INDRAPRASTHA INSTITUTE *of*
INFORMATION TECHNOLOGY **DELHI**

Authenticated Encryption for Memory Constrained Devices

Ph.D. Thesis Defense

Date: 26th March 2021, Friday
Time: 4:00 PM to 5:30 PM

Google Meet link: meet.google.com/sxs-ffqa-qir

Advisor: Dr. Donghoon Chang, Dr Somitra Sanadhya

Examiner

- Dr. Mridul Nandi, Indian Statistical Institute, Kolkata
- Dr. Sourav Mukhopadhyay Indian Institute of Technology Kharagpur
- Dr. C Pandu Rangan, Indian Institute of Technology Madras

Abstract: It is common knowledge that encryption is a useful tool for providing confidentiality. Authentication, however, is often overlooked. Authentication provides data integrity; it helps ensure that any tampering with or corruption of data is detected. It also provides assurance of message origin. Authenticated encryption (AE) algorithms provide both confidentiality and integrity/authenticity by processing plaintext and producing both ciphertext and a Message Authentication Code (MAC). It has been shown too many times throughout history that encryption without authentication is generally insecure. This has recently culminated in a push for new authenticated encryption algorithms. There are several authenticated encryption algorithms in existence already. However, these algorithms are sometimes difficult to use in resource-constrained environments.

This thesis focuses on designing authenticated encryption schemes suitable for memory-constrained environments. In many practical applications, the users of an AE scheme use a cryptographic module to perform encryption, decryption, and tag verification. Usually, this cryptographic module has a very small memory. Due to its limited storage, it can't store the complete ciphertext to first verify the tag and then conditionally decrypt it. Similarly, it can't store the complete plaintext while decrypting, and output it only if the tag is valid. This becomes an issue that is particularly relevant in the case of long messages. In authenticated encryption schemes, there are two techniques for handling long ciphertexts while working within the constraints of a low buffer size: Releasing unverified plaintext (RUP) or Producing intermediate tags (PIT). In this work, in addition to the two techniques, we propose another way to handle a long ciphertext with a low buffer size by storing and releasing only one (generally, or only a few) intermediate state without releasing or storing any part of an unverified plaintext and without the need of generating any intermediate tag. In this context, we have designed two schemes sp-AELM which is sponge based and dAELM which is a deterministic AE scheme. Brief details about these work are given below.

1. sp-AELM is a sponge-based authenticated encryption scheme that provides support for memory-constrained devices. We also provide security proof for privacy and authenticity in an ideal permutation model, using a code-based game-playing framework. Furthermore, we also present two more variants of sp-AELM that serve the same purpose and are more efficient than sp-AELM.
2. We also analyzed sponge-based CAESAR submissions using our proposed technique, to determine their potential to support limited memory constraints.
3. dAELM is a deterministic authenticated encryption scheme providing support for memory-constrained devices. Deterministic AE (DAE) is used in domains such as the key wrap, where the available message entropy omits the overhead of a nonce. For limiting memory usage, our idea is to use a session key to encrypt a message and share the session key with the user depending upon the verification of a tag. We provide the security proof of the proposed construction in the ideal cipher model.
4. We have shown a simple PA attack on an existing SAEB authenticated encryption scheme. Further, we have proposed a modification to SAEB to overcome this attack. We have proposed two modified versions of SAEB called RSAEB v1 and RSAEB v2: the first one provides PA1 security in nonce respecting scenario and another one provides PA1 in nonce misuse scenario and PA2. PA2 is a stronger security notion than PA1, which comes at the cost of an additional pass.