ПРИСКОРЕНА РЕАЛІЗАЦІЯ ШИФРУВАННЯ ДАНИХ

Рисований О.М., Малихін А.В., Соболенко С.С.
Національний технічний університет "Харківський політехнічний інститут", м. Харків

В роботі було проаналізовано процес шифрування [1-3] даних за рахунок використання інструкцій процесора наборів MMX, SSE та AVX. Застосовано форму паралелізму - Data Parallelism, яка дозволила ефективно використовувати ресурси система (CPU, GPU) та знизити час обробки великих обсягів даних.

Основою обработки масиву даних інструкціями AVX є цикл:

```
vmovups ymm0,[rsi]    ; buff
vmovups ymm1,[r15]  ; key
vxorpd ymm2,ymm0,ymm1;
vmovups [rdi],ymm2
```

Видобуток у швидкості обробки досягнутий за рахунок використання 256 розрядних регістрів ymm. В роботі виміряно час виконання шифрування великого масиву даних для всіх технологій паралельної обробки великого масиву даних за допомогою блока коду:

```
rdtsc ; edx,eax
shl rdx,32;
add rdx, rax;
mov r14, rdx;
```

Використані рішення сприяли збільшенню ефективності шифрування великих об'ємів даних. Та ще раз було доказано, що світові тенденції шифрування даних свідчать про постійний розвиток та еволюцію методів і підходів до досягнення цієї мети. Розробники активно працюють над знаходженням нових рішень та використовують передові технології для захисту інформації.

Література:

1. Кудряшов В.Є., Коломійцев О.В., Рисований О.М., Мегельбей В.В., Жирна О.В. Методика числового моделювання визначення показника ефективності стрільби ракетою по різних цілях при відпрацюванні цілевказівки з батарейного командного пункту. Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. 1(19) (2024). Харків. 2024. С. 107-116. https://doi.org/10.37701/dndivsovt.19.2024.13.

2. Рисований О.М., Ігнатьєв К.І., Рибалка Р.В., Рудаковський Д.Р. Механізм шифрування повідомлень з максимальною довжиною // Інформатика, управління та штучний інтелект. Тези одинадцятої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – С.127. https://web.kpi.kharkov.ua/ai/wp-content/uploads/sites/249/2024/10/TEZY_IUSHI_2024.pdf.

3. Рисований О.М. Криптостійний генератор псевдовипадкової наслідності з використанням майстер-ключа // Проблеми інформатики та моделювання (ПІМ-2024). Тези двадцять четвертої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – С. 120. (150 с.) https://web.kpi.kharkov.ua/pim/wp-content/uploads/sites/248/2024/10/Programma_PYM_2024_09_20.pdf.