

عنوان مقاله:

حمله ای جدید به شبکه مخلوط مرکب جیکوبسون

محل انتشار:

فصلنامه پدافند الکترونیکی و سایبری، دوره 7، شماره 3 (سال: 1398)

تعداد صفحات اصل مقاله: 7

نویسندگان:

محمود سلماسی زاده - دانشگاه شریف

سیدامیر مرتضوی - استاد یار، دانشگاه تبریز

جواد مهاجری - استاد یار، پژوهشکده الکترونیک، دانشگاه صنعتی شریف

خلاصه مقاله:

شبکه مخلوط مرکب جیکوبسون شبکه ای مخلوط است که با استفاده توام از رمزنگاری متقارن و غیر متقارن، گمنام سازی پیام های طولانی را به صورتی بسیار کارا ممکن می سازد. در این مقاله، حمله ای جدید به شبکه مخلوط مرکب جیکوبسون ارائه می شود که ویژگی صحت این شبکه مخلوط را نقض می کند. نشان خواهیم داد که با استفاده از این حمله در صورت تبانی یکی از فرستنده ها با اولین سرور مخلوط کننده، این سرور قادر خواهد بود که پیام تمامی فرستنده ها را با پیام های دلخواه خود جایگزین کند.

کلمات کلیدی:

رمز شبکه مخلوط، شبکه مخلوط مرکب، گمنامی، صفر دانشی، تسهیم راز

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/970930>

