عنوان مقاله:
یک طرح امضای مبتنی بر شناسه با تاییدکننده مشخص جدید به همراه کاربرد آن در خانههای هوشمند

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 5, شماره 4 (سال: 1396)

تعداد صفحات اصل مقاله: 13

نویسندگان:
محمد بهشتی آتشگاه - *دانشگاه صنعتی مالک اشتر*

محمدرضا عارف - *دانشگاه صنعتی شریف*

مرتضی براری - *استادیار دانشگاه صنعتی مالک اشتر*

مرتضی براری - *استادیار دانشگاه صنعتی مالک اشتر*

خلاصه مقاله:
در یک طرح امضا با تاییدکننده مشخص قوی، امضاکننده قادر میشود تا امضا را برای یک گیرنده خاص صادر نماید؛ یعنی تنها گیرنده مشخصی که مدنظر امضاکننده است میتواند اعتبار امضای صادرشده را بررسی نماید. البته باید طرح امضا به گونهای باشد که هیچ بخش سومی قادر به بررسی اعتبار امضا نباشد یا به عبارت دیگر، تاییدکننده مشخص نتواند امضا را به بخش سومی منتقل کند. در این مقاله، یک طرح امضای مبتنی بر شناسه جدید با تاییدکننده مشخص جدید ارائه میکنیم که در مدل سروش تصادفی و براساس فرض BDH دارای اثبات امنیتی است. طرح ارائهشده تمامی ملزومات امنیتی یک طرح امضای با تاییدکننده مشخص را برآورده مینماید. علاوه بر آن، طرح ارائهشده ویژگی محافظت از حریم خصوصی کاربر را برآورده ساخته و همچنین به لحاظ کارآمدی از حیث اندازه امضای خروجی و محاسبات لازم برای فازهای صادرشدن امضا و تایید آن با دیگر طرحهای موجود قابل مقایسه بوده و جزو طرحهای سبکوزن محسوب میشود. در نهایت نیز برخی از سناریوهای کاربردی طرح ارائهشده را در فضای اینترنت اشیا معرفی میکنیم.

کلمات کلیدی:
طرح امضای مبتنی بر شناسه, امضا با تاییدکننده مشخص, اینترنت اشیا خانه هوشمند, رایانش ابری, اثبات امنیتی, زوج سازی دوخطی