عنوان مقاله:
یک طرح تسهیم راز مقاوم در برابر تقلب مبتنی بر گراف

محل انتشار:
شانزدهمین کنفرانس بین المللی انجمن رمز ایران (سال: 1398)

تعداد صفحات اصل مقاله: 8

نویسندگان:
میثم نوروزی - *دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران*

ترانه اقلیدسی - *پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران*

محمدرضا عارف - *دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران*

خلاصه مقاله:
طرح تسهیم راز آستانه ای امکان تسهیم یک راز را در میان تعدادی از اعضا، بهنام شرکتکنندگان، با ارائه سهم هایی به آنان فراهم میسازد. بازیابی راز تنها به کمک تعداد مشخص از سهم ها امکان پذیر است. بازیابی درست راز در این طرحها منوط به رفتار درست شرکت کنندکان است. اما در دنیای واقعی ممکن است برخی از شرکت کنندگان تلاش کنند سهم های نادرستی ارائه دهند، که تقلب نام دارد. یک طرح تسهیم راز مقاوم این امکان را فراهم میکند که با حضور تعدادی متقلب همچنان راز به درستی بازیابی شود. در این مقاله طرح تسهیم راز مقاومی ارائه میشود که با وجود تعداد بیشینه ممکن از شرکتکنندگان متقلب، راز به درستی بازیابی شود. در این طرح برای متقلب ها تواناییهای زیادی در نظر میگیریم. آنان میتوانند سهم های خود را متناسب با سهم های سایرین تغییر دهند و با یکدیگر ارتباط داشته باشند تا بهترین شیوه را برای تقلب به کارگیرند. این طرح امکان شناسایی و حذف متقلبها را به کمک یک گراف جهتدار فراهم میسازد و نسبت به طرحهای پیشین از پیچیدگی کمتری برای بازیابی راز برخوردار است. در عین حال دارای طول سهم کمتری نسبت به طرحهای موجود است، که به کاهش سربار مخابراتی طرح میانجامد. به این ترتیب، طرح تسهیم راز پیشنهادی از دو جنبه پیچیدگی بازیابی راز و طول سهم از کارآیی بیشتری نسب به طرحهای موجود برخوردار است.

کلمات کلیدی:
تسهیم راز، تسهیم راز مقاوم، شناسایی متقلب، متقلب عجول، گراف جهتدار، کد احراز اصالت پیام