A COMPARATIVE STUDY ON SIGNATURE SCHEMES FOR IOT DEVICES

Dan Dan Berendsen, Miray Ayşen, Dr. Zekeriya Erkin
Cyber security group, Department of Intelligent Systems, Delft University of Technology
d.d.j.z.berendsen@tudelft.nl

1. Motivation

- 8.74 billion Internet of things (IoT) devices [1]
- Used in hospitals, transport and houses, thus containing sensitive data
- Personal identifiable information
- IoT device authentication/ identification for secure communication = signature schemes
- Authentication and message integrity
- Small hardware area, less computational power and space

2. Research question

How do IoT signature schemes compare in performance to each other and what is a possible improvement?

- What is the current state of signature schemes in IoT?
- Comparison between schemes
- Suitability for IoT
- What are the shortcomings of the current schemes?
- **How could these flaws be solved**

3. Method

- Literature study
- Find flaws and suggest improvement

4. Comparison criteria

The schemes are compared on these scheme characteristics.

- Key size & signature size
- Computation costs
- Security level

5. Results

Table 1. Security level and their RSA, DSA and ECC key sizes in bits [28]

Security level	RSA key size	DSA key size	ECC key size
80	1024	p=1024, q=160	160-223
112	2048	p=2048, q=224	224-255
128	3072	p=3072, q=256	256-383
192	7680	p=7680, q=384	384-511
256	15360	p=15360, q=512	>512

Table 2. Signature sizes in bits for security level 80.

RSA	SCDSA	ECC CLS
1024	320	328

- Breakable by Shor's algorithm [5] in the future
- Quantum computing resistant schemes

Table 3. W-OTS schemes comparison [6][7][8]

Scheme	w	signature size	Signing cost	Security level
W-OTS+	128	21	992	1,302s	113*
W-OTS	256	455	992	14,105	128
W-OTS^{prf}	128	8	1440	0,720s	100

- SCDSA [3], ECC CLS [4] suitable candidates.
- W-OTS variants, XMSS [9] as suitable candidates

6. Conclusion

- SCDSA, ECC CLS currently suitable
- Future proof
- Post-quantum
- W-OTS+, XMSS

7. Future Work

- Hybrid schemes
- Other security reduction

[1] Statista. (2021).*Number of Internet of Things (IoT) connected de-vices worldwide from 2019 to 2030* .Retrieved 2021-04-23,from https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
[2] Barker, E. (2016-01-28). NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management: General (PDF). *National Institute of Standards and Technology*: 53. doi:10.6028/NIST.SP.800-57pt1r4.
[3] M. A. Mughal, X. Luo, A. Ullah, S. Ullah and Z. Mahmood, A Lightweight DigitalSignature Based Security Scheme for Human-Centered Internet of Things, in *IEEE Access*, vol. 6, pp. 31630-31643, 2018, doi: 10.1109/ACCESS.2018.2844406
[4] Du, H., Wen, Q., Zhang, S., Gao, M., A new provably secure certificateless signature scheme for Internet of Things, *Ad Hoc Networks*, Volume 100, 2020, 102074, ISSN 1570-8705, doi:10.1016/j.adhoc.2020.102074.
[5] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-
[6] Dods, C., Smart, N. P., Stam, M. (2005, December). Hash based digital signatureschemes. In IMA International Conference on Cryptography and Coding(pp. 96-115). Springer, Berlin, Heidelberg.
[7] Buchmann, Johannes Dahmen, Erik Ereth, Sarah Hülsing, Andreas Rückert, Markus.(2011). On the Security of the Winternitz One-Time Signature Scheme . *International Journal of Applied Cryptography*. 3. 363-378. 10.1007/978-3-642-21969-6_23.
[8] Hülsing, A. T. (2013). W-OTS+ - shorter signatures for hash-based signatureschemes. In A. Youssef, A. Nitaj, A. E. Hassanien (Eds.), *Progress in Cryptolo-gyâAFRICACRYPT 2013: 6th International Conference on Cryptology in Africa*, Cairo,Egypt, June 22-24, 2013. Proceedings (pp. 173-188). (Lecture Notes in Computer Science(LNSC); Vol. 7918). Springer. https://doi.org/10.1007/978-3-642-38553-7_10
[9] Buchmann, J., Dahmen, E., HÃŒlsing, A. (2011, November). XMSS-a practical forward secure signature scheme based on minimal security assumptions. In *International Workshop on Post-Quantum Cryptography*(pp. 117-129). Springer, Berlin, Heidelberg.