УДК 681.3.06

В.Ю. Ковтун, О.О. Кузнецов, С.Ю. Стасєв

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

НЕСИМЕТРИЧНІ КРИПТОСИСТЕМИ НА ГІПЕРЕЛІПТИЧНИХ КРИВИХ НАД ПОЛЯМИ ПАРНОЇ ХАРАКТЕРИСТИКИ

Розглянуті несиметричні криптосистеми на гіпереліптичних кривих другого роду над полями парної характеристики, наведені результати експериментальних досліджень ефективності їх програмної реалізації, проведено порівняння отриманих результатів з криптосистемами на еліптичних кривих.

криптосистеми, гіпереліптичні криві

Вступ

Постановка проблеми в загальному вигляді та аналіз літератури. В умовах стрімкої комп'ютеризації сучасного суспільства особливої актуальності набувають питання інформаційної безпеки, найбільш складним з яких є захист цінної конфіденційної і секретної інформації в державних та приватних підприємствах, в органах управління, банківській і інших системах [1 - 10]. Комплексне вирішення задач захисту інформаційного простору України покладається на Національну систему конфіденційного зв'язку, в якій за допомогою криптографічних і технічних засобів забезпечуються послуги конфіденційності, цілісності, автентичності та доступності інформації. У той же час, поява нових методів криптоаналізу в сукупності з можливостями сучасної обчислювальної техніки висувають підвищені вимоги до стійкості сучасних криптографічних засобів, а підвищення обсягів оброблюваних даних у сучасних комп'ютерних системах і мережах висуває підвищені вимоги до їх швидкодії. Таким чином, в умовах суперечливих чинників, що різко загострилися, імовірнісно-часові вимоги до сучасних криптографічних засобів захисту інформації істотно зросли [11 - 17]. Перспективні криптоалгоритми повинні забезпечувати швидке криптографічне перетворення великих обсягів даних, високий рівень забезпечуваної стійкості до сучасних методів криптоаналізу з теоретично обгрунтованою моделлю безпеки. Актуальним напрямом у цьому сенсі є розробка несиметричних криптосистем, що допускають функціонування в інфраструктурі відкритих ключів, дослідження ефективності програмної і апаратної реалізації. Найбільш поширені і добре вивчені несиметричні криптоалгоритми ґрунтуються на зведенні завдання безключового читання до вирішення теоретико-складнісної задачі дискретного логарифмування в групі точок еліптичної кривої (ЕК), про що свідчить їх стандартизація [2 - 10]. За останні десятиліття з'явилася значна кількість робіт, присвячених дослідженню їх стійкості до криптоаналізу, практичній реалізації [1, 17 - 20]. Як можлива альтернатива в деяких роботах запропоновані криптосистеми на гіпереліптичних кривих (ГЕК), які, як відомо, є багатшим джерелом скінчених абелевих груп [11, 12]. У той же час відкритим залишається питання ефективної реалізації таких криптосистем, дослідження «тонкої» організації їх загальносистемних параметрів.

Метою статті є викладення основних результатів, отриманих авторами при побудові несиметричних криптосистем на ГЕК, дослідження ефективності їх програмної реалізації, проведення порівняльних досліджень з криптосистемами на ЕК.

Реалізація обчислень в скінчених полях. Відомо, що при додаванні дивізорів використовуються перетворення в скінчених полях [11 - 17]. Дослідимо у зв'язку з цим ефективність реалізації арифметичних перетворень у простих і двійкових полях.

У роботах [15, 16] детально розглянуті алгоритми арифметичних перетворень у скінчених полях. Реалізація цих алгоритмів виконана мовою C++. У табл. 1 наведені умови проведення експериментальних досліджень. Поля, для яких проводилося порівняння, були запозичені із списку рекомендованих ЕК [17]. У табл. 2 наведені результати експериментальної оцінки часу виконання полевих операцій.

Таблиця 1

Умови проведення експериментальних оцінок часу виконання алгоритмів, що реалізують операції в полі

Номер колонки	Джерело	Процесор	Операційна система	Компілятор	Особливості реалізації
1	[15]	Intel, Pentium II 400 MHz	MS Windows 2000	MS Visual C++ 6.0	З використанням асемблера
2	автори	AMD, Athlon XP 2500+ MHz	MS Windows XP	MS Visual C++ 2005	Без використання асемблера

Таблиця 2

Експериментальні оцінки часу виконання операцій у двійковому полі

Двійкова довжина поля	Операція	1, мкс	2, мкс
163	Додавання	0,10	0,022
	Множення, метод Comb	3,0	2,35
	Множення, метод Карацуби	3,92	-
	Зведення до модуля	0,18	0,039
	Піднесення до квадрата	0,4	0,089
	Інвертування, розширений алгоритм Евкліда	30,99	44,53
233	Додавання	0,12	0,026
	Множення, метод Comb	5,07	3,56
	Множення, метод Карацуби	7,04	-
	Зведення до модуля	0,22	0,034
	Піднесення до квадрата	0,55	0,097
	Інвертування, розширений алгоритм Евкліда	53,22	76,25
283	Додавання	0,13	0,031
	Множення, метод Comb	6,23	4,281
	Множення, метод Карацуби	8,01	-
	Зведення до модуля	0,35	0,144
	Піднесення до квадрата	0,75	0,207
	Інвертування, розширений алгоритм Евкліда	70,32	92,34

У табл. 3 розглядаються поля, які використовуються як базові для ГЕК, а в табл. 4 – ті, що є порядком групи.

Таблиця 3

Експериментальні оцінки часу виконання операцій у базових полях

Назва поля	Поле	Операція	Час, мкс
БП1	$\mathbf{GF}\left(2^{89}\right)$: $p1(t) = t^{89} + t^{38} + 1$	Додавання	0,012
		Множення, метод Comb	1,188
		Зведення до модуля	0,079
		Піднесення до квадрата	0,108
		Інвертування, розширений алгоритм Евкліда	20,78

Таблиця 4

Експериментальні оцінки часу виконання операцій у полях – порядках групи

Назва поля	Поле	Операція	Час, мкс
ПП1	$\mathbf{GF}(p_{173})$: $p_7 = 191561942608242456073498418252108663615312031512914969$	Додавання	0,031
		Множення, метод Comb	37,5
		Зведення до модуля	28,672
		Піднесення до квадрата	32,4
		Інвертування, розширений алгоритм Евкліда	42,2

З метою порівняння продуктивності криптосистем на ГЕК наведемо також результати експериментальної оцінки криптосистем на ЕК.

Продуктивність криптосистем на ЕК. При проведенні експериментальних оцінок перетворень у групі точок ЕК були використані криві, рекомендовані в [17]. При реалізації перетворень у проектних координатах були використані також роботи [18 - 20].

Таблиця 5

Експериментальні оцінки часу виконання перетворення в групі точок еліптичної кривої

Операція	B-163, мс	B-233, мс	B-283, мс
Скалярне множення, метод Lim-Lee	0,36	0,41	0,92
Скалярне множення, метод «піднести до квадрата і помножити», проміжні обчислення в проектних координатах Lopez-Dahab	1,79	4,0	5,20
Скалярне множення, метод «піднести до квадрата і помножити» в афінних координатах	12,11	29,14	43,45
Передобчислювання для скалярного множення методом Lim-Lee	468,0	953,0	1281,0
Формування цифрового підпису за допомогою методу Lim-Lee	0,688	1,406	1,891
Перевірка цифрового підпису за допомогою методу Lim-Lee і методу «додати і подвоїти, зліва направо»	3,937	8,969	13,39

Продуктивність криптосистем на ГЕК. При програмній реалізації перетворень в якобіані ГЕК був використаний метод Harley'a, який був модифікований для випадку двійкового поля. Це дозволило значною мірою оптимізувати обчислення. Оцінка складності операцій в якобіані ГЕК другого роду над полем парної характеристики наведена в табл. 6.

Проведемо аналіз перетворень в якобіані ГЕК другого роду, який дозволить вибрати безпосередньо вид кривої і перетворення, що забезпечують найменшу обчислювальну складність для неї.

Таблиця 6

Складність операцій в якобіані ГЕК другого роду над полем парної характеристики в полевих операціях методом Harley

Род	Умови	Додавання			Змішане додавання			Подвоєння			Змішане подвоєння		
		()-1	^2	*	()-1	^2	*	()-1	^2	*	()-1	^2	*
2	Афінні координати												
	$h_i \in F_2$ [30]	1	2	25				1	1	27			
	$f_4 = 0$ [24]	1	3	21				1	5	20			
	$h_2 = 0,\ f_4 = 0$ [24]	1	3	21				1	5	17			
	$h(x) = x,\ f_4 = 0,\ f_3 = f_2 = 0$ [22]							1	6	9			
	$h(x) = x,\ f_4 = 0,$ $f_3 = f_2 = 0$ [22]							1	6	9			
	$h(x) = x,$ $f(x) = x^5 + f_3 x^3 + \varepsilon x^2 + f_0,$ $\varepsilon \in \mathbf{F}_2$ [27]	1		24				1	5	13			
	$\deg(h) = 2,\ h_0 = 0,\ h_1 \in \mathbf{F}_q,$ $f(x) = x^5 + \varepsilon x^4 + f_1 x + f_0,$ $\varepsilon \in \mathbf{F}_2$ [27]	1		25				1	4	22			
	$h_1 \in \mathbf{F}_q,\ h_2 = h_0 = 0,$ $f_4 = f_1 = 0$ [29]							1	5	9			
	$h_1 = 1,\ h_2 = h_0 = 0,$ $f_4 = f_1 = 0$ [29]							1	6	5			
	$\deg(h) = 2,\ h_0 = 0,\ h_1 \in \mathbf{F}_q,$ $f_3 = f_2 = 0$ [49]							1	5	17			
	$\deg(h) = 2,\ h_0 = 0,\ h_1 \in \mathbf{F}_2,$ $f_3 = f_2 = 0$ [49]							1	6	12			

С точки зору практичного застосування, інтерес викликають перетворення в Якобіані кривих роду 2.

Аналіз результатів оцінок складності, наведених у табл. 6, дозволяє зробити висновок, що на сьогоднішній день найбільш ефективними є перетворення: Byramjee, Duquesne [27] і Lange [24].

У програмній реалізації використовувався опис різних вхідних даних з роботи [23], алгоритми перетворень у найбільш поширених випадках з [24].

Консолідуємо складності перетворень для різних вхідних даних у табл. 7.

У чарунках таблиці, які знаходяться на перетині стовпчиків і рядків, що є вхідними даними, представлені складності алгоритмів додавання відповідних дивізорів.

Таблиця 7

Складності алгоритмів складання дивізорів у залежності від дивізорів, які додаються

Вхідні дані	$D_1 = P_1$		$D_1 = 2P_1$		$D_1 = P_1 + P_2$	
$D_1 = P_1$	4M+4S+6A+1I	1	55A+7S+35M+2I	2	33A+16M+5S+2I	3
$D_1 = -P_1$	3A+1S	4	9A+3M	5	9A+3M	5
$D_1 = P_2$	4A+5M+1I	6	19A+1S+11M+1I	7	33A+16M+5S+2I	3
$D_1 = 2P_1$	55A+7S+35M+2I	2	31A+6S+23M+1I	8	58A+7S+34M+4I	9

Продовження табл. 7

Вхідні дані	$D_1 = P_1$		$D_1 = 2P_1$		$D_1 = P_1 + P_2$	
$D_1 = P_1 + P_2$	33A+16M+5S+2I	3	58A+7S+34M+4I	9	31A+6S+23M+1I / (23A+4S+14M+1I)	8
$D_1 = -P_1 + P_2$	9A+3M	5	18A+1S+13M+2I	10	10A+4S+6M+2I	11
$D_1 = P_1 + P_3$	33A+5S+16M+2I	3	58A+7S+34M+4I	9	58A+7S+34M+4I	9
$D_1 = -P_1 + P_3$	9A+3M	5	18A+1S+13M+2I	10	18A+1S+13M+2I	10
$D_1 = P_3 + P_4$	19A+1S+11M+1I	7	33A+3S+21M+1I / (21A+2S+11M+1I)	12	33A+3S+21M+1I / (21A+2S+11M+1I)	12

Через дріб указуються складності алгоритмів додавання дивізорів ваги 2, у разі, коли результуючий дивізор має вагу 1.

Експериментальна оцінка часу виконання криптоперетворень. Для оцінки часу виконання перетворень авторами проведена серія експериментів. У табл. 8 наведені параметри, які підлягали експериментальній оцінці.

Таблиця 8

Перелік параметрів, які оцінювалися при експериментальній оцінці часу виконання операцій в якобіані ГЕК другого роду в афінному представленні дивізорів

№	Операція
1	Додавання дивізорів ваги 2, $D_1 = P_1 + P_2 - 2\inf$, $D_2 = P_3 + P_4 - 2\inf$, точки з носіїв дивізорів - різні
2	Додавання дивізорів ваги 1, $D_1 = P_1 - \inf$, $D_2 = P_2 - \inf$, точки з носіїв дивізорів - різні
3	Подвоєння дивізора ваги 2, $D_1 = P_1 + P_2 - 2\inf$, точки з носіїв дивізорів - різні
4	Подвоєння дивізора ваги 1, $D_1 = P_1 - \inf$, точки з носіїв дивізорів - різні
5	Передобчислення для скалярного множення методом Lim-Lee дивізора ваги 2, $D_1 = P_1 + P_2 - 2\inf$
6	Скалярне множення дивізора ваги 2, $D_1 = P_1 + P_2 - 2\inf$, методом Lim-Lee
7	Скалярне множення дивізора ваги 2, $D_1 = P_1 + P_2 - 2\inf$, методом «додати та подвоїти, зліва направо»
8	Передобчислення для скалярного множення методом Lim-Lee дивізора ваги 1, $D_1 = P_1 - \inf$
9	Скалярне множення дивізора ваги 1, $D_1 = P_1 - \inf$, методом Lim-Lee
10	Скалярне множення дивізора ваги 1, $D_1 = P_1 - \inf$, методом «додати та подвоїти, зліва направо»

У табл. 9 перелічені криві, які були використані при проведенні експериментів.

Таблиця 9

Криві, які використовувались при проведенні експериментів

Назва кривої	Опис кривої
K1	Крива: $y^2 + (x^2 + x + 1)y = x^5 + x^4 + 1$ Базове поле: БП1. Порядок якобіана: 2 * 191 561 942 608 242 456 073 498 418 252 108 663 615 312 031 512 914 969. Порядок базового дивізора: ПП1. Кофактор: 2. Базовий дивізор ваги 2 (різні точки в основі): u_0 = 0x01a6134a 0x5c78fcef 0x6da993ed; u_1 = 0x0134536f 0x04b7df74 0x0c9fff03; $u_2 = 1$; v_0 = 0x0190fd61 0x66888e97 0xe8ade21c; v_1 = 0x01f55c1b 0x8a5bb7de 0x5abfca3b. Базовий дивізор ваги 1: u_0 = 0x0002844c 0x09d3ccf5 0x0c0c4384; $u_1 = 1$; $u_2 = 0$; v_0 = 0x008255ff 0x5742cfc4 0xcb699820; $v_1 = 0$. Джерело: [31].

Нижче наводяться результати експериментальних оцінок часу виконання групових операцій для перелічених у табл. 9 кривих за умов, вказаних у табл. 8.

Таблиця 10

Експериментальні оцінки часу виконання операцій в якобіані ГЕК другого роду в афінному представленні дивізорів

Крива	1, мс	2, мс	3, мс	4, мс	5, мс	6, мс	7, мс	8, мс	9, мс	10, мс
K1	0,045	0,025	0,045	0,025	2031,0	0,79	3,23	2016,0	0,71	3,05

З табл. 10 видно, що використання дивізорів ваги 1 є найбільш перспективним, оскільки дозволяє скоротити обчислювальні ресурси. На це ж було звернено увагу в публікації [32], що є, поза сумні-

вом, перспективним напрямом досліджень у сенсі оптимізації обчислень базових дивізорів ваги 1.

Для переходу від суто теоретичних досліджень продуктивності криптоперетворень до оцінки продуктивності безпосередньо криптосистеми авторами реалізована схема DSA [5], де як група був вибраний якобіан ГЕК другого роду над двійковим полем. У табл. 11 наводяться параметри, які оцінювалися в ході експериментальних досліджень.

Таблиця 11

Перелік параметрів, які оцінювалися при експериментальній оцінці часу виконання криптографічних перетворень в якобіані ГЕК другого роду в афінному представленні дивізорів

№	Операція
1	Передобчислення для скалярного помноження методом Lim-Lee дивізора ваги 2, $D_1 = P_1 + P_2 - 2\inf$
2	Формування цифрового підпису, базовий дивізор ваги 2, $D_1 = P_1 + P_2 - 2\inf$, методом Lim-Lee
3	Перевірка цифрового підпису, базовий дивізор ваги 2, $D_1 = P_1 + P_2 - 2\inf$, методом Lim-Lee та методом «додати та подвоїти, зліва направо»
4	Передобчислення для скалярного множення методом Lim-Lee дивізора ваги 1, $D_1 = P_1 - \inf$
5	Формування цифрового підпису, базовий дивізор ваги 1, $D_1 = P_1 - \inf$, методом Lim-Lee
6	Перевірка цифрового підпису, базовий дивізор ваги 1, $D_1 = P_1 - \inf$, методом Lim-Lee та методом «додати та подвоїти, зліва направо»

Нижче наведені експериментальні оцінки часу виконання криптографічних перетворень для перелічених вище в табл. 8 кривих для параметрів з табл. 11.

Таблиця 12

Експериментальні оцінки часу виконання криптографічних перетворень в якобіані ГЕК другого роду в афінному представленні дивізорів

Крива	1, мс	2, мс	3, мс	4, мс	5, мс	6, мс
K1	2031,0	1,39	13,47	2016,0	1,29	13,22

Висновки

У даній роботі наведені результати ефективної програмної реалізації криптосистеми на ГЕК другого роду над двійковими полями. Видно, це перший подібний результат у вітчизняній криптографії [1, 3, 9, 10, 18 – 20, 25, 26].

Отримані результати проведених експериментальних досліджень свідчать про сумірну продуктивність формування і перевірки цифрового підпису на ЕК і ГЕК, реалізованих за схемою DSA (див. дані таблиць 5 і 12). Це, у свою чергу, дозволяє стверджувати про реальну альтернативу криптосистем на ЕК – проведені експериментальні дослідження свідчать про високі конструктивні показники криптосистем на ГЕК.

Подяки. Автори виражають щирі подяки Colm O'hEigeartaigh, а також Jan Pelzl за допомогу, надану при виконанні програмної реалізації.

Список літератури

1. В.Ю. Ковтун, Збитнев С.И., Шевченко Д.В., Гиневский А.М. Исследование алгоритмов решения задачи дискретного логарифма на эллиптической и гиперэллиптических кривых // Восточно-Европейский журнал передовых технологий. – 2004. – Вып. № 6 (12). – С. 155-167.

2. ANSI X9.42–1998: Public Key Cryptography for The Financial Service Industry: Agreement of Symmetric Keys on Using Diffie–Hellman and MQV Algorithms. – 1998. – 93 p.

3. ГОСТ Р 34.10–1994. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. – М.: Госстандарт России, 1994. – 24 с.

4. ISO/IEC FCD 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves, Final Committee Draft. – 2001.

5. IEEE P1363–2000: Standard Specifications for Public Key Cryptography. – 2000. – 206 p. – [Електрон. ресурс]. – Режим доступу: Available at: http://www.ieee.org.

6. ANSI X9.62–1998: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). – 1998. – 192 p.

7. ANSI X9.42–1998: Public Key Cryptography for The Financial Service Industry: Agreement of Symmetric Keys on Using Diffie–Hellman and MQV Algorithms. – 1998. – 93 p.

8. ANSI X9.63–1999 Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. – 1999. – 207 p.

9. ГОСТ Р 34.10–2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Госстандарт России, 2001. – 24 с.

10. ДСТУ 4145–2002. Інформаційні технології. Кри-

нтографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К.: Держстандарт України, 2002. – 40 с.

11. Koblitz N. Hyperelliptic cryptosystems // Journal of cryptology. – 1989. – No.1. – P. 139-150.

12. Menezes A.J., Wu Y., Zuccherrato R.J. An elementary introduction to hyperelliptic curves // Technical report CORR96-19, Department of combinatorics and optimization, University of Waterloo, Waterloo, Ontario, 1996. In: Koblitz, N.: Algebraic aspects of cryptography, Springer-Verlag, Berlin Heidelberg New York. 1998.

13. R. Moreno, J.M. Miret, F. Sebe. A hyperelliptic cryptosystem based // P1363 IEEE standard.

14. N.P.Smart. On the Performance of Hyperelliptic Cryptosystems // Advances in Cryptology – Eurocrypt'99. – LNCS 1592. – Berlin: Springer, 1999. – P. 165-175.

15. Hankerson D., Lopez J., Menezes A. Software implementation of elliptic curve cryptography over binary fields / In Cetin K. Koc and C. Paar editors // Workshop and embedded systems. – CHES'99. – LNCS 1717. – Berlin: Springer–Verlag, 2000. – P.1-24.

16. Brown M., Hankerson D., Lopez J., Menezes A. Software implementation of the NIST elliptic curves over prime fields // Research Report CORR 2000–56. Department of Combinatorics and Optimization, University of Waterloo. – Canada: Waterloo, Ontario, 2000. – 21 p.

17. National Institute of Standards and Technology, Recommended Elliptic Curves for Federal Government Use, Appendix to FIPS 186-2, 2000. – 43 p.

18. Ковтун В.Ю., Смирнов А.А., Стасева Я.Ю. Представление точек эллиптической кривой над двоичными полями // Системи обробки інформації. – Х.: ХВУ, 2002. – Вип. № 6 (22). – С. 228-232.

19. Ковтун В.Ю., Збитнев С.И., Ильясова О.Е. Арифметические операции на эллиптической кривой над двоичным полем в проективных координатах // Радиотехника: Всеукраинский межведомственный научно-технический сборник. – Х.: ХНУРЭ, 2005. – Вып. № 141. – С. 97-107.

20. Ковтун В.Ю. Метод сложения точек эллиптической кривой в проективных координатах Лопеса-Дахаба // Системи обробки інформації. – Х.: ХВУ, 2004. - Вип. 12 (40). – С. 83-88.

21. Nagao K. Improving Group Law Algorithms for Jacobians of Hyperelliptic Curves / W. Bosma, editor // ANTS IV, LNCS 1838. – Berlin: Springer-Verlag. – P. 439-448.

22. Wollinger T. Software and hardware implementation of hyperelliptic curve cryptosystems. PhD dissertation: Electronics and informatics. – Worchester Polytecnic Institute. – Germany: Bochum, 2004. – 218 p.

23. Harley R. Fast arithmetic on genius two curves. – 2000. Available at: http://cristal.inria.fr/harley/hyper/, adding.txt and doubling.c.

24. Lange T. Efficient arithmetic on genus 2 hyperelliptic curves over finite fields via explicit formulae // Cryptology ePrint Archive. – Report 2002/121. – 2002. – 13 p. – [Електрон. ресурс]. – Режим доступу: Available http://eprint.iacr.org.

25. Ковтун В. Ю., Збитнев С. И. Арифметические операции в якобиане гиперэллиптической кривой рода 2 в проективных координатах с уменьшенной вычислительной сложностью // Восточно-Европейский журнал передовых технологий. – 2004. – № ½ (13). – С. 14-22.

26. Ковтун В.Ю. Преобразования в якобиане гиперэллиптической кривой рода 2 в проективных координатах над полем нечетной характеристики // Радиотехника: Всеукраинский межведомственный научно-технический сборник. – Х.: ХНУРЭ, 2006. – № 144. – С. 102-110.

27. Byramjee B., Duquesne S. Classification of genus 2 curves over F2 and optimization of their arithmetic // Cryptology ePrint Archive. – Report 2004/107. – 2004. – [Електрон. ресурс]. – Режим доступу: Available at: http://eprint.iacr.org.

28. Lange T. Weighted coordinates on genius 2 hyperelliptic curves // Cryptology ePrint Archive. – Report 2002/153. –2002. – 20 p. Available at: http://eprint.iacr.org.

29. Lange T., Stevens M. Efficient Doubling on Genus Two Curves over Binary Fields // Selected Areas in Cryptography. – Springer-Verlag. – LNCS 3357. – 2004. – P. 170-181.

30. Sugizaki H., Matsuo K., Chao J., Tsujii S. An extension of Harley addition algorithm for hyperelliptic curves over finite fields of characteristic two // Technical report IEICE. – ISEC2002–09. – IEICE`2002. – 2002. – 8 p.

31. Lange T. Efficient arithmetic on hyperelliptic curves. PhD dissertation: Mathematics and informatics. – Germany: Essen, 2001. – 122 p. – [Електрон. ресурс]. – Режим доступу: Available at: http://www.exp-mayh.uni-essen.de/~lange/KoblitzC.html.

32. Katagi M., Kitamura I., Akishita T., Takagi T., Novel Efficient Implementations of Hyperelliptic Curve Cryptosystems using Degenerate Divisors // Cryptology ePrint Archive. – Report 2006/203. – 2004. – [Електрон. ресурс]. – Режим доступу: Available at: http://eprint. iacr.org.

Надійшла до редколегії 14.04.2007

Рецензент: д-р техн. наук, проф. І.Д. Горбенко, Харківський національний університет радіоелектроніки, Харків.