عنوان مقاله:

پیاده سازی و آنالیز شاخص رمزنگاری AES در GPU

محل انتشار:

ششمین همایش ملی فناوریهای نوین در مهندسی برق، کامپیوتر و مکانیک ایران (سال: 1402)

تعداد صفحات اصل مقاله: 10

نویسنده:

فرخ لقا ملائی – فارغ التحصیل مهندسی کامپیوتر گرایش نرم افزار، دانشگاه غیرانتفاعی هاتف ، زاهدان ، ایران

خلاصه مقاله:

GPU در حال ادامه دادن به روند عملکرد بهتر خود نسبت به CPU می. می باشد. در این مقاله به منظور بهبود کارایی الگوریتم AES، یک پیاده سازی از CUDA از پردازش کد کتاب رمز الکترونیکی (ECB) و فرایند رمزگشایی حالت بازخورد رمز (CBC) بر روی GPU پیشنهاد شده است. در پیاده سازی ما، - T boxهای مکررا قابل دسترسی به حافظه به اشتراک گذاشته شده بر روی تراشه اختصاص داده شد و سطح جزئیات که یک ریسمان بلوک ۱۶ AES بایتی را بکار میگیرد تصویب شد. در نهایت ما به بالاترین عملکرد در حدود ۶۰ Gbps توان عملیاتی بر GPU NVIDIA Tesla C۲۰۵۰ دست یافتیم که تا ۵۰ بار سریعتر از پیاده سازی متوالی بر اساس پردازنده ۲.۶۶GHz Intel Core i۷-۹۲۰ بود. علاوه بر این، ما بهینه سازی تحت برخی سناریوهای برنامه عملی مانند پردازش GPU همپوشانی و انتقال داده را مورد بحث قرار دادیم.

کلمات کلیدی:

AES، GPU، CUDA، کتاب رمز الکترونیکی ، بازخورد رمز، محاسبات موازی

لینک ثابت مقاله در پایگاه سیویلیکا: