Journal of Computing and Security

2024, Volume 11, Number 2
http://www.jcomsec.org

رمزگذاری کارآمد مبتنی بر ویژگی و سیاست کلید بدون استفاده از زوج‌نگاری مبتنی بر RSA برای کاربردهای سبک

صدیقه خواجوئی نژاد[آ]، سام جبه‌داری[آ,*]، حمید حاج سیدجوادی[ب,*]، سیدمحمدحسین معطر[ج]

[آ] دانشگاه آزاد تهران شمال.
[ب] دانشگاه شاهد.
[ج] دانشگاه آزاد مشهد.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 19 October 2024
اصلاح: 04 March 2025
پذیرش: 11 May 2025
انتشار آنلاین: 06 June 2025

کلمات کلیدی:
کارایی، رمزنگاری RSA، رمزنگاری مبتنی بر ویژگی، سیاست کلید، ابطال کلید، ساختار دسترسی، امضای مبتنی بر ویژگی، سبک‌وزن.

چکیده

اعمال کنترل دسترسی بر روی داده‌های رمزگذاری شده، جنبه‌ای حیاتی از امنیت شبکه است. اگرچه رمزگذاری مبتنی بر ویژگی (ABE) یک راه‌حل مناسب ارائه می‌دهد، اما با محدودیت‌هایی نیز همراه است، که در درجه اول پیچیدگی محاسباتی بالای آن به دلیل استفاده از عملیات زوج‌نگاری است. در این مقاله، ما اولین طرح رمزگذاری مبتنی بر ویژگی مبتنی بر رمزگذاری RSA را پیشنهاد می‌کنیم که بدون زوج‌نگاری بوده و کارآمدتر از رویکردهای مبتنی بر زوج‌نگاری قبلی است. این طرح به ویژه برای کاربردهای سبک مانند برنامه‌های کاربردی در اینترنت اشیا (IoT) مناسب است. طرح رمزگذاری پیشنهادی، رمزگذاری مبتنی بر ویژگی با سیاست کلید (KP-ABE) است که به سیاست دسترسی آن اجازه می‌دهد هر تابع بولی در فرم نرمال فصلی (DNF) باشد. طرح ما همچنین به چالش ابطال کلید می‌پردازد که اغلب در طرح‌های ABE مشکل‌ساز است. مزایای کلیدی طرح ما، کارایی و سادگی آن در مقایسه با سایر طرح‌های ABE است که معمولاً به عملیات زوج‌نگاری پیچیده متکی هستند. علاوه بر این، ما یک طرح امضای مبتنی بر ویژگی (ABS) مبتنی بر RSA ارائه می‌دهیم.

* نویسنده مسئول.
آدرس‌های رایانامه: se_khajouei_nejad@yahoo.com،
sam.jabbehdari@iau.ac.ir، h.s.javadi@shahed.ac.ir،
moattar@mshdiau.ac.ir

ISSN: 2322-4460