## عنوان مقاله:

مدلسازی و تحلیل کمی پروتکلهای امنیتی مبتنی بر بررسی مدل احتمالی و ابزار PRISM

## محل انتشار:

ششمین کنفرانس بین المللی انجمن رمز ایران (سال: 1388)

تعداد صفحات اصل مقاله: 7

## نویسندگان:

مجتبی اکبرزاده - *آزمایشگاه مهندسی کارایی و اتکاپذیری دانشکده مهندسی کامپیوتر دانشگاه*

محمد عبداللهی ازگمی - *آزمایشگاه مهندسی کارایی و اتکاپذیری*

## خلاصه مقاله:

روشهای صوری و فنون درستی یابی ، از ابزارهای تحلیل سیستم ها هستند هدف این مقاله ارائه روشی برای درستی یابی و تحلیل پروتکلهای امنیتی است ویژگی اصلی روش ارائه شده دراین مقاله بهره گیری از فنون بررسی مدل احتمال برای تحلیل پروتکلهای امنیتی است با استفاده از فنون بررسی مدل احتمالی، پروتکلهای امنیتی را می توان به صورت کمی مورد بررسی قرار داد مزیت بسیار مهم درستی یابی کمی پروتکل قابلیت بررسی دقیق یک پروتکل در برابر مهاجمین مختلف و همچنین امکان مقایسه چندین پروتکل با یکدیگر در مقابل مهاجمین مختلف است.

## کلمات کلیدی:

پروتکلهای امنیتی، درستی یابی، بررسی مدل احتمالی، روشهای صوری