Analysis and Design of Cryptographic Hash Functions

Pieter Retief Kasselman

Voorgelê ter vervulling van 'n deel van die vereistes vir die graad Magister in Ingenieurswese in die Fakulteit Ingenieurswese, Universiteit van Pretoria.

18 November 1999

Summary

Analysis and Design of Cryptographic Hash Functions

by

P. R. Kasselman and W. T. Penzhorn

Department of Electrical, Electronic and Computer Engineering

University of Pretoria

MEng Electronic Engineering

Indexing Terms: Hash Functions, Cryptanalysis, Cryptography, Message Integrity Code, Message Authentication Code, Differential Cryptanalysis, Boolean Functions, MD4, MD5, HAVAL.

Cryptographic hash functions are one of the primitive building blocks commonly used in information security. They form an important building block for authentication protocols, encryption algorithms, digital signatures and integrity checking algorithms. Two important properties of hash functions used in cryptographic applications are collision resistance and one-wayness. In this dissertation the focus is on collision resistance.

The dissertation provides a detailed overview of existing cryptographic hash functions, including definitions of fundamental properties, generic threats, and popular designs for cryptographic hash functions. Special attention is given to dedicated cryptographic hash functions related to the MD4 hash function.

Between 1990 and 1994 a number of practical cryptographic hash functions were designed and implemented, following the design principles of MD4. These cryptographic hash functions include MD4, MD5, SHA, SHA-1, HAVAL, RIPEMD-128 and RIPEMD-160. These functions were designed to exhibit the properties of collision resistance and one-wayness.

In this dissertation the attacks by Dobbertin on MD4 and MD5 are reconstructed. A novel approach is introduced that allows the execution of the attack on MD4 to be optimised. This new approach allows a reduction in computation time for a collision by a factor 64.

Based on these attacks a generalised attack is formulated. The generalised attack provides a new framework for the analysis of the collision resistant property of any cryptographic hash function.

This newly derived framework for the analysis of cryptographic hash functions is then applied to reduced versions of SHA and HAVAL. The results obtained in this investigation are the first cryptanalytical result to be published on the HAVAL hash function. The investigation shows that a collision can be found for a reduced version of HAVAL in less than a minute on a 200 MHz Pentium Pro personal computer. This result suggests that three and even four round HAVAL should not be used for security applications where message integrity and non-repudiation is required.

Based on the findings of these cryptanalytic attacks, a new set of design criteria for dedicated cryptographic hash functions is formulated. The design criteria aim to alleviate the common weaknesses identified in dedicated hash functions such as MD4, MD5, SHA, SHA-1 and HAVAL. Thereby the generalised attack developed in this dissertation can be thwarted.

Samevatting

Analise en Ontwerp van Kriptografiese Hutsfunksies

deur

P. R. Kasselman and W. T. Penzhorn
Department Elektriese, Elektroniese en Rekenaar Ingenieurswese
Universiteit van Pretoria
M Ing Electroniese Ingenieurswese

Indekseringterme: Hutsfunksies, Kripto-analisie, Kriptografie, Boodskap Integriteit Kode, Boodskap Stawing Kode, Differensiële Kriptoanalise, Boolese Funksies, MD4, MD5, HAVAL.

Kriptografiese hutsfunksies is een van die primitiewe boublokke wat algemeen gebruik word in informasiesekerheid. Dit vorm 'n belangrike boublok vir stawingsprotokolle, enkripsiealgoritmes, digitale handtekeninge en integriteitmeganismes. Twee belangrike eienskappe van hutsfunksies is weerstand teen botsings en die eenrigtingeienskap. In hierdie verhandeling val die fokus op die botsingweerstandseienskap.

Die verhandeling bevat 'n volledige oorsig van bestaande kriptografiese hutsfunksies, insluitend definisies van fundamentele eienskappe, generies bedreigings en populêre ontwerpe vir kriptografiese hutsfunksies. Spesiale aandag word gegee aan toegewyde kriptografiese hutsfunksies wat verwant is aan die MD4 hutsfunksie.

Tussen 1990 en 1994 is 'n aantal kriptografies hutsfunksies ontwerp en geïmplimenteer. Hierdie ontwerpe is gegrond op die ontwerpsbeginsels van MD4. Die kriptografiese hutsfunksies sluit in MD4, MD5, SHA, SHA-1, HAVAL, RIPEMD-128 en RIPEMD-160. Hierdie funksies is almal ontwerp om die eenrigting en botsingsweerstand eienskappe te vertoon.

In hierdie verhandeling word die aanvalle van Dobbertin op MD4 en MD5 gerekonstrueer. 'n Unieke benadering word voorgestel wat die aanval op MD4 optimeer. Die nuwe benadering verminder die berekeningkompleksiteit om 'n botsing te verkry met 'n faktor 64.

'n Veralgemeende aanval word geformuleer op grond van hierdie aanvalle. Die veralgemeende aanval voorsien 'n nuwe raamwerk vir die analise van die botsingsweerstand eienskap van enige toegewydte kriptografiese hutsfunksie.

Hierdie nuwe raamwerk vir die analiese van kriptografiese hutsfunksies word dan toegepas

op afgeskaalde weergawes van SHA en HAVAL. Die resultate van hierdie studie is die eerste kripto-analitiese resultate wat vir HAVAL gepubliseer is. Die studie toon dat 'n botsing vir die laaste twee rondtes van drierondte HAVAL verkry kan word in minder as 'n minuut op 'n 200 MHz Pentium Pro persoonlike rekenaar. Hierdie resultaat dui aan dat drie en selfs vier rondte HAVAL nie gebruik moet word vir sekuriteitstoepassings waar boodskapintegriteit vereis word nie.

Op grond van die kriptoanalitiese resultate word 'n nuwe stel ontwerpskriteria vir toegewyde kriptografiese hutsfunksies geformuleer. Die ontwerpskriteria is daarop gemik om die gedeelde swakhede geïdentifiseer in toegewyde hutsfunksies soos MD4, MD5, SHA, SHA-1 en HAVAL te vermy. Hierdeur kan die veralgemeende aanval wat in die verhandeling ontwikkel is gefnuik word.

Acknowledgements

I would like to make use of this opportunity to thank the following individuals and organisations.

My study leader, Prof. W.T. Penzhorn for his contributions, suggestions and encouragement throughout this project.

Prof. G.J. Kühn for the many stimulating conversations on the topic of cryptology.

Dr Bart Preneel and Antoon Bosselaers from the COSIC research group at the Katholieke Universiteit Leuven, Belgium for their comments on my work and suggesting the analysis of the HAVAL hash function.

My wife, Marelize, for her continued support and companionship throughout this project.

Ciphertec cc for the opportunity to perform research on the topic of cryptographic hash functions.

The management of Nedcor Bank Ltd for the time afforded to me in order to complete this dissertation.

CONTENTS