عنوان مقاله:

Construction of Side Channel Attack Resistant S-Boxes Using Genetic Algorithms Based on Coordinate Functions

محل انتشار:

مجله نوآوری های مهندسی برق و کامپیوتر, دوره 10, شماره 1 (سال: 1401)

تعداد صفحات اصل مقاله: 10

نویسندگان:

B. Khadem - *Faculty of Computer Engineering, Imam Hussein Comprehensive University, Tehran, Iran*

S. Rajavzadeh - *Faculty of Mathematics, Payam-e-Noor University (PNU) Graduate Center, Tehran, Iran*

خلاصه مقاله:

kground and Objectives: Substitution-box (S-Box) is one of the essential components creating confusion and nonlinear properties in cryptography. To strengthen a cipher against various attacks, including side channel attacks, these boxes need to have numerous security properties. In this paper, a novel S-Box construction method is introduced aimed at improving the resistance of S-Boxes against power analysis attacks.Methods: In the preprocessing phase of this approach, a suitable initial S-Box with some basic security properties was generated by adopting a fast algorithm. Then, in the main stage, using the initial S-Box, we generate new S-Boxes which not only have the properties of the initial S-Box but also have significantly improved under another set of security properties. To do this, new S-Boxes were generated using a genetic algorithm on a particular subset of the linear combination set of coordinate functions of the initial S-Box.Results: The performed experiments demonstrated that the values of all security properties of these new S-Boxes, especially the measures of transparency order, signal-to-noise ratio, confusion coefficient, bijection property, fixed point, and opposite fixed points, have been substantially improved. For example, our experiments indicate that ۷۰, ۲۲۰, ۲۰۷۱, ۴۳, and ۴۰۶ S-Boxes are found better than the initial S-Box, respectively, in the dimensions of ۴×۴ through ۸×۸Conclusion: In this paper, a new S-Box construction method is introduced where the properties related to side channel attacks are improved, without destroying other security features. Besides, some results obtained from generated S-Boxes in the dimensions of ۴×۴ through ۸×۸ demonstrated that the generated S-Boxes are not only improved relative to the initial S-Box, but also in certain cases, considerably better than some well-known S-Boxes.

کلمات کلیدی:

Substitution Box (S-Box), Side Channel Attack (SCA), Coordinate Functions, Security Properties