عنوان مقاله:

Compound of Reversible One-Dimensional CA Rules for Two-Dimensional CA with Cryptographic Applications

محل انتشار:

چهاردهمین کنفرانس بین المللی سالانه انجمن کامپیوتر ایران (سال: 1388)

تعداد صفحات اصل مقاله: 6

نویسندگان:

Hoda Maleki - *Computer Engineering Department, Amirkabir University of Tehran,Iran*

Babak Sadeghiyan - *Computer Engineering Department, Amirkabir University of Tehran,Iran*

خلاصه مقاله:

Reversible Cellular Automata is applicable in cryptographic functions. A reversible CA can be obtained by employing reversible rules. In this paper, we propose 65280 two-dimensional reversible CA rules by compounding one-dimensional reversible rules. We produce these rules by alternately applying onedimensional CA rule f1 to the rows and applying another rule f2 to the columns of the con figuration matrix of twodimensional CA. In addition to describing these rules, we consider the required cryptographic properties such as completeness, strict avalanche criteria, non-linearity, and differential-profile flatness for our proposed approach. According to the obtained results, 9463 rules are specified as appropriate rules for the purpose of applying in cryptographic functions. Only 510 rules do .not satisfy any of the mentioned cryptographic properties and the other remain rules satisfy some of the properties

کلمات کلیدی:

Two-dimensional cellular automata, Cryptographic property, Reversible cellular automata rule

لینک ثابت مقاله در پایگاه سیویلیکا: