ITL BULLETIN FOR APRIL 2019

TIME TO STANDARDIZE THRESHOLD SCHEMES FOR CRYPTOGRAPHIC PRIMITIVES

Luís Brandão, Michael Davidson, Nicky Mouha, Apostol Vassilev
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

The Computer Security Division (CSD) at the National Institute of Standards and Technology (NIST) promotes the security of implementations and operations of cryptographic primitives, such as signatures and encryption. This security depends not only on the theoretical properties of the primitives, but also on the abilities to withstand attacks on their implementations and to ensure authorized modes of operation. To advance this capability, NIST has initiated the NIST Threshold Cryptography Project to drive an effort to standardize threshold schemes. These schemes enable distribution of trust placed on human operators, and also offer a path to prevent single-points of failure at the technology level. They can be used to enhance the secrecy of cryptographic keys, as well as the integrity and availability of implemented primitives, including to provide resistance against side-channel attacks that exploit inadvertent leakage from real implementations.

Introduction

As cryptography becomes ubiquitous, it is increasingly relevant to address the potentially disastrous breakdowns resulting from differences between ideal and real implementations of cryptographic algorithms. These differences give rise to a range of attacks that exploit vulnerabilities in order to compromise diverse aspects of real-world implementations. Furthermore, even when implementation flaws are not known, a conventional cryptographic module operated by a single operator is vulnerable to said operator becoming compromised and going rogue, for example a compromised bank employee in charge of digitally signing off on high-value transactions. Threshold schemes have the potential to enable more-secure modes of operation, by letting multiple components contribute to the operation in a way that attains the desired security goals even if f out of n of the components are compromised. However, these schemes also present new challenges for the standardization and validation of security assertions about their implementations.

In this article we overview the effort of the NIST Threshold Cryptography Project towards the standardization of threshold schemes for cryptographic primitives, which have the potential to mitigate single-points of failure in the technology and human elements. We highlight two components: the NIST Internal Report "Threshold Schemes for Cryptographic Primitives" (NISTIR 8214), positioning a preparatory framework and several representative questions; and the NIST Threshold Cryptography Workshop 2019, which brought together stakeholders for sharing perspectives from industry, academia and government. We then conclude with an observation of the step that lays ahead.

Secret sharing for protecting secrets at rest

As a toy example, consider that a secret key k is an integer between 0 and 10, and that someone (called the *dealer*) holding this key would like to *split* it across a set of n = 5 friends, such that:

(a) any combination of f + 1 = 3 friends is able to recover the secret;

(b) any coalition of up to f = 2 friends cannot learn anything about the secret.

The desired splitting can be achieved with Shamir secret-sharing. The dealer starts by choosing random coefficients c_1 and c_2 for a polynomial $p(x) = k + c_1\, x + c_2\, x^2$ (mod 11) of degree f = 2, over the integers modulo 11. The polynomial is random, except for evaluating to the secret when x = 0, i.e., $p(0) = k$. The plot below illustrates the evaluation points when k = 6, c_1 = 9 and c_2 = 8.

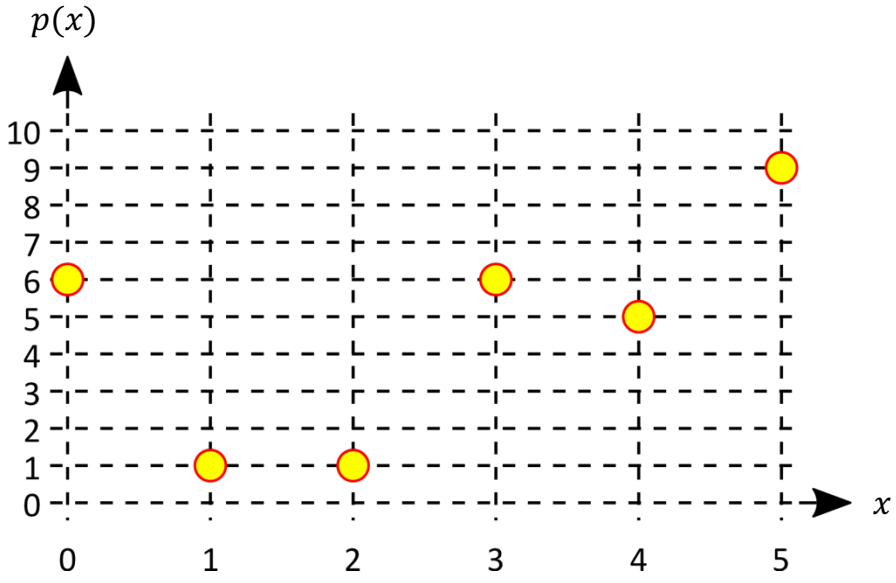

Figure 1: The secret $p(0)$ and its shares $p(x) = 6 + 9\, x + 8\, x^2$ (mod 11)

Then, to *split* the secret, the dealer gives to each of the five friends the share $p(i)$, along with the identifier i, with i from 1 through 5. This *secret sharing* satisfies the intended properties:

(a) Any subset of three friends can combine their shares to recover the secret, by interpolating the polynomial at value x = 0. This is possible since any three distinct points completely define the polynomial of degree 2 (similar to how any two points define a straight line).

(b) Any isolated pair of shares $(i, p(i))$ and $(j, p(j))$ contains no information about the secret, since for any possible candidate secret k' there is a polynomial p' that is consistent with the candidate secret and the two shares, i.e., satisfying $p(0) = k'$, $p'(i) = p(i)$ and $p'(j) = p(j)$.

The big picture, beyond secret sharing

Secret sharing provides a way to enhance confidentiality of data at rest, while the use of a secret is not required. *But how to prevent the secret from being ever recombined when executing a cryptographic algorithm, such as signing or decrypting, dependent on the key?* As a solution, threshold cryptography enables cryptographic primitives to be implemented via *threshold schemes*: multiple components contribute to the intended operation in a way that attains the desired security goals even if f out of n of its components are compromised. The parties independently or collaboratively calculate shares of the output, without revealing the input shares to one another. This may be facilitated by certain mathematical properties, such as homomorphisms, or by cryptographic "secure computation" protocols. This approach can be used to enhance several security goals of interest, including the secrecy of cryptographic keys, integrity and availability, among others.

Threshold schemes can be applied to various cryptographic primitives, to enhance their security properties, and to mitigate diverse types of attacks. Here are three examples of possible features:

- **Avoiding the dealer.** If an application intends to define a new key in a distributed manner, then even the cryptographic key can be distributed while being selected, without relying on any *dealer*, such that the key is never (not even during setup) in any one location.

- **Robustness.** In the simple secret-sharing example, a single incorrect share could lead to a reconstruction of an incorrect secret. Using more sophisticated techniques (e.g., verifiable secret sharing), the interacting agents can verify the correctness of intermediate computation results that depend on the secret shares of other parties. This enables enhanced integrity, besides enhanced confidentiality.

- **Side-channel resistance.** Threshold schemes also offer a potential to strengthen resistance against side-channel attacks, which exploit inadvertent leakage from real implementations. Circuits with a threshold design can become more resistant to some side-channel attacks that exploit noisy leakage. For example, for a differential power analysis attack with physical access to a whole cryptographic module, the exploitation of noisy leakage may in some models require collecting a number of traces exponential in the number of shares.

Threshold schemes aimed for NIST-approved algorithms, such as for Digital Signature Standard (DSS) signing (FIPS 186-4) and pair-wise (private|public) key-establishment (SP 800-56A), for Rivest–Shamir–Adleman (RSA) decryption and corresponding pair-wise (private|public) key-establishment (SP 800-56B), and for Advanced Encryption Standard (AES) enciphering and deciphering (FIPS 197), can incorporate the above mentioned properties.

Along with the potential benefits of threshold schemes, there are a number of associated challenges. For example, in comparison with a conventional 1-out-of-1 non-threshold scheme, the use of an f-out-of-n scheme may increase the attack surface of the system. The actual effects depend on attack models and system model characteristics. Therefore, the use (and standardization) of threshold schemes must be considered carefully and approached methodically.

NISTIR 8214 — positioning the approach

The NISTIR 8214 considers challenges and opportunities related to standardization of threshold schemes for cryptographic primitives. It includes examples illustrating security tradeoffs under variations of system model and adversaries; it enumerates several high-level *characterizing features* of threshold schemes; and it poses representative questions to take into account when considering the standardization of concrete threshold schemes. The report is thus a preparation for setting an initial framework for addressing the standardization problem. A main insight arising from the report is the multi-dimensionality of the problem.

Characterizing features. An "f-out-of-n" property is not sufficient to imply better security than a conventional scheme. Diverse implementation aspects affect security tradeoffs across different contexts. Therefore, the report proposes that a basis for discussion and comparison of threshold schemes should take into account the following characterizing features:

- **Kinds of threshold.** A system may have a threshold f_C for confidentiality and another f_I for integrity, often with tradeoffs. Even for the same type of security property the thresholds can vary with the system model (e.g., type of communication synchrony).

- **Communication interfaces.** A threshold scheme introduces new communication interfaces, with the environment and/or between components. For example, a threshold scheme may require that each client communicates separately with each component; in another scheme, a client may remain unaware of a threshold implementation while it communicates with the system. The possible communication channels between components may also constitute an additional attack surface.

- **Executing platform.** In some threshold systems the components are distributed across locations and operators, and use diversity at several other levels (e.g., operating system, vendor, architecture); other threshold systems are implemented at the level of a threshold circuit design within a single localized device.

- **Setup and maintenance.** Some systems make restrictive assumptions about the deployment scenario, including about synchrony of communication channels, availability of certain trusted components (e.g., a global clock), and the possibility to recover from compromise of individual components (e.g., by proactive or reactive recovery).

Each of these features spans distinct options that affect security in a different way, possibly in relation to other factors. For example, the application context (e.g., signature vs. encryption) may affect the sought security properties. A threshold scheme for use in a signature application may relegate the integrity property if verifying signature correctness can be accomplished by the application.

Other important considerations. The NISTIR proceeds with identifying other essential questions for the standardization endeavor. For example:

- **Validation.** In the federal context, entities required to use standardized cryptography are also required to use validated implementations (FIPS 140-2). Therefore, promoting the use of threshold cryptography includes taking into account how implementations of new threshold schemes can be tested and validated.

- **Representative questions.** The report also poses a number of representative questions to consider when looking at concrete schemes. These questions deal, for example, with the kind of proofs of security to aim for, the kind of required implementations, and the security assertions that can be made about the system.

The NISTIR leaves open the challenge of defining criteria to ask for and select from a potential pool of candidate threshold schemes. The final version (March 2019) of the report followed a period of public comments to the draft version (July 2018). The public feedback praised the initiative and provided valuable suggestions. As supplementary documentation, we also made available a "diff" with a detailed accounting of the changes introduced in the final version.

NTCW 2019 — the first NIST Threshold Cryptography Workshop

"NIST believes that robust, widely understood, and participatory development processes produce the strongest, most effective, most trusted, and broadly accepted cryptographic standards and guidelines" (NISTIR 7977). In this vein, NISTIR 8214 set the basis for organizing a workshop that would bring together, for open interaction, stakeholders from academy, industry and government. On March 11–12, 2019, about 80 participants gathered in Gaithersburg for the first NIST Threshold Cryptography Workshop (NTCW 2019). The international composition included members with affiliations from three different continents and spanning industry, academia and government. The event was also webcast over the Internet. After a welcoming message by the CSD chief, the event comprised 15 slots from external submissions (2 panels, 5 papers and 8 presentation proposals), 2 invited keynotes, 4 presentations from NIST, and 2 slots (one in the end of each day) for feedback from the attendees.

The conference talks covered several topics: threshold schemes in general (motivation and implementation feasibility); NIST standardization of cryptographic primitives (diverse standards; and a status update on elliptic curves and on the post-quantum cryptography project); a post-quantum threshold public-key encryption scheme; threshold signatures (adaptive security; elliptic curve digital signature algorithm); validation of cryptographic implementations; threshold circuit design (tradeoffs, pitfalls, combined attacks, verification tools); secret-sharing with leakage resilience; distributed symmetric-key encryption; applications and experience with threshold cryptography (multi-signatures in Bitcoin, multi-prime RSA in an electronic national identification system, cloud and crypto-currencies, use of secret sharing).

Throughout the workshop, the attendees also shared several perspectives in moments of interactive feedback, in the scope of question-and-answer moments after the talks and during the panels, as well as during one feedback slot in the end of each day. Covered topics included the granularity level (small modules vs. full functionality) to consider for standardization; differences between the scenarios of multi-party vs. single-device threshold circuit design; and possible ways to collaborate with stakeholders during the standardization effort. The attendees complimented the NIST initiative, including the quality of the NISTIR as a helpful document laying down the rationale for tradeoffs, and the organization of the workshop. The shared opinions also expressed confidence in NIST driving the threshold cryptography

effort of standardization, considering the tradition and experience in developing prior successful cryptographic standards in an open way.

Conclusion

NIST aims at driving an open and transparent process towards standardization of threshold schemes for cryptographic primitives. The envisioned standardization provides an avenue for promoting a new level of security for cryptographic implementations and operations in the real world. This provides a number of opportunities but also requires dealing with a number of challenges.

The positive feedback on the report (NISTIR 8214) and on the workshop (NTCW 2019) confirm that threshold cryptography is ripe for standardization. We are thus now starting a new phase in the NIST Threshold Cryptography Project. The next step is the identification of focus areas for standardization. An immediate challenge is producing a preliminary proposal for criteria for the development of standards of threshold schemes. Such an endeavor has to consider the high-dimensionality of the space of solutions, including defining validation guidelines to address regulatory requirements. An important feature to promote here is the collaboration with the community of interested stakeholders.

Additional Resources

- NISTIR 8214: https://doi.org/10.6028/NIST.IR.8214
- The NIST TC Project webpage: https://csrc.nist.gov/projects/threshold-cryptography

ITL Bulletin Publisher: Katherine Green
Information Technology Laboratory
National Institute of Standards and Technology
katherine.green@nist.gov