عنوان مقاله:

Signature in Even Blocks: A Modification to the Davies and Price Method

محل انتشار:

یازدهمین کنفرانس مهندسی برق (سال: 1382)

تعداد صفحات اصل مقاله: 8

نویسنده:

Faramarz Hendessi - *Department of Electrical & Computer Engineering Isfahan University of Technology, Isfahan, IRAN*

خلاصه مقاله:

In this paper, Davies and Price hash functioning method with application in digital signature is studied. This hash function uses a block cipher algorithm as a one way function. It is shown that by a simple modification of the Davies and Price method, the system can be made immune to the birthday attack. It is also shown that the proposed method, called signature in even blocks, is much faster than the Rivest-Shamir-Adleman (RSA) algorithm and much more reliable than the Davies and Price method.

کلمات کلیدی:

Hash Functioning, Digital Signature, RSA, DES, Davies and price Algorithm