عنوان مقاله:
حملهای به طرح اشتراک سر مبتنی بر اتوماتای سلولی

محل انتشار:
دوازدهمین کنفرانس سالانه انجمن کامپیوتر ایران (سال: 1385)

تعداد صفحات اصل مقاله: 6

نویسندگان:
آزاده نعمت زاده - *دانشگاه صنعتی امیرکبیر*

وحید کاظم پور - *دانشگاه صنعتی امیرکبیر*

برنا جعفرپور - *دانشگاه صنعتی امیرکبیر*

بابک صادقیان - *عضو هیات علمی دانشگاه صنعتی امیرکبیر*

خلاصه مقاله:
در طرحهای اشتراک سر یک مقدار محرمانه بین افراد شرکتکننده به گونهای توزیع میشود که هر فرد به تنهایی قادر به کشف رمز نیست ولی هر زیرگروه مجاز قادر به اشتراکگذاری سهم خود و محاسبه مقدار محرمانه است. یکی از جدیدترین مدلهای ارائه شده برای اشترا ک سر، طرحی مبتن ی بر اتوماتای سلولی با حافظه اس ت. در این مقاله، حمله ای برای تقلب د ر طرح اشتراک سر مبتنی بر اتوماتای سلولی با حافظه ارائه شده ا ست. در این حمل ه، افراد متقلب با به اشتراک گذاری مقدار نادرست سهم خود، قادر به محاسبه مقدار تقلب هستن د. افراد درس تکار از وقوع تقلب بیاطلاعاند و مقدار نادرست سر را به جای مقدار درست آن در نظر میگیرند. در این مقاله، چگونگی محاسبه مقدار تقلب در صورت حضور افراد متقلب ارائه و اثبات شده است. افراد متقلب با استفاده از این مقدار قادر به بازسازی مقدار درست سر هستند.

کلمات کلیدی:
اشتراک سر، تقلب، اتوماتای سلولی، طرح آستانهای