Call 2021a for Feedback on Criteria for Threshold Schemes

NIST Multi-party Threshold Cryptography

2021-July-02: https://csrc.nist.gov/projects/threshold-cryptography

Please send comments to threshold-MP-call-2021a@nist.gov by September 13, 2021.

In a **multi-party threshold scheme**, the secret key needed to operate a cryptographic primitive is "secret shared" across n parties. The operation (e.g., signing, decryption) is then distributively executed, while the key remains secret even if f (the threshold number of) parties are corrupted.[1]

The NIST multi-party threshold cryptography (MPTC) project has received useful feedback on threshold schemes. This has included various comments about draft NIST internal reports (IR) 8214 and 8214A, and presentations in the NTCW 2019 and MPTS 2020 workshops. Currently, a new IR, 8214B, is being prepared to specify **criteria** to support a future call for proposals of **multi-party threshold schemes**. The subsequent evaluation of those proposals will serve as a basis to support the development of **guidelines and recommendations** (G&R) about threshold schemes. A draft of IR 8214B, to be open for public comments, is planned for late 2021.

In advance to draft IR 8214B, this document is an earlier **call for feedback on selected topics of criteria**. The following paragraphs, with some level of informality in the midst of nuanced notions in multi-party / distributed systems, advance a preparatory positioning about six topics. These are open to improvement based on feedback, which is welcome from expert stakeholders. It is particularly useful to hear about the benefits of being more stringent or loose in any of the topics. It is also useful to hear about reference approaches to thresholdization of concrete primitives. For timely consideration, comments should be compiled in a **p**ortable **d**ocument **f**ormat (PDF) file, with up to six pages, letter size, and sent by email, by September 13, 2021. Voluntary template files for feedback are attached in .odt (**o**pen **d**ocument **t**ext) and .tex (La**TeX**) formats.

1. Scope of proposals. The future call for proposals will be intended to gather expert submissions of concrete threshold schemes for primitives that are *interchangeable* (in the sense of IR 8214A, Section 2.4) with[2] ECDSA, EdDSA, RSA signing/decryption, RSA keygen, AES, and ECC-based key agreement.[3] After an evaluation period, and possibly various stages for tweaks,

[1] In this document, f denotes the *corruption* threshold (maximum number of tolerated corruptions) with respect to key hiding. Different properties can have different associated thresholds. In complement, a *participation* threshold denotes the minimum number k (with $k > f$) of parties needed to generate the intended output, e.g., a "3-out-of-5 threshold signature" can be such that any subset of $k = 3$ honest parties can generate a signature, whereas $k - 1$ cannot.

[2] **Legend:** ECDSA: **E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm. EdDSA: **E**dwards **C**urve **D**igital **S**ignature **A**lgorithm. RSA: **R**ivest-**S**hamir-**A**dleman. Keygen: **key-gen**eration. ECC: **E**lliptic **C**urve **C**ryptography. AES: **A**dvanced **E**ncryption **S**tandard. PreQC: **pre-q**uantum **c**ryptography; PQC: **p**ost-**q**uantum **c**ryptography.

[3] Proposals of distributed (threshold) keygen for ECC-based schemes and AES can be associated to the proposals of corresponding threshold signing/encryption/decryption. Proposals of RSA keygen will be considered separately from proposals of RSA signing/decryption, although still taking into account the need for interoperability.

new proposals, and filtration of suitable approaches, the NIST MPTC project may produce differentiated G&R on threshold schemes for each primitive, and possibly also focused on useful building blocks. To better serve the evaluation process and the elaboration of G&R documentation, the future call is expected to request that submitted proposals include a reference open-source implementation, and a disclosure of known applicable patent claims. Additional notes:

- **Interchangeability:** In the scope of ECC-based signatures, it is particularly relevant to analyze the applicability of, and tradeoffs between, probabilistic and deterministic threshold schemes with interchangeable signature verification, possibly leading to differentiated G&R.
- **PreQC:** The utility of threshold schemes for preQC primitives may be affected in the future by advances in quantum computation, possible deprecation of existing standards, and developments of new PQC standards.
- **PQC:** While the present scope does not include the thresholdization of primitives in evaluation by the NIST-PQC project, the experience to be gained with the current scope should be useful for future considerations about threshold PQC. Also, post-quantum security can be considered in gadgets and in the thresholdization of AES.

2. Idealization of security. A proposal of threshold scheme must be supported on a **simulation**-based and/or a **game**-based security formulation. This entails defining an ideal **functionality** (as in the ideal-real simulation paradigm, e.g., in the universal composability framework) and/or an idealized adversarial **game** (or set of games). The proposal must discuss whether/which known useful properties are not captured by the idealized security formulation.[4] The proposal must include a proof ("security proof") that, in a suitable adversarial context (see item 3), the proposed threshold scheme satisfies the proposed security formulation, e.g., by showing "emulation" of the ideal functionality, or by showing that a non-negligible adversarial advantage in the game implies breaking an assumption. The analysis must identify the required cryptographic assumptions and any possibly-idealized trusted components in the setup or operations. It must also consider the (in)security consequences of foreseen real instantiations of the setup and ideal components.

3. Security vs. adversaries.

Security with respect to how an adversary corrupts up to f parties:

(a) **Active.** Proposed threshold schemes must aim for **active security** (i.e., against active corruptions, which enable corrupted parties to "maliciously" deviate from the protocol), as opposed to *passive* only.

(b) **Adaptive.** There is a strong preference for considering threshold schemes that achieve **adaptive security** (i.e., against adaptively chosen corruptions), as compared to *static* only,

[4] For example, even though availability is a generically desirable property, a security formulation may on purpose specify that an adversary is allowed to abort protocol executions, so that the formulated security notion is achievable. As another example (now of an unsuitable formulation), a sole requirement of hiding and binding for a commitment scheme would not suffice for a use (e.g., committing bids in an auction) that would also require a non-malleability property.

with respect to critical safety properties (e.g., unforgeability). There is also a need for **practical feasibility**. Feedback is welcome on: (i) security formulations and reference approaches that simultaneously enable both qualities; and/or (ii) possible acceptable tradeoffs.

(c) **Proactive.** Threshold schemes should be compatible with mechanisms of **proactive** (and reactive) recovery, which attempt to recover possibly corrupted parties back to an uncorrupted state. This is especially important to better handle a persistent **mobile** adversary than continuously attempts to corrupt more parties. With respect to refreshing secret shares, the solutions can be based on a modularized phase of secret-resharing (see item 6), though also specifying the needed conditions (e.g., requirement of some initial/final agreement by a qualified quorum) for its integration.

To achieve security against the mentioned types of corruption, proposals of threshold schemes can consider security formulations with reduced liveness/availability, such as "**security with abort**".[5] This compromise is known to be necessary in some settings, depending on f/n and on the assumptions about the communication network (e.g., about the synchrony and reliability of channels). Still, when possible, there is value in attaining liveness/availability features, such as enabled by **identifiable abort**, **robustness**, **fairness** or even **guaranteed output delivery**. The pertinence of some of these termination options can also depend on the system model, including on how concurrent operations are handled, on who are the beneficiaries of the output (e.g., compare the parties in a threshold keygen vs. the client in a threshold signing).

4. System model. A proposal of threshold scheme must strive for a clear description that facilitates understanding various options across possible deployment scenarios.

(a) **Participants.** There is a **threshold entity** composed on n "parties". On the onset, all parties "know who" are the n parties, namely agreeing on n identifiers (possibly public keys to support authenticated channels).[6] For some operations, such as threshold keygen, the *beneficiaries* of the computation are the parties themselves, who end with a new (secret sharing) state that may require agreement (possibly in a sense of "security with **unanimous** abort"), and/or an administrator (e.g., who needs to accept a new public key). For other operations, such as threshold signing, the beneficiaries can be an external client, who initiates the computation with a request, and intends to determine an output. The client may or may not be aware of (and be able to interact distinctively based on) the n-party threshold composition (see "shared-I/O" interfaces[7] in Section 2.3 of IR 8214A). The possibility of **concurrent** execution requests must be considered. A baseline description can assume that there is a

[5] With "security with unanimous abort" the honest parties agree on whether or not there was an abort. This can be useful, for example, for a threshold keygen or secret resharing where the honest parties should collectively agree on having achieved a new secret-shared state. With "selective abort" (non-unanimous) some parties might be unaware that others have aborted. The suitability of the latter version needs to be carefully considered.

[6] The suitability of keys needs to be confirmed, locally or interactively, possibly using zero-knowledge proofs.

[7] These define whether or not a client can separately send/receive input/output shares to/from each party.

(possibly malicious) **proxy** that can: intermediate the communication between clients and the threshold entity, and authorize requested operations (e.g., the signing of a message).

(b) **Distributed systems and communication.** The description can decouple (i) classical distributed-systems' building blocks (e.g., consensus, reliable broadcast) from the (ii) essential cryptographic operations of the secure multiparty computation over (or of) a secret-shared key, as long as the interface and rules for composition are clearly specified. The specification of instantiations of the former (i), making use of weaker resources (e.g., enabling broadcast based on point-to-point channels), can be provided by reference to existing specifications & open-source implementations, while evaluating the impact of those replacements. A baseline description can make strong assumptions about the communication network, including synchrony and reliability of transmission. However, the proposal must discuss the pitfalls of deployment in environments with weaker guarantees (e.g., with asynchronous and unreliable channels), and possible mitigations. Different threshold schemes may be better suited to different communication environments, namely across the possible guarantees (and lack thereof) in terms of **synchrony**, **broadcast**, and **reliability**. It is important to understand how security guarantees break across these environments. The protocol can be described with various phases (e.g., offline, online, secret resharing), possibly with differentiated requirements.

5. Threshold profiles. For each primitive (see item 1) for thresholdization, it may be useful to consider differentiated solutions across various threshold parametrizations. For f/n: (i) S2PC ($(f, n) = (1, 2)$); (ii) honest majority ($f < n/2$); (iii) two-thirds honest majority ($f < n/3$); (iv) dishonest majority ($f \geq n/2$). For standalone n: "two" ($n = 2$); "small" ($3 \leq n \leq 8$); "medium" ($9 \leq n \leq 64$); and "large" ($n > 64$). The notion of "threshold profile" may be used to identify parametrization ranges. A threshold scheme proposal can focus on a single threshold profile or on several. The proposal must discuss the diversity of thresholds associated with various security properties. Future G&R may consider a suite of threshold schemes to cover various profiles. There is value in identifying motivating applications for adoption of threshold schemes in each profile.

6. Building blocks. Some building blocks (sometimes called gadgets) can be useful across various threshold schemes. A notable building block is Shamir **secret sharing** (and Lagrange interpolation), either in the clear or homomorphically (e.g., "in the exponent"). Other secret sharing variants may also be useful. Other examples of gadgets are **garbled circuits**, **oblivious transfer**, **commitments**, **secret resharing** (possibly for new values f and n), **multiplicative-to-additive share conversion**, **additively homomorphic encryption**, some **zero-knowledge proofs**, **consensus** and **broadcast**. To the extent possible, proposals of threshold schemes should modularize the description of gadgets. This means that a high-level description of the threshold scheme uses references to the interface and security properties of the gadgets, but not necessarily to low-level details. Then, a lower level description can be made for one (or more) possible instantiation of each needed gadget. While some future G&R documents may focus on gadgets, the decision to do so within the MPTC project will be subordinate to their utility for concrete threshold schemes. The upcoming call for proposals might also call for separate proposals of properly motivated gadgets.