Introduction

CHAPTER 1

Background

CHAPTER 2

Related Work

CHAPTER 3

Approach Overview

CHAPTER 4

Library design

CHAPTER 5

Library use

CHAPTER 6

Heuristics

CHAPTER 7

Measurements

CHAPTER 8

Analysis

Conclusion

Bibliography

[1] Gregory V Bard, Nicolas T Courtois, Chris Jefferson: *Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over GF (2) via SAT-solvers*, in: (2007).

[2] Roberto J Bayardo Jr, Robert Schrag: *Using CSP look-back techniques to solve real-world SAT instances*, in: *AAAI/IAAI*, 1997, pp. 203–208.

[3] Koen Claessen et al.: *SAT-solving in practice*, in: *Discrete Event Systems, 2008. WODES 2008. 9th International Workshop on*, IEEE, 2008, pp. 61–67.

[4] Ivan Bjerre Damgård: *A design principle for hash functions*, in: *Advances in Cryptology—CRYPTO'89 Proceedings*, Springer, 1990, pp. 416–427.

[5] Martin Davis, George Logemann, Donald Loveland: *A machine program for theorem-proving*, in: *Communications of the ACM* 5.7 (1962), pp. 394–397.

[6] Martin Davis, Hilary Putnam: *A computing procedure for quantification theory*, in: *Journal of the ACM (JACM)* 7.3 (1960), pp. 201–215.

[7] Tobias Eibach, Enrico Pilz, Gunnar Völkel: *Attacking Bivium using SAT solvers*, in: *Theory and Applications of Satisfiability Testing–SAT 2008*, Springer, 2008, pp. 63–76.

[8] RT Faizullin, IG Khnykin, VI Dylkeyt: *The SAT solving method as applied to cryptographic analysis of asymmetric ciphers*, in: *arXiv preprint arXiv:0907.1755* (2009).

[9] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno: *Cryptography engineering: design principles and practical applications*, John Wiley & Sons, 2012.

[10] Ekawat Homsirikamol et al.: *Security margin evaluation of SHA-3 contest finalists through SAT-based attacks*, in: *Computer Information Systems and Industrial Management*, Springer, 2012, pp. 56–67.

[11] Dejan Jovanović, Predrag Janičić: *Logical analysis of hash functions*, Springer, 2005.

[12] Philipp Jovanovic, Martin Kreuzer: *Algebraic attacks using SAT-solvers*, in: *Groups–Complexity–Cryptology* 2.2 (2010), pp. 247–259.

[13] Jonathan Katz, Yehuda Lindell: *Introduction to modern cryptography: principles and protocols*, CRC Press, 2007.

[14] Bin Li, Michael S Hsiao, Shuo Sheng: *A novel SAT all-solutions solver for efficient preimage computation*, in: *Design, Automation and Test in Europe Conference and Exhibition, 2004. Proceedings*, vol. 1, IEEE, 2004, pp. 272–277.

[15] João P Marques-Silva, Karem A Sakallah: *GRASP: A search algorithm for propositional satisfiability*, in: *Computers, IEEE Transactions on* 48.5 (1999), pp. 506–521.

[16] Alfred J Menezes, Paul C Van Oorschot, Scott A Vanstone: *Handbook of applied cryptography*, CRC press, 2010.

[17] Ralph Charles Merkle: *Secrecy, authentication, and public key systems.* In: (1979).

[18] Ilya Mironov, Lintao Zhang: *Applications of SAT solvers to cryptanalysis of hash functions*, in: *Theory and Applications of Satisfiability Testing-SAT 2006*, Springer, 2006, pp. 102–115.

[19] Paweł Morawiecki, Marian Srebrny: *A SAT-based preimage analysis of reduced KECCAK hash functions*, in: *Information Processing Letters* 113.10 (2013), pp. 392–397.

[20] Vegard Nossum: *SAT-based preimage attacks on SHA-1*, in: (2012).

[21] Constantinos Patsakis: *RSA private key reconstruction from random bits using SAT solvers.* In: *IACR Cryptology ePrint Archive* 2013 (2013), p. 26.

[22] Bruce Schneier: *Applied cryptography: protocols, algorithms, and source code in C*, john wiley & sons, 2007.

[23] Mate Soos, Karsten Nohl, Claude Castelluccia: *Extending SAT solvers to cryptographic problems*, in: *Theory and Applications of Satisfiability Testing-SAT 2009*, Springer, 2009, pp. 244–257.

[24] Martin Stanek: *Základy kryptológie*, Lecture Notes, 2004.

[25] Grigori S Tseitin: *On the complexity of derivation in propositional calculus*, in: *Automation of Reasoning*, Springer, 1983, pp. 466–483.