On the (in)Security of ChaCha20 against Physical Attacks

Shivam Bhasin

Temasek Labortaries, Nanyang Technological University Singapore,
sbhasin@ntu.edu.sg

The stream cipher ChaCha20 and the Poly1305 authentication are adopted in several products including Google Chrome [1], or OpenSSL [2] etc. For instance, Google Chome often uses ChaCha20 for secure communication when the underlying platform lacks hardware support for AES. The two algorithms have potential to be adopted across multiple domains in the future. The ChaCha20-Poly1305 cipher suite is advertised as being easier to implement in a side-channel resistant way [3], especially compared to ciphers based on substitution permutation networks. However, the side-channel security claim is only limited to timing based leakage. In this talk, we investigate the security of ChaCha20 against two commonly known physical attacks: *side-channel attacks* and *fault attacks*.

The first part focuses on power [4] or electromagnetic [5] based side-channels. The development of the omnipresent Internet of Things (IoT), or the connected car increases the amount of embedded appliances, which can be attacked using these side-channels. Hence, it is important to understand the security of deployed cryptographic algorithms not only against attacks on the timing side-channels but a wider attack suite. We analyze the stream cipher ChaCha20 [3, 6] and show how the secret key can be completely extracted. While first attack recovers the key from initial round of ChaCha20, another attack demonstrates key retrieval exploiting the final addition.

The second part will look into active attacks realised using fault injection [7]. Often stream ciphers are believed to be harder to attack against fault injection attacks owing to the complexity of the required offline analysis. We propose four differential fault analysis (DFA) attacks on ChaCha20 running on a low cost microcontroller, using the instruction skip and instruction replacement fault models. The attacks target the keystream generation module at the decryption site, and entirely avoid nonce misuse. We practically demonstrate our proposed attacks using a laser fault injection setup.

The talk is based on recent joint works. The part on side-channel attack is based on recent work with Bernhard Jungk from NTU, Singapore [8]. Fault attacks was investigated with co-authors from IIT Kharagpur, India and NTU, Singapore [9].

References

1. Bursztein, E.: Speeding up and strengthening HTTPS connections for Chrome on Android (2014) https://security.googleblog.com/2014/04/speeding-up-and-strengthening-https.html.

2. Staruch, M.: Support for ChaCha20-Poly1305 (2015) https://github.com/openssl/openssl/issues/304.
3. Nir, Y., Langley, A.: ChaCha20 and Poly1305 for IETF Protocols. IETF RFC 7539 (2015)
4. Kocher, P., Jaffe, J., Jun, B.: Differential Power Analysis. In: Annual International Cryptology Conference, Springer (1999) 388–397
5. Agrawal, D., Archambeault, B., Rao, J.R., Rohatgi, P.: The EM Side—Channel(s). In: International Workshop on Cryptographic Hardware and Embedded Systems, Springer (2002) 29–45
6. Bernstein, D.J.: ChaCha, a variant of Salsa20. In: Workshop Record of SASC - The State of the Art of Stream Ciphers. (2008)
7. Barenghi, A., Breveglieri, L., Koren, I., Naccache, D.: Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. Proceedings of the IEEE **100** (2012) 3056–3076
8. Jungk, B., Bhasin, S.: Don't fall into a trap: Physical side-channel analysis of chacha20-poly1305. In: 2017 Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE (2017) 1110–1115
9. Kumar, S.D., Patranabis, S., Breier, J., Mukhopadhyay, D., Bhasin, S., Chattopadhyay, A., Baksi, A.: A practical fault attack on arx-like ciphers with a case study on chacha20. In: Fault Diagnosis and Tolerance in Cryptography (FDTC), 2017 Workshop on, IEEE (2017)