УДК 519.9

Даниленко Д. А.[1], студент.

Оптимізація еліптичних кривих

[1] Київський національний університет імені Тараса Шевченка, 83000, м. Київ, пр-т. Глушкова 4д,
e-mail: ozar1024@gmail.com

D. Danylenko[1], student.

Optimization of elliptic curves

[1] Taras Shevchenko National University of Kyiv, 83000, Kyiv, Glushkova st., 4d,
e-mail: ozar1024@gmail.com

У статті представлені результати реалізації класичних алгоритмів обчислень, арифметики Монтгомері і Катацуби в реалізації ГОСТ Р 34.10-2012 на основі еліптичних кривих. Мета даної роботи – підрахунок кількості операцій кожної дії для подальшого порівняння. Арифметика Монтгомері не вигідна, якщо використовується тільки додавання і множення. Операції Карацуби виграшні лише при достатньо довгих числах.

Ключові слова: еліптичні криві, арифметика Монтгомері, алгоритм Карацуби.

Existing algorithms that underlie modern cryptography may be at risk due to the progress of solving mathematical problems. The software must be easily updated, allowing to keep in touch with mathematical progress and technical achievements in the industry. As a solution to all problems is proposed cryptography based on elliptic curves over finite fields. Methods elliptical cryptographic techniques similar to other asymmetric algorithms: The assumption of the complexity of the mathematical problem, in this case - the discrete logarithm in the group of points of elliptic curves. Unlike similar assignments integer factorization and discrete logarithms, positive results in one of them threatened elliptical cryptography.The article presents the results of the classical computational algorithms, Montgomery reduction and Katatsuby algorithm in the implementation of GOST R 34.10-2012 based on elliptic curves. The aim of this work - counting the number of operations of each action for future comparison. Montgomery arithmetic is not profitable only for addition and multiplication. Karatsuba algorithm wins only at sufficiently long numbers.

Key Words: Elliptic curves, Montgomery reduction, Karatsuba algorithm.

Статтю представив д. ф.-м. н., проф. Анісімов А. В.

У Лас-Вегасі на конференції Black Hat з особливою заявою виступили четверо дослідників кібербезпеки: Алекс Стеймос, Том Ріттер , Томас Птачек і Джавед Семюель. Існуючі алгоритми, що лежать в основі сучасної криптографії, можуть перебувати в небезпеці у зв'язку з прогресом вирішення математичних завдань.

Загальновідомо, що в основі асиметричної криптографії лежить два ключа: один може зашифрувати дані, інший використовується для їх розшифрування. Передбачається, що деякі математичні операції важкі і можуть бути виконані лише за експоненціальний час. Однак, існування таких функцій, тобто властивість експоненціального зростання складності, так і залишається недоведеною гіпотезою.

Найбільш поширені асиметричні алгоритми – алгоритм Діффі-Хеллмана, RSA, DSA – покладаються на складність двох завдань: факторизації цілих чисел і дискретного логарифмування. Але були отримані швидкі алгоритми дискретного логарифмування, що мають обмежене застосування. На даний момент не існує відомих способів використання цих напрацювань у практичній криптографії, але навіть ці математичні досягнення лякають

криптографів. Дослідники проводили аналогії з атаками на SSL виду BEAST, CRIME і BREACH. Використані для цих атак особливості асиметричної криптографії довгі роки вважалися суто теоретичними і не мають практичного застосування, але все виявилось інакше.

Під загрозою будуть оновлення з новими методами криптографії для операційних систем і прикладного ПО: оскільки програми спираються на цифрові підписи, швидко з'являться підроблені пакети оновлень.

В якості вирішення всіх проблем пропонується криптографія на основі еліптичних кривих над скінченними полями. Методи еліптичної криптографії схожі з методами інших асиметричних алгоритмів: є припущення про складність математичної задачі, в даному випадку – дискретного логарифмування в групах точок еліптичних кривих. На відміну від подібних завдань факторизації цілих чисел і дискретного логарифмування, позитивні результати в одній з них не загрожують еліптичній криптографії.

Еліптична крива – безліч точок (x, y), що задовольняють рівняння $y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$.

Це рівняння може розглядатися над довільними полями і, зокрема, над кінцевими полями, що представляють для криптографії особливий інтерес.

У криптографії еліптичні криві розглядаються над двома типами кінцевих полів: простими полями непарної характеристики ($Z_p, p > 3$ – просте число) і полями характеристики 2.

Слід зазначити, що в Z_p у кожного ненульового елемента є або два квадратних кореня, або немає жодного, тому точки еліптичної кривої розбиваються на пари вигляду (x, y) і $(x, -y)$.

Для використання еліптичної криптографії всі учасники повинні узгодити всі параметри, що визначають еліптичну криву, тобто набір параметрів криптографічного протоколу. Еліптична крива визначається константами a і b.

Для знаходження кривої для набору параметрів використовуються два методи:

•Вибрати випадкову криву, потім скористатися алгоритмом підрахунку точок.

•Вибрати точки, після чого побудувати криву по них, використовуючи техніку множення.

Існує декілька класів криптографічно «слабких» кривих, яких слід уникати:

• Криві над F_{2^m}, де m – не просте число. Шифрування схильне до атак Вейля.

• Криві з $|E(F_q)| = q$ вразливі для атаки, яка відображає точки даної кривої в адитивну групу поля F_q.

Для обчислення суми пари точок на еліптичній кривій потрібно не тільки кілька операцій додавання і множення в F_q, а й операція звернення, тобто для заданого $x \in F_q$ знаходження такого $y \in F_q$, що $xy = 1$, яка на один-два порядки повільніше, ніж множення.

У зв'язку з цим був реалізований ГОСТ Р 34.10-2012 та спроба пришвидшення його роботи з допомогою арифметики Монтгомері і Карацуби. Це дало змогу порівняти ефективність алгоритмів при різних обставинах з класичними алгоритмами обчислень.

Особливість арифметики Монтгомері дозволяє уникати повільної операції ділення. Для його виконання ми шукаємо обернений елемент (який займає більшу половину часу) та додаткову редукцію. Ділень стає менше, але додавань і множень врази більше, що не є вигідно (Рис. 1-4). Оскільки для операцій в даній системі потрібно спочатку робити редукцію, а потім обернену редукцію, то це не ефективно, якщо використовується тільки додавання і множення.

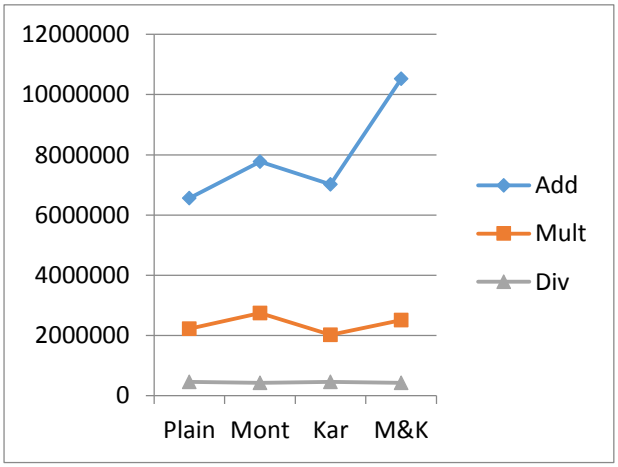

Рис. 1 Довжина слова 20

Арифметика Карацуби орієнтована на пришвидшення операції множення. Результати показують, що даний алгоритм стає невигідним зі зменшенням кількості слів у порядку кривої. Наприклад для довжини слова 5: множень стає менше на 5000, кількість додавань збільшується на 75000 (Рис. 4). А для довжини 20: множень менше на 200000, додавань більше на 500000 (Рис. 1). З цього можна зробити висновок, що чим довші числа, тим більша перевага використання алгоритму Карацуби.

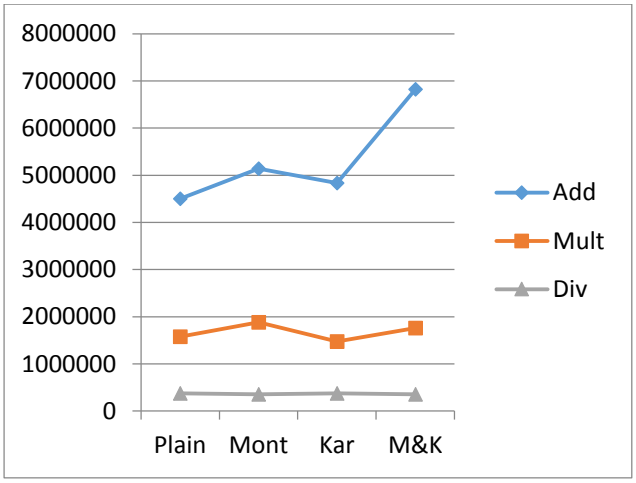

Рис. 2 Довжина слова 15

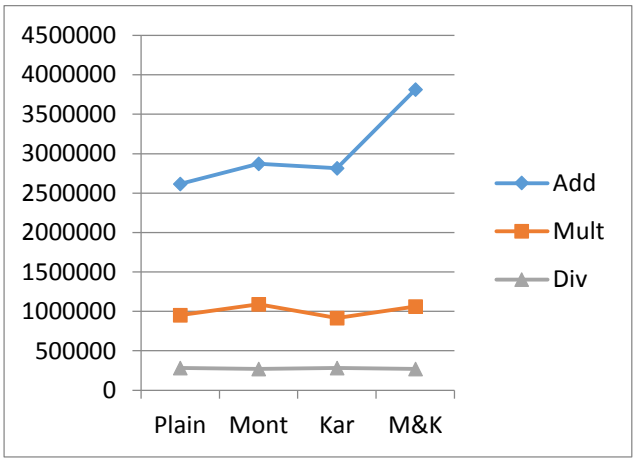

Рис. 3 Довжина слова 10

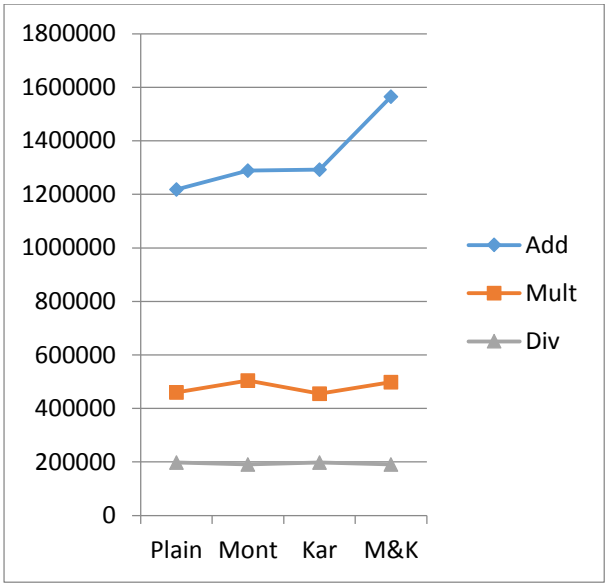

Рис. 4 Довжина слова 5

У загальному і цілому дослідники закликають індустрію інформаційних технологій почати підтримувати еліптичну криптографію вже сьогодні, а також упевнитися в захищеності систем: вони не повинні покладатися на застарілі алгоритми та протоколи. Програмне забезпечення повинно бути легко оновлюваним, дозволяючи тримати зв'язок з математичним прогресом і технічними досягненнями галузі. Криптоапокаліпсіс може і не статися, але готовність до нього обов'язкова вже зараз.

Список використаних джерел

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / М.: ТРИУМФ, 2002 – 816 с.
2. *Семёнов Г.* Цифровая подпись. Эллиптические кривые / «Открытые системы» № 7-8/2002 – 9 с.
3. A. Menezes, P. van Oorschot, S. Vanstone. Chapter 14. Efficient Implementation / Handbook of Applied Cryptography. — CRC-Press, 1996. — p. 816.
4. Cetin K. Koc, Tolga Acar, Analyzing and Comparing Montgomery Multiplication Algorithms / IEEE Micro,1996. pp. 26–33.
5. *Кнут Д.* Искусство программирования. (3-е изд.) / М.: Вильямс, 2007. — 832 с.

References

1. SCHNEIER B.(1994) *Applied Cryptography*/ ISBN John Wiley & Sons, p. 816.
2. SEMENOV G. (2002) *Digital signature. Elliptic curves* / ISBN "Open Systems» № 7, p. 9.
3. MENEZES A., VAN OORSCHOT P., VANSTONE S. (1996) *Chapter 14. Efficient Implementation* / Handbook of Applied Cryptography. — CRC-Press, p. 816.
4. CETIN K. KOC, TOLGA ACAR (1996) *Analyzing and Comparing Montgomery Multiplication Algorithms* / IEEE Micro p. 26-33.
5. KNUTH D. (2007) *The Art of Computer Programming (3rd ed.)* / ISBN Addison-Wesley Professional, p. 832.

Надійшла до редколегії 25.07.14