ایران عرضه
فروشگاه کالاهای دانلودی

بخشی از ترجمه مقاله

عنوان فارسی مقاله :

رمزنگاری با ماشین های سلولی

عنوان انگلیسی مقاله :

cryptography with cellular automata

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

One approach to the problem of finding the seed [6] uses the near linearity of the rule (1). Equation (1) can be written in the alternative form $a_{i-1} = a_i'$ XOR (a_i OR a_{i+1}). Given the values of cells in two adjacent columns, this allows the values of all cells in a triangle to the left to be reconstructed. But the sequence provided gives only one column. Values in the other column can be guessed, and then determined from the consistency of Boolean equations for the seed. But in disjunctive normal form the number of terms in these equations increases linearly with N, presumably making their solution take a time more than polynomial in N.

The cellular automaton (1) can be implemented efficiently on an integrated circuit; it requires less than ten gate delay times to generate each output bit, and can thus potentially be used in a variety of high-bandwidth cryptographic applications.

یک رویکرد برای مساله‌ی یافتن دانه [۶]، از خطی بودن تقریبی قاعده‌ی (۱) استفاده می‌کند. معادله‌ی (۱) را می‌توان در فرم جایگزین $a_i' = a_{i-1} XOR (a_i OR a_{i+1})$ نوشت. با ارائه‌ی مقادیر سلول‌ها در دو ستون مجاور، این، امکان ساختن مقادیر همه‌ی سلول‌ها را در یک مثلث در سمت چپ را فراهم می‌کند. اما دنباله‌ی فراهم شده تنها یک ستون را ارائه می‌دهد. مقادیر در ستون دیگر را می‌توتان حدس زد و سپس از سازگاری معادلات بولی برای سرعت تعیین کرد. اما در فرم نرمال فصلی، تعداد جملات در این معادلات به طور خطی با N افزایش می‌یابد، که به طور پیش فرض باعث می‌شود که راه‌حل آن‌ها زمان بیشتری از چند جمله‌ای در N صرف کند.

ماشین سلولی (۱) را می‌توان به طور کارامدی روی یک مدار ادغام شده اجرا کرد؛ آن نیاز به کمتر از ده زمان تاخیر ورودی برای تولید هر بیت خروجی دارد و بنابراین می‌تواند به طور بالقوه در طیف وسیعی از برنامه‌های کاربردی رمزنگاری با پهنای باند بالا مورد استفاده قرار گیرد.

ایران عرضه
مرجع مقالات
ترجمه شده

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.

برای جستجوی جدیدترین مقالات ترجمه شده، اینجا کلیک نمایید.