عنوان مقاله:
تحلیل امنیتی طرح امضای وکالتی آستانه در برابرحمله تبانی

محل انتشار:
اولین کنفرانس دانشجویی فناوری اطلاعات ایران (سال: 1389)

تعداد صفحات اصل مقاله: 6

نویسندگان:
محمد بهشتی آتشگاه - *کارشناسی ارشد دانشگاه جامع امام حسین (ع)، دانشکده برق*

محمود گردشی - *عضو هیئت علمی دانشگاه جامع امام حسین (ع) دانشکده برق مرکز تحقیقا ت فتح*

خلاصه مقاله:
طرحهای امضای وکالتی آستانه که در سالهای اخیر موردتوجه زیادی قرار گرفته اند حاصل ترکیب طرحهای امضای وکالتی و رمزنگاری حوزه آستانه می باشد از زمان بیان اولین طرح امضای وکالتی آستانه حملات زیادی به آنها اعمال شده است یکی از این حملات حمله تبانی است که در میان حملات مطرح شده جایگاه ویژه ای دارد دراین مقاله ما طرح Tzeng را در برابر حملات جدید تبانی تحلیل و ارزیابی کرده و نشان خواهیم داد که طرح مذکور علاوه بر ضعف در برابر حملات دیگر در مقابل حملات تبانی نیز ضعیف است.

کلمات کلیدی:
امضای دیجیتالی، طرح امضای وکالتی، امضای وکالتی استانه، حمله تبانی