بخشی از ترجمه مقاله

عنوان فارسی مقاله :

نظریه و برنامه های کاربردی ماشین های خودکار در پنهان شناسی

عنوان انگلیسی مقاله :

Theory and Applications of Cellular Automata

in Cryptography

توجه !

بخشی از ترجمه مقاله

VIII. CONCLUSION I
n this work we have proved analytically that CA with EXNOR rules (i.e., 51, 153, and 195) can generate an alternating group. It is found that alternating groups form a set of fundamental transformations. Using these fundamental transformations a block cipher scheme is proposed in this paper. A scheme for stream ciphers is also proposed employing PCA. Keystream generators of the stream ciphers consist of PCA and rule selector. The complexity of the proposed schemes compare with the available schemes reported so far. The complexity can be further increased with an increase in block size for block cipher and in number of CA cells in the stream ciphers. Enciphering and deciphering process of the proposed schemes follow the same protocol. One of the main advantages of proposed schemes is the use of simple, regular, modular and cascadable structure of CA as the basic building block that ideally suits for VLSI implementation.

6.نتیجه گیری

در این اثر، ما به طور تحلیلی اثبات کرده ایم CA با قوانین EXNOR (یعنی 51،153 و 195) میتواند یک گروه متناوب را ایجاد نماید. کشف شد، گروه های متناوب ،مجموعه ای از تغییر شکلهای اساسی را شکل میدهند. با استفاده از این تغییر شکلهای اساسی، یک طرح رمز بلوکی، در این مقاله ارائه میشود. یک طرح برای رمزهای جریان، هم با بکارگیری PCA ارائه میشود. مولدهای جریان اصلی رمزهای جاری از PCA و گزینشگر قانون تشکیل میشوند. پیچیدگی طرحها با طرحهای موجود گزارش شده تاکنون، مقایسه میشوند. پیچیدگی میتواند به علاوه با افزایش در اندازه ی بلوک برای رمز بلوکی و تعداد سلولهای CA در رمزهای جاری بیشتر شود. فرایند رمزگذاری و رمزگشایی طرحهای ارائه شده، پروتکل مشابه را دنبال میکند. یکی از مزایای اصلی طرحهای ارائه شده، استفاده از ساختار ساده، منظم ، مولکولی و پشت سر هم CA به صورت بلوک سازنده ی اصلی است که به طور ایده الی برای اجرای VLSI مناسب است.