January 2017, Volume 4, Number 1 (pp. 39--39)
http://www.jcomsec.org
Journal of Computing and Security

# تسهیم راز چندگانه اجتماعی تصدیق‌پذیر امن در مدل متخاصمانه فعال

نصراله پاک‌نیت [آ،*]، زیبا اسلامی [ب]

[آ] پژوهشکده علوم اطلاعات، پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، تهران، ایران.
[ب] گروه علوم داده‌ها و کامپیوتر، دانشگاه شهید بهشتی تهران، تهران، ایران.

**اطلاعات مقاله**

*تاریخچه مقاله:*
دریافت: 02 Octoboer 2017
اصلاح: 02 January 2018
پذیرش: 23 April 2018
انتشار آنلاین: 25 July 2018

*کلمات کلیدی:*
تسهیم راز، تسهیم راز اجتماعی، رمزگذاری متقارن، امنیت محاسباتی، مدل اعتماد.

**چکیده**

تسهیم راز اجتماعی، که برای اولین بار در سال ۲۰۱۰ توسط نجومیان و همکاران معرفی شده است، تسهیم یک راز مابین مجموعه‌ای از کاربران با صلاحیت‌های متغیر در طول زمان را ممکن می‌سازد. بررسی پیشینه مساله نشان می‌دهد که طرح‌های تسهیم راز اجتماعی موجود قادر به تسهیم تنها یک راز در هر بار اجرای خود هستند. برای حل این نقطه ضعف، در این مقاله از طرح‌های رمزگذاری متقارن استفاده کرده، یک طرح تسهیم راز چندگانه اجتماعی ارائه می‌کنیم و نشان می‌دهیم که طرح ارائه شده در مدل متخاصمانه فعال دارای امنیت محاسباتی است. علاوه‌براین، در راستای نشان دادن کارایی طرح ارائه شده، طرح ارائه شده را با تنها طرح تسهیم (یک) راز اجتماعی موجود و امن در مدل متخاصمانه فعال مقایسه می‌کنیم.



* نویسنده مسئول.
آدرس‌های رایانامه: pakniat@irandoc.ac.ir (ن. پاک‌نیت)،
z_eslami@sbu.ac.ir (ز. اسلامی)
ISSN: 2322-4460 