Accepted Manuscript

A provably secure non-iterative hash function resisting birthday attack

Shenghui Su, Tao Xie, Shuwang Lü

PII: S0304-3975(16)00154-7
DOI: http://dx.doi.org/10.1016/j.tcs.2016.02.023
Reference: TCS 10663

To appear in: *Theoretical Computer Science*

Received date: 28 October 2015
Revised date: 10 February 2016
Accepted date: 15 February 2016

Please cite this article in press as: S. Su et al., A provably secure non-iterative hash function resisting birthday attack, *Theoret. Comput. Sci.* (2016), http://dx.doi.org/10.1016/j.tcs.2016.02.023

A Provably Secure Non-iterative Hash Function Resisting Birthday Attack

Shenghui Su [1, 2, 4(✉)], Tao Xie [1], and Shuwang Lü [3]

[1] School of Computers, National University of Defense Technology, Changsha 410073, PRC
[2] Laboratory of Trusted Computing, Beijing University of Technology, Beijing 100124, PRC
[3] School of Computers, University of Chinese Academy of Sciences, Beijing 100039, PRC
[4] Laboratory of Computational Complexity, BFID Corporation, Beijing 100098, PRC
reesse@126.com

Abstract. To examine the integrity and authenticity of an IP address efficiently and economically, this paper proposes a new non-iterative hash function called JUNA that is based on a multivariate permutation problem and an anomalous subset product problem to which no subexponential time solutions are found so far. JUNA includes an initialization algorithm and a compression algorithm, and converts a short message of n bits which is regarded as only one block into a digest of m bits, where $80 \le m \le 232$ and $80 \le m \le n \le 4096$. The analysis and proof show that the new hash is one-way, weakly collision-free, and strongly collision-free, and its security against existent attacks such as birthday attack and meet-in-the-middle attack is to $O(2^m)$. Moreover, a detailed proof that the new hash function is resistant to the birthday attack is given. Compared with the Chaum-Heijst-Pfitzmann hash based on a discrete logarithm problem, the new hash is lightweight, and thus it opens a door to convenience for utilization of lightweight digital signing schemes.

Keywords: Hash function; Compression algorithm; Non-iterative structure; Provable security; Birthday attack; Meet-in-the-middle attack

1 Introduction

Message digests outputted by a hash function may be utilized to examine the integrity and authenticity of IP addresses in a transmitted data packet so as to prevent the source address and destination address from being tampered or forged.

Let $\hat{h}$ be a hash function, and usually, it has the four properties as follows [1][2][3]:

① given a message m, it is very easy to calculate the message digest $d = \hat{h}(m)$, where d is also called a hash output, namely $\hat{h}$ is computable;

② given a digest d, it is very hard to calculate the message m according to $d = \hat{h}(m)$, namely $\hat{h}$ is one-way;

③ given any arbitrary message m, it is computationally infeasible to find another message m' such that $\hat{h}(m) = \hat{h}(m')$, namely $\hat{h}$ is weakly collision-free;

* This work is supported by MOST with Project 2009AA01Z441 and NSFC with Project 61472476.