

عنوان مقاله:

کاربرد توابع کپی ناپذیر فیزیکی در افزایش امنیت سخت افزارهای رمزنگار

محل انتشار:

سومین کنفرانس مهندسی برق و الکترونیک ایران (سال: 1390)

تعداد صفحات اصل مقاله: 8

نویسندگان:

طه یاسین رضاپور - دانشجوی کارشناسی ارشد فناوری اطلاعات

رضا ابراهیمی آتانی - استادیار گروه مهندسی کامپیوتر دانشگاه گیلان

خلاصه مقاله:

اعتماد در فعل و انفعالات از راه دور چالشی اساسی در محیطهای محاسبات توزیع شده می باشد برای کسب اعتماد بخش واقع شده در فاصله دور یا همان remote سیستم محاسباتی باید قادر به تضمین حفظ حریم خصوصی در مالکیت معنوی و یکپارچگی اجرای برنامه باشد متأسفانه بسترهای نرم افزاری سنتی نمی توانند چنین تضمینی را در مقابل تهدیدات فیزیکی موجود فراهم نمایند یک سیستم محاسباتی ایمن باید بتواند اختیار تصدیق بستر نرم افزاری خود را به بخش remote داده و تضمین اجرای درست برنامه را حتی با وجود تهدیدهای فیزیکی به آن بدهد استفاده از توابع کپی ناپذیر فیزیکی یا PUF رویکردی مناسب برای مقابله با تهدیدات فیزیکی و بالا بردن امنیت سخت افزارها به شمار می رود. در این مقاله استفاده از توابع PUF ها برای ایجاد امنیت و جلوگیری از حملات مورد بررسی قرار می گیرد.

کلمات کلیدی:

توابع کپی ناپذیر فیزیکی PUF، امنیت سخت افزار، کارت های هوشمندانه smartcards، بسته های Tamper-Proof، پرداخت الکترونیکی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/125489>

