One-pager on Feedback Items for the Single-Device Track of the Threshold Cryptography Project

The NIST-TC team, July 06, 2020

As described in NISTIR 8214A, the NIST Threshold Cryptography (TC) project is organized into two main tracks: single-device and multi-party. This document outline topics for feedback for the **single-device track**, as a preparation to devise criteria for consideration of threshold schemes We welcome public feedback sent to threshold-crypto@nist.gov.

For the single-device track, the preliminary roadmap identifies a focus on threshold schemes for the Advanced Encryption Standard (AES, FIPS 1997), which is a NIST-approved primitive. This focus intends to identify various threshold techniques tailored to and specifically beneficial for AES. As a baseline, two attack scenarios are considered: side-channel attacks; and combined (side-channel and fault injection) attacks. For both cases, it is useful to identify threshold circuit designs that enhance the confidentiality of the key (prevent its leakage); enhanced integrity (error detection and/or correction) is also of interest in the second case.

There is also interest in identifying techniques that, while applicable to AES, may extend their usefulness to various lightweight symmetric-cryptography primitives with potential for future standardization. Whereas it may be difficult to pick a "best" approach or technique, given the diversity of possible methods, application scenarios, and tradeoffs, it is useful to hear about multiple suitable alternatives.

A. Models and paradigms

1. **Security modeling.** Define a system model and threat model suitable for threshold circuit designs. Identify paradigms for security analysis, desirable properties to achieve, and the adversarial settings in which the threshold schemes enable a higher resistance to side-channel and/or fault attacks.
2. **Constructions at a high-level.** Identify practical construction paradigms for threshold circuit design. Succinctly describe each differentiated construction approach, and the suitable conditions for deployment. Where possible, tentatively enumerate building blocks (e.g., random-number generation, secret-sharing, ...) with common aspects across different approaches.
3. **Applications.** Describe application settings where it would be beneficial to have standards for threshold schemes for single-device implementation of AES.

B. Implementation, testing and validation

1. **Parameters.** Propose parameters (e.g., masking order, number of shares) for realistic implementations of threshold circuit designs. Where possible, quantify the increase in adversarial effort required to exfiltrate secrets or induce incorrect outputs.
2. **Benchmarking.** Suggest benchmarking parameters (threshold vs. conventional; various platforms) for assessing security and efficiency.
3. **Open-source.** List links to open-source implementations, and for each of them explain very briefly the relevance and distinctive features.
4. **Validation.** Suggest testing & validation procedures, and security profiles for adoption into the NIST Cryptographic Algorithm Validation Program (CAVP).

C. References to prior work

1. **Scientific references.** Enumerate relevant peer-reviewed bibliographic references (doi; link to freely accessible version) and explain in a few sentences their relevance to the development of criteria.
2. **Intellectual property.** Identify existing intellectual property / licensing conditions that may be directly relevant in the context of standardization (for context, see the ITL patent policy). This does not include all patents related to cryptographic primitives. The specific interest is on disclosure of patents relevant to potential guidance to include in upcoming standards for threshold schemes.