NIST Cybersecurity White Paper *csrc.nist.gov*

Profiles for the Lightweight Cryptography Standardization Process

Larry Bassham
Çağdaş Çalık
Kerry McKay
Nicky Mouha
Meltem Sönmez Turan

Computer Security Division
Information Technology Laboratory

April 26, 2017

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

Abstract

This document describes the first two profiles for NIST's lightweight cryptography project. Profile I provides authenticated encryption with associated data (AEAD) and hashing functionalities for both hardware-oriented and software-oriented constrained environments. Profile II provides AEAD only in hardware-oriented constrained environments.

Keywords

Constrained devices; lightweight cryptography; standardization

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's Cybersecurity programs, projects and publications, visit the Computer Security Resource Center, csrc.nist.gov. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is available at www.nist.gov and www.nist.gov/itl.

Table of Contents

List of Appendices

1 Note to the Readers

In 2013, NIST initiated a lightweight cryptography project to understand the need for dedicated lightweight cryptography standards, and to design a transparent process for standardization. In 2016, NIST announced its decision to develop and maintain a portfolio of lightweight algorithms that are approved for limited use, where conventional standards are impractical to implement or use within the device or application. In March 2017, NIST published the NISTIR 8114 *Report on Lightweight Cryptography* [1] that summarized the finding of the lightweight cryptography project and explained NIST's plans for standardization of lightweight algorithms.

In the context of the NIST lightweight cryptography project, NIST plans to publish a call for submissions document for lightweight cryptography based on the feedback received from the community. The call for the submissions document will include profiles that describe security and performance requirements of the candidates. This document includes two draft profiles that are planned to be included in the call for submission. Comments on the profiles should be sent to lightweight-crypto@nist.gov with the subject line "Official comment on draft profiles" until **June 16, 2017**.

2 Profiles

The algorithms in the NIST's lightweight cryptography portfolio will be recommended in the context of one or more *profiles*. A profile is a set of engineering requirements that consists of:

- *Functionality* provided by the algorithm(s) (e.g., authenticated encryption),
- *Design goals* for the intended applications (e.g., efficient for short messages),
- *Physical characteristics* of the environment implementation resides in (e.g., hardware or software),
- *Performance characteristics* (e.g., latency, throughput, or power),
- *Security characteristics* (e.g., security strength, relevant attack models, side-channel resistance).

The role of a profile is to lay out the requirements that submitted algorithms must exhibit to be considered for admission into NIST's lightweight portfolio. After algorithms are added to the portfolio, their associated profiles provide context to the applications where the use of the algorithms are recommended by NIST.

The profiles are intended to specify requirements for lightweight algorithms that:

- satisfy performance requirements on specific platforms that are not met by current NIST standards;
- offer significant implementation or performance improvements compared to the current NIST standards on specific platforms; and
- provide security against cryptanalysis, even in the presence of side-channel information.

In the profiles, the focus is on providing certain types of functionalities rather than providing requirements for a particular underlying primitive (such as a (tweakable) block cipher, stream cipher, or cryptographic permutation). The main reason is that these primitives are typically used together with a mode to provide a cryptographic functionality, but the profiles are designed to be neutral with respect to the choice of the primitive. Both the performance and the security of the algorithm depend in a critical way on the selection of the modes. For example, block ciphers cannot be parallelized in CBC encryption mode, the security of CBC breaks down if the IVs are predictable and various implementation failures may occur when encryption and authentication are combined.

3 Profile Descriptions

The scope of NIST’s lightweight cryptography project includes all cryptographic algorithms that are needed in constrained environments. However, the initial focus of the project is on symmetric-key cryptography and hashing. For secret-key cryptography, the main goals are to provide entity authentication, confidentiality and data authentication. All three goals can be provided by an algorithm for Authenticated Encryption with Associated Data (AEAD).

An AEAD algorithm takes a nonce N, plaintext P, and an associated data A, and transforms it into a ciphertext C and a tag T. To support the scenario where only message authentication is needed, the authenticated encryption algorithm should support a plaintext of length zero. It should also be possible to have both a zero-length plaintext and a zero-length associated data, which may be useful in basic challenge-response protocols for entity authentication, where the challenge could consist of only the nonce N, and the response could be the tag T, or a truncation of the tag T.

From a security point of view, an AEAD algorithm should ensure both the confidentiality of the plaintexts (under adaptive chosen-plaintext attacks) and the integrity of the ciphertexts (under adaptive forgery attempts). It is assumed that the nonce will not be repeated for multiple encryptions under the same key, but no nonce uniqueness assumption is made for decryption.

Data limits may be difficult to enforce in practice and rekeying can come at a high cost, and the use of pre-shared keys may be desirable or even necessary for some applications. Therefore, the AEAD algorithm should allow a large amount of data to be processed securely under the same key.

It is expected that for some applications a cryptographic hash function can be provided as well, preferably sharing logic with the AEAD algorithm so that implementing the functions together can be done more efficiently than implementing unrelated AEAD and hash algorithms. A hash function H takes a message M and transforms it into a hash output $H(M)$. From a security point of view, it should be computationally infeasible to find a collision or a (second) preimage. The hash function should also be resistant against length extension attacks. In particular, if part of the message is a secret key that is unknown to the attacker, it should be infeasible for this attacker to construct a hash value corresponding to a different message that contains the same secret key. In several practical applications, hash functions are required to satisfy other security properties as well, such as retaining some level of security when the output is truncated.

After considering the comments received during the workshops and the comment period of NISTIR 8114, NIST developed two initial profiles;

- Profile I – Authenticated Encryption with Associated Data (AEAD) and hashing for constrained software and hardware environments, and
- Profile II – AEAD for constrained hardware environments.

For lightweight cryptography, it is desirable for the AEAD algorithm and hash function to target both constrained hardware and embedded software environments. These requirements are captured in Profile I. However, we expect that some highly constrained applications may not be realizable in software, but may necessitate a hardware implementation. Furthermore, these applications may be too constrained to implement both functionality for AEAD and hashing, and would therefore only implement an AEAD algorithm. This scenario is captured in Profile II (See Figure 1).

Note that any algorithm that matches Profile I also provides the functionality that is needed for Profile II. As such, any algorithm that matches Profile I could also be considered for Profile II. It remains to be seen during the lightweight project whether algorithms that target Profile II have sufficient implementation advantages compared to those that target Profile I, in order to motivate the existence of Profile II next to Profile I. As stated earlier, algorithms for both Profile I and Profile II should have significant improvements over current NIST standards in constrained environments.

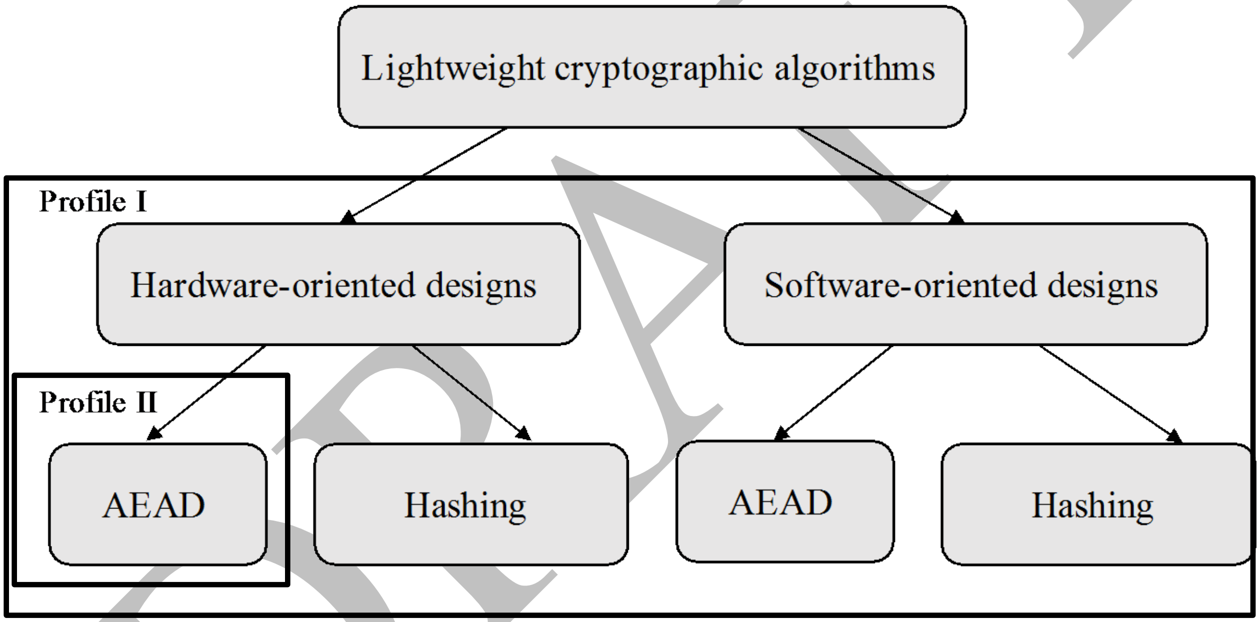
Lightweight cryptographic algorithms
Profile I
Hardware-oriented designs
Software-oriented designs
Profile II
AEAD
Hashing
AEAD
Hashing

Figure 1 Profile I considers AEAD and hashing algorithms with a focus on constrained hardware and embedded software environments. Profile II considers hardware-oriented AEAD only.

3.1 Profile I – AEAD and Hashing for Constrained Environments

This profile is intended for the applications that require a good performance in both constrained hardware and software environments. Both AEAD and hashing are supported.

Profile I - AEAD and Hashing for Constrained Environments	
Functionality	Authenticated encryption with associated data and hashing
Design goals	- Performs significantly better in constrained environments (hardware and embedded software platforms) compared to current NIST standards. - Both algorithms should be optimized to be efficient for short messages (e.g., as short as 8 bytes). - The message length shall be an integer number of bytes.
Physical characteristics	- Compact hardware implementations and embedded software implementations with low RAM and ROM usage should be possible.
Performance characteristics	- The performance on ASIC and FPGA should consider various standard cell libraries, the flexibility to support various implementation strategies (low energy, low power, low latency), with significant improvements over current NIST standards. - The performance on microcontrollers should consider a wide range of 8-bit, 16-bit and 32-bit microcontroller architectures. - The preprocessing of a key (in terms of computation time and memory footprint) should be efficient.
Security characteristics	**AEAD** - A key length of 128 bits shall be supported. A longer key length may be supported, for example to provide security in the multi-key setting, or security against quantum computers. - Nonce lengths of up to 128 bits shall be supported. - Tag lengths of up to 128 bits shall be supported. - Plaintext lengths of up to 2^{50}-1 bytes shall be supported. - Associated data of up to 2^{50}-1 bytes shall be supported. - At least 2^{50}-1 bytes can be processed securely under a single key. - Cryptanalytic attacks should require at least 2^{112} computations on a classical computer in a single-key setting. - Lends itself to countermeasures against various side-channel attacks, including timing attacks, simple and differential power analysis (SPA/DPA), and simple and differential electromagnetic analysis (SEMA/DEMA). **Hashing** - Cryptanalytic attacks should require at least 2^{112} computations on a classical computer. - Hash outputs of 256 bits must be supported, and longer hash values may be supported as well. - A maximum message length of 2^{50}-1 bytes shall be supported. - Lends itself to countermeasures against various side-channel attacks, including timing attacks, simple and differential power analysis (SPA/DPA), and simple and differential electromagnetic analysis (SEMA/DEMA).

3.2 Profile II – AEAD for Constrained Hardware Environments

This profile is intended for the most constrained applications, which are realized in hardware to avoid the overhead of a software implementation. To further reduce the implementation cost, this profile does not support hashing, but supports AEAD only.

Profile II – AEAD for Constrained Hardware Environments	
Functionality	Authenticated encryption with associated data
Design goals	- Performs significantly better compared to current NIST standards. - The performance for short messages (e.g., as short as 8 bytes) is important. - The message length shall be an integer number of bytes.
Physical characteristics	- Targeted towards constrained hardware platforms. - Compact hardware implementations should be possible.
Performance characteristics	- The performance on ASIC and FPGA should consider a wide range of standard cell libraries and vendors. - Flexibility to support various implementation strategies (low energy, low power, low latency) - The preprocessing of a key (in terms of computation time and memory footprint) should be efficient.
Security characteristics	- A key length of 128 bits shall be supported. A longer key length may be supported, for example to provide security in the multi-key setting, or security against quantum computers. - Nonce lengths of up to 128 bits shall be supported. - Tag lengths of up to 128 bits shall be supported. - Plaintext lengths of up to 2^{50}-1 bytes shall be supported. - Associated data of up to 2^{50}-1 bytes shall be supported. - At least 2^{50}-1 bytes can be processed securely under a single key. - Cryptanalytic attacks should require at least 2^{112} computations on a classical computer in a single-key setting. - Lends itself to countermeasures against various side-channel attacks, including timing attacks, simple and differential power analysis (SPA/DPA), and simple and differential electromagnetic analysis (SEMA/DEMA).

Appendix A—References

[1] National Institute of Standards and Technology (2017) Report on Lightweight Cryptography (U.S. Department of Commerce, Washington, D.C.), National Institute of Standards and Technology Internal Report 8114. https://doi.org/10.6028/NIST.IR.8114