عنوان مقاله:
یک طرح تعمیم یافته برای استخراج کلید بیومتریک از الگوی تایپ

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 5, شماره 1 (سال: 1396)

تعداد صفحات اصل مقاله: 11

نویسندگان:
امیر بیدختی - *دانشگاه شریف*

سیدمرتضی پورنقی - *دانشگاه قم*

امیرحسین خلیلی تیرانداز - *علم و صنعت*

خلاصه مقاله:
در این مقاله، یک طرح تعمیم یافته برای استخراج کلید بیومتریک از روی نمونه های الگوی تایپ کاربر (بیومتریک رفتاری) مطرح شده و امنیت آن نشان داده می شود. در طرح پیشنهادی، ابتدا ویژگی های مناسبی از الگوی تایپ کاربر استخراج می شود. سپس به کمک یک طرح تسهیم راز مناسب، بسته به میزان یکتا بودن هر ویژگی تعدادی سهم مجاز برای بازسازی کلید مخفی به آن تخصیص داده می شود. این سهم ها در میان اعداد تصادفی پنهان می شوند. در جلسه ی آزمون، مجددا ویژگی های الگوی تایپ استخراج شده و در صورت صحت هر ویژگی، یک سهم درست به دست خواهد آمد. اگر این تعداد از حدی که در طرح تسهیم راز مقاوم مشخص شده است، بیشتر باشد بازسازی کلید مخفی امکان خواهد داشت. طرح دارای دو پارامتر است که بر خلاف طرح های پیشین به آن قابلیت تنظیم رابطه ی FAR و FRR را می دهد. طرح پیشنهادی قادر است ۲۵ الی ۵۰ بیت کلید را بسته به نوع صفحه کلید (صفحه کلیدهای سنتی یا صفحه کلیدهای لمسی) با نرخ EER = ۰.۰۴ استخراج نماید. نشان می دهیم که استفاده از این طرح به عنوان عامل تکمیلی در کنار کلمه ی عبور امنیت را ۲ تا ۳ برابر افزایش می دهد. این طرح در کنترل دسترسی، حفاظت از دستگاه های حساس و ... قابل استفاده است.

کلمات کلیدی:
رمزنگاری بیومتریک, الگوی تایپ, مدیریت کلید, آنتروپی, تسهیم راز