عنوان مقاله:

Rainbow Table TMTO Attack Optimization Considering Online Sequential Search Time

محل انتشار:

سومین کنفرانس الکترونیکی بین المللی فن آوری اطلاعات،حال و آینده (سال: 1393)

تعداد صفحات اصل مقاله: 5

نویسندگان:

Mohammad hadi - *Electrical Engineering Department Sharif University of Technology Tehran, Iran*

Mohammad Moeini Jahromi - *Computer Engineering Department Payame Noor University Tehran, Iran*

Hamid Reza Rezaiy - *STRIK Sharif University of Technology Tehran, Iran*

خلاصه مقاله:

In this paper, we propose an optimizedparameter selection procedure for rainbow table TimeMemory Trade-Off (TMTO) attack with sequential onlinesearch. Unlike previous works that mainly deal withminimizing required memory in the rainbow table TMTOattack, we simultaneously focus on the required memory andonline search time. Our parameter selection technique isoptimized regarding the minimization of the requiredmemory subject to a certain success probability and amaximum online search time. Obtained results are twocompact mathematical expressions for determining rainbowtable TMTO attack parameters, number and length ofchains. The application of our optimized parameter selectionprocedure is also shown in a sample example.

کلمات کلیدی:

Time-Memory Trade-Off (TMTO) Attack; Online Search; Constrained Optimization; Cardano Cubic Formulas