну модель гібридного криптографічного перетворення направленого шифрування на ідентифікаторах та алгебраїчних решітках, а також гібридний метод направленого шифрування на ідентифікаторах та алгебраїчних решітках, який базується на цій моделі. Стійкість запропонованого методу базується на задачі пошуку найкоротшого вектора в решітці, застосування якої дозволило підвищити складність криптографічного аналізу методом повного перебору направленого шифрування на ідентифікаторах із субекспоненціального рівня до експоненціального рівня.

Застосування цього гібридного методу дозволило також підвищити швидкісні показники на два-три порядки по відношенню до класичних систем на ідентифікаторах. Результати було одержано за допомогою розробленої програмної моделі.

Список літератури: 1. Горбенко, Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія / Ю.І. Горбенко, І.Д. Горбенко. – Х. : Форт, 2010. – 608с. 2. Горбенко, І.Д. Аналіз стійкості обчислювальних задач, що засновані на білінійних відображеннях / І.Д. Горбенко, Л.В. Макутоніна // Радиотехника. – 2012. – Вип. 171. – С. 79 – 89. 3. Бондаренко, М.Ф. Обчислювальна складність основних задач на алгебраїчних решітках / М.Ф. Бондаренко, Л.В. Макутоніна // Прикладная радиоэлектроника. – 2013. – Т. 12, № 2. – С. 258 – 264. 4. Горбенко, І.Д. Аналіз криптографічних алгоритмів на ідентифікаторах, що використовують алгебраїчні решітки / І.Д. Горбенко, Л.В. Макутоніна // Прикладная радиоэлектроника. – 2012. – Т. 11, №2. – С. 200 – 209. 5. American National Standard X9.98-2010. Lattice-Based Polynomial Public Key Encryption Algorithm Part 1: Key Establishment: Part 2: Data Encryption, 2010. 6. Макутоніна, Л.В. Методи та моделі криптографічних перетворень з доказовою стійкістю, що засновані на ідентифікаторах та алгебраїчних решітках : дис. ... канд. техн. наук за спеціальністю 05.13.21 – Системи захисту інформації / Макутоніна Лідія Вікторівна. – Харків, 2015.

Харківський національний університет
імені В.Н. Каразіна

Надійшла до редколегії 17.04.2015