Spook: Updates on the Round-2 Submission

Davide Bellizia[*], Francesco Berti[*], Olivier Bronchain[*], Gaëtan Cassiers[*], Sébastien Duval[*], Chun Guo[*], Gregor Leander[†], Gaëtan Leurent[‡], Itamar Levi[*], Charles Momin[*], Olivier Pereira[*], Thomas Peters[*], François-Xavier Standaert[*], Balazs Udvarhelyi[*], Friedrich Wiemer[†].

September 18, 2020.
URL: https://www.spook.dev/

Abstract

We detail updates of the Spook candidate to the NIST lightweight cryptography competition. Among others, we discuss new leakage-resistance proofs under weaker assumptions, new implementation results (both in software and hardware, unprotected and protected against side-channel analysis), and we propose a tweak in order to increase Spook's security margins without affecting its performances. We also list platforms and metrics for which the candidate should perform better than current standards, together with target use cases for which it is optimized.

1 New proofs/arguments supporting the security claims

Spook is an authenticated encryption algorithm aimed at lightweight implementations, with a specific focus on security against side-channel attacks at low energy cost. The main advances we made since the round-2 submission in terms of security proofs and arguments are:

- Protected implementations of Spook can leverage the "leveling" concept, where various parts of the implementation have various levels of security against side-channel attacks. More precisely, Spook offers strong guarantees of integrity and confidentiality against leakage (see Section 4) given that the tweakable block cipher Clyde used for (ephemeral) key generation and tag generation is strongly protected against Differential Power Analysis (DPA), while the bulk of the computation (i.e., the Shadow permutation) requires much weaker protections or even no protections at all. In the initial analysis of the TETSponge mode of operation Spook relies on, the strongly protected tweakable block cipher was modeled as leak-free [GPPS20]. We show in [BBB$^+$20] that, for the integrity guarantees that are at the core Spook's leakage security claims, it can be relaxed into a weaker unpredictability with leakage assumption.

- In addition, we witnessed and extended continuous efforts in improving the security guarantees offered by masked implementations that would be the default option to implement the strongly protected Clyde tweakable block cipher. For software, our current designs are based on state-of-the-art proposals by third parties (e.g., [GR17, BGR18]). For hardware, we advanced the state-of-the-art in glitch-resistant masking in a work to appear in IEEE Transactions on Computers [CGLS20]. The Hardware Private Circuits presented in this paper offer strong composability guarantees in the presence of physical defaults at limited implementation cost, and these guarantees can additionally be verified at arbitrary orders for full circuits.

[*] ICTEAM Institute, Université catholique de Louvain, Louvain-la-Neuve, Belgium.
[†] Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany.
[‡] Team COSMIQ , Inria Paris Research Center, France.

Besides, we mention the consolidating effort recently published at Crypto 2020 [BBC+20], which discusses the combinations of mode-level and implementation-level physical security features that Spook (and other lightweight ciphers) leverage(s), and extends the talk "*Analyzing the Leakage-Resistance of some Round-2 Candidates of the NIST's Lightweight Crypto Standardization Process*", which was given during the Lightweight Crypto Workshop, in November 2019. It provides a quantified view of the energy gains that leveled implementations enable (in Section 4.1).

2 New software and hardware implementations

Extending the implementation results of our submission, Spook now comes with:

- Optimized unprotected hardware implementations. The latest results are submitted to SILC 2021 [MCS] and have been sent to the GMU benchmarking initiative[1]. These results (available on the Spook website) are already for the tweaked version discussed in Section 6. Preliminary results showing that the use of two resource-sharing primitives (i.e., Shadow and Clyde) only leads to very limited performance overheads can also be found in [BBB+20].

- Protected (leveled) hardware implementations based on the Hardware Private Circuits approach in order to mask the Clyde tweakable block cipher. Those are available on the Spook website, are described in the aforementioned submission to SILC 2021 [MCS], and are the basis of an ongoing side-channel cryptanalysis challenge (see Section 3 for the details).

- Optimized unprotected software implementations for embedded (e.g., ARM Cortex-M) and high-end (e.g., x86_64) platforms (both available on the Spook website).

- Protected (leveled) software implementations (available on the Spook website), which have served as a basis for the CHES 2020 Capture the Flag – see Section 3 for the details – and are based on the results of [GR17, BGR18] to mask the Clyde tweakable block cipher.

We note that unprotected software implementation results for Spook are also available in third-party evaluations. For embedded microcontrollers, we refer to Rhys Weatherley's webpage[2] and the NIST LWC Software Performance Benchmarks on Microcontroller[3]. For higher-end devices we refer to Supercop[4]. These various results confirm that Spook performs very well in this context, especially in 32-bit devices, even if unprotected implementations are not its primary use case.

We note also that externally-developed masked software implementations start to be available as well. Our preferred reference for this purpose is the TORNADO framework from Eurocrypt 2020, which comes with the verification of minimum (probing) security guarantees [BDM+20]. These results show that Clyde is the best in class among the analyzed ciphers. (see https://www.youtube.com/watch?v=XJeg-cyqQtg at 18:35). Rhys Weatherley's webpage provides additional results.

3 New third-party analysis and implications

In terms of mathematical cryptanalysis, the most relevant work is the one by Derbez et al., recently presented at Crypto 2020, which analyzes the Shadow permutation [DHL+20]. Its main results are a distinguisher against the full permutation and a collision attack against a reduced-round version,

[1] https://cryptography.gmu.edu/athena/.

[2] https://rweather.github.io/lightweight-crypto/index.html.

[3] https://lwc.las3.de/.

[4] https://bench.cr.yp.to/primitives-aead.html.

which can lead to forgeries against (reduced) Spook in the nonce-misuse setting. As mentioned by the authors of [DHL+20], neither the distinguisher nor the collision attack threaten the confidentiality or integrity of the full Spook (which does not rely on a hermetic sponge strategy). See [BBB+20] for a discussion. However, the collision attack highlights that the heuristic used to select the number of rounds of Shadow is not conservative. Constructive discussions with Derbez et al. led us to consider tweaks in order to improve security margins against this attack more efficiently than by simply increasing the number of rounds, which is discussed in more detail in Section 6.

In terms of side-channel cryptanalysis, the most relevant results come from a side-channel cryptanalysis challenge that served as the CHES 2020 Capture the Flag: https://ctf.spook.dev/. The winning team (evaluators from the German BSI) launched advanced attacks against the embedded software targets with 3, 4, 6 and 8 shares. Results confirm the difficulty to reach high security levels in such low-noise devices with limited number of shares. Yet, they also highlight that the exponential security amplification of masking takes place. The best attack complexities are 25, 200, 4000 and 70,000 traces for 3, 4, 6 and 8 shares, respectively. We insist that these targets were not selected to optimize the security vs. performance tradeoff but to enable an interesting challenge where advanced attack techniques can be demonstrated. Improving this security vs. performance tradeoff is an important direction for further research. Yet, these results and the high cost of masked implementations already justifies the relevance of the leveled implementation concept.

Regarding the hardware targets, implementations of Clyde based on the Hardware Private Circuits approach using 2, 3 and 4 shares are still proposed in an ongoing challenge.

4 Goals and target applications

Spook aims to improve over existing standards in two main cases: (*i*) implementations in embedded microcontrollers, 32-bit typically, with good resistance against side-channel attacks at limited energy cost, and (*ii*) hardware implementations with excellent resistance against side-channel attacks at limited energy cost. Besides, it also aims at (*iii*) being competitive (in terms of standard performance metrics) in contexts and applications where side-channel attacks are not a concern.

We believe these goals, and the design choices made for the Spook mode of operation and its components match the requirements of lightweight cryptography for the following reasons.

Regarding the leakage-resistance of the mode, our first focus is on integrity guarantees. An example of motivation is the secure software update mentioned during the "*Lightweight Trusted Computing*" presentation of the NIST Lightweight Cryptography Workshop 2019[5]. In this context, integrity guarantees have to hold with both encryption and decryption leakages, which has been formalized as Ciphertext Integrity with nonce Misuse-resistance and Leakage in encryption and decryption (CIML2) [BPPS17]. Leveled implementations of Spook are CIML2-secure by only protecting the Clyde tweakable block cipher against side-channel analysis and letting all the other parts of the computation leak in an unbounded manner. As already mentioned, such leveled implementations enable significant energy gains. Furthermore, this CIML2 security holds with beyond-birthday bounds. Concretely, while unbounded leakages may only be obtained by determined adversaries in certain contexts (e.g., [KPP20] or [BBC+20], Section 4.4), beyond-birthday security ensures that even such powerful attacks against the ephemeral states of Spook will not lead to forgeries with less than $2^{n-\log(n)}$ (offline) time complexity. We therefore use it as a solid justification for the strong integrity offered by the efficient leveled implementations we promote.

[5] https://csrc.nist.gov/Events/2019/Lightweight-Cryptography-Workshop-2019.

Spook also provides the best confidentiality guarantees that can be obtained for a one-pass online mode, which is CCA security with misuse-resilience and Leakage in encryption (CCAmL1) [BBC+20]. Confidentiality in the presence of leakage is for example motivated by medical applications (mentioned during the "*Update on NIST Lightweight Cryptography Standardization*" presented in November 2019 and linked in Footnote 5), where sensitive data may be manipulated. Such guarantees are particularly relevant to mitigate emerging (remote) attack vectors such as screaming channels [CPM+18], when attacking the long-term key is hard and targeting the ephemeral secrets may be the best option [CFS20]. In this respect, it is worth observing that given the state size that enables beyond-birthday CIML2 security, adding an ephemeral key evolution mechanism to improve confidentiality guarantees (e.g., thanks to a sponge design) comes almost for free. Concretely, it ensures that confidentiality in encryption is maintained as long as the processing of the message blocks resists Simple Power Analysis (SPA) attacks. Besides, the combination of CCAmL1 with CIML2 ensures that any attack against the confidentiality of Spook will only have "local" impact (i.e., affect the confidentiality of some messages, encrypted with the targeted ephemeral secret).

Regarding the Shadow and Clyde components, their selection (and the use of two primitives) takes advantage of some additional tweaks that the literature on side-channel attacks and countermeasures provides. In particular, the use of two primitives allows an interesting separation of duties. On the one hand, only the tweakable block cipher used for the key & tag generation has to be strongly protected against side-channel attacks and its smaller state size is convenient for this purpose (it reduces the AND complexity which is beneficial for masking – see [BDM+20] and [BBC+20], Section 4.2). Using a tweakable block cipher for the tag generation also makes it possible to verify the validity of a tag without the need to compute it (and therefore to tolerate unbounded leakages for this part of the computation). On the other hand, the permutation allows a very efficient processing of the message blocks with weaker requirements for side-channel security.

Eventually, Spook provides excellent performances when side-channel attacks are not a concern. First, the use of shared components between Shadow and Clyde makes the cost of an unprotected Spook nearly identical to the cost of Shadow. In other words, the overheads over a standard sponge design are limited in this context. Second, the use of implementation-based countermeasures for the key and tag generation enables canceling their overheads when not required by an application, or if only one (e.g., encryption) party requires such protections (see [BBC+20], Section 4.4).

We mention that all the security guarantees of Spook come with an optional multi-user flavor (thanks to an optional public key) that is in general relevant for IoT applications. We also mention that the mode of operation of Spook is compatible with solutions for the encryption of long messages segmented into several smaller packets such as SpookChain [CGP+19]. This "session feature" can be used as a partial tagging mechanism which allows decrypting multi-round conversations when only a limited memory is available, and saves the execution of one tweakable block cipher per segment (i.e., the highly protected and more expensive part in a leveled implementation). It is for example relevant in an IoT context where a sensor would send one measurement per minute or less.

5 Target platforms & metrics for which Spook performs well

The typical platforms for Spook are 32-bit embedded microcontrollers and hardware/FPGA implementations. In both cases, the primary metric is the energy per byte. In software, such a metric is strongly correlated with the cycle count [EGG+12]. In software and hardware, the most significant gains are expected to be observed when high security against (ideally) worst-case side-channel attacks has to be provided (e.g., following the discussion in [BS20]). Such gains can reach significant factors in case of long messages for which the amortization that leveling enables best plays its role. But as shown in [BBC+20] (Section 4.1), short messages (e.g., a few blocks long) already bring benefits and the overheads for single-block messages (over simpler modes like OCB) are small. Besides, as shown by the results of Section 2, Spook also behaves well in unprotected settings.

6 Planned tweak proposals

Following discussions with Derbez et al., we analyzed tweaks that would improve the security margins of Spook against the collision attack of Crypto 2020 against a reduced-round Shadow [DHL+20]. It turns out that changing the D (diffusion) layer used once every two rounds in Shadow, and making it MDS, increases such margins more efficiently than increasing the number of rounds. It also mitigates the similarity properties that the attack exploits more structurally. Combined with other light tweaks for the round constants of Spook, it is shown in [BBB+20] that the corresponding Spook v2 reaches nearly identical performance levels as Spook v1. In case Spook is accepted as a finalist, Spook v2 would therefore be our candidate. Note that all the ongoing side-channel cryptanalysis and benchmarking efforts outlined in this note are already for Spook v2.

Acknowledgments. Gaëtan Cassiers, Thomas Peters and François-Xavier Standaert are respectively research fellow, research associate and senior research associate of the Belgian Fund for Scientific Research (FNRS-F.R.S.). This work has been funded in part by EU and the Walloon Region through the ERC Project 724725 (SWORD), the FEDER Project USERMedia (convention 501907-379156), the Wallinov TRUSTEYE project and the Win2Wal project PIRATE.

References

[BBB+20] Davide Bellizia, Francesco Berti, Olivier Bronchain, Gaëtan Cassiers, Sébastien Duval, Chun Guo, Gregor Leander, Gaëtan Leurent, Itamar Levi, Charles Momin, Olivier Pereira, Thomas Peters, François-Xavier Standaert, Balazs Udvarhelyi, and Friedrich Wiemer. Spook: Sponge-based leakage-resistant authenticated encryption with a masked tweakable block cipher. *IACR Trans. Symmetric Cryptol.*, 2020(S1):295–349, 2020.

[BBC+20] Davide Bellizia, Olivier Bronchain, Gaëtan Cassiers, Vincent Grosso, Chun Guo, Charles Momin, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Mode-level vs. implementation-level physical security in symmetric cryptography - A practical guide through the leakage-resistance jungle. In *CRYPTO (1)*, volume 12170 of *Lecture Notes in Computer Science*, pages 369–400. Springer, 2020.

[BDM+20] Sonia Belaïd, Pierre-Évariste Dagand, Darius Mercadier, Matthieu Rivain, and Raphaël Wintersdorff. Tornado: Automatic generation of probing-secure masked bitsliced implementations. In *EUROCRYPT (3)*, volume 12107 of *Lecture Notes in Computer Science*, pages 311–341. Springer, 2020.

[BGR18] Sonia Belaïd, Dahmun Goudarzi, and Matthieu Rivain. Tight private circuits: Achieving probing security with the least refreshing. In *ASIACRYPT (2)*, volume 11273 of *Lecture Notes in Computer Science*, pages 343–372. Springer, 2018.

[BPPS17] Francesco Berti, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. On Leakage-Resilient Authenticated Encryption with Decryption Leakages. *IACR Trans. Symmetric Cryptol.*, 2017(3):271–293, 2017.

[BS20] Olivier Bronchain and François-Xavier Standaert. Side-channel countermeasures' dissection and the limits of closed source security evaluations. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(2):1–25, 2020.

[CFS20] Giovanni Camurati, Aurélien Francillon, and François-Xavier Standaert. Understanding screaming channels: From a detailed analysis to improved attacks. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(3):358–401, 2020.

[CGLS20] Gaëtan Cassiers, Benjamin Grégoire, Itamar Levi, and François-Xavier Standaert. Hardware private circuits: From trivial composition to full verification. *IACR Cryptol. ePrint Arch.*, 2020:185, 2020.

[CGP$^+$19] Gaëtan Cassiers, Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Spookchain: Chaining a sponge-based AEAD with beyond-birthday security. In *SPACE*, volume 11947 of *Lecture Notes in Computer Science*, pages 67–85. Springer, 2019.

[CPM$^+$18] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. Screaming channels: When electromagnetic side channels meet radio transceivers. In *ACM Conference on Computer and Communications Security*, pages 163–177. ACM, 2018.

[DHL$^+$20] Patrick Derbez, Paul Huynh, Virginie Lallemand, María Naya-Plasencia, Léo Perrin, and André Schrottenloher. Cryptanalysis results on spook - bringing full-round shadow-512 to the light. In *CRYPTO (3)*, volume 12172 of *Lecture Notes in Computer Science*, pages 359–388. Springer, 2020.

[EGG$^+$12] Thomas Eisenbarth, Zheng Gong, Tim Güneysu, Stefan Heyse, Sebastiaan Indesteege, Stéphanie Kerckhof, François Koeune, Tomislav Nad, Thomas Plos, Francesco Regazzoni, François-Xavier Standaert, and Loïc van Oldeneel tot Oldenzeel. Compact implementation and performance evaluation of block ciphers in attiny devices. In *AFRICACRYPT*, volume 7374 of *Lecture Notes in Computer Science*, pages 172–187. Springer, 2012.

[GPPS20] Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Towards low-energy leakage-resistant authenticated encryption from the duplex sponge construction. *IACR Trans. Symmetric Cryptol.*, 2020(1):6–42, 2020.

[GR17] Dahmun Goudarzi and Matthieu Rivain. How Fast Can Higher-Order Masking Be in Software? In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *LNCS*, pages 567–597, 2017.

[KPP20] Matthias J. Kannwischer, Peter Pessl, and Robert Primas. Single-trace attacks on keccak. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(3):243–268, 2020.

[MCS] Charles Momin, Gaëtan Cassiers, and François-Xavier Standaert. Unprotected and masked hardware implementations of spook v2. *Submission to SILC 2021.*