عنوان مقاله:
طرحی جدید برای تعیین هویت بر مبنای منحن یهای بیضوی و دوتایی ویل

محل انتشار:
چهارمین کنفرانس انجمن رمز ایران (سال: 1386)

تعداد صفحات اصل مقاله: 7

نویسندگان:
مسعود هادیان دهکردی - *دانشکده ریاضی دانشگاه علم و صنعت ایران*

رضا علیمرادی - *مرکز تحقیقات ریاضیات کاربردی دانشگاه علم و صنعت ایران*

خلاصه مقاله:
هدف اصلی در پروتکل های تعیین هویت شناسایی دقیق افراد مجاز برای ورود به یک سیستم م یباشد. مهمترین ویژگیهای یک پروتکل عبارتند از سطح امن یت و میزان اجرایی بودن آن. ما در این مقاله ابتدا منحنی بیضوی و دوتایی ویل را معرفی و سپس به بیان برخ ی روابط ر یاضی موجود م یپردازیم و بعد از آن با معرف ی برخی پروتکل ها در زم ینه تع یین هو ی ت روشه ایی جدی د برای تعیین هویت بر مبنای منحن یهای بیضوی و دوتایی ویل ارائه و سطح امنیت و میزان اجرایی بودن آنها را نشان م یدهیم.

کلمات کلیدی:
تعیین هویت، منحنی بیضوی، دوتایی ویل، پروتکل چالش و واکنش، اثبات با اطلاع صفر