Brief notes on Gadgets and Modularity in the NIST Threshold Call

Presented* on September 28th @ MPTS 2023 (Virtual)

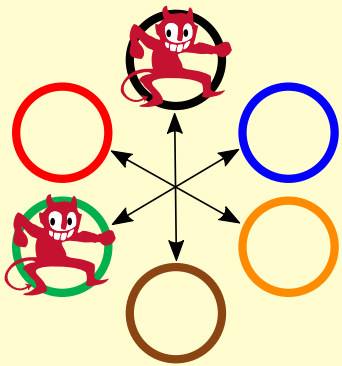
NIST Workshop on **M**ulti-**P**arty **T**hreshold **S**chemes 2023

Hosted by the Cryptographic Technology Group @ NIST
National **I**nstitute of **S**tandards and **T**echnology

* Luís Brandão (NIST/Strativia: Foreign Guest Researcher [non-employee] at NIST, contractor from Strativia).
Expressed opinions are those of the speaker/author and should not be construed as official views of NIST.

Gadgets in the NIST Call for Multi-Party Threshold Schemes

The Threshold Call scope includes:



- **Threshold schemes** for primitive across multiple subcategories (C1.1–C1.5; C2.1–C2.7)

- **Gadgets** (e.g., garbled circuit) useful to support the threshold setting (C2.8)

Example gadgets @ §A.8 of the Threshold Call (NISTIR 8214C ipd)

- garbled circuits
- oblivious transfer
- commitments
- consensus
- broadcast
- generation of correlated randomness
- secret resharing (possibly for new f or k, and new n)
- multiplicative-to-additive share conversion
- additively homomorphic encryption (AHE)
- MPC or ZKP friendly hashing

- *Gadgets can be proposed in a **standalone manner** in a submission, **or as a module** in a more encompassing submission in the scope of other subcategories.*
- *A **standalone** submission of an auxiliary gadget (and possible threshold versions) should make a **strong case for its utility** in supporting the threshold environment, and/or in supporting various concrete threshold schemes (in scope of other subcategories).*

Main components of a submission package

Check	#	Item
☐	M1	Written specification (S1–S16)
☐	M2	Reference implementation (Src1–Src4)
☐	M3	Execution instructions (X1–X7)
☐	M4	Experimental evaluation (Perf1–Perf5)
☐	M5	Additional statements

We favor **modularity** as an important principle.

A submission package can include/propose various **objects** (schemes/gadgets).

Each **component** will then map all such **objects** [NEXT SLIDES].

Modularizing M1 (Written specification)

- **M1:** a single PDF file (we will provide a LaTeX template)
- The PDF document may contain **multiple "parts"**, each enclosing the spec. of an object (threshold scheme or gadget) being proposed for subsequent public analysis.
- Abstract example: one submission with **3** threshold schemes and **9** building blocks:
  - a preliminary "part" with five (5) "**only-used**" gadgets (high-level interface and properties)
  - four (4) main "parts" to thoroughly specify the other four (4) building blocks
  - three (3) other main "parts" thoroughly describe each of the three threshold schemes.
- The revised Call is planned to allow **different "parts" to identify different sets of authors/submitters**. We hope this facilitates forming more comprehensive teams.
- Each forming team is encouraged to reach out to / **invite in advance the main inventors/authors** of the scheme/object specified in each main "part" of M1.

Modularizing M2 (open-source reference implementation)

- Each "part" in M1 (written spec) may have a respective **subfolder** in M2 (source code).
- **Only-used gadgets.** Even gadgets that are "only-used" (but not thoroughly specified in M1) must also include a corresponding open-source implementation in M2.
- **Attribution.** Naturally, the source-code obtained from external sources must contain proper attribution and have a corresponding compatible open-source license.

Modularizing M2 (open-source reference implementation)

- Each "part" in M1 (written spec) may have a respective **subfolder** in M2 (source code).
- **Only-used gadgets.** Even gadgets that are "only-used" (but not thoroughly specified in M1) must also include a corresponding open-source implementation in M2.
- **Attribution.** Naturally, the source-code obtained from external sources must contain proper attribution and have a corresponding compatible open-source license.

Modularizing M5 (additional statements)

The statement for each submitter will identify the applicable parts of the submission.

- **Simplest case:** all authors assume responsibility for every component/part.
- **Complex case:** different submitters claim responsibility for different components/parts.

Thank you for your attention!

Brief notes on Gadgets and Modularity in the NIST Threshold Call

September 28th @ Virtual

We appreciate followup comments: workshop-mpts2023@nist.gov

MPTS 2023
(Sept. 26–28)

Threshold Call
(Draft)

MPTC-Forum
(email list)

PEC-Forum
(email list)