بخشی از ترجمه مقاله

عنوان فارسی مقاله :

تابع هش یک طرفه بر مبنای کدهای Goppa

عنوان انگلیسی مقاله :

One-way Hash Function Based on Goppa Codes « OHFGC »

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل

با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

VI.) Conclusion

We have presented a new variant of a hash function based on the syndrome decoding. This variant uses the generation of a parity check matrix of a Goppa code rational, which is among codes the most widely used in cryptography and has a pseudo-random character. Our proposal is promising, indeed it is more than resist quantum computers, and it has a variable size that meets our needs to choose the size of the hash we desire and increases safety.

6) نتیجه گیری

در اینجا گونه جدیدی از تابع هش بر مبنای رمزگشایی سندرم را مطرح کرده ایم. این گونه از تولید ماتریس بررسی توازن کد Goppa استفاده می کند که در میان کدها، کاربردی ترین مورد در رمزنگاری بوده و دارای کاراکتر شبه تصادفی می باشد. پیشنهاد ما امیدوارکننده است، در واقع بیش از مقاومت در برابر کامپیوترهای کوانتوم است و دارای اندازه متغیری است که نیازهای ما برای تامین اندازه هش مطلوب را تامین و ایمنی را افزایش می دهد.