Homomorphic Secret-Sharing with Certified Deletion

Nikhil Pappu[†]

[†]Portland State University
nikpappu@pdx.edu

October 1, 2024

Abstract

Contents

1 Preliminaries

[GVW12]

2 HSS with Certified Deletion

3 HSS-CD from VBB Obfuscation

We construct a (1,2)-HSS-CD scheme $\mathsf{HSS\text{-}CD} = \mathsf{HSS\text{-}CD}.(\mathcal{Share}, \mathcal{Eval}, \mathcal{Del}, \mathcal{Vrfy})$ using the following building blocks:

- PRF Family $\{F_{\mathsf{k}}\}_{\mathsf{k}}$.
- SKE-CD scheme $\mathsf{SKE\text{-}CD} = \mathsf{SKE\text{-}CD}.(\mathsf{KG}, \mathcal{Enc}, \mathcal{Dec}, \mathcal{Del}, \mathcal{Vrfy})$ with classical decryption property and algorithm CDec.
- VBB Obfuscation for the following programs:

  $\mathsf{P}_1(C, u)$ {Hard-coded values: k, sk}:
  - Compute $v = \mathsf{CDec}(\mathsf{sk}, u)$.
  - Output $F_{\mathsf{k}}(C, v)$.

  $\mathsf{P}_2(C, u)$: {Hard-coded values: k, sk}:
  - Compute $v = \mathsf{CDec}(\mathsf{sk}, u)$.
  - Output $F_{\mathsf{k}}(C, v) \oplus C(v)$.

The construction is as follows:

$\mathsf{HSS\text{-}CD}.\mathcal{Share}(1^\lambda, i, b)$:

1. Generate $\mathsf{k} \leftarrow \{0,1\}^\lambda$.
2. Generate $\mathsf{sk} \leftarrow \mathsf{KG}(1^\lambda)$.
3. Compute $ct \leftarrow \mathcal{Enc}(\mathsf{sk}, b)$.
4. Compute $\mathsf{OP}_i = \mathsf{VBB.Obf}(\mathsf{P}_i)$ using the values k, sk.
5. Output $sh_i = (ct, \mathsf{OP}_i)$.

$\mathsf{HSS\text{-}CD.Eval}(1^\lambda, C, sh_i)$:

References

[GVW12] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Functional encryption with bounded collusions via multi-party computation. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 162–179. Springer, Heidelberg, August 2012. (Cited on page 3.)