سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:

Multiple-Chi-square Tests and Their Application on Distinguishing Attacks

محل انتشار:

هشتمین کنفرانس انجمن رمز ایران (سال: 1390)

تعداد صفحات اصل مقاله: 6

نویسندگان:

Ali Vardasbi - *Department of Electrical Engineering Sharif University of TechnologyTehran, Iran*

Mahmoud Salmasizadeh, - *Electronics Research Center Sharif University of Technology Tehran, Iran*

Javad Mohajeri - *Electronics Research Center Sharif University of Technology Tehran, Iran*

خلاصه مقاله:

Chi-square tests are vastly used for distinguishing random distributions, but extra care must be taken when using them on several independent variables. We noticed, the chisquare statistics, in some previous works, was computed half of its real value. Thus, to avoid possible future confusions, we formulize multiple-chi-square tests. To show the application of multiple-chi-square tests, we introduce two new tests and apply them to Trivium as a special case. These tests are modifications of ANF monomial test and, when applied to Trivium with the same number of rounds, .the data complexity of them is roughly times smaller than that of previous ANF monomial test

کلمات کلیدی:

Multiple-Chi-square Test; Distinguishing Attacks; Trivium; Boolean Functions

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/125108