January 2019, Volume 6, Number 1
http://www.jcomsec.org

Journal of Computing and Security

توسیعی بر چارچوب CryptoPAi برای تحلیل صوری پروتکل های رأی گیری الکترونیکی

حمیدرضا محروقی [آ،*]، رسول جلیلی [ب]

[آ] استادیار گروه مهندسی کامپیوتر دانشگاه امام رضا(ع)، مشهد، ایران.
[ب] دانشیار دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف،تهران، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 16 October 2018
اصلاح: 4 August 2019
پذیرش: 9 October 2019
انتشار آنلاین: 2 December 2019

کلمات کلیدی:
درستی‌یابی صوری، جبر پردازه‌ای، منطق شناختی، پروتکل رأی‌گیری الکترونیکی.

چکیده

CryptoPAi یک چارچوب عملیاتی ـ شناختی ترکیبی برای بیان و تحلیل پروتکل های امنیتی با پشتیبانی واقعی از ساختارهای رمزنگاری است. این چارچوب شامل یک فرمالیسم جبر پردازهای برای بیان عملیاتی و یک توسیع شناختی از حسابان μ با عملگر گذشته برای ساختارهای رمزنگاری است. در این مقاله، چارچوب CryptoPAi را با ساختارهای رمزنگاری بیشتری گسترش می‌دهیم. انگیزه اصلی و کاربردی این توسیع از حوزه پروتکل‌های رأی‌گیری الکترونیکی ناشی شده است و پس از آن، کاربرد چارچوب توسعه یافته را در این حوزه بررسی میکنیم. این چارچوب پشتیبانی صریحی از ساختارهای رمزنگاری را فراهم میکند، که از اساسی‌ترین مؤلفه‌ها و اجزای پروتکل‌های امنیتی و رأی‌گیری الکترونیکی است. چارچوب توسعه یافته خود را روی پروتکل رأی‌گیری الکترونیکی FOO اعمال می‌کنیم. همچنین نمونه وارسی کننده‌ـمدل این چارچوب را در ابزار منطق بازنویسیMaude ارتقا می دهیم و از آن برای ساخت مدل‌ها و وارسی برخی ویژگی‌ها در آن مدل‌ها استفاده می‌کنیم.

* نویسنده مسئول.
آدرس‌های رایانامه: mahrooghi@ce.sharif.edu (ح. محروقی)،
jalili@sharif.ir (ر. جلیلی)
ISSN: 2322-4460