Paper 2007/474

Notes on the Wang et al. 2^{63} SHA-1 Differential Path

Martin Cochran

Abstract

Although advances in SHA-1 cryptanalysis have been made since the 2005 announcement of a 2^{63} attack by Wang et al., the details of the attack have not yet been vetted; this note does just that. Working from Adi Shamir's 2005 CRYPTO rump session presentation of Wang et al.'s work, this note corroborates and presents the differential path and associated conditions for the two-block attack. Although the error analysis for the advanced condition correction technique is not verified, a method is given which yields a two-block collision attack on SHA-1 requiring an estimated 2^{62} SHA-1 computations if the original error analysis by Wang et al. is correct.

Note: Added the second-block differential path and fixed several errors in the first-block differential path. Many thanks to Thomas Peyrin for finding the errors and sending me the second-block path.

Metadata

Available format(s)

PDF

Category

Cryptographic protocols

Cryptographic Hash Functions | Cryptanalysis | SHA-1

Contact author(s)

Martin Cochran @ colorado edu

History

2008-08-25: last of 3 revisions

2007-12-19: received

See all versions

Short URL

https://ia.cr/2007/474

License

BibTeX

Copy to clipboard

```
@misc{cryptoeprint:2007/474,
      author = {Martin Cochran},
      title = {Notes on the Wang et al. $2^{63}$ {SHA}-1 Dif1
      howpublished = {Cryptology {ePrint} Archive, Paper 200
      year = {2007},
      url = {https://eprint.iacr.org/2007/474}
}
```