УДК 004.382

А.Р. Добуш

Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

ПЕРЕВАГИ РЕАЛІЗАЦІЇ У НВІС ПРИСТРОЇВ ДЛЯ ОБРОБКИ ЦИФРОВОГО ПІДПИСУ, ЩО ҐРУНТУЄТЬСЯ НА ВЛАСТИВОСТЯХ ГРУП ТОЧОК ЕЛІПТИЧНОЇ КРИВОЇ

Розглянуто стан і напрями розвитку цифрових підписів. Визначено переваги цифрового підпису, що ґрунтується на властивостях груп точок еліптичних кривих для реалізації на НВІС. Описано математичний апарат дій над точками еліптичних кривих у полях Галуа. Визначено переваги пристроїв, які виконують цифровий підпис на основі властивостей точок груп еліптичних кривих. Обґрунтовано необхідність збільшення розрядності елементів поля Галуа, як напрям розвитку чинного в Україні стандарту. Виконано порівняльний аналіз методів вибору довжини ключа для забезпечення достатньої криптографічної стійкості.

Ключові слова: цифровий підпис, еліптичні криві, афінні координати, стандарти ECDSA.

The state and trends of digital signatures. Advantages, digital signature, based on the properties of point groups of elliptic curves for implementation in VLSI. The mathematical apparatus of the action points of elliptic curves in the Galois fields. Advantages of devices that perform based on elliptic curves. The necessity of increasing the bit Galois field elements, as the direction of the current standard in Ukraine. Compare different techniques of choosing key length, to provide sufficient security level.

Key words: digital signature, elliptic curves, affine coordinates, ECDSA standards.

Вступ

У сучасній криптографії широко використовується математичний апарат еліптичних кривих. Алгоритми шифрування та електронного цифрового підпису будуються на основі операцій у групі точок еліптичної кривої. При цьому криптографічна стійкість цифрового підпису, що базується на криптографічних перетвореннях у групі точок еліптичної кривої, ґрунтується на складності дискретного логарифмування в групі точок еліптичної кривої. В державних стандартах Росії та України для забезпечення достатньої стійкості рекомендують використовувати числа порядку до 2^{512} як параметри кривої. На початок 2012 р. всі розглянуті в статті методи вибору довжини ключа не рекомендують використовувати ключі з довжиною, меншою за 149 бітів.

1. Огляд літературних джерел і окреслення проблеми

Основними недоліками програмної реалізації стандартів [1] і [2] є недостатня стійкість до зламу, недостатня продуктивність, особливо при обробці інтенсивних потоків даних. Тому виникає необхідність у створенні апаратних засобів для виконання операцій над елементами скінченних полів.

Не викликає сумнівів, що заходи щодо захисту критично важливих інформаційних систем мають відповідати численним міжнародним, національним, корпоративним нормативним і методичним документам. У [3] вказано такі міжнародні стандарти:

- **IEEE 1363.** Цей стандарт містить практично всі алгоритми з відкритим ключем. Зокрема, він охоплює ECDH (Elliptic curve Diffie-Hellman), ECDSA(Elliptic curve digital signature algorithm), ECMQV (Elliptic curve Menezes-Qu-Vanstone) і ECIES (Elliptic curve integrated encryption scheme). Крім того, цей стандарт містить хороший додаток, що охоплює всі основні теоретико-числові алгоритми, які необхідні для криптографії з відкритим ключем [4].
- **ANSI X9.62** [5], і **X9.63**[6]. Ці два стандарти зосереджуються на еліптичних кривих і розглядають ECDSA в X9.62 і ECDH, ECMQV і ECIES в X9.63. Вказані стандарти обумовлюють формат повідомлень, які будуть використовуватися, і містять список рекомендованих кривих.
- **FIPS 186.2 .** Цей стандарт цифрового підпису є покращенням попереднього FIPS 186, який детально описує тільки алгоритм DSA. Стандарт FIPS 186.2 визначає і DSA (Digital signature algorithm) і ECDSA і надається список кривих, які рекомендують використовувати в установах уряду США.

• **SECS [7].** Стандарт створила індустріальна група на чолі з Certicom. За суттю він відображає стандарт [5] , але SECS доступніший в Інтернеті.

Хоча сьогодні використання [2] забезпечує більш ніж достатній рівень захисту, але, зважаючи на швидкий розвиток техніки і алгоритмів криптографічного аналізу, покращення державного стандарту зі зворотною сумісністю є актуальним вже тепер. Стандарти [2] та аналогічний стандарт [1] обмежуються максимальною розрядністю використовуваного поля 509 двійковими розрядами, тоді як в стандарті IEEE 1363 [4] наведені поля в оптимальному нормальному базисі зі степенем розширення основного поля до 998, і до кожного подані коефіцієнти незвідного многочлена.

У [8] описано ієрархічні рівні алгоритмів, які використовується для виконання операцій над точками еліптичних кривих. Зважаючи на таку складність і необхідність опрацювання багаторозрядних елементів полів Галуа, в [9] та [10] зазначено, що при реалізації цифрового підпису на базі універсальних процесорів важко досягти високих рівнів продуктивності.

У [11] обґрунтовано доцільність використання саме оптимального нормального базису. Показано, що апаратно множення в поліноміальному і нормальному базисах потребує приблизно однакових апаратних витрат часу. Однак найпрацемісткіша операція над елементами поля Галуа GF(2^m) – обчислення оберненого елемента в нормальному базисі виконується на порядок швидше.

У [12] вказана відповідність криптографічної стійкості довжин ключів ECDSA і DSA, де обґрунтовано використання саме цифрового підпису, що базується на властивостях груп точок еліптичної кривої. Також, з огляду на [13], де рекомендується збільшити мінімальну використовувану розрядність ключа, та рекомендації [14] – [19], актуальним є огляд перспектив збільшення довжини ключа цифрового підпису.

2. Цілі статті

Метою роботи є визначення стану і напрямів розвитку цифрових підписів на основі властивостей груп точок еліптичної кривої, перспективи збільшення розрядності елементів поля Галуа *GF* (2^m), де m>509, для виконання операцій над точками еліптичних кривих відповідно до вимог стандарту ДСТУ 4145-2002. Також метою роботи є визначення переваг реалізації на НВІС виконання операцій над точками еліптичних кривих.

3. Визначення еліптичної кривої

Еліптична крива $E(F_2^m)$ над скінченним полем F_2^m – це множина пар (x,y) елементів цього поля, що задовольняють рівняння кривої в афінних координатах в нормальній формі Вейєрштрасса

$$y^2 + xy = x^3 + Ax^2 + B \quad (1)$$

де $A, B \in F_2^m$, $B \neq 0$, разом із приєднаною нескінченною віддаленою точкою *O*. Пара (*x,y*) елементів основного поля називається афінними координатами точки еліптичної кривої. Нескінченно віддалена точка *O* не має афінних координат. Елементи *A, B* основного поля називаються коефіцієнтами рівняння еліптичної кривої. Кількість точок еліптичної кривої разом з нескінченною точкою називається порядком еліптичної кривої.

Поряд з афінними координатами точки також існують проективні координати. Класичне рівняння Вейєрштрасса для таких координат має вигляд:

$$y^2z + xyz = x^3 + Ax^2z + Bz^3 \quad (2)$$

а точками проективної еліптичної кривої є трійки елементів основного поля (x:y:z), що задовольняють рівняння 2, причому хоча б одна з цих координат відмінна від нуля. Використання двокрапки у запису проективних координат означає, що трійки координат, отримані одна з іншої множенням на ненульовий елемент основного поля, відповідають тій самій проективній точці еліптичної кривої і також задовольняють проективне рівняння Вейєрштрасса. У проективному зображенні нескінченно віддалена точка має координати (0,1,0). Для переходу від афінних координат до проективних використовуються співвідношення:

(x,y) **à** (x:y:1); (3)

O **à** (0,1,0); (4)

Для переходу від проективних координат до афінних використовується співвідношення:

якщо z = 0, то (x:y:z) **à** O (5)

якщо z ≠ 0, то (x:y:z) **à** (xz^{-1},yz^{-1}) (6)

Додавши точки еліптичної кривої, як результат ми отримуємо іншу точку цієї кривої. Правила додавання точок еліптичної кривої в афінних координатах можна записати так:

1. P + O = O + P F_2^m

2. Якщо P(x,y) ∈ E F_2^m, тоді (x,y)+(x,x+y) = O. Точка (x,x+y) позначається як –P і називається мінус P, точка –P також є точкою цієї еліптичної кривої.

3. Якщо P = (x1,x2) ∈ E F_2^m, Q = (x2,y2) ∈ E F_2^m, де P ≠ ± Q тоді P+Q = (x3,y3), де

$$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + \left(\frac{y_1 + y_2}{x_1 + x_2}\right) + x_1 + x_2 + A \tag{7}$$

$$y_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1 \tag{8}$$

Геометричну ілюстрацію додавання наведено на рис. 1.

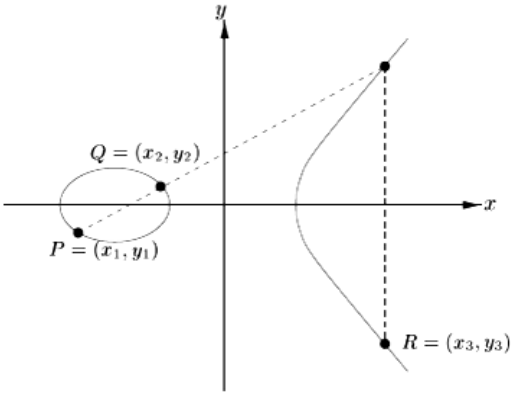

Рис. 1. Геометрична ілюстрація додавання точок на еліптичній кривій

Подвоєння точки в афінних координатах

Якщо P = Q., p = (x1,y1), P ⅃ E F_2^m,P≠ -P, тоді 2P = (x3,y3), де:

$$x_3 = x_1^2 + \frac{B}{x_1^2} \tag{9}$$

$$y_3 = x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3 \tag{10}$$

Геометричну ілюстрацію подвоєння можна побачити на рис. 2

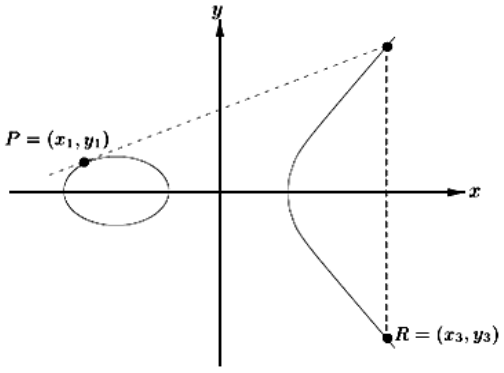

Рис. 2. Геометрична ілюстрація подвоєння

Основною операцією в групі точок еліптичної кривої є скалярний добуток точки на число. Як показано на рис. 3, множення точки на число відбувається за допомогою операцій додавання точок і подвоєння точки.

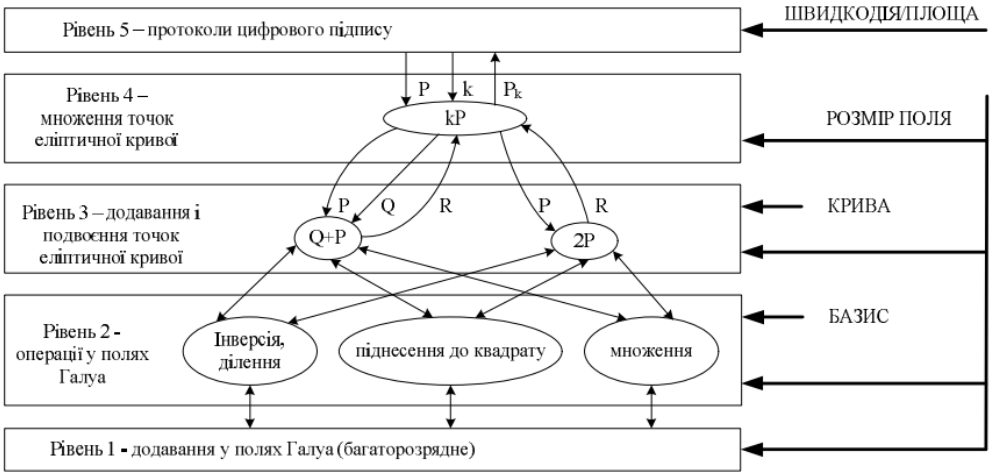

Рис.3. Ієрархічні рівні алгоритмів

Для множення точки P≠0 на велике ціле число можна використовувати способи, цілком аналогічні тим, що застосовуються для піднесення цілого числа до степеня k. Наприклад, якщо $k = \sum_{i=0}^{t-1} k_i 2^i$ – двійкове зображення числа, то точку Q = kP можна обчислити так:

1. Приймають Q ß O.
2. Для *i* від t-1 до 0 обчислюють Q ß 2Q, якщо $k_i = 1$, то додатково обчислюють Q ß Q+P.

4. Параметри ECDSA

Методи реалізації і характеристики криптографічних перетворень на еліптичній кривій залежать від таких параметрів:

1. Видів поля GF(q), над яким задається еліптична крива GF(p) чи GF (2m), де p – просте, m – ціле.
2. Представлення елементів поля в розширеному полі Галуа GF (2m) (поліноміальне чи нормальне).
3. Видів еліптичної кривої E() GF(q) (випадкова крива, крива Кобліца).
4. Представлення точок еліптичної кривої (афінне чи проективне).

Останнє дає змогу підвищити продуктивність, без втрати безпеки криптосистеми, тобто не зменшує складності розв'язання задачі дискретного логарифма в групі точок еліптичної кривої і тому є одним з основних підходів до зменшення складності перетворень у групі точок еліптичної кривої.

Щоб не генерувати власну еліптичну криву, кожен користувач може застосовувати ту саму криву *E* над полем *Zp* та точку *P* порядку *n*; ці характеристики називають системними параметрами. В цьому випадку відкритим ключем користувача буде лише точка Q. Відповідно, ключ буде меншого розміру.

5. Поля Галуа

Полем називають множину елементів, на якій визначено дві операції. Одна з них називається додаванням і позначається *a+b*, а інша – множенням і позначається *a-b*, навіть якщо ці операції не є звичайними операціями додавання і множення чисел. Для того, щоб множина елементів, на якій задані операції додавання і множення, була полем, необхідно, щоб для кожної з цих операцій виконувалися всі групові аксіоми, а саме комутативність *(a+b = b+a* і *ab = ba)*, асоціативність *(a+(b+c) = (a+b)+c* і *a(bc) = (ab)c)*, а також виконувався дистрибутивний закон, тобто для трьох будь-яких елементів поля a, b, c була справедлива рівність *a(b+c) = ab+ac* і *(b+c)a = ba+ca*.

Варто відмітити, що групові властивості для операції множення справедливі для всіх ненульових елементів поля.

Кількість елементів поля q називають порядком поля. Скінченні поля використовуються для побудови більшості відомих кодів і їх декодування.

Найменше число елементів, які утворюють поле, дорівнює 2. Таке поле повинне містити 2 одиничних елементи: **0** щодо операції додавання і **1** щодо операції множення. Це поле *GF(2),* або двійкове.

Залежно від значення q розрізняють прості або розширені поля. Поле називають простим, якщо q – просте число. Для позначення простих чисел використовуватимемо символ p. Просте поле утворюють числа за модулем p: *0, 1, 2., p-1*, а операції додавання і множення виконуються за модулем p. Якщо ж поле утворене з q^m елементів, то таке поле називають розширенням поля степеня m над *GF(p),* або розширеним полем. Воно містить p^m елементів і позначається $GF(p^m)$. Надалі розглядатимемо поля $GF(2^m)$. Будь-яке скінченне поле $GF(2^m)$ є m-вимірним вектором над полем *GF(2).* Многочлен $f(t)$ степеня m над полем *GF(2)* – це многочлен вигляду

$$f(t) = t_m + f^{m-1}t_{m+1} + \ldots + f_0 \qquad (11)$$

де коефіцієнти многочлена f належать *GF(2).* Операції над такими многочленами виконуються як операції над звичайними многочленами, тільки операції над коефіцієнтами виконуються в полі *GF(2).*

Многочлен $f(t)$ ненульового степеня називається незвідним над полем $GF(2^m)$, якщо він ділиться без залишку над цим полем на самого себе і на многочлени нульового степеня. Елемент x скінченного поля $GF(2^m)$ називається коренем многочлена $f(t)$, якщо $f(x)=0$. Якщо x – корінь незвідного многочлена $p(x)$ степеня m, то елементи $(x^{m-1}, \ldots, 1)$ утворюють базис скінченного поля $GF(2^m)$ як векторного простору над полем *GF(2).* Такий базис називається поліноміальним. Многочлен, коренем якого є примітивний елемент, називається примітивним многочленом. Якщо як $P(x)$ вибрати примітивний многочлен степеня m, незвідний над полем *GF(2)* m, отримаємо поле $GF(2^m)$ зі всіх 2^m двійкових послідовностей довжини m. Поліноміальний базис задається примітивним многочленом.

Елементи скінченного поля в поліноміальному базисі зображаються многочленами степеня, не більшого за $m-1$ або, що еквівалентно, двійковими рядками довжини m, що складаються з коефіцієнтів таких многочленів. Операції додавання і множення у скінченному полі в такому разі – це операції над многочленами степеня не вище за $m-1$ зі зведенням результату за потреби за модулем примітивного многочлена.

Додавання двох елементів виконується як додавання відповідних многочленів або як додавання за модулем 2 відповідних до цих многочленів двійкових рядків. Множення двох елементів виконується як множення відповідних многочленів з подальшим зведенням результатів за модулем примітивного многочлена.

Нормальним базисом поля *GF(2)* є множина:

$$B = \{q, q^2, q^{2^2}, \ldots, q^{2^{m-1}}\} \qquad (12)$$

Елементи множини можна подати у вигляді двійкових рядків $(a_0\ a_1\ a_2\ \ldots\ a_{m-1})$

$$a_0 q + a_1 q^2 + a_2 q^{2^2} + \ldots + a_{m-1} q^{2^{m-1}} \qquad (13)$$

Залежно від параметра T розрізняють типи нормального базису і нормальні поліноми:

якщо T = 1: $p(x) = t^m + t^{m-1} + \ldots + t^2 + t + 1$;

якщо T = 2: $p_0(t) = 1, p_1(t) = t+1, p_{i+1}(t) = tp_i(t) + p_{i-1}(t),\ i = 1, \ldots, m$.

6. Використання спеціалізованих процесорів для операцій над елементами полів Галуа

У сучасних системах захисту інформації операції над елементами полів Галуа традиційно реалізуються на базі універсальних програмованих процесорів. При цьому в [9] зазначено, що забезпечується висока гнучкість систем, простота налаштування та експлуатації, однак через структурні особливості універсальних програмованих процесорів важко досягти високих рівнів продуктивності, особливо при обробці даних, які надходять з одного чи декількох високошвидкісних каналів. Ситуація дещо покращується у разі використання програмованих процесорів зі спеціалізованою чи доповненою системами команд, де частина обчислень за

алгоритмами виконується у спеціалізованих операційних пристроях. Однак, внаслідок ітераційного виконання алгоритмів, тут також важко досягти високих швидкісних показників.

Істотний приріст продуктивності обробки даних досягається у разі використання апаратно-орієнтованих процесорів для виконання криптографічних алгоритмів. Тут операційний пристрій процесора орієнтований на виконання повного чи частини потокового графа криптографічного алгоритму, при цьому часто використовується конвеєрна організація обчислень, що дає змогу досягти максимальних рівнів продуктивності.

Виконання базових операцій перелічених алгоритмів шифрування на універсальних процесорах приводить до значних часових затрат на виконання цих операцій, і, як наслідок, зниження продуктивності обробки даних. Це зумовлено невідповідністю систем команд процесора та режимів адресації використовуваним операціям.

У [10] зазначено, що для обробки даних великої розрядності доцільно ввести у НВІС засоби підтримки багатопроцесорних конфігурацій. Також розширення та спеціалізація системи команд НВІС відповідно до алгоритму підвищить ефективність виконання алгоритмів асиметричного шифрування. Поява нових асиметричних алгоритмів шифрування та їх застосування для побудови криптографічних протоколів зумовлює необхідність створення програмованих НВІС асиметричного шифрування, які б могли виконувати послідовність операцій над числами великої розрядності, й отже, перенести процедуру організації протоколу на спеціалізовану НВІС.

З іншого боку, є задачі захисту інформації у смарт-картках, де необхідна продуктивність роботи пристрою шифрування повинна бути вищою, ніж в універсальних процесорах, але під час проектування таких пристроїв потрібно оптимізувати енергоспоживання і площу, яку займатиме пристрій на кристалі. В такому випадку перспективними є “мінімальні” структури пристроїв шифрування, які апаратно виконують заданий алгоритм із використанням мінімуму ресурсів.

Необхідно зазначити, що технічні характеристики НВІС великою мірою залежать від типу та рівня оптимізації використаних алгоритмів. Тому актуальним є розроблення нових алгоритмів шифрування та алгоритмів виконання модульних операцій, орієнтованих на виконання у вигляді НВІС.

7. Стійкість ECDSA

Щоб підтримати такий рівень надійності, як і в DSA (з 160-бітовим q та 1024-бітовим p), порядок базової точки еліптичної кривої повинен мати довжину 160 бітів. У цьому випадку DSA та ECDSA підписи мають однакову довжину (320 бітів).

Алгоритми DSA і ECDSA використовують те саме підписуюче рівняння: $s = k^{-1}\{h(m) + dr\} \bmod n$. В обох алгоритмах величини, що важко генеруються, є системними параметрами, що загальновідомі, і генерувати їх можна окремо.

Проте є деякі переваги ECDSA над DSA. По-перше, приватний ключ d та число k в ECDSA є статистично унікальними і непередбачуваними, а не просто випадковими, як у DSA, що робить алгоритм надійнішим. Крім того, завдяки складності проблеми дискретного логарифмування за однакової довжини ключа систему ECDSA важче зламати.

Пристрої, які виконують цифровий підпис на основі еліптичних кривих, вимагають менше місця, менше енергії, менше пам’яті й менше ресурсів, ніж інші системи. Це дає змогу здійснювати шифрування в платформах, які обмежені в продуктивності чи енергоспоживанні, таких як бездротові пристрої, кишенькові комп’ютери, смарт-карти, а також “тонкі клієнти”. Еліптична криптографія також забезпечує істотний виграш у ситуації, коли ефективність має велике значення.

Довжина поточного ключа DSA, рекомендованого NIST для старих державних програм у Сполучених Штатах Америки, становить 2048 бітів. Ключ ECDSA значно менший – 224 біти, але водночас забезпечує такий самий рівень безпеки. Ця перевага тільки зростає зі збільшенням розрядності ключа.

У [12] наведено порівняння криптографічної стійкості DSA і ECDSA відносно довжини ключа в бітах.

Таблиця 1

Порівняння криптографічної стійкості ECDSA і DSA відносно довжини ключа

№	ECDSA (size of *n* in bits)	DSA (modulus size in bits)
1	112	512
2	160	1024
3	224	2048
4	256	3072
5	384	7680
6	512	15360

В табл. 2 наведено порівняння рекомендацій щодо довжини ключа для ECDSA, яка повинна забезпечувати достатню криптографічну стійкість.

Прослідковується така закономірність: чим раніше розроблено рекомендації, тим меншу мінімальну довжину ключа пропонують на майбутні роки. Також в [13] рекомендується не використовувати ключі цифрового підпису розміром 160 бітів після 2010 року. Це дає змогу зробити висновок, що розмір ключа втрачає свою криптографічну стійкість раніше, ніж передбачено в різноманітних розрахунках, і вже у наш час є актуальним розроблення методів і засобів для збільшення розрядності полів Галуа для українського стандарту [2].

Таблиця 2

Рекомендації щодо довжини ключа

Метод, рік видання	Рік	Довжина ключа
[14] Lenstra/Verheul, 2000	2012	149
[15] Lenstra Updated, 2004	2012	152
[16] Ecrypt II, 2011	2011-2014	160
[17] NIST, 2011	2011-2030	224
[18] FNISA, 2010	2010-2020	200
[19] BSA (signatures only), 2011	2011-2015	224

Висновки

Розглянуто стан і напрями розвитку цифрових підписів. Визначено переваги використання НВІС для реалізації цифрового підпису, що ґрунтується на властивостях груп точок еліптичних кривих. Описано математичний апарат дій над точками еліптичних кривих у полях Галуа. Визначено переваги пристроїв, які виконують цифровий підпис на основі еліптичних кривих. Аналіз використання полів Галуа GF(2^m), де m>509, для оброблення цифрових підписів показує можливість подальшого розвитку чинного в Україні стандарту на формування і перевіряння цифрового підпису.

1. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. 2. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – Київ. Державний комітет України з питань технічного регулювання та споживчої політики, 2003. 3. Ian F.Blake, Gadiel Seroussi, Nigel P. Smart Advances in Elliptic Curve Cryptography London Mathematical Society Lecture Note Series (No. 317) – 2005.4. IEEE P1363 / D9(Draft Version 9). Standard Specifications for Public Key Cryptography, 1999. 5. AMERICAN NATIONAL STANDARD X9.62-1998 (Draft version), Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).6.AMERICAN NATIONAL STANDARD X9.63-1999 (Draft version) Public Key Cryptography For The Financial Services Industry:Key Agreement and Key Transport Using Elliptic Curve

Cryptography.7. http://www.secg.org/download/aid-780/sec1-v2.pdf *2009 p.8. Глухов В.С., Еліас Р. Виявлення помилок признаходженні оберненого елемента в Гауссівському нормальному базисі типу 2 Полів Галуа GF(2^m) // Радіоелектронні і комп'ютерні системи. – 2010. – № 6(47). – С. 129–133. 9. Мельник А., Морозов Ю., Мельник В., Коркішко Т. Проблеми і тенденції розвитку апаратних засобів захисту інформації// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ. – 2002. – Вип. 5. – С. 168–162. 10. Коркішко Т., Мельник А. Стан та напрямки розвитку надвеликих інтегрованих схем захисту інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ. – 2000. – С. 275 – 281. 11. Глухов В.С. Порівняння поліноміального та нормального базисів представлення елементів полів Галуа // Вісник Національного університету "Львівська політехніка". – 2007. – С. 22–27. 12. MuthuKumar B., Jeevananthan S. Performance Enhanced Co-Processor for Elliptic Curve Cryptography over GF (p) European Journal of Scientific Research ,ISSN 1450-216X Vol.68 No.4 (2012), pp. 544-555. 13. Recommendation for Key Management // Special Publication 800-56 Part 1 Rev. 3,* NIST*, 05/2007 14. Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, PKC2000: p. 446-465, 01/2000.15. Handbook of Information Security, Arjen K. Lenstra, 06/2004. 17.Yearly Report on Algorithms and Keysizes (2011), D.SPA.16 Rev. 1.0, ICT-2007-216676 ECRYPT II, 06/2011. 17. Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 3, NIST, 05/2011. 18. Mécanismes cryptographiques - Règles et recommandations, Rev. 1.20, FNISA , 01/2010.19. Algorithms for Qualified Electronic Signatures, BNetzA, BSI, 05/2011.*

УДК 681.3

С.В. Івасьєв
Інститут мікропроцесорних систем керування об'єктами електроенергетики
Карпатського державного центру інформаційних засобів і технологій
Національної академії наук України

МЕТОД ФАКТОРИЗАЦІЇ ВЕЛИКОРОЗРЯДНИХ ЧИСЕЛ У БАЗИСІ РАДЕМАХЕРА

Подано теоретичні основи та метод факторизації великорозрядних чисел Мерсена, проаналізовано основні властивості та розподіл чисел Мерсена. Наведено метод факторизації Ферма. Розроблено алгоритм факторизації великорозрядних чисел Мерсена та алгоритм знаходження залишку в базисі Радемахера.

Ключові слова: метод факторизації, великорозрядні числа Мерсена, базис Радемахера.

The paper presents the theoretical basis and method for factorization large-digit numbers Mersen, analyzed the basic properties of numbers and distribution Mersen numbers. The method of factorization Farm. An algorithm for factoring big Mersen numbers and algorithm for finding balance in the basis of Rademacher was created.

Key words: method for factorization, large-digit numbers Mersen, basis Rademacher.

Вступ

Важливим завданням опрацювання інформаційних потоків у комп'ютерних системах є розроблення нових методів та алгоритмів виконання операцій з великорозрядними числами (ВРЧ) [1], які широко використовуються в системах захисту інформаційних потоків. Найвідоміша реалізація алгоритму шифрування RSA, Ель–Гамаля, а також електронного цифрового підпису [1] ґрунтується на алгоритмічній складності задачі факторизації чисел. Відомі алгоритми факторизації ВРЧ характеризуються великою обчислювальною складністю. Тому задачі криптографії систем захисту, основані на використанні цих методів та тестів простоти для великих параметрів крипто-перетворень, стають практично нездійсненними.