عنوان مقاله:
امضای دیجیتال گروهی آستانه

محل انتشار:
هشتمین کنفرانس سالانه انجمن کامپیوتر ایران (سال: 1381)

تعداد صفحات اصل مقاله: 7

نویسندگان:
حسن بولوردی - *دانشگاه صنعتی شریف (دانشکده مهندسی برق)*

جواد مهاجری - *دانشگاه صنعتی شریف (پژوهشکده الکترونیک)*

محمود سلماسی زاده - *دانشگاه صنعتی شریف (پژوهشکده الکترونیک)*

خلاصه مقاله:
امضای دیجیتال گر وهی به هر کدام از افراد یک گروه این امکان را می دهد که از طرف کل گروه اقدام به امضاءنمودن یک پیام نمایند . کل گروه تنها دارای یک کلید عمومی است و هر کدام از اشخاص کلید خصوصی خاص خود را دارند . پس از امضاء شدن یک پیام تنها مدیر گروه قادر است تشخیص دهد که امضا ء توسط کدام یک از اعضای گروه انجام پذیرفته است . در این مقاله روشی جدید برای امضای دیجیتال گروهی ارائه می کنیم که دارای خاصیت امضای دیجیتال آستانه t از k باشد . بدین مفهوم که در یک گروه k نفری برای امضاء نمودن یک پیام از طرف کل گروه حداقل t نفر از اعضای گر وه باید مشارکت داشته باشند ولی هر زیرمجموعة t-1 نفری و یا کمتر از آن قادر به انجام چنین کاری نباشند . این روش امضاء در برابر حملة ائتلاف (Coalition Attack) نیز مقاوم است

کلمات کلیدی:
سیستم های رمزنگاری کلید عمومی، امضای دیجیتال گروهی، امضای دیجیتال آستانه، طرح تقسیم راز، فرمول درون یابی لاگرانژ

لینک ثابت مقاله در پایگاه سیویلیکا: