On the design and cryptanalysis of a one-way hash

Carl Ellison[1], Victor Miller[2], Eran Tromer[3] and Rebecca Wright[4]

[1] Microsoft, One Microsoft Way, Redmond WA, 98025, cme@microsoft.com
[2] Center for Communications Research, Princeton, NJ 08540, USA
[3] Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, 32 Vassar Street, G682, Cambridge, MA 02139, tromer@csail.mit.edu
[4] Department of Computer Science and DIMACS, Rutgers University, Piscataway, NJ, 08854, USA, rebecca.wright@rutgers.edu

Abstract. In this paper we describe a novel one-way hash function that is compliant with the NIST hash function competition draft criteria. We analyze its security properties in the indistinguishability framework, and its instantiations in several contexts. Performance is analyzed in software and hardware, and shown to be competitive with present standards. We proceed to describe its cryptanalytic status and practical applications. Some of are techniques are of potential independent interest.

Keywords: hash function, random oracle, SHA-1, one-way function, two-way function

1. Introduction

One-way hash,
I've designed the perfect one-way hash.
Compression function that's so elegant,
it's Merkle-Damgard with a bit of salt,
and it's secure –

'cause it's a one way hash.
Well, the submission was a bit of a rush,
so there's no provable reduction nor
some rationale for all those ANDs and XOR.
But it's so nice!

And when it hashes,

it hashes so fi-i-ine.

I hope that John

picks the function that's mi-i-ine.

2. Security properties

It does X.509, OAEP, HMAC and RNG,
'cause it's a one-way hash.
I've proposed the perfect one-way hash.
The NIST requirements? It has them all!
Can't be distinguished from an oracle.
(What do you mean?)

And it's preimage resistant
(of either kind).
And no collision exists
(none that I could find).

3. Performance

One-way hash –

It nicely fits within the L1 cache.

And when compared to functions such as SHA,

It's takes just half the circuit area.

And it's so fast!

4. Cryptanalysis

My one-way hash,
it's now on e-print and they say it's trash.
Those nasty bastards of cryptanalysts,
They get their kick from twiddling bytes and bits,
and broke my hash.

It has differentials that go
straight through all the rounds,
and via a linear
system the input's found.

They say's inversion's fast,

design's half-assed,

But then, recast ...

5. Applications

... it's a two-way hash!
That must be worth a million tons of cash!
Who needs that boring Davies-Meyer mode,
when you can buy my secret patent code!
It works both ways!

It has preimages,
two for the price of one.
And if you want a collision,
Then sure you can.

6. Conclusions and implications

One-way hash,
yes, those cryptographers can be so harsh.
But they're just paranoid, it's all tinfoil.
The market is as happy with snake oil.
So I'll get rich!

And when it hashes,
it hashes so fi-i-ine.
I hope that John
picks the function that's mi-i-ine.

One-way hash,

who needs a one-way hash,

One-way hash.

Acknowledgments:

We are indebted to Daniel J. Bernstein and Tanja Lange for motivating this research, reviewing drafts and providing valuable comments.

This work extends previous results of W. M. “Billy” Joel.

Signal processing provided by courtesy of the Nir Space Station.

Portions of this research were conducted in Warsaw, graciously supported by Kris Gaj and ENIGMA Information Security Systems Sp. z o.o.

Performed at the CRYPTO'07 rump session, 21 August 2007, to the tune of Billy Joel's “Uptown Girl”.

Lyrics and introduction:

Eran Tromer

Singers:

Carl Ellison

Victor Miller

Rebecca Wright