Security of VSH in the Real World

Markku-Juhani O. Saarinen

Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
m.saarinen@rhul.ac.uk

Abstract. In Eurocrypt 2006, Contini, Lenstra, and Steinfeld proposed a new hash function primitive, VSH, *very smooth hash*. In this brief paper we offer commentary on the resistance of VSH against some standard cryptanalytic attacks, including preimage attacks and collision search for a truncated VSH. Although the authors of VSH claim only collision resistance, we show why one must be very careful when using VSH in cryptographic engineering, where additional security properties are often required.

1 Introduction

Many existing cryptographic hash functions were originally designed to be *message digests* for use in digital signature schemes. However, they are also often used as building blocks for other cryptographic primitives, such as pseudorandom number generators (PRNGs), message authentication codes, password security schemes, and for deriving keying material in cryptographic protocols such as SSL, TLS, and IPSec.

These applications may use truncated versions of the hashes with an implicit assumption that the security of such a variant against attacks is directly proportional to the amount of entropy (bits) used from the hash result. An example of this is the HMAC$-n$ construction in IPSec [1]. Some signature schemes also use truncated hashes. Hence we are driven to the following slightly nonstandard definition of security goals for a hash function usable in practice:

1. **Preimage resistance.** For essentially all pre-specified outputs X, it is difficult to find a message Y such that $H(Y) = X$. The difficulty should be $\approx 2^l$ when there are l pre-specified bits in X.
2. **2nd-preimage resistance.** Given a pre-specified message X, it is difficult to find another message Y so that $H(X) = H(Y)$. The difficulty should be $\approx 2^l$ when there are l pre-specified bits that match in the hashes.
3. **Collision resistance.** It should require $\approx 2^{l/2}$ effort to find any two messages X and Y that produce a collision $H(X) = H(Y)$ in l pre-specified bits in the hashes.

In addition to the above three usual goals, we state a fourth, more informal goal – **pseudorandomness**. In essence, we would like a PRNG, stream cipher, or other derived design that relies on a hash function to have at least $\approx 2^{l/2}$ security, as if it was secured with a "real" pseudorandom function.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 95–103, 2006.

Pseudorandomness implies that a hash has good statistical properties and resistance against a wide array of distinguishing attacks.

All of the mentioned desirable properties are difficult if not impossible to prove without nonstandard assumptions. We note that proofs based on assumptions are themselves assumptions, whether their origins are in the traditions of symmetric or asymmetric cryptanalysis. An assumption based on the sieving phase of the NFS factoring algorithm may seem like a "hard problem" to a researcher who has spent a lot of time tweaking the sieving phase of the NFS factoring algorithm. On the other hand, a researcher who has dedicated years of effort into symmetric cryptanalysis may feel that symmetric cryptography possesses equally well studied "hard problems", while also allowing more efficient overall implementation.

A "political" standardisation consideration is that (by definition) VSH has a backdoor in the secret factorisation of n. In the past it has been difficult to popularise cryptographic technologies that rely on trusted third parties.

In our opinion VSH is a simple, elegant design that is based on a plausible complexity-theoretic assumption (VSSR: Very Smooth number nontrivial modular Square Root). However, it should not be considered a general-purpose hash function as usually understood in security engineering.

On VSH Security Claims

"VSH is not a Hash Function."
– Arjen K. Lenstra, Eurocrypt 2006 [1]

Collision resistance is the only property proven for VSH. In Section 3 of the VSH paper [2], short message inversion (equivalent to preimage resistance) is considered and one possible "solution" is provided. As will be shown in Section 2.1 of this paper, the solution is not adequate.

The authors therefore clearly expected VSH to exhibit some level of preimage and 2nd preimage resistance. These are standard requirements in the very definition of a "cryptographic hash function". The authors of VSH are very clear in that "VSH should not be used to model random oracles". Random oracle behaviour is not a standard hash function security requirement.

Some researchers tend to concentrate their efforts on showing that their hash functions provide collision resistance, while ignoring other security properties. However, it is well known that collision resistance does not imply preimage-resistance or other important hash function properties.

To illustrate this point, we present a classical counter-example. Consider an $l+1$-bit hash $H'(x)$ that has been constructed from an l - bit hash H as follows:

$$\text{If } |x| < l-1 \text{ then } H'(x) = x \,||\, 1 \,||\, 0\, 0 \cdots 0.$$
$$\text{If } |x| \geq l-1 \text{ then } H'(x) = H(x) \,||\, 1.$$

[1] Quoted with permission. During the conference A.K. Lenstra used some of the results from this note in his presentation, with appropriate credit. This has led some people to mistakenly think that the results in this note were already contained in [2]. All cryptanalytic results presented in this paper are by the author; a draft was circulated with the authors of VSH before Eurocrypt 2006.