Міністерство освіти і науки України
Вінницький національний технічний університет
Вінницька філія ВАТ „Укртелеком"
Інститут кібернетики ім. В.М. Глушкова НАНУ
Вінницьке обласне правління науково-технічного товариства радіотехніки, електроніки та зв'язку
Державний науково-дослідний інститут індикаторних приладів

Department of education and science of Ukraine
Vinnitsa national technical university
Vinnitsa branch of OJC „Ukrtelecom"
Institute of cybernetics NASU
Vinnitsa regional governing of scientific-technical society of the radio engineering, electronics and connection
State scientific-research institute of indicators devices

Матеріали II Міжнародної науково-технічної конференції

СУЧАСНІ ПРОБЛЕМИ МІКРОЕЛЕКТРОНІКИ, РАДІОЕЛЕКТРОНІКИ, ТЕЛЕКОМУНІКАЦІЙ ТА ПРИЛАДОБУДУВАННЯ (СПМРТП-2006)

м. Вінниця, Україна
16-19 листопада 2006 року

Proceeding of II International Conference

MODERN PROBLEMS OF MICRO-ELECTRONICS, RADIOELECTRONICS, TELECOMMUNICATIONS AND INSTRUMENT MAKING (MPMRTIM-2006)

Vinnitsa, Ukraine
16-19 November 2006

УНІВЕРСУМ-Вінниця
2006

УДК 621.38+621.39+681.2
С 91

Друкується за рішенням Вченої Ради Вінницького національного технічного університету Міністерства освіти і науки України

Відповідальний редактор В.М. Кичак

Матеріали статей опубліковані в авторській редакції

С 91 **Сучасні проблеми мікроелектроніки, радіоелектроніки, телекомунікацій та приладобудування (СПМРТП-2006).** Матеріали другої Міжнародної науково-технічної конференції. м.Вінниця, 16-19 листопада 2006 року. – Вінниця: УНІВЕРСУМ-Вінниця, 2006. – 154 с.

ISBN 966-641-195-4

Збірка містить матеріали доповідей II Міжнародної конференції з сучасних проблем мікроелектроніки, радіоелектроніки, телекомунікацій та приладобудування за сімома основними напрямками: математичне моделювання в радіоелектроніці та телекомунікаціях; захист інформації в телекомунікаційних системах та мережах; новітні технології в електроніці; радіовимірювальні пристрої та системи; цифрові пристрої та системи; радіоелектронні пристрої на базі негатронів; обробка сигналів та зображень в радіоелектронних та телекомунікаційних системах.

УДК 621.38+621.39+681.2

ISBN 966-641-195-4

УДК 681.3.06

В. Сокирук (м. Вінниця, Україна)

ШВИДКА ПРОГРАМНА РЕАЛІЗАЦІЯ БСШ НА ОСНОВІ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ЗА МОДУЛЕМ 2^n

В роботі [1] запропоновано блоковий симетричний шифр (БСШ), в основу якого покладені арифметичні операції за модулем 2^n (де n – розмір блоку), операція додавання за модулем 2 та операція перестановки k-розрядних блоків n-розрядного цілого числа. Пропонувалось для вирішення різних криптографічних задач використовувати перестановки при значеннях k = 32, k = 16, k = 8 та k = 1. Статистичний аналіз БСШ на основі арифметичних операцій за модулем 2^n, проведений в роботі [2], показав, що статистичні закономірності повністю відсутні у випадку використання дзеркальної перестановки розрядів n-розрядного цілого числа.

В даній роботі розглядаються деякі результати тестування продуктивності швидкої програмної реалізації даного БСШ з перестановкою розрядів при k = 1 та значенням n = 128. Цільовою платформою для експериментів було обрано найбільш розповсюджену у світі платформу x86, для якої доступний широкий вибір 32-розрядних процесорів, та операційну систему Windows XP.

БСШ реалізований мовою Ansi C з використанням команд асемблера для реалізації перестановки розрядів і не використовує мультимедійних розширень MMX, SSE та ін. Для компіляції використовувався компілятор Intel Compiler 8.0 з включеними опціями оптимізації.

Оцінка продуктивності програмної реалізації БСШ проводилась за методикою, що була запропонована NIST під час проведення конкурсу AES і докладно описана в роботі [3]. Згідно цієї методики продуктивність БСШ вимірюється в кількості тактів процесора, необхідних для виконання таких операцій: зашифрування блоку даних, розшифрування блоку шифротексту, розгортання ключа для зашифрування та розшифрування.

Тестування проводилось для таких процесорів: Intel Pentium III (1), Intel Pentium M (2), Intel Pentium 4 (3), AMD Duron (4) та AMD Athlon 64 (5). Результати тестування наведені в табл. 1.

Таблиця 1

Продуктивність програмної реалізації БСШ на основі арифметичних операцій за модулем 2^n

Платформа / Операція	1	2	3	4	5
Зашифрування	178	154	208	178	140
Розшифрування	178	153	209	178	141
Розгортання ключа для зашифрування	537	465	623	531	420
Розгортання ключа для розшифрування	986	826	1201	889	699

Отримані результати свідчать про те, що продуктивність програмної реалізації БСШ на основі арифметичних операцій за модулем 2^n є високою для найбільш розповсюджених 32-х розрядних процесорів і перевищує продуктивність відомих БСШ [3].

Програмна реалізація БСШ, що розглядається в даній роботі, містить тільки звичайні арифметичні та логічні операції, тому продуктивність залежить тільки від особливостей внутрішньої побудови процесора. Цим пояснюється різниця в значеннях, отриманих для різних процесорів. Так, найбільш ефективними з точки зору мінімальної кількості тактів, що потребуються для виконання тієї чи іншої операції, є сучасні процесори Intel Pentium M та AMD Athlon 64. Внутрішня архітектура цих процесорів містить ряд переваг, що дозволяє їм найбільш ефективно виконувати машинний код, що містить переважно арифметичні операції множення та додавання 32-розрядних цілих чисел.

Література

1. Сокирук В.В., Лужецький В.А. Блоковий симетричний шифр на основі модульної арифметики // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 10. – 2005. – С. 122-126

2. Сокирук В.В., Лужецький В.А. Побудова статистично безпечного БСШ на основі арифметичних операцій за модулем // Інформаційні технології та комп'ютерна інженерія. – 2006. - № 1. – С. 158-163.

3. Kazumaro Aoki, Helger Lipmaa. Fast Implementations of AES Candidates // Proceedings of 3rd AES conference, New York, 2000. -- P. 106-120.