Preimage Attacks Against Spectral Hash and PTX Functions.

Ethan Heilman
Boston University

ABSTRACT

This paper presents a novel pre-image attack on SHA-3 candidate Spectral Hash (shash), which was until now thought to be resistant to pre-image attacks.

PTX (Permute Transform XOR) functions are an idealisation of shash [1] in which its pseudo-random functions have been replaced with random oracles. We extend our previous practical collision attacks on PTX functions to practical pre-image attacks against all PTX functions [3]. As shown in our previous work, the security of shash depends on the security of PTX functions, thus our result also applies to the pre-image security of shash.

Our technique is to use the chaining variable collision introduced in our previous attack, which reduces PTX functions, under a special set of inputs, to a series of random oracles XORed together.

$$PTX(x) = RO(x_0) \oplus RO(x_1) ... \oplus RO(x_m)$$

Note that while this property does not hold for every input x, it does hold for an infinite number of them. Finding a set of inputs to those random oracles such that the outputs, $y = RO(x)$, are an orthogonal basis of the output space is trivial [2]. Using this basis we span the entire output space of the hash function, therefore we can generate arbitrary outputs of our choosing. That is, for any output, we can compute a pre-image in constant time.

BODY

We break the pre-image security of PTX and shash by reducing it to the trivially solvable problem [2] of finding independent random vectors.

REFERENCES

[1] G. Saldamlı, C. Demirkıran, M. Maguire, C. Minden, J. Topper, A. Troesch, C. Walker, Ç. K. Koç. Spectral hash. Submission to NIST, 2008.

[2] C. Cooper. On the rank of random matrices. *Random Struct. Algorithms*, 16:2000, 2000.

[3] E. Heilman. Attacks against permute-transform-xor compression functions and spectral hash. *IACR Cryptology ePrint Archive*, 2009.

Volume 3 of Tiny Transactions on Computer Science