عنوان مقاله:
بررسی روش های پیاده سازی معکوس الگوریتم MD5

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(message digest یک روش رمزنگاری است که به عنوان تابع درهمساز رمزنگارانه استفاده می شود. این الگوریتم یک رشته با طول متفاوت را به عنوان ورودی میگیرد و یک خلاصه پیام امدی ۵ یا اثر انگشت با طول128 بیت می سازد. هش های MD5 به لحاظ تئوری مستقیما قابل برگشت نیستند اما راه هایی برای رمزگشایی پسوردهای MD5وجود دارد.رمزگشایی هش ها به دو روش صورت می گیرد : 1) روش brute-force؛ 2) روش . Cryptanalytic. در اینمقاله ما سعی داریم پیاده سازی های مختلفی از معکوس MD5 ، را بررسی کنیم .

کلمات کلیدی:
معکوس، تابع در هم ساز، Rainbow, CUDA, MD5, GPU

لینک ثابت مقاله در پایگاه سیویلیکا: