Implementation and Analysis of Apple's
CSAM Detection System

Alessandro Baccarini
anbaccar@buffalo.edu
University at Buffalo
December 1, 2021

1. Introduction

2. Streaming threshold PSI with associated data

Symbol	**Meaning**
$\mathcal{U}$	Universe of hash values
$X \subseteq \mathcal{U}$	Set of hash values the server has, s.t. $\lvert X \rvert = n$. Every hash is distinct.
$\bar{Y} = ((y_i, id_i, ad_i))$	Triples the client has, s.t. $\lvert \bar{Y} \rvert = m, i \in [1, m]$.
$y \in \mathcal{U}$	Hash value
$id \in \mathcal{ID}$	Unique identifier of a triple
$ad \in \mathcal{D}$	Associated data of a triple
$id(\bar{Y})$	Set of id's of triples in $\bar{Y}$
$id(\bar{Y} \cap X)$	Set of id's of triples in $\bar{Y}$ whose y is also in X
$\bar{Y}_{id} \in \mathcal{ID}^m$	List of all id's in the triples in $\bar{Y}$
$\bar{Y}_{id,ad} \subseteq (\mathcal{ID} \times \mathcal{D})$	(Projection) Set of id's and ad's in the triples in $\bar{Y}$
$\bar{Y}[T] \subseteq (\mathcal{U} \times \mathcal{ID} \times \mathcal{D})^{\leq m}$	(Selection) For a set of id's $T \subseteq \mathcal{ID}$, this is the list of triples in $\bar{Y}$ whose id's are in T
$x \leftarrow d$	Assignment of value d to variable x
$x \xleftarrow{\$} \mathcal{X}$	x is a RV sampled uniformly over a finite set $\mathcal{X}$
$x \xleftarrow{\$} A(\cdot)$	x is the output of a randomized algorithm A

Table 1: PSI notations.

3. Building Blocks

Cryptographic primitives:

- $(\mathrm{Enc}, \mathrm{Dec})$ denotes a symmetric encryption scheme with key space $\mathcal{K}'$ and satisfies standard symmetric key security properties (AES128-GCM).
- $E(\mathbb{F}_p)$ is an elliptic curve of prime order q, with G as a fixed generator of $E(\mathbb{F}_p)$. Assume Decision Diffie-Hellman (DDH) holds in $E(\mathbb{F}_p)$ (NIST P256).
- $H : \mathcal{U} \to E(\mathbb{F}_p) \setminus \{\mathcal{O}\}$ is a hash function modeled as as random oracle.
- $H' : E(\mathbb{F}_p) \to \mathcal{K}'$ is secure key derivation function; the uniform distribution on $E(\mathbb{F}_p)$ mapped to an "almost" uniform distribution on $\mathcal{K}'$ (HKDF, based on HMAC)

- Shamir secret sharing on an element of $\mathcal{K}'$ to obtain shares in $\mathbb{F}_{\mathrm{Sh}}^2$ for some field $\mathbb{F}_{\mathrm{Sh}}$ that is sufficiently large such that when choosing $t+1$ random elements from $\mathbb{F}_{\mathrm{Sh}}$, the probability of a collision is low.
- A pseudorandom function (PRF) $F : \mathcal{K}'' \times \mathcal{ID} \to \mathbb{F}_{\mathrm{Sh}}^2 \times \mathcal{X} \times \mathbb{R}$, where the sets $\mathcal{X}$ and $\mathbb{R}$ are the domain and range of a detectable hash function, respectively (HMAC).

3.1. The Diffie-Hellman random self reduction

3.2. Detectable hash functions

3.3. Cuckoo Tables (Cuckoo Hashing)

We provide a brief overview of Cuckoo Hashing, which is a technique designed for resolving collisions in hash tables and provides a worst-case $\Theta(1)$ lookup and deletion time.

4. Threshold PSI-AD using the DH random self reduction

4.1. tPSI-AD protocol walkthrough

We now walk through every step up the warm-up tPSI-AD protocol outlined in [1]. We let t denote the threshold, m be an upper bound on the number of triples the client will process, and $n = |X|$.

The specific protocol we are implementing occurs in four phases: S-Init, C-Init, C-Gen-Voucher, and S-Process, where S and C refer to the Server and Client, respectively.

Protocol 1 $(pdata, skey) \leftarrow \mathsf{S\text{-}Init}(X)$

Protocol 2 $ckey \leftarrow \mathsf{C\text{-}Init}(pdata)$

Protocol 3 $voucher \leftarrow \mathsf{C\text{-}Gen\text{-}Voucher}(pdata, ckey, (y, id, ad))$

Protocol 4 $\mathsf{S\text{-}Process}(pdata, skey, voucher)$

References

[1] Abhishek Bhowmick, Dan Boneh, Steve Myers, and Kunal Talwar Karl Tarbe. The Apple PSI System. https://www.apple.com/child-safety/pdf/Apple_PSI_System_Security_Protocol_and_Analysis.pdf.

A. Mathematical Reference

A.1. Finite Fields

Definition A.1. *A* (finite) finite $\mathbb{F}$ *is a set defined with operations* $+, \times$ *such that the following hold:*

- $\mathbb{F}$ *is abelian with respect to "+," where we let 0 denote the identity element.*
- $\mathbb{F} \setminus \{0\}$ *is abelian with respect to "×," where we let 1 denote the identity element. We write* ab *in place of* $a \times b$*.*
- (Distributivity:) $\forall a, b, c \in \mathbb{F}$, *we have* $a \times (b + c) = ab + ac$

The additive inverse of $a \in \mathbb{F}$ denoted by $-a$ is a unique element that satisfies $a + (-a) = 0$, and the multiplicative inverse of $a \in \mathbb{F} \setminus \{0\}$ denoted a^{-1} is the unique element that satisfies $aa^{-1} = 1$.

The *order* of a F is the number of elements in $\mathbb{F}$, provided $\mathbb{F}$ is finite. If q is a prime power $q = p^r$ for a prime p and positive integer r, we can establish the field $\mathbb{F}_p$ of prime order q.