Compilation of Public Feedback to NISTIR 8214B-ipd

NIST Multi-Party Threshold Cryptography Project[1]

Updated: December 23, 2022

The present document compiles four public comments received by email via nistir-8214b-comments (at) nist (dot) gov, in reply to the call for public comments on NISTIR 8214B ipd (the **i**nitial **p**ublic **d**raft of the NIST Internal report 8214B) published on August 12th, 2022. A future document will publish a "diff" between the final and the ipd versions of NISTIR 8214B, along with comments on the changes between the two versions.

Contents

[1]Webpage: https://csrc.nist.gov/projects/threshold-cryptography; email address: threshold-MP-call-2021a@nist.gov.

Item 1: The contacts page of NISTIR 8214B ipd

The initial public draft (ipd), with digital object identifier (doi) 10.6028/NIST.IR.8214B.ipd is available via the NIST Computer Security Resource Center (CSRC), at: https://csrc.nist.gov/publications/detail/nistir/8214b/draft. The contacts page of NISTIR 8214B ipd is copied below, showing the email address where to submit public comments.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies
Copyright, Fair Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
This version is the initial public draft (ipd).

How to cite this NIST Technical Series Publication
Luís T. A. N. Brandão, Michael Davidson (2022). Notes on Threshold EdDSA/Schnorr Signatures. (National Institute of Standards and Technology, Gaithersburg, MD) NIST IR 8214B ipd. https://doi.org/10.6028/NIST.IR.8214B.ipd

NIST Author ORCID iDs
Luís T. A. N. Brandão: 0000-0002-4501-089X
Michael Davidson: 0000-0002-4862-5697

Contact Information
nistir-8214B-comments@nist.gov

Public Comment Period
August 12, 2022 – October 24, 2022

Submit Comments
Only via email: nistir-8214B-comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Item 2: Feedback from Erik Aronesty

From: Erik Aronesty <...@q32.com>
Sent: Tuesday, October 4, 2022 10:05
To: nistir-8214B-comments <nistir-8214B-comments@nist.gov>
Subject: criticality of establisting a distributed key secure from mitm attacks

any time threshold cryptography is used, it's important to stress that the secure establishment of a secret key should be

- simple to implement
- easy to understand

1. simple approach:

i am a big advocate of the simple, pedersen multi round secure dkg with precommitments, rather than more complex constructs that can produce multifactor keys with fewer commitments, but are inherently difficult to code and prove secure

- each factor publishes commitments to public keys
- only after commitments are received are keys published
- keys are published along with posk (proof of secret key)

2. there are many ways to restart a failed key establishment

- exclude the node (assume it's an attacker)
- restart without exclusion (assume it's a mistake)

strategies to prevent denial of service may not always be warranted. denial of service might be the correct outcome until the user is notified and the node manually removed (for example)

3. falling back to chain-of-trust methods can result in a significant loss of security

at the heart of threshold cryptography is the notion of *not trusting a central or single-point of failure*. falling back on TLS certificates for communication during key establishment, for example, should be discouraged, and mechanism for establishing direct E2E encrypted channels, including QR codes, and manual, out-of-band verification of e2e encryption keys are important

4. channel contagion should be discussed

threshold cryptography provides no benefit if the attacker can use the cryptographic system itself to "jump" between devices. mechanisms for obscuring the identity of devices participating in threshold systems, including relay onion routing, should be discussed

Item 3: Feedback from Chelsea Komlo

From: Chelsea Komlo <...@uwaterloo.ca>
Sent: Thursday, October 20, 2022 19:13
To: nistir-8214B-comments <nistir-8214B-comments@nist.gov>
Subject: Comments on NISTIR-8214B

Dear all,

Please see attached for comments and recommendations for NIST draft 8214B: "Notes on Threshold EdDSA/Schnorr Signatures."

Thanks, happy to discuss further if there are any questions or discussion.
Chelsea

Item 3: Feedback from Chelsea Komlo

Feedback on "Notes on Threshold EdDSA/Schnorr Signatures"

Chelsea Komlo

October 2022

1 Introduction

NIST recently put out a document summarizing the state of the art in threshold EdDSA signatures, suggested directions for future work, and recommendations for a public call for threshold EdDSA schemes. This document outlines several recommendations that, if added, would strengthen the document and increase the likelihood of success in adoption.

2 Comment One: Specify Single-Party EdDSA over a Generic Group

Currently, the document references EdDSA single-party signatures with respec to only curves 25519 and 448. However, there is likely interest to use both single-party and threshold EdDSA over additional curves.

To address this interest, the FROST IETF draft [1] defines group operations with respect to a generic prime-order group, and then defines operations with respect to this generic group. The draft additionally defines single-party Schnorr signature generation and verification with respect to this generic group; see Appendix B. It would be helpful for NIST to standardize single-party Schnorr in a similar manner, as having a threshold signature standard where no single-party standard yet exists may lead to confusion down the road.

> Suggestion: Define a standard for single-party Schnorr signatures over a generic prime-order group, and define how various elliptic curve groups can be employed with respect to this standard.

3 Comment Two: Decouple Threshold Key Generation from Signing

The draft currently separates key generation as a generic method from threshold EdDSA signing. Doing so is important, as practitioners are often confused which

Item 3: Feedback from Chelsea Komlo

key generation mechanisms can be used with which schemes.

> Suggestion: In the public call for threshold schemes, require independent and distinct key generation and threshold signature submissions.

4 Comment Three: Clarify which Schemes Require Session Identifier Agreement

The document currently implies that agreement on a session identifier is required for all probabilistic threshold schemes. However, FROST only requires that participants not re-use nonces, and its proof of security does not assume that participants agree on a session identifier. Instead, FROST assumes that participants only agree upon the message to be signed, the set of signers, and which signer commitments are employed to generate the group commitment R.

Agreement on a session identifier can be prohibitive in certain deployment settings and implies a greater degree of trust in the entity which chooses it. Hence, it is important to clarify which schemes require session identifier agreement as a security requirement, and which do not.

> Suggestion: Clearly specify which schemes strictly require session identifier agreement and which schemes do not.

5 Comment Four: Differentiate Broadcast Channels from an Untrusted Coordinator

In their strictest definition, broadcast channels assume the following properties:

1. *Consistent.* Each player has the same view of the messages which are broadcasted.
2. *Authenticated.* Players can strongly authenticate which messages were broadcasted by which players. In practice, this requirement is generally fulfilled by an existing PKI.
3. *Reliable Delivery.* All players can be assured that their broadcasted messages were in fact sent to all other players.
4. *Synchronous.* The network ensures that all messages are sent and received in a round before proceeding to the next round.

Requiring a broadcast channel therefore implies infrastructure (such as a PKI) and additional network rounds. Some multi-party schemes require all of these properties for their proof of security to hold. For example, schemes that are in the honest-majority setting such as the DKG by Gennaro et al. [3] strongly require these properties.

Item 3: Feedback from Chelsea Komlo

However, for some threshold signature schemes such as FROST, the scheme simply requires an *untrusted coordinator*. Here, the coordinator is simply required to forward messages between participants. However, if the coordinator fails to do so, the scheme simply results in a denial of service attack, as opposed to a security break.

> Suggestion: Clarify the difference between broadcast channels and an untrusted coordinator. Further, state explicitly which schemes strictly require a broadcast channel for security, and which assume only an untrusted coordinator.

6 Comment Five: Specify ZKPoK Requirements for Simulatable Schemes

The document currently specifies that a generic ZKPoK is required for three-round Schnorr signatures proven to be simulatable with respect to single-party Schnorr signatures. However, the choice of ZKPoK in fact impacts the security of the scheme. The document should in fact say that for simulatability, an online-extractable ZKPoK is required, which in practice is Fischlin's transform [2].

Specifying this requirement is important, as otherwise it could be confused that any ZKPoK is allowed (for example, a simple Schnorr proof of knowledge), which is not the case. Further, use of Fischlin's transform dramatically impacts both how the sscheme is implemented, as well as its efficiency. Hence, the requirement of *which* ZKPoKs are assumed is an important requirement to specify to practitioners.

> Suggestion: Clarify that the ZKPoK required for three-round simulatable schemes *must* be online-extractable, and give examples of which ZKPoKs fulfill this requirement (i.e, Fischlin) and which do not (i.e, Schnorr).

References

[1] D. Connolly, C. Komlo, I. Goldberg, and C. Wood. Two-round threshold schnorr signatures with frost.

[2] M. Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In V. Shoup, editor, *CRYPTO 2005, Santa Barbara, California, USA, August 14-18, 2005*, volume 3621 of *LNCS*, pages 152–168. Springer, 2005.

[3] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure distributed key generation for discrete-log based cryptosystems. In J. Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory*

Item 3: Feedback from Chelsea Komlo

and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, volume 1592 of *Lecture Notes in Computer Science*, pages 295–310. Springer, 1999.

Item 4: Feedback from Jonathan Katz

From: Jonathan Katz <...@gmail.com>
Sent: Monday, October 24, 2022 08:58
To: nistir-8214B-comments <nistir-8214B-comments@nist.gov>
Subject: typo in draft

In line 1350, should it instead read "an adversary may be able to select a message with a noticeable relation to R"?

Item 5: Feedback from Arash afshar

From: Arash Afshar <...@coinbase.com>
Sent: Monday, October 24, 2022 10:32
To: nistir-8214B-comments <nistir-8214B-comments@nist.gov>
Cc: Yehuda Lindell
Subject: Comments on "NIST Internal Report 2 NIST IR 8214B ipd"

To Luís T. A. N. Brandão, Michael Davidson,

Thank you for your notes on threshold EdDSA/Schnorr signatures. It was a great write up which provided a great coverage of the problem and the state of the art. After reading the document, we, the applied cryptography group at Coinbase, have some comments and recommendations for how to improve the document as described below. We would be happy to meet and discuss these further if needed.

- Section "A template threshold Schnorr/EdDSA signature" (line 998): In the threshold setting, proactive security becomes more important to protect against situations where an attacker corrupts one party at timestep 1 and then corrupts another party at timestep 2 (and so on). In this setting, over time, the attacker can gather all the key shares and reconstruct the full private signing key. Therefore, we recommend that a threshold scheme to have a “refresh” method as part of its template. The refresh method can either be run periodically or run after each signature operation to create fresh shares of the keys to the parties. We stress that this does not necessarily mean that full adaptive security is needed, since one can define a “static proactive model” where the adversary chooses who to corrupt at the beginning of each epoch.
- Section "Distributed key generation (DKG) approach" (Lines 1028-1045): This section does not have any reference to newer DKG papers and therefore does not describe some of the simulation based techniques of proving the security of DKG models. We recommend describing these newer simulation based approaches, for example as described in Lin22
- Section "MPC-based threshold (deterministic) EdDSA" (Line 1171): We advise against recommending MPC-friendly hash functions since these are far less well-studied than standard hash functions. As we know hash functions are extraordinarily hard to get right.

  Instead, our recommendation is to study and standardize the following statement: probabilistic threshold signature schemes can be used in place of a deterministic non-threshold scheme. You have indeed made a similar argument in section 6.1 and we recommend that the usage of threshold probabilistic schemes be recommended during the standardization process. This should at least be the case given the state of the art today which incurs a severe performance penalty for deterministic signing. As the report also shows, deterministic signing in MPC is much easier to get wrong.
- In section 4.4, when describing the two approaches to proving the security of signing: We recommend making the following point regarding the modularity of DKG and Signing based on how the signing protocol has been proven: simulatability vs game-based – if the signing is proven with an ideal functionality, then security is maintained for any secure key generation scheme. So, if BIP032 is secure, for example, then the threshold scheme will be secure when BIP032 key generation is used. This isn’t true of game-based definitions which would typically have to be reproven secure for each different derivation method.
- Lines 1224-1227 (when describing Lin22): We ask to reword the sentences to tell the reader that indeed the two ways of output the signature are equivalent, e.g., outputting (r,s) vs (e,s) and therefore the change to make the scheme interchangeable w.r.t EdDSA is trivial.

Best regards,
Arash Afshar
Applied Cryptography Group @ Coinbase