Privacy-Preserving Identity Systems

No Author Given

No Institute Given

Bellare Properties - Anonymity | uncorrupt opener | fully corrupt issuer - Traceability | partially corrupt opener | uncorrupt issuer - Non-frameability | fully corrupt opener | fully corrupt issuer

[BCK+22]

Correctness

1. the signature should be valid
2. the opening algo should correctly identify the Signer given the message and signature
3. the proof returned by opening algo should be accepted by the judge

Formalize correctness with an experiment involving an adversary.

involved: Adversary, signature scheme, adversary A, secparam k.

$$Adv^{corr}_{GS,\mathcal{A}}(k) = \Pr[\mathsf{Exp}^{corr}_{GS,\mathcal{A}}(k) = 1]$$

We say the dynamic group signature scheme GS is correct if $Adv^{corr}_{GS,\mathcal{A}}(k) = 0$ for any adversary $\mathcal{A}$ and any $k \in \mathbb{N}$, the adversary is not computationally restricted.

Experiment $\mathsf{Exp}^{corr}_{GS,\mathcal{A}}(k)$

This says 1. run GKg with secparam, get gpk, ik, ok 2. Corrupt users set is 0

Construction 1: Proof of Zero(C)

Public Parameters: $g_1, g_2, h_1 \in \mathbb{G}$

Inputs: C such that $C = g_1^m g_2 h^r$, $\mathcal{P}$ knows $m, r \in \mathbb{Z}_q$.

1. $\mathcal{P}$ samples $\alpha, \rho \leftarrow\!\!\$\, [q-1]$ and sends $T \leftarrow g_1^\alpha g_2 h_1^\rho$
2. $\mathcal{V}$ sends challenge $c \leftarrow\!\!\$\, [q-1]$
3. $\mathcal{P}$ sends $s \leftarrow \alpha + cm, u \leftarrow \rho + cr$
4. $\mathcal{V}$ verifies that $g_1^s g_2^c h_1^u = C^c T$

Theorem 1. *Construction 1 is a Σ-protocol for the relation:*

$$\mathcal{R} = \{(C, g_1, g_2, h, q), (m, r) \mid C = g_1^m g_2 h_1^r\}$$

Proof. Folklore

Theorem 2 (Perfect Completeness). *Construction 1 is a $\Sigma-$protocol for the relation $\mathcal{R}$ with perfect completeness:*

Proof. We prove completeness by showing that for any $(C, g, h, q), (m, r) \in \mathcal{R}$, when both $\mathcal{P}$ and $\mathcal{V}$ follow the protocol, $\mathcal{V}$ accepts with $\Pr = 1$.

Let $x = (C, g_1, g_2, h, q)$ be common input and $w = (m, r)$ be $\mathcal{P}$'s private input. Consider an execution of the protocol where:

1. $\mathcal{P}$ samples $\alpha, \rho \leftarrow\!\!\$\, [q-1]$ and sends $T \leftarrow g_1^\alpha g_2 h^\rho$
2. $\mathcal{V}$ sends challenge $c \leftarrow\!\!\$\, [q-1]$
3. $\mathcal{P}$ responds with $s \leftarrow \alpha + cm, u \leftarrow \rho + cr$

Verification holds by

$$\begin{aligned} g_1^s g_2^c h_1^u &\stackrel{?}{=} C^c T \\ g_1^{\alpha+cm} g_2^c h^{\rho+cr} &\stackrel{?}{=} (g_1^m g_2 h^r)^c g_1^\alpha g_2 h^\rho \\ g_1^{\alpha+cm} g_2^c h^{\rho+cr} &= g_1^{\alpha+cm} g_2^c h^{\rho+cr} \end{aligned} \tag{1}$$

Thus, an honest verifier always accepts an honest prover's proof.

Theorem 3 (Soundness). *Construction 1 is a $\Sigma-$protocol for the relation $\mathcal{R}$ with soundness:*

Proof. We prove completeness by showing that for any $(C, g, h, q), (m, r) \in \mathcal{R}$, when both $\mathcal{P}$ and $\mathcal{V}$ follow the protocol, $\mathcal{V}$ accepts with $\Pr = 1$.

Let $x = (C, g_1, g_2, h, q)$ be common input and $w = (m, r)$ be $\mathcal{P}$'s private input. Consider an execution of the protocol where:

1. $\mathcal{P}$ samples $\alpha, \rho \leftarrow\!\!\$\, [q-1]$ and sends $T \leftarrow g_1^\alpha g_2 h^\rho$

2. $\mathcal{V}$ sends challenge $c \leftarrow\!\!\$\, [q-1]$
3. $\mathcal{P}$ responds with $s \leftarrow \alpha + cm, u \leftarrow \rho + cr$

Verification holds by

$$\begin{aligned} g_1^s g_2^c h_1^u &\stackrel{?}{=} C^c T \\ g_1^{\alpha+cm} g_2^c h^{\rho+cr} &\stackrel{?}{=} (g_1^m g_2 h^r)^c g_1^\alpha g_2 h^\rho \\ g_1^{\alpha+cm} g_2^c h^{\rho+cr} &= g_1^{\alpha+cm} g_2^c h^{\rho+cr} \end{aligned} \tag{2}$$

Thus, an honest verifier always accepts an honest prover's proof.

Commitment Scheme

References

BCK+22. M. Bellare, E. Crites, C. Komlo, M. Maller, S. Tessaro, and C. Zhu. Better than Advertised Security for Non-interactive Threshold Signatures. In *Advances in Cryptology – CRYPTO 2022*, pages 517–550, Cham, 2022. Springer Nature Switzerland.