NISTIR 8268

Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry A. McKay
Çağdaş Çalık
Donghoon Chang
Larry Bassham

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8268

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8268

Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process

Meltem Sönmez Turan
Kerry A. McKay
Çağdaş Çalık
Donghoon Chang
Larry Bassham

Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8268

October 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Internal Report 8268
19 pages (October 2019)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8268

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: lightweight-crypto@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

The National Institute of Standards and Technology (NIST) is in the process of selecting one or more authenticated encryption and hashing schemes suitable for constrained environments through a public, competition-like process. In February 2019, 57 candidate algorithms were submitted to NIST for consideration. Among these, 56 were accepted as first-round candidates in April 2019, marking the beginning of the first round of the NIST Lightweight Cryptography Standardization Process. Due to the large number of submissions and the short timeline of the process, NIST has decided to eliminate some of the algorithms from consideration early in the first evaluation phase in order to focus analysis on the more promising submissions. This report describes the evaluation criteria and selection process based on public feedback and internal review of the first-round candidates and provides the list of 32 candidate algorithms selected for the second round of the evaluation process.

Keywords

authenticated encryption; cryptography; hash functions; lightweight cryptography.

Supplemental Content

The NIST Lightweight Cryptography Standardization Process webpage is available at:

https://csrc.nist.gov/projects/lightweight-cryptography

To join the lwc-forum@list.nist.gov email list, mailto:lwc-forum+subscribe@list.nist.gov.

Acknowledgments

NIST is grateful for the efforts of all the submission teams who developed, designed, and analyzed lightweight cryptography submission packages. The cryptographic community's response of 57 candidate algorithms submitted to the standardization process was very encouraging.

The success of the NIST Lightweight Crypto Standardization Process relies on the efforts of the researchers from the cryptographic community that provide security, implementation, and performance analysis of the candidate algorithms. NIST thanks the cryptographic community that has analyzed the proposals and shared their comments through the forum or published papers on various technical aspects of the candidates.

The authors of this internal report acknowledge and appreciate contributions by their colleagues at NIST: Lily Chen, Andrew Regenscheid, Ray Perlner, Dustin Moody, Luís Brandão, Craig Kenney, Richard Williams Jr., John Kelsey, Jacob Alperin-Sheriff, Yi-Kai Liu, and Sara Kerman who reviewed candidate algorithms and public comments, provided technical and administrative support, and participated in meetings to discuss the selection of the second-round candidates.

Table of Contents

1 Introduction 1
2 Evaluation Criteria and Selection Process 3
2.1 Acceptance of the First-round Candidates 3
2.2 Selection of the Second-round Candidates 3
2.2.1 Maturity of the Candidates 3
2.2.2 Cryptanalysis of the Candidates 5
3 Next Steps 8
References 9

1 Introduction

The National Institute of Standards and Technology (NIST) has initiated the Lightweight Cryptography (LWC) standardization process to solicit, evaluate, and standardize lightweight cryptographic algorithms that are suitable to be used in constrained environments (e.g., radio frequency identification, sensor networks) where the performance of current NIST cryptographic standards is not acceptable. The initial focus is on symmetric cryptography, and one or more authenticated encryption and hashing schemes are expected to be selected through a public, competition-like process.

In July 2015, NIST held the First Lightweight Cryptography Workshop to get public feedback on the constraints and limitations of the target devices and requirements and characteristics of existing and emerging applications of lightweight cryptography. A second workshop was held in October 2016. In March 2017, NIST published NISTIR 8114, *Report on Lightweight Cryptography* [19] and announced that it has decided to create a portfolio of lightweight algorithms through an open, competition-like process. In April 2017, NIST published the draft whitepaper *Profiles for the Lightweight Cryptography Standardization Process* [6] to solicit feedback on proposed functionalities for initial inclusion in the portfolio.

In May 2018, NIST published Federal Register Notice [1], referring to the draft *Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process,* for public comment. The requirements and evaluation criteria were updated based on public feedback. In August 2018, NIST published Federal Register Notice [2], announcing the final *Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process* and calling for nominations of cryptographic algorithms that provide authenticated encryption with associated data (AEAD) and optional hashing functionalities.

The LWC submission process included an optional early-review process that aimed to increase the quality of submissions. NIST provided feedback to eight submissions that were received by January 4, 2019. By the February 25, 2019, submission deadline, NIST received 57 submission packages to be considered for standardization. The submission teams were allowed to amend their submission packages by March 29, 2019, to reduce the effects of the 35-day U.S. government shutdown when NIST was unable to review submissions or communicate with submitters. Among 57 submissions, 56 were accepted as first-round candidates in April 2019, marking the beginning of the first round of the NIST LWC Standardization Process. Submission packages of the first-round candidates were posted online at the NIST LWC project webpage [28] for public review.[1] The timeline of major events in the NIST LWC Standardization Process is given in Table 1.

The standardization process has benefited significantly from the knowledge gained during the CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) contest [7] that aimed to select algorithms that offer advantages over the Advanced Encryption Standard (AES) using the Galois/Counter Mode (GCM). Because of this, the timeline for

[1] NIST made minor updates to the submission packages to add accessibility features and to create a uniform directory structure across all submissions.

standardization is planned to be shorter than other similar processes (e.g., five-year Secure Hash Algorithm-3 (SHA-3) competition, four-year AES competition). Spreading limited resources across a large number of submissions reduces the quality of evaluations per submission. It also takes a significantly longer time to have reliable performance analysis for comparison. Hence, NIST has decided to shorten the duration of the first round of the process from 12 months to four months and to reduce the number of candidates from 56 to 32 in order to focus analysis on the more promising candidates. The second-round candidates were announced on August 30, 2019.

The purpose of this report is to provide a public record of the first round of the NIST LWC standardization process. This report describes the evaluation criteria and selection process based on public feedback and internal review of the first-round candidates, and summarizes the reasoning for the early elimination of 24 candidates.

Table 1 Timeline of the LWC Standardization Process

Date	Event
July 20-21, 2015	First Lightweight Cryptography Workshop at NIST
August 11, 2016	(Draft) NISTIR 8114 *Report on Lightweight Cryptography* [18] is published.
October 17-18, 2016	Second Lightweight Cryptography Workshop at NIST
March 28, 2017	NISTIR 8114 *Report on Lightweight Cryptography* [19] is published.
April 26, 2017	(Draft) *Profiles for Lightweight Cryptography Standardization Process* [6] is published.
May 14, 2018	*Federal Register Notice* [1] is published. (Draft) *Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process* [27] is published.
August 27, 2018	*Federal Register Notice* [2] is published. *Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process* [29] is published.
February 25, 2019	Submission deadline
March 29, 2019	Amendment deadline
April 18, 2019	Announcement of the first-round candidates [17]
August 30, 2019	Announcement of the second-round candidates [40]
November 4-6, 2019	Third Lightweight Cryptography Workshop

2 Evaluation Criteria and Selection Process

2.1 Acceptance of the First-round Candidates

After receiving 57 submissions to the standardization process, NIST researchers reviewed the submission packages for completeness and properness based on the requirements provided in [29]. These requirements can be summarized as:

- The submission packages shall include a cover sheet, algorithm specifications and supporting documentation, and intellectual property statements.
- The submissions shall meet the minimum acceptability requirements on algorithm specification, design rationale, security levels, limits on the message lengths, the number of variants, etc.
- The submission packages shall include portable reference software implementations in C for all members of the family that comply with the provided application program interface.

In April 26, 2019, NIST announced 56 submissions as first-round candidates as listed in Table 2.

2.2 Selection of the Second-round Candidates

The evaluation criteria for the standardization process were provided in the call for submissions [29]. The most important criterion of the process is the cryptographic security of the submissions. The implementation characteristics (in terms of performance and cost) of the submissions in constrained environments is another important criterion. The implementations of the candidates are also expected to lend themselves to countermeasures against side-channel attacks.

Selecting the second-round candidates was challenging due to the diversity of candidates in terms of their functionality, underlying components, design approaches, supported key and tag sizes, and features. Table 2 provides a classification of the first-round candidates based on their functionalities and underlying cryptographic components.

In this round of the project, there were two major selection criteria: maturity of the candidates, and cryptanalysis of the candidates.

2.2.1 Maturity of the Candidates

The submissions with significant third-party analysis or that based their security claims on well-understood design principles were favored for round 2 selection. However, submissions that used designs in such a way that existing analysis is no longer applicable were not considered as strong, nor were submissions that did not provide sufficient analysis to support security claims. NIST observed that the maturity levels of the first-round candidates varied significantly. The submissions that were removed from consideration only due to maturity are given below.

Fountain, Yarará and Coral. There was no public third-party security analysis on these designs prior to submission, and the security analysis within the submission package did not sufficiently support the security claims.

Table 2 Classification of first-round candidates based on their functionalities and underlying cryptographic components

Submissions with AEAD and Hashing Functionality	***Submissions with only AEAD Functionality***
Permutation based ACE ASCON CLX DryGASCON GAGE and InGAGE Gimli HERN and HERON KNOT ORANGE PHOTON-Beetle Shamash and Shamashash SIV-TEM-PHOTON SNEIK SPARKLE (SCHWAEMM and ESCH) Subterranean 2.0 Sycon Xoodyak Yarará and Coral *Block cipher based* Saturnin SIV-Rijndael *Tweakable block cipher based* SKINNY-AEAD and SKINNY-HASH *Stream cipher based* Triad	*Permutation based* CiliPadi Elephant Fountain ISAP Oribatida SPIX SpoC WAGE *Block cipher based* COMET FlexAEAD GIFT-COFB HyENA LAEM Limdolen mixFeed Pyjamask SAEAES Simple SUNDAE-GIFT TinyJAMBU TRIFLE *Tweakable block cipher based* ForkAE ESTATE Lilliput-AE LOTUS-AEAD, and LOCUS-AEAD Qameleon Remus Romulus Spook Thank Goodness It's Friday (TGIF) *Stream cipher based and others* Bleep64 CLAE Grain-128AEAD Quartet

Shamash and Shamashash. Although the security analysis of Shamash and Shamashash is claimed to rely on the analysis of ASCON, the specification of Shamash and Shamashash did not sufficiently address the security implications of the differences between the two designs.

2.2.2 Cryptanalysis of the Candidates

After the announcement of the first-round candidates, the candidates received various levels of third-party analysis. Table 3 summarizes the third-party analysis that raised security concerns during the first round of the process. The tweaks suggested by designers to eliminate the concerns were not considered during evaluation. Practical attacks (e.g., forgery attacks) due to implementation bugs were not considered to be a reason for elimination. NIST researchers checked implementation updates to verify that they were consistent with the original specifications. It should be noted that NIST did not publish the updated source codes for this round on the official project webpage but encouraged the teams to host websites for their submissions where corrected implementations, additional files, and documents related to their submission could be made available.

Table 3 Summary of attacks and observations on the first-round candidates

Attacks & Observations	***Candidates***
Forgery attacks	Bleep64 [5, 41], CLAE [38], FlexAEAD [11, 12], GAGE and InGAGE [4], HERN and HERON [21], Liliput-AE [9, 10], Limdolen [35, 36], Qameleon [13], Quartet [33], Remus [14], Simple [23], SIV-Rijndael256 [8], SIV-TEM-PHOTON [8], SNEIK [15], Sycon [24], TGIF [14], Triad [25]
Length-extension attacks	CiliPadi [3], FlexAEAD [20]
Distinguishing attacks	Limdolen [31]
Undesirable properties	LAEM [22], SNEIK [32, 34], CLX [26], TRIFLE [16, 37, 39]

The submissions that were removed from consideration due to third-party analysis are given below.

Bleep64. Neves [30] observed a weakness in the initialization phase where two related nonce values lead to the same output with high probability. Dobraunig and Rotella [41] found a practical forgery attack by giving signed differences to a previously obtained valid ciphertext block. These results have been extended by Bartlett et al. [5].

CiliPadi. Bagheri and Sadeghi [3] showed that CiliPadi is vulnerable against practical length-extension attacks.

CLAE. CLAE does not properly handle the padding of short messages which leads to trivial forgeries. Schrottenloher [38] showed additional forgery attacks with colliding ciphertexts.

CLX. The security of CLX relies on a new permutation that has a sliding property. This property is a cause for concern. Mege [26] described how this property can be used to mount an attack on the primary variant.

FlexAEAD. Eichlseder et al. [11, 12] showed a forgery attack on FlexAEAD. Additionally, Mege [20] showed that FlexAEAD is vulnerable against length-extension attacks.

GAGE and InGAGE. Bagheri et al. [4] observed that for the primary version with 128-bit tag and 232-bit state, a forgery attack is possible when the remaining 104-bit final output state is correctly guessed. It is trivial to filter out the wrong guesses with any valid input-output pair where the length of ciphertext is at least 104 bits.

HERN and HERON. Mege [21] found a forgery attack on Hern that exploits weak domain separation between associated data and message. The attack practically demonstrates colliding tag values for different pairs of associated data and message inputs.

LAEM. LAEM does not support empty plaintext as input by design, which prevents it from being used as a Message Authentication Code (MAC) [22]. The algorithm also has an undesirable property of generating ciphertexts where the size is approximately double that of the plaintext.

Liliput-AE. Dunkelman et al. [9, 10] reported a related-tweak differential characteristic for the tweakable block cipher Lilliput-TBC with probability 1. The characteristic can be used to mount a practical forgery attack on the AEAD scheme in the nonce-misuse resistant mode and also allows the construction of valid ciphertext-tag pairs in the nonce-respecting mode.

Limdolen. Neves [31] showed a full-round distinguisher for the underlying block cipher of Limdolen. Rohit [35, 36] showed structural weaknesses in Limdolen that lead to practical forgery attacks.

Qameleon. Jha et al. [13] observed that the tweak value of the last block cipher does not depend on the input size but depends only on the nonce. This observation was used to mount an efficient forgery attack.

Quartet. Perrin et al. [33] showed that a practical forgery attack with just one forgery attempt is possible with success probability 2^{-9} using a differential characteristic of the underlying permutation with probability 2^{-6}.

Remus and *TGIF.* Remus variants N1/M1/N3 and TGIF variants N1/M1 generate a 128-bit one-time secret value L for each key-nonce pair to perform authenticated encryption. Jha et al. [14] presented an attack to recover L, which leads to forgeries.

Simple. Mege [23] demonstrated how the lack of domain separation between processing associated data and plaintext could be used to mount forgery attacks.

SIV-Rijndael256 and *SIV-TEM-PHOTON.* Datta et al. [8] described a forgery attack that exploits a lack of domain separation between full and partial associated data blocks. In particular, the

ciphertexts are identical when two distinct padded associated data strings (one full block and one partial block) are the same and all other parameters are equal.

SNEIK. Perrin [32, 34] found a differential characteristic of the SNEIK permutation with probability 1, where all 16 input words and all 16 output words have the same difference, and Khairallah [15] showed how to use the characteristic to mount an efficient forgery attack.

Sycon. Mege [24] showed a forgery attack in AEAD variants due to improper domain separation between associated data and plaintext. The attack demonstrates construction of identical tag values for different message and associated data pairs.

Triad. Mege [25] discovered that Triad-AE is vulnerable to forgery attacks due to the lack of domain separation between the processing of the associated data and plaintext.

TRIFLE. Several observations have been made that highlight undesirable properties in the block cipher TRIFLE-BC. NIST believes that these properties are cause for concern. In particular, the combination of S-box fixed points [37], subspace transitions, ability to decrypt a quarter of the state over two rounds without knowledge of the key, and long single active bit trails [39] could be combined to mount attacks. An iterative differential characteristic on reduced-round TRIFLE-BC that leverages these properties was independently described by Lui and Isobe [16].

3 Next Steps

On August 30, 2019, NIST announced the second-round candidates [40]. NIST strongly encourages public evaluation of the second-round candidates and publication of the results throughout the process. For the second-round candidates, NIST will give the submission teams the opportunity to provide updated specifications and implementations to correct typos and implementation bugs. The deadline for these updates was September 27, 2019, 11:59PM EDT. NIST will review the proposed modifications and publish the accepted updates shortly afterwards. No design changes are accepted in this phase.

Second Round Candidates

ACE	ISAP	SKINNY-AEAD & SKINNY-HASH
ASCON	KNOT	SPARKLE (SCHWAEMM and ESCH)
COMET	LOTUS-AEAD & LOCUS-AEAD	SPIX
DryGASCON	mixFeed	SpoC
Elephant	ORANGE	Spook
ESTATE	Oribatida	Subterranean 2.0
ForkAE	PHOTON-Beetle	SUNDAE-GIFT
GIFT-COFB	Pyjamask	TinyJAMBU
Gimli	Romulus	WAGE
Grain-128AEAD	SAEAES	Xoodyak
HyENA	Saturnin	

For the second round, performance will play a larger role in the selection criteria. Submitters are encouraged to provide optimized implementations for a variety of platforms. It is estimated that the second phase of evaluation and review will last approximately 12 months. After the end of the second round, NIST is planning to focus on a small number of candidates for the final round of the selection process.

NIST will host the Third Lightweight Cryptography Workshop in Gaithersburg, MD on November 4-6, 2019, to discuss candidate algorithms, including design strategies, implementations, performance, cryptanalysis, and target applications.

References

[1] "Announcing Request for Comments on Lightweight Cryptography Requirements and Evaluation Criteria; Notice," 83 Federal Register 22251 (May 14, 2018), pp 22251-22251. Available at https://www.federalregister.gov/d/2018-10127

[2] "Announcing Request for Nominations for Lightweight Cryptographic Algorithms; Notice," 83 Federal Register 43656 (August 27, 2019), pp 43656-43657. Available at https://www.federalregister.gov/d/2018-18433

[3] Bagheri N (May 25, 2019) OFFICIAL COMMENT: CiliPadi. Official comments received on CiliPadi. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/CiliPadi-official-comment.pdf

[4] Bagheri N (May 7, 2019) Re: Official comment:GAGE AEAD. Official comments received on GAGE and InGAGE. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/GAGE-and-InGAGE-official-comment.pdf

[5] Bartlett H (June 19, 2019) OFFICIAL COMMENT: Bleep64. Official comments received on Bleep64. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Bleep64-official-comment.pdf

[6] Bassham LE, III, Çalık Ç, McKay KA, Mouha N, Sönmez Turan M (April 26, 2017) (Draft) Profiles for the Lightweight Cryptography Standardization Process. National Institute of Standards and Technology Draft Whitepaper. Available at https://csrc.nist.gov/publications/detail/white-paper/2017/04/26/profiles-for-lightweight-cryptography-standardization-process/archive

[7] CAESAR Committee (2019) CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness. Available at https://competitions.cr.yp.to/caesar.html

[8] Datta N (April 25, 2019) OFFICIAL COMMENT: Forgery against SIV-Rijndael256-AEAD and SIV-TEM-PHOTON-AEAD. Official comments received on SIV-Rijndael256. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/SIV-Rijndael256-AEAD-official-comment.pdf

[9] Dunkelman O (July 11, 2019) Official comment: Lilliput-AE. Official comments received on Lilliput-AE. Available at

https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Lilliput-AE-official-comment.pdf

[10] Dunkelman O, Keller N, Lambooij E, Sasaki Y (July 25, 2019) A Practical Forgery Attack on Lilliput-AE. Cryptology ePrint Archive: Report 2019/867. Available at https://eprint.iacr.org/2019/867

[11] Eichlseder M (April 19, 2019) OFFICIAL COMMENT: FlexAEAD. Official comments received on FlexAEAD. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/FlexAEAD-official-comment.pdf

[12] Eichlseder M, Kales D, Schofnegger M (June 7, 2019) Forgery Attacks on FlexAE and FlexAEAD. Cryptology ePrint Archive: Report 2019/679. Available at https://eprint.iacr.org/2019/679

[13] Jha A (June 14, 2019) OFFICIAL COMMENT: Qameleon. Official comments received on Qameleon. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Qameleon-official-comment.pdf

[14] Jha A (July 24, 2019) Re: [lwc-forum] OFFICIAL COMMENT: REMUS [AD-INT]. Official comments received on REMUS. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/REMUS-official-comment.pdf

[15] Khairallah M (April 18, 2019) Forgery Attack on SNEIKEN. Cryptology ePrint Archive: Report 2019/408. Available at https://eprint.iacr.org/2019/408

[16] Liu F, Isobe T (June 19, 2019) Iterative Differential Characteristic of TRIFLE-BC. Cryptology ePrint Archive: Report 2019/727. Available at https://eprint.iacr.org/2019/727

[17] McKay KA (April 18, 2019) Round 1 Candidates. Email to lwc-forum. Available at https://groups.google.com/a/list.nist.gov/forum/?hl=en#!topic/lwc-forum/7WewNDzxDeo

[18] McKay KA, Bassham LE, III, Sönmez Turan M, Mouha N (August 11, 2016) (Draft) Report on Lightweight Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) 8114. Available at https://csrc.nist.gov/publications/detail/nistir/8114/draft

[19] McKay KA, Bassham LE, III, Sönmez Turan M, Mouha N (March 28, 2017) Report on Lightweight Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) 8114. Available at https://doi.org/10.6028/NIST.IR.8114

[20] Mege A (June 3, 2019) OFFICIAL COMMENT: FlexAEAD. Official comments received on FlexAEAD. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/FlexAEAD-official-comment.pdf

[21] Mege A (July 12, 2019) OFFICIAL COMMENT: HERN & HERON. Official comments received on HERN & HERON. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/HERN-and-HERON-official-comment.pdf

[22] Mege A (June 10, 2019) OFFICIAL COMMENT: LAEM. Official comments received on LAEM. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/LAEM-official-comment.pdf

[23] Mege A (June 10, 2019) OFFICIAL COMMENT: SIMPLE. Official comments received on Simple. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/SIMPLE-official-comment.pdf

[24] Mege A (June 5, 2019) OFFICIAL COMMENT: Sycon. Official comments received on Sycon. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/SYCON-official-comment.pdf

[25] Mege A (July 15, 2019) OFFICIAL COMMENT: Triad. Official comments received on Triad. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Triad-official-comment.pdf

[26] Mege A (2019) Slide Attack on CLX-128. Accepted to Lightweight Cryptography Workshop 2019.

[27] National Institute of Standards and Technology (May 14, 2019) DRAFT Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/Draft-LWC-Submission-Requirements-April2018.pdf

[28] National Institute of Standards and Technology (2019) Lightweight Cryptography. Available at https://csrc.nist.gov/Projects/lightweight-cryptography

[29] National Institute of Standards and Technology (August 27, 2018) Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/final-lwc-submission-requirements-august2018.pdf

[30] Neves S (April 20, 2019) Bleep64: bad initialization. Email to lwc-forum. Available at https://groups.google.com/a/list.nist.gov/forum/?hl=en#!topic/lwc-forum/O-f-ogbUeTU

[31] Neves S (April 18, 2019) Differential distinguisher for the full Limdolen128 blockcipher. Email to lwc-forum. Available at https://groups.google.com/a/list.nist.gov/forum/?hl=en#!topic/lwc-forum/rHWE52Ay8MU

[32] Perrin L (April 19, 2019) Attacks against SNEIK. Email to lwc-forum. Available at https://groups.google.com/a/list.nist.gov/forum/?hl=en#!topic/lwc-forum/gFlsAbZr_QI

[33] Perrin L (July 5, 2019) OFFICIAL COMMENT: Quartet. Official comments received on Quartet. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Quartet-official-comment.pdf

[34] Perrin L (April 8, 2019) Probability 1 Iterated Differential in the SNEIK Permutation. Cryptology ePrint Archive: Report 2019/374. Available at https://eprint.iacr.org/2019/374

[35] Rohit R (May 17, 2019) OFFICIAL COMMENT: Limdolen. Official comments received on Limdolen. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Limdolen-official-comment.pdf

[36] Rohit R, Gong G (August 6, 2019) Practical Forgery Attacks on Limdolen and HERN. Cryptology ePrint Archive: Report 2019/907. Available at https://eprint.iacr.org/2019/907

[37] Sarkar S (April 25, 2019) Re: TRIFLE S-box has some structural weakness. Email to lwc-forum. Available at https://groups.google.com/a/list.nist.gov/forum/?hl=en#!topic/lwc-forum/NcMMP7inccg

[38] Schrottenloher A (June 11, 2019) OFFICIAL COMMENT: CLAE. Official comments received on CLAE. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/CLAE-official-comment.pdf

[39] Sim SM (June 26, 2019) OFFICIAL COMMENT: TRIFLE. Official comments received on TRIFLE. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/TRIFLE-official-comment.pdf

[40] Sönmez Turan M (August 30, 2019) NIST Lightweight Cryptography Project - Second-round candidates. Email to lwc-forum. Available at https://groups.google.com/a/list.nist.gov/forum/?hl=en#!topic/lwc-forum/-G6VEqTN5fg

[41] Yann R (May 3, 2019) OFFICIAL COMMENT: Bleep64. Official comments received on Bleep64. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Bleep64-official-comment.pdf