مجله "پدافند الکترونیکی و سایبری"، سال اول، شماره ۱، بهار ۱۳۹۲، ص ۲۳-۳۴

یک (t , n) طرح امضای وکالتی آستانه با تأییدکننده مشخص جدید و اثبات امنیتی آن در مدل استاندارد

محمد بهشتی آتشگاه[1*]، محمود گردشی[2]، محمدرضا عارف[3]

۱- کارشناسی ارشد، دانشگاه جامع امام حسین (ع)، تهران ۲- مربی، دانشگاه جامع امام حسین (ع)، تهران ۳- استاد، آزمایشگاه تئوری اطلاعات و مخابرات امن(ISSL)، دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران

(دریافت: ۹۱/۹/۱۹ ، پذیرش: ۹۱/۱۱/۲۸)

چکیده

در یک (t , n) طرح امضای وکالتی آستانه با تأییدکننده مشخص، صاحب امضاء، قابلیت امضای خود را به گروه n نفره از نمایندگان خود اعطاء می‌نماید تا در صورت توافق حداقل t نفر، بتوانند روی متن موردنظر امضای وکالتی صورت دهند. البته، این امضاء برای یک گیرنده مشخص صادر می‌شود و بنابراین، تنها او می‌تواند اعتبار امضاء را بررسی نماید. در این مقاله، یک (t , n) طرح امضای وکالتی آستانه با تأییدکننده مشخص جدید، ارائه شده و نیز نشان داده می‌شود که طرح ارائه‌شده، در مدل استاندارد دارای امنیت اثبات‌پذیر است. امنیت طرح ارائه‌شده، بر اساس فرض سختی مسأله دیفی- هِلمن دوخطی گپ GDBH استوار است.

واژه‌های کلیدی:

طرح امضای وکالتی، طرح امضای وکالتی آستانه، امنیت اثبات‌پذیر، مدل استاندارد، زوج‌سازی دوخطی

A New (t,n) Designated Verifier Threshold Proxy Signature Scheme in the Standard Model

Mohammad Beheshti Atashgah[1*], Mahmoud Gardeshi[2], Mohammad Reza Aref[3]

1,2- Imam Hossein University, Tehran, Iran 3- Information Systems and Security Lab (ISSL), EE Department, Sharif University of Technology, Tehran, Iran

Abstract

In a designated verifier threshold proxy signature scheme, an original signer can delegate his\her signing power to proxy signers such that any or more out of proxy signers can sign messages on behalf of the original signer but or less of the proxy signers cannot generate a valid proxy signature. Of course, the signature is issued for a designated receiver and therefore only the designated receiver can validate the proxy signature. In this paper, we propose a new designated verifier threshold proxy signature scheme and also show that our proposed scheme has provable security in the standard model. The security of proposed scheme is based on the assumption.

Keywords

Proxy signature scheme, Threshold proxy signature scheme, Provable security, Standard model, Bilinear pairing.

* Corresponding Author Email: M.Beheshti.A@gmail.com