

Preview Writeup Template for the NIST Threshold Call

Version: 0.2 (February 24, 2026)*

Abstract: The NIST Threshold Call (NIST IR 8214C) establishes a “Preview” phase for public presentations of plans of upcoming package submissions. This document is the PDF compilation of the LaTeX-based template for “Preview Writeups.” A previous version was available for the first round of previews (January 2026). The present version improves a few editorial features. By using this template, teams will produce their preview writeup with a predictable and accessible format, facilitating the public analysis across the set of submissions.

Note: The present page is just a cover page, not to be included in actual Preview Writeups.

Selected notes about the LaTeX code:

1. It should be compiled with a recent LuaLaTeX version (mid-2025 onward).
2. It aims at accessible PDF/A & PDF/UA (`{a-4, ua-2}` or `{a-2, ua-1}`) compliance.
3. A metadata file gathers all info needed for the cover and verso compilation.
4. A `bib-addenda` file enables enhancing bibliographic items with links to accessible sources.
5. Formatting code is “hidden” in the `./format` folder, allowing authors to focus on content.

First round of previews. In January 2026, 23 teams submitted 26 preview writeups, and gave corresponding preview talks at the NIST Workshop on Multi-party Threshold Schemes (MPTS) 2026. The writeups and slide decks are accessible via the project and workshop pages:

- MPTS 2026: <https://csrc.nist.gov/events/2026/mpts2026>
- MPTC project: <https://csrc.nist.gov/projects/threshold-cryptography/tcall-1>

Other rounds. The NIST Threshold Call sets two more rounds for submission of preview writeups. In the meantime, updates to previous preview writeups are also accepted.

*Produced by Luís Brandão (FGR, Contractor at NIST); email comments to MPTC-Submissions@list.nist.gov.

Page intentionally blank

“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: Preview Writeup 0.1 (2026-02-24)¹

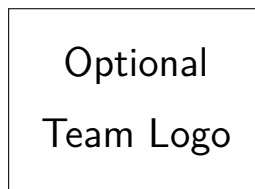
Team name: <ShortCatchyTeamName>: <Optional Extended Team Name>

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.

Proposed crypto-systems:

Keywords: Threshold Cryptography; NIST Threshold Call; Add meaningful Keywords



(Logo AI-generated with <Agent name>)

Document License: Optional license (e.g., CC BY 4.0 International)

¹Preliminary 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,a5†}, Fourth Author^{i4,a5a4}, Fifth Author^{i5,a1}, Sixth Author^{i6,a2,a3‡}, Seventh Author^{i7,a3}, Eighth Author^{i8,a5}

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:

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>-PW.pdf".
- **Page size:** Use letter size (11" x 8.5") pages, in portrait orientation, with 1" margins.
- **Font:** Latin Modern Sans (for the main text), 12 pt size. Headings and footnotes can respectively have larger and smaller font sizes. Special symbols (e.g., $\mathcal{A} : \pi$) and math content (e.g., $1 + 1$) can use different fonts (e.g., Latin Modern Math).
- **Cover and Verso.** The automatic cover and verso contents should each fit into a single page. The metadata file has toggles and commands that allow compact formatting in case of extensive team information.
- **Sections.** The main sections (after the verso page, and before the References) shall occupy **at most six pages** for description of the submission plan / crypto-systems. Use Title Case in headings of (sub)sections. One extra page is acceptable for including notes of comparison with other preview writeups (see Section 6). In the preview writeup, do not include appendices after the references section.

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: Consider using version 0.1 for the initial version submitted by email to NIST. Teams will have the opportunity to revise their preview writeup before it is published by NIST, and before the public session of presentations. **The initial version of a preview writeup for public posting should show "Preview Writeup 1.0" in the cover.** Future updates are possible, and should then increment the version number, e.g., 1.1, 1.2, and so forth, or 2.0 (if prepared for a subsequent round of presentations).

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.

6. Comparison with Other Submissions

If applicable, please explain the main differences between your proposed crypto-system(s) and others (from other teams) also proposed for submissions of the same type of crypto-systems (e.g., threshold schemes for the same primitive or within the same category in case there are no subcategories). The idea is to facilitate assessing to which extent the various submissions may be complementary, redundant, competing, have interchangeable building blocks, etc.

Example aspects of comparison: applicable threshold profile, underlying techniques/approach, security properties, efficiency, applicability.

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.

For each bib item, if the document pointed by the doi (when applicable) is not freely available to the public (e.g., if it is behind a paywall), then **please add an addendum field with a hyperlinked reference to a freely accessible version of the referenced work**, preferably with author-retained control over possible updates.

Even if the doi referenced document is not pay-walled, consider (when applicable) including a hyperlink to the version available on the IACR [Eprint Archive](#), or some other mainstream eprint free repository such as [arXiv](#). The addendum can also be used for a succinct clarification of alternative meaningful versions (e.g., journal).

If directly editing bib entries is inconvenient, then the file `zz-91-bib-addenda.tex` can be used to modularly specify for any bib entry (based on its key) a note to appear in the end of the printed reference. Example usage:

- `\bibiacr{citekey}{YYYY/NNNN}` for an addendum “Also at [ia.cr/YYYY/NNNN](#)”
- `\bibarxiv{citekey}{NNNN.NNNNN}` for an addendum “Also at [arXiv:NNNN.NNNNN](#)”
- `\bibfinalnote{citekey}{arbitrary note}` for an addendum “*arbitrary note*”

A more generic (but still experimental; will fail on some inputs) command `\bibfieldadd{citekey}{field}{some content}` can be used to append *some content* to a chosen *field* of the bib entry with a given *citekey*.

[TestTag] Test Author. *Test Title in a @misc Style Bib Entry*. Original howpublished content. Original note content. Example ad-hoc note using `\bibfieldadd`. August 2025. DOI: [NN.NNNN/NNNN.NNNN](#). URL: <https://www.example.com/testURL-in-alternative-to-a-hyperlinked-doi>. Original addendum content. Ad-hoc addendum using `\bibfieldadd`. Ad-hoc “**final note**” using `\bibfinalnote`.

[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. 2026. DOI: [10.6028/NIST.IR.8214C](#).

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