



تحلیل بومیانگ mCrypton دور- کاهش یافته

پارسا یوسف پور^آ، عطیه میرزائی^ب، سیاوش احمدی^{ج*}، محمد رضا عارف^ب

^آ دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران.
^ب آزمایشگاه سیستم‌های اطلاعاتی و امنیت (ISSL)، دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران.
^ج پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران.

چکیده

اطلاعات مقاله

با توجه به تقاضای روزافزون رمزنگاری امن و در عین حال سبک در محیط‌های دارای محدودیت منابع، نظیر برچسب‌های RFID و شبکه‌های حسگری بی‌سیم، استفاده از رمزهای قالبی سبک برای حفاظت از داده‌های حساس در این تجهیزات، با رعایت محدودیت‌های سخت‌گیرانه توان، مساحت و تاخیر، اهمیت فراوانی یافته است. در پاسخ به چالش طراحی چنین رمزهایی، رمزهای قالبی سبک زیادی از جمله mCrypton پیشنهاد شده‌اند. با این حال، ارزیابی دقیق امنیت این رمزها ضروری است، زیرا وجود آسیب‌پذیری در آن‌ها می‌تواند معماری امنیتی کل سیستم را تهدید کند. در این مقاله، نخستین کاربرد حمله بومیانگ، که روشی ترکیبی مبتنی بر چارچوب‌های بومرنگ و یویو است، بر روی نسخه دور- کاهش یافته رمز قالبی mCrypton ارائه می‌شود. برای این منظور، یک تمایزگر جدید ۵ دوری طراحی شده و سپس حمله بازیابی کلیدی ارائه می‌شود که بهتر از حملات پیشین ۵ دوری به این رمز است. با بازتعریف تعاریف ساختاری و تطابق چارچوب بومیانگ با ساختار شبکه جایگشت-جانشینی (SPN) در mCrypton، حمله پیشنهادی ما به پیچیدگی داده 2^{26} ، پیچیدگی زمانی $XOR + 2^{25} En. 2^{23.02}$ و پیچیدگی حافظه 2^{12} قالب دست می‌یابد.

© 2026. تمامی حقوق محفوظ است.

تاریخچه مقاله:

دریافت: 06 December 2025

اصلاح: 28 June 2026

پذیرش: 13 July 2026

انتشار آنلاین: 22 September 2026

کلمات کلیدی:

بومرنگ، یویو، mCrypton، تمایزگر، بازیابی کلید.

* نویسنده مسئول.

آدرس‌های رایانامه: par.yousef123@sharif.ir (پ. یوسف پور)،

atiyeh.mirzaie@ee.sharif.edu (ع. میرزائی)،

s.ahmadi@sharif.edu (س. احمدی)، aref@sharif.edu (م. عارف)

تمامی حقوق محفوظ است. ISSN: 2322-4460 © 2026

