عنوان مقاله:
روش های پیاده سازی معکوس الگوریتم MD5 با استفاده از GPU

محل انتشار:
کنفرانس بین المللی پژوهش های کاربردی در فناوری اطلاعات، کامپیوتر ومخابرات (سال: 1394)

تعداد صفحات اصل مقاله: 7

نویسندگان:
نجمه درینی - *گروه کامپیوتر، واحد علوم و تحقیقات سیرجان، دانشگاه آزاد اسلامی سیرجان، ایران*

رضا نورمندی پور - *گروه کامپیوتر، واحد علوم و تحقیقات سیرجان، دانشگاه آزاد اسلامی سیرجان، ایران*

خلاصه مقاله:
MD5؛ یک روش رمزنگاری است که به عنوان تابع درهم ساز، رمزنگارانه استفاده می شود. این الگوریتم یک رشته با طول متفاوت را به عنوان ورودی می گیرد و یک خلاصه پیام ام دی 5 یا اثرانگشت با طول 128 بیت می سازد. هش های MD5 به لحاظ تئوری مستقیماً قابل برگشت نیستند اما راه هایی برای رمزگشایی پسوردهای MD5 وجود دارد. الگوریتم های رمزنگاری مش یکی از مهمترین توابع در امنیت اطلاعات می باشد. از مهمترین خصوصیات این توابع یک طرفه بودن آنهاست یعنی با روش معکوس نمی توان به متن اصلی رمز شده دست پیدا کرد. برای رمزگشایی از هش ها دو رو روش وجود دارد. اولین روش که به نام بروت فورس شناخته می شود، در این روش مقادیر هش تولید می شوند و یک به یک با مقدار مورد نظر ما مقایسه می شوند. این روش زمان بر می باشد و با افزایش طول پیام زمان محاسبه هم افزایش می یابد. روش بعدی به نام روش معاوضه زمان- حافظه شناخته می شود. در این روش مقادیر هش از پیش محاسبه شده و برای جستجوی بعدی ذخیره می شود. این روش به مقدار زیادی حافظه نیاز دارد. واحد پردازش گرافیکی (GPU) در ابتدا جهت انجام کارهای گرافیکی کامپیوتر و کم کردن کارهای CPU طراحی گردید ولی چندی بعد، به دلیل داشتن هسته های بسیار زیاد که هر یک قادر به انجام کارهای کوچک ولی به صورت همزمان می بودند، جهت انجام کارهای محاسباتی پیشرفته نیز استفاده شد، به همین دلیل، GPU، می توانند برنامه هایی که قادر به تفکیک به قسمت های کوچک می باشند را به صورت موازی، با سرعت بیشتری نسبت به CPU اجرا کنند. برای برنامه نویسی بر روی GPU، از دو زبان برنامه نویسی CUDA و OpenCL استفاده می کنند. CUDA یک معماری محاسبات موازی است که توسط شرکت Nvidia ارائه شده است و فقط بر روی کارت گرافیک های همین شرکت اجرا می شود که در سطح نرم افزاری، شامل یک سری دستورالعمل و در سطح سخت افزار شامل موتور پردازش موازی در GPU است. CUDA هم واسط های برنامه نویسی سطح پایین و هم واسط های برنامه نویسی سطح بالا را فراهم می کند. به همین دلیل سرعت برنامه هایی که با CUDA نوشته می شود از زبان برنامه نویسی دیگر یعنی OpenCL بیشتر می باشد. در این مقاله ما سعی داریم پیاده سازی های مختلفی از معکوس MD5، را بر روی GPU بررسی کنیم.

کلمات کلیدی:
منکوس، تا ع در هم ساز، CUDA, MD5,, GPU