A Comparative Study of the TEA[1], XTEA[2], PRESENT[3] and Simon[4] lightweight cryptographic schemes

Paul E.A. Adriaanse, Miray Ayşen**, Zekeriya Erkin****
Cyber Security Group, Department of Intelligent Systems
Delft University of Technology

1. Background

- 25 billion IoT devices projected to grow to 60 billion.[5]
- Many IoT devices have constrained capabilities preventing the use of complex cryptography schemes.
- Compromised devices can pose a threat to both the privacy and physical safety of users.
- Lightweight cryptography schemes have been developed to provide security in these constrained environments.

2. Terminology

ASIC: Application Specific Integrated Circuit.
Gate Equivalents (GE): Unit of area equivalent to the size of the smallest NAND gate in the implementation architecture.
Equivalent Keys: Keys that yield identical encryptions.

3. Research Aim

By doing a literary study:

- **Find how TEA, XTEA, PRESENT & Simon compare.**
  - What vulnerabilities do the schemes have?
  - How do ASIC implementations perform?
- **Find which schemes are better suited for use in constrained devices.**

4. Results

TEA:

- All key have 3 equivalent keys, making TEA unfit for use in hashing.[8]
- Reported vulnerable to related-key attacks.[9]

PRESENT:

- Several attacks reported.[10, 11]

XTEA:

- Attacks only reported on reduced versions.[12, 13, 14]
- Area too large for use in constrained devices.[15]

Simon:

- Attacks only reported on reduced version. [16, 17]

Table 1. Summarized comparison of best performing implementations.

Scheme	Area (GE)	Throughput (kbps)	Power (µW)	Energy per bit (pJ/bit)
XTEA[6]	3490	200	61	305
PRESENT-80[3]	1570	200	5	10
Simon64/128[7]	944	4,2	0,762	181,4
Simon64/128[7]	1403	133,3	1,239	9,295

5. Conclusion

- TEA and PRESENT are possibly unsuitable due to their vulnerabilities.
- XTEA is unsuitable due its required implementation area.
- Simon provides flexible & acceptable performance while no problematic vulnerabilities are known.

References

[1] Wheeler, D. J., & Needham, R. M. (1994). Tea, a tiny encryption algorithm. In *International workshop on fast software encryption* (pp. 363–366).
[2] Wheeler, D. J., & Needham, R. M. (1998). Correction to xtea. *Unpublished manuscript, Computer Laboratory, Cambridge University, England*, 1(2), 17.
[3] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., . . .Vikkelsoe, C. (2007). Present: An ultra-lightweight block cipher. In P. Paillier & I. Verbauwhede(Eds.), *Cryptographic hardware and embedded systems - ches 2007* (pp. 450–466). Berlin, Heidelberg: Springer Berlin Heidelberg.
[4] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2013). *The simon and speck families of lightweight block ciphers.* Cryptology ePrint Archive, Report 2013/404. (https://eprint.iacr.org/2013/404)
[5] Balaji, S., Nathani, K., & Santhakumar, R. (2019). IoT Technology, Applications and Challenges:A Contemporary Survey. *Wireless Personal Communications, 108*(1), 363–388. Retrieved from https://doi.org/10.1007/s11277-019-06407-w doi: 10.1007/s11277-019-06407-w
[6] Kitsos, P., Sklavos, N., Parousi, M., & Skodras, A. N. (2012). A comparative study of hardware architectures for lightweight block ciphers. *Computers Electrical Engineering*, 38(1), 148-160. Retrieved from https://www.sciencedirect.com/science/article/pii/S0045790611001984 (Special issue on New Trends in Signal Processing and Biomedical Engineering) doi: https://doi.org/10.1016/j.compeleceng.2011.11.022
[7] Yang, G., Zhu, B., Suder, V., Aagaard, M., & Gong, G. (2015). The simeck family of lightweight block ciphers. *IACR Cryptol. ePrint Arch., 2015*, 612.
[8] Andem, V. R. (2003). *A cryptanalysis of the tiny encryption algorithm* (Unpublished doctoral dissertation). University of Alabama.
[9] Kelsey, J., Schneier, B., & Wagner, D. (1997). Related-key cryptanalysis of 3-way, biham-des,cast,des-x, newdes, rc2, and tea. In Y. Han, T. Okamoto, & S. Qing (Eds.), *Information and communications security* (pp. 233–246). Berlin, Heidelberg: Springer Berlin Heidelberg.
[10] Faghihi Sereshgi, M. H., Dakhilalian, M., & Shakiba, M. (2016). Biclique cryptanalysis of MIBS-80 and PRESENT-80 block ciphers. *Security and Communication Networks*, 9(1), 27-33.
[11] Lee, C. (2014). Biclique cryptanalysis of present-80 and present-128.*The Journal of Supercomputing, 70*(1), 95–103.
[12] Ko, Y., Hong, S., Lee, W., Lee, S., & Kang, J. S. (2004). Related key differential attacks on 27 rounds of XTEA and full-round GOST. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3017*, 299–316. doi:10.1007/978-3-540-25937-4_19
[13] Isobe, T., & Shibutani, K. (2012). Security analysis of the lightweight block ciphers xtea, led and piccolo. In W. Susilo, Y. Mu, & J. Seberry (Eds.), *Information security and privacy* (pp. 71–86). Berlin, Heidelberg: Springer Berlin Heidelberg.
[14] Lu, J. (2009). Related-key rectangle attack on 36 rounds of the xtea block cipher. *International Journal of Information Security, 8*(1), 1–11. doi: 10.1007/s10207-008-0059-9
[15] Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018, Jun 01). A review of lightweight block ciphers. *Journal of Cryptographic Engineering, 8*(2), 141-184. Retrieved from https://doi.org/10.1007/s13389-017-0160-y doi: 10.1007/s13389-017-0160-y
[16] Alkhzaimi, H., & Lauridsen, M. M. (2013). Cryptanalysis of the simon family of block ciphers.IACR Cryptol. ePrint *Arch.,2013*, 543.
[17] Chen, H., & Wang, X. (2016). Improved linear hull attack on round-reduced simon with dynamic key-guessing techniques. In T. Peyrin (Ed.),*Fast software encryption* (pp. 428–449). Berlin,Heidelberg: Springer Berlin Heidelberg.

TU Delft

July 2nd 2021

Paper: http://resolver.tudelft.nl/uuid:5acf8b8e-524e-4918-b378-65fb130e744f

Contact: *P.E.A.Adriaanse@student.tudelft.nl | **M.Aysen@tudelft.nl | ***Z.Erkin@tudelft.nl