Adaptations from CGGMP21

J.-P. Aumasson A. Hamelink L. Meier

14-07-2021

Our implementation tries to follow the original specification provided in [CGGMP21], but we detail here the modifications we applied.

Broadcast considerations

Abort identification requires the use of a reliable broadcast channel. Unfortunately, this condition is hard to meet in practice when the network is modeled as point-to-point. The protocol generally requires the message from the first round to be reliably broadcast, and so for this step we use the *"echo broadcast"* from Goldwasser and Lindell.

In the keygen and refresh protocols, the broadcasted message is a commitment, so we need to add an extra round of communication to make sure the parties agree on the first set of messages. For the signing protocol, the "echo round" can be done in parallel during the second round.

The main disadvantage of this approach is that an adversary can cause an abort by simply sending different messages to different parties. It therefore makes little sense to implement the indentifiable abort aspect of the signing protocol since an adversary could simply cause an annonymous abort at the start of the protocol.

On the flip side, the user of the library only needs to provide authenticity and integrity between the point-to-point connections between parties.

Threshold Keygen/Refresh Protocols

In the original paper, the TSS functionality is such that the keygen needs to run the refresh protocol right after. Moreover, the scheme is not adapted to the threshold case.

We implement a combined Keygen/Refresh protocol, where we highlight the differences in blue and red respectively.

- Keygen performs the refresh at the same time, so there is no need to two protocols.

- Both protocols now use a threshold t for Shamir secret sharing ($t+1$ secret key shares are required to reconstruct the full secret).
- Optionally, we can also include the extra *El Gamal* keys Y, but since we only care about the 4 round signing protocol, we ignore it.
- If we want to prove this scheme secure, then we would need to change the idea threshold signature functionality. Indeed, it currently assumes refresh is run after keygen. We would need to change the ideal functionality, and adapt the protocol to the t, n case.
- The main difference is that we add a final round of communication where the parties prove in zero-knowledge that they know their new secret share.

We define the SSID as $\mathsf{ssid} = (\mathsf{sid}, ...)$ where $\mathsf{sid} = (q, G, t, n, \{P^{(j)}\}_{j=1}^n)$ and where ... is the public information that all parties already know. When the SSID is used as header for the message, it will most likely be its hash so that we don't send too much information in each message. Moreover, the computation of this hash should be the same for all parties (i.e. deterministic).

Round 1 Interpret

$$\mathsf{ssid} = (\mathsf{sid}, \rho_{old}, \{\mathsf{pk}_{old}^{(j)}\}_{j=1}^n, \{N_{old}^{(j)}\}_{j=1}^n, \{s_{1,old}^{(j)}\}_{j=1}^n, \{s_{2,old}^{(j)}\}_{j=1}^n),$$

where $\mathsf{sid} = (q, G, t, n, \{P^{(j)}\}_{j=1}^n)$, and retrieve private input $\mathsf{sk}_{old}^{(i)}$.

- Sample $x^{(i)} \in \mathbb{F}_q$.
  - $X^{(i)} \leftarrow x^{(i)} \acute{\mathrm{L}} G$.
- Sample 4κ-bit safe primes $p^{(i)}, q^{(i)}$.
  - $N^{(i)} \leftarrow p^{(i)} \cdot q^{(i)}$.
- Sample $\lambda^{(i)} \in \mathbb{Z}_{N^{(i)}}^*$, $r \in \mathbb{Z}_{\phi(N^{(i)})}^*$.
  - $s_1^{(i)} \leftarrow r^2 \bmod N^{(i)}$.
  - $s_2^{(i)} \leftarrow r^{2\lambda} \bmod N^{(i)}$.
- Sample $f^{(i)}(Z) \in \mathbb{F}_q[Z]$, such that $f^{(i)}(Z) = x^{(i)} + \sum_{l=1}^t f_l^{(i)} Z^l$.
  - $x_i^{(i)} \leftarrow f^{(i)}(i)$
  - Define VSS polynomial coefficients $F_l^{(i)} \leftarrow f_l^{(i)} \acute{\mathrm{L}} G$, for $l = 1, \dots, t$.
- Sample $a^{(i)} \in \mathbb{F}_q$.
  - $A^{(i)} \leftarrow a^{(i)} \acute{\mathrm{L}} G$.
- Sample $\rho^{(i)}, u^{(i)} \in \{0,1\}^\kappa$.
- $V^{(i)} \leftarrow \mathsf{H}(\mathsf{ssid}, i, \rho^{(i)}, \{F_l^{(i)}\}_{l=1}^t, X^{(i)}, A^{(i)}, N^{(i)}, s_1^{(i)}, s_2^{(i)}, u^{(i)})$.

Broadcast $(\mathsf{ssid}, i, V^{(i)})$.

Round 1 (Echo) Upon reception of $(\mathsf{ssid}, i, V^{(j)})$ from all $P^{(j)}$:

- $E^{(i)} \leftarrow \mathsf{H}(\mathsf{ssid}, V^{(1)}, \dots, V^{(n)})$.

Broadcast $(\mathsf{ssid}, i, E^{(i)})$.

Upon reception of $(\mathsf{ssid}, i, E^{(j)})$ from all $P^{(j)}$:

- $E^{(i)} \stackrel{?}{=} E^{(j)}$.

Deliver $(\mathsf{ssid}, i, V^{(j)})$ from all $P^{(j)}$ for the next round.

Round 2 Upon reception of $(\mathsf{ssid}, i, V^{(j)})$ from all $P^{(j)}$:

Send $(\mathsf{ssid}, i, \rho^{(i)}, \{F_l^{(i)}\}_{l=1}^t, X^{(i)}, A^{(i)}, N^{(i)}, s_1^{(i)}, s_2^{(i)}, u^{(i)})$ to all.

Round 3 Upon reception of $(\mathsf{ssid}, j, \rho^{(j)}, \{F_l^{(j)}\}_{l=1}^t, X^{(j)}, A^{(j)}, N^{(j)}, s_1^{(j)}, s_2^{(j)}, u^{(j)})$ from $P^{(j)}$:

- $V^{(j)} \stackrel{?}{=} \mathsf{H}(\mathsf{ssid}, j, \rho^{(j)}, \{F_l^{(j)}\}_{l=1}^t, X^{(j)}, A^{(j)}, N^{(j)}, s_1^{(j)}, s_2^{(j)}, u^{(j)})$.
- $\log_2 N^{(j)} \stackrel{?}{=} 8\kappa$.

If all checks pass:

- $\rho \leftarrow \bigoplus_j \rho^{(j)}$.
- $F^{(j)}(Z) \leftarrow X^{(j)} + \sum_{l=1}^t Z^l \acute{\mathrm{L}} F_l^{(j)}$, for all $P^{(j)}$.
- $C_j^{(i)} \leftarrow Enc_j(f^{(i)}(j))$, for all $P^{(j)}$.
- $\psi_{\mathsf{mod}}^{(i)} \leftarrow \mathsf{Prove}(\mathsf{mod}, (\mathsf{ssid}, \rho, i), N^{(i)}; (p^{(i)}, q^{(i)}))$.
- $\psi_{\mathsf{prm}}^{(i)} \leftarrow \mathsf{Prove}(\mathsf{prm}, (\mathsf{ssid}, \rho, i), (N^{(i)}, s_1^{(i)}, s_2^{(i)}); \lambda^{(i)})$.

Send $(\mathsf{ssid}, i, \psi_{\mathsf{mod}}^{(i)}, \psi_{\mathsf{prm}}^{(i)}, C_j^{(i)})$ to each $P^{(j)}$.

Round 4 Upon reception of $(\mathsf{ssid}, j, \psi_{\mathsf{mod}}^{(j)}, \psi_{\mathsf{prm}}^{(j)}, C_j^{(j)})$ from $P^{(j)}$:

- $x_i^{(j)} \leftarrow Dec_j(C_i^{(j)}) \mod q$.
- $F^{(j)}(i) \stackrel{?}{=} x_i^{(j)} \acute{\mathrm{L}} G$.
- $\mathsf{Verify}(\mathsf{mod}, (\mathsf{ssid}, \rho, j), N^{(j)}; \psi_{\mathsf{mod}}^{(j)})$.
- $\mathsf{Verify}(\mathsf{prm}, (\mathsf{ssid}, \rho, j), (N^{(j)}, s_1^{(j)}, s_2^{(j)}); \psi_{\mathsf{prm}}^{(j)})$.

If all checks pass:

- $\mathsf{sk}^{(i)} \leftarrow \mathsf{sk}_{old}^{(i)} + \sum_{j=1}^n x_i^{(j)}$.
- $F(Z) \leftarrow \mathsf{pk}_{old} + \sum_{j=1}^n F^{(j)}(Z)$.
- $\mathsf{pk} \leftarrow F(0)$.
- $\mathsf{pk}^{(j)} \leftarrow F(j)$, for all $P^{(j)}$.
- $\psi_{\mathsf{sch}}^{(i)} \leftarrow \mathsf{Prove}(\mathsf{sch}, (\mathsf{ssid}, \rho, i), (\mathsf{pk}^{(i)}, A^{(i)}); (\mathsf{sk}^{(i)}, a^{(i)}))$.

Send $(\mathsf{ssid}, i, \psi_{\mathsf{sch}}^{(i)})$ to all.

Output Upon reception of $(\mathsf{ssid}, i, \psi_{\mathsf{sch}}^{(j)})$ from $P^{(j)}$:

- $\mathsf{Verify}(\mathsf{sch}, (\mathsf{ssid}, \rho, j); (\mathsf{pk}^{(j)}, A^{(j)}); \psi_{\mathsf{sch}}^{(j)})$.

If all checks pass, save:

- Secret $\mathsf{sk}^{(i)}, p^{(i)}, q^{(i)}$.
- $\mathsf{ssid} \leftarrow (\mathsf{sid}, \rho, \{\mathsf{pk}^{(j)}\}_{j=1}^n, \{N^{(j)}\}_{j=1}^n, \{s_1^{(j)}\}_{j=1}^n, \{s_2^{(j)}\}_{j=1}^n)$.

Signing

Interpret $\mathsf{ssid} = (\mathsf{sid}, \rho, \{\mathsf{pk}^{(j)}\}_{j=1}^n, \{N^{(j)}\}_{j=1}^n, \{s_1^{(j)}\}_{j=1}^n, \{s_2^{(j)}\}_{j=1}^n, \{P^{(j)}\}_{j\in S}, m)$, where S is a subset of $\{1, \ldots, n\}$ of size at least $t+1$, and m is the message to be signed.

The protocol goes exactly as before, except that the `Session` will use S to determine Lagrange coefficients and apply them to the set of public keys, as well as the signer's secret share. Therefore, the resulting shares represent an additive sharing of the secret, and the original protocol can be used.