FROST Messages & Data Serialization

April 13, 2021

Contents

1 Overview **1**

2 Headers **1**

3 Data **2**

3.1 Key Generation with DKG 2

3.1.1 Round One 2

3.1.2 Round Two 2

3.2 Key Generation with Dealer 3

3.3 Preprocessing 3

3.4 Signing 3

3.4.1 Round One 3

1 Overview

The following document describes the byte-level structure of messages sent in FROST. Each message consists of a header of fixed size followed by the actual payload of the message.

2 Headers

All messages have the following header:

Bytes	Field Name	Data Type
1	Message Type	`u8`
1	Version	`u8`
2	Sender ID	`u16`
2	Receiver ID	`u16`

The `Message Type` and `Version` fields specify the data that follows after the header. The sender is uniquely identified by the `Sender ID` field and the receiver is uniquely identified by the `Receiver ID` field.

3 Data

Messages in FROST are split into four general domains. The following sections describe each domain and its messages.

3.1 Key Generation with DKG

These messages are sent during the Distributed Key Generation (DKG).

3.1.1 Round One

Broadcast the public commitment $\vec{C}$ and σ

Header:
`Message Type = 1`
`Version = 1`

Data:

Bytes	Description	Data Type
2	Size of the commitment `n`	`u16`
512 * `n`	Commitments to individual coefficents	`[AffinePoint; n]`
TBA	σ_i	

3.1.2 Round Two

Broadcast the Secret Shares

Header:
`Message Type = 2`
`Version = 1`

Data:

Bytes	Description	Data Type
256	Secret share `f_i(l)`	`Scalar`

3.2 Key Generation with Dealer

3.3 Preprocessing

3.4 Signing

3.4.1 Round One

Share Signing Commitments

Header:

```
Message Type = 3
Version = 1
```

Data:

Bytes	Description	Data Type
2	Number of signing commitments `n`	`u16`
1024 * `n`	Signing commitments	`[SigningCommitment; n]`