

ПЕРЕЛІК ПОСИЛАНЬ

1. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозрядних чисел. //Київ – 2003.
2. Карацуба А.А., Офман Ю.П. Умножение многоразрядных чисел на автоматах //ДАН СССР. — 1962. т.145. — С. 293-294.
3. Шенхаге А., Штрассен В. Быстрое умножение больших чисел // Кибернет. сб. — 1973. — вып. 10. — С. 87-98.
4. Cook S. A., Aanderaa S. O. On the minimum computation time of functions, Thesis, Harvard University, 1966. — P. 26-50.
5. Березовский А.И., Задирака В.К., Шевчук Л.Б. О тестировании быстродействия алгоритмов и программ вычисления основных операций асимметричной криптографии /Кибернетика и системный анализ № 5, 1999. - с. 61-68.
6. Задирака В.К., Игисинов К. Анализ погрешности округления алгоритма быстрого преобразования Фурье и некоторых его приложений для режима с плавающей запятой [Текст] / Задирака В.К. // Киев, 1972 р. (Препр. Ин-т кибернетики им. В.М. Глушкова АН УССР: 72-23). – 593 с.
7. Задирака В.К. О сравнении некоторых алгоритмов вычисления оценок интеграла Фурье в корреляционной функции [Текст] / Математическое обеспечение ЭЦВМ // Киев: Ин-т кибернетики им. В.М. Глушкова АН УССР, 1971 р. – 249-250 с.
8. Чефранов, Олександр Г та Махмуд, Ахмед Й (2013), протокол обміну ключами, заснований на матриці, заснованому на Діффі-Гелмана, інформаційні науки та системи.
9. Daemen, J., & Rijmen, V. (2010). Блок-шифр Rijndae.
10. Daemen, J., & Rijmen, V. (2002). Дизайн Rijndael: AES - вдосконалений стандарт шифрування.
11. Daemen, Joan, Rijnen, & Vincent. (2002). Дизайн Rijndael, AES - Розширений стандарт шифрування. Берлін: Спрінгер.
12. Fruhwirth, C. (2011). LUKS Специфікація формату на диску.

13. Деніел Пейдж Паралельна криптографічна арифметика з використанням надмірного представлення монтгомерії // Транзакції в комп'ютерах, 2014 р., с. 1474-1482.
14. Шен Лян Посібник для шпигування програміста Java Native Interface (JNI) // 2008 р.
15. JCUDA, <http://www.jcuda.de/>, 2017 р.
16. (Schneier, Products that Blowfish., 2013a), (Schneier, Products that Use Twofish, 2013b), (Fruhworth, 2011), (Chan, 2015).
17. Grama, A., Karypis, G., Kumar, V., & Gupta, A. (2003). Вступ до паралельних обчислень.
18. Hasselbring, W., Jodeleit, P., & Kirsch, M. (1998). Реалізація паралельних алгоритмів на основі оцінювання та трансформації прототипів. Обчислювальні опитування АСМ.
19. Рогоза А.В. Швидкі алгоритми обчислювання криптопримітивів / А.В. Рогоза // Матеріали Міжнародної наукової інтернет-конференції «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення». – м.Тернопіль, 11 червня 2019 р. – с.53-54.
20. Рогоза А.В. Ефективні алгоритми обчислення криптопримітивів в паралельній системі обчислень / А.В. Рогоза, В.К. Задірака // Матеріали III всеукраїнської науково-практичної конференції молодих вчених та студентів «Інформаційні системи та технології управління» (ІСТУ-2019) – м. Київ.: НТУУ «КПІ ім. Ігоря Сікорського», 20-22 листопада 2019 р. – с.97-101.
21. Рогоза А.В. Сравнительный анализ криптографических алгоритмов / А.В. Рогоза, В.К. Задирака // материалы LIII Международной научной конференции «Актуальные научные исследования в современном мире» / Москва, г. 2019, с.104-108.
22. Рогоза А.В. Порівняльний аналіз криптографічних алгоритмів / А.В. Рогоза, В.К. Задірака // матеріали III Міжнародної наукової конференції «Наукові теорії сьогодення та перспективи розвитку наукової думки» (ІСТУ-2019) – м. Київ, р. 2019, с.105-109.

23. Прокопин В.В. Актуальные проблемы стратегического развития экономики, 2015, с. 58-63.

24. Technical information on Bitcoin's processes, keys and purposes. Available at: <https://bitcoin.org/en/hot-it-works> (accessed December 1, 2017).