عنوان مقاله:
پیچیدگی محاسباتی عملیات رمزنگاری و رمزگشایی سیستمهای کلید همگانی RSA و McEliece

محل انتشار:
چهارمین کنفرانس انجمن رمز ایران (سال: 1386)

تعداد صفحات اصل مقاله: 6

نویسندگان:
حسام محمدحسینی - *بخش مهندسی برق و کامپیوتر دانشگاه تربیت مدرس*

پیام امانی - *دانشکده مهندسی برق دانشگاه صنعتی خواجه نصیرالدین طوسی*

احمدرضا شرافت - *بخش مهندسی برق و کامپیوتر دانشگاه تربیت مدرس*

خلاصه مقاله:
در این مقاله پیچیدگی محاسباتی عملیات رمزنگاری/رمزگشایی سیستمهای رمزنگاری کلید همگانی RSA و McEliece محاسبه و مقایسه شدهاند. معیار محاسبه پیچیدگی، تعداد عملیات باینری لازم برای هر بار رمزنگار ی/رمزگشایی یک قالب از اطلاعات در هر یک از سیستمها در نظر گرفته شده است. با این معیار، مرتبه تعداد عملیات باینری لازم برای رمزنگاری/رمزگشایی در هر یک از سیستمهای فوق به صورت تابعی از پارامترهای سیستم متناظر محاسبه شده است. نتایج محاسبات نشان میدهند که حجم عملیات (باینری) لازم برای هر بار رمزنگاری/ رمزگشایی یک قالب پیام در سیستمMcEliece به مراتب کمتر از سیستم RSA است. با توجه به شباهت دیگر سیستمهای رمزنگاری مبتنی بر تئوری کدینگ به سیستم،McEliece نتایج این مقاله را میتوان به کمتر بودن حجم عملیات باینری لازم برای رمزنگاری/ رمزگشایی در سیستمهای رمزنگاری مبتنی کدینگ در مقایسه با سیستمهای رمزنگاری مبتنی بر نظریه اعداد تعمیم داد. این ویژگی، چنین سیستمهایی را برای استفاده در کاربردهای نیازمند امنیت در شبکهای با محدودیت توان پردازشی و یا محدودیت عمر باتری در گرهها، برای مثال در شبکههای بیسیم، مناسب میسازد؛ زیرا حمله رمزشکنی موثری به رمزنگاری مبتنی بر تئوری کدینگ موجود نیست. در پایان، نتایج بدست آمده را با نتایج مقالات موجود مقایسه و تفاوت آنها را توضیح دادهایم.

کلمات کلیدی:
سیستم رمزنگاری، McEliece ، سیستم رمز نگاری ،RSA رمزنگاری کلید همگانی، مرتبه محاسباتی

لینک ثابت مقاله در پایگاه سیویلیکا: