"Preview Writeup": In anticipation of a package submission to the NIST Threshold Call

Title: <Catchy Name: Our Family of Crypto-Systems>

Subtitle: <Optional Subtitle: For Easier Conveyance of the Technical Scope>

Version: 0.1 (2025-07-28)[1]

Team name: <ShortCatchyTeamName>: <Optional Extended Team Name>

Team members: First Author, Second Author, Third Author, Fourth Author, Fifth Author, Sixth Author, Seventh Author, Eighth Author

Abstract: Include here an abstract with 150–200 words. Explain technical acronyms and do not include citation tags (such as [Ref]). The "preview writeup" represents a plan for a subsequent package submission within the scope of the NIST Threshold Call. The acceptance of the "preview writeup" will be followed by a corresponding public presentation in a NIST workshop. The preview is intended to (i) facilitate communication and collaboration across teams; (ii) promote the identification of opportunities for teams to strengthen their composition; and (iii) form an early expectation of the coverage of categories of the Threshold Call.

Categories of proposed crypto-systems: ECC KeyGen (N4.1); Threshold ECDSA Signature (N1.2); ZKPoK of <...> (S6); Gadget <...> (S7)

Keywords: Threshold Cryptography; NIST Threshold Call

Optional

Team Logo

[1] Preliminary version submitted to NIST-MPTC for review

Preview writeup. This document is provided to NIST for online publication, to foster public awareness and support public discussion within the scope of the NIST First Call for Multi-Party Threshold Schemes [NIST-IR8214C]. This "preview writeup" represents a good-faith plan for a subsequent "package submission". However, until the deadline for package submission, the team may still modify its own composition and the submission plan, including possible changes to the technical scope, and/or the used techniques or achieved results.

Team members: First Author [i1,a1*,a3], Second Author [i2,a2,a3], Third Author [i3,a3,a4†], Fourth Author [i4,a4], Fifth Author [i5,a1], Sixth Author [i6,a2,a3‡], Seventh Author [i7,a3], Eighth Author [i8,a4]

Open Researcher and Contributor Identifiers (ORCID):

i1 (0000-0002-1825-0097); i2 (0000-0002-1825-0097); i3 (0000-0002-1825-0097); i4 (0000-0002-1825-0097); i5 (0000-0002-1825-0097); i6 (0000-0002-1825-0097); i7 (0000-0002-1825-0097); i8 (0000-0002-1825-0097)

Affiliations:

[a1] Department Name A1, University Name B1 @ City and/or State, Country

[a2] Department Name A2, University Name B2 @ City and/or State, Country

[a3] [Office Name A3,] Company Name B3 @ City and/or State, Country

[a4] Division Name A4, Agency Name B4 @ City and/or State, Country

Associateship clarifications:

* Ph.D. student (non-employee). † Associate (visiting researcher). ‡ Work performed while on sabbatical leave.

Main contacts:

- **Team mailing list:** <team-catchy-name@list.<domain>.<TLD>
- **Primary technical contact person:** <author name>, <email address>
- **Secondary contact person 1:** <author name>, <email address>
- **Secondary contact person 2:** <author name>, email address

Produced by humans. The team hereby confirms that the content in this preview writeup: (i) was produced by the team members, and (ii) was not produced by generative artificial intelligence (AI), with the possible exception of AI-proposed grammar improvements, minor integrated suggestions, or some well-identified and short localized portions of auxiliary content (e.g., some illustration); and (iii) was proofread by the team members.

1. Introduction

Introduce the scope and purpose of the planned package submission, mentioning the crypto-systems that will be proposed (specified, implemented, evaluated), the (sub)categories they fit in, their real-world pertinence, and the overall fit within the Threshold Call's goal of gathering a public body of reference material.

Formatting of the preview writeup:

- **Writeup file:** Compile the document into a tagged portable document format (PDF) file (already achieved in this template), with name as in "`<team-name>-preview-v0-1.pdf`".
- **Space:** The preview writeup shall be **at most six pages**, excluding {cover, verso page, references}, with letter size (11" x 8.5"), portrait orientation, 1" margins. Do not include appendices after the references section.
- **Font:** Latin Modern Sans (for the main text), 12 pt size. Headings and footnotes can respectively have larger and smaller font sizes. Special symbols and math content can use different fonts (e.g., Latin Modern Math).

Submission process: Email the preview writeup to MPTC-submissions@list.nist.gov, with subject "Threshold Call Preview Writeup: <title>", and cc'ing your team's mailing list. Every team member should then acknowledge receipt by sending a reply email with the note: "I have reviewed the submitted preview writeup, agree with its content, and confirm being part of the submitting team."

Versioning: Use version 0.1 for the initial version submitted by email. Teams will have the opportunity to revise their preview writeup before it is published by NIST, before the public session of presentations. The version for publication should be set to 1.0.

The following sequence of sections and topics is a suggestion, not strictly required. Each team decides which depth to use in the explanation of their plan, not exceeding the limit on number of pages.

2. Specification

High-level notes on:

- **Organization:** How the specification document will be organized with regard to the explanation of various crypto-systems; which main (families of) complex building blocks will be modularized and/or may be of independent interest for analysis; whether differentiated teams may be identified across various "parts" of the specification?
- **System model:** The chosen system model, including trusted setup, networking, and threshold profiles; the involved technical approaches and techniques.
- **Security:** High-level notes about security: formulation, goals and properties with regard to adversarial goals and capabilities; assumptions; security strength estimation.

3. Open-Source Implementation

High-level notes on:

1. **Code structure:** The main modules to be included in the *core code*, and which programming language(s) will be used; the open-source libraries to potentially include as *bundle dependencies* and as *external dependencies*; which compiler and compilation options; the build script(s) and the benchmarking script(s).
2. **Code progress and availability:** The status of the code development; whether there is already a public Git-compatible repository with some code available for early public testing.
3. **Implementation of the networking model:** How the main networking functionalities (e.g., broadcast, or reliable transmission) are intended to be implemented (or modeled) in practice in the baseline platform.
4. **Testing:** Identify challenges related to testing and reproducibility. Comment on envisioned testing of protocol results in case of malicious behavior (by one or some of the parties), and arbitrary (non-optimal and/or pessimistic) networking conditions.

4. Experimental performance evaluation

High-level notes on:

1. **Performance:** Expected (or measured) performance, and possible comparisons with performance of different related techniques.
2. **Platform:** Anticipated challenges when using the baseline platform (single computer, with 16 cores and 64 GB of RAM, as mentioned in the response to item F2b.3.1 in the compilation of public comments [PubComs2PD] on the 2pd); comparison with results/challenges with other (possibly more suitable) platforms.

5. Licensing, patent claims, and funding

1. The open-source licenses (from the open-source initiative) in your *core code*, and in the chosen dependencies (bundled and external).
2. Preliminary list of known patents that (i) do or could have claims that may cover the contents of the submission, and (ii) include a team member who is one of the inventors, applicants, or assignees, or who is sponsored by or employed by an entity that holds the corresponding patent rights. (This can be a list of citation tags, to be detailed in the References section.)
3. Consider acknowledging external research funding associated with the planned submission.

References

To remove this box, call \togglefalse{SHOW_PREAMBLE_IN_REFS} in `zz-00a-pkgs-cmds-form.tex`

Include at least the most significant references pertaining to your work. List also (if already determined) the Git-compatible public repository where you expect to include your core-code and bundled dependencies.

In each bib entry, include:

- field `doi` when applicable; if not applicable, then include a field `url`
- `addendum = {\aaIACR{YYYY/NNNN}}` (if there is an available ia.cr version)

[NIST-IR8214C] Luís T. A. N. Brandão and René Peralta. *NIST First Call for Multi-Party Threshold Schemes*. (National Institute of Standards and Technology) NIST Internal Report (NISTIR) 8214C. 2025. DOI: 10.6028/NIST.IR.8214C.

[PubComs2PD] NIST-MPTC. *Compilation of Public Comments on NISTIR 8214C 2pd*. National Institute of Standards and Technology, Multi-Party Threshold Cryptography. June 2025. URL: https://csrc.nist.gov/files/pubs/ir/8214/c/2pd/docs/nistir-8214c-2pd-public-feedback.pdf.