عنوان مقاله:
انتخابات الکترونیکی k از L بر اساس سیستم رمزنگاری همریخت

محل انتشار:
دوازدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1394)

تعداد صفحات اصل مقاله: 6

نویسندگان:
سجاد رضایی ادریانی - *پژوهشگر دانشگاه صنعتی مالک اشتر*

سیدمهدی سجادیه - *استاد یار دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)*

علی زاغیان - *استاد یار دانشگاه صنعتی مالک اشتر اصفهان*

خلاصه مقاله:
در این مقاله یک طرح انتخابات الکترونیکی از نوع انتخابات از پیشنهاد شده است که از چندین مسیول استفاده می کند که می توان آن را در انواع انتخابات یک نفر از L نفر (مثل انتخابات ریاست جمهوری) و یا بیشتر از یک نفر از L نفر (مثل انتخابات مجلس) و حتی در نظر سنجی نیز به کار برد. همچنین به دلیل طراحی اثبات های صفر دانش رای دهنده دقیقا به نامزد رای داده و امکان تولید رای معیوب که صحت انتخابات را دچار خدشه کند نیست علاوه بر این با به کارگیری چندین مسیول و نیز طرح آستانه ای الجمال امکان تبانی مسیولین باهم یا تبانی آنها با خراب کاران از بین رفته و عدالت در نتیجه ی انتخابات به دست می آید لذا با توجه به این خاصیت ها، پروتکل پیشنهادی دارای خواصی از جمله محرمانگی، بدون رسید بودن، وارسی عمومی و فردی (اثبات های صفر دانش انجام شده باعث احراز این خاصیت می شوند)، سلامت در انتخابات، کامل بودن و عدالت در نتیجه ی انتخابات است.

کلمات کلیدی:
رای گیری الکترونیکی، رمزنگاری همریخت، سیستم الجمال، انتخابات k از L