Universität
Basel

Lowering the Cost of Metadata-Hinding Communcation with cryptographic Privacy

Ugur Turhal – ugur.turhal@unibas.ch

2nd November, 2023

1. Introduction

2. Bachground

3. Express

4. Filtering out malformed DPFs

5. Auditor

Introduction

Main Goal

□ How can a whistler blower be protected

Something is going wrong

Make it public

Figure 1: Symbolic representation

Words

Background

- Metadata: Information a data set. example: EXIF
  - How it was collected?
  - When it was collected?
  - Where was is it collected?
  - example: EXIF
- Onion Routing: Technique for anonymous communication over a computer network. In an onion network, messages are encapsulated in layers of encryption, analogous to the layers of an onion.
- Tor: is an open-source privacy network that enables anonymous web browsing. Tor users’ digital data and communications are shielded using a layered approach that resembles the nested layers of an onion

End-to-End encrypted messaging apps

Whistleblower wants to communicate with a journalist, this are the options:

Figure 2: Messaging apps

Problem: Metadata

a) Who are my friends

b) Who am I talking to

c) How often do I talk to them

This metadata could be even more sensitive, than the message it self.

Anoynmizing Proxy

To avoid this sort of collection metadata two widley used systems for whistleblowsers:

Figure 3: Widley used communcation tools

Problem, vulnerable to:

a. Global adversairies

   1..1 This could be: Nation state attacks, since they could/can control all nodes in a network.

Express Overview

1. 2-Server system, which is secure against:
   - Arbitrary many clients
   - Up to one malicous Server
2. This opperations are supported:
   - Register a Mailbox
   - Private write into a Mailbox
   - Read from Mailbox

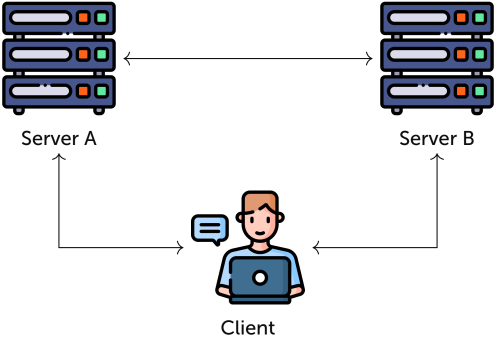
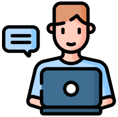


Figure 4: Schema of Express

Private Writing - Client

Example: Client wants to write Hi to Adress 3.



Client

x	$f(x)$
0	0
1	0
2	0
3	`Hi!`
4	0

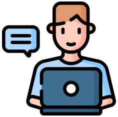
To write privately, the whistlerblower has to use a secret share.

Private Writing - Secret share

Example: The message `Hi!` will be divded in to two vectors: f_1 and f_2. This shares are called: Distributed Point Functions (DPFs).

1. DPFs have the size $\log$(N)
2. And time generation is in $\log$(N)

N = number of Mailboxes.



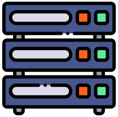
Client

x	$f_1(x)$
0	"abc"
1	"xf$"
2	"tg"
3	"!7≈"
4	"ihV"

x	$f_2(x)$
0	"abc"
1	"xf$"
2	"tg"
3	""2!)"
4	"ihV"

Private Writing - Secret share Server A

Example: The message `Hi!` will be divded in to two vectors: f_1 and f_2



Server A

x	$f_1(x)$
0	”abc”
1	”xf$”
2	”tg”
3	”!7≈”
4	”ihV”

Private Writing - Secret share Server B

Example: The message `Hi!` will be divded in to two vectors: f_1 & f_2

Server B

x	$f_1(x)$
0	”abc”
1	”xf$”
2	”tg”
3	””2!)”
4	”ihV”

Express Overview

Express

1. 2-Server system, which is secure against:
   - Arbitrary many clients
   - Up to one malicous Server

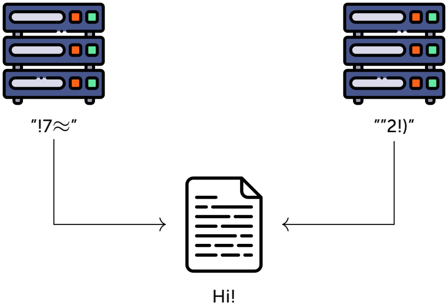


Figure 5: Schema of Express

What if malicious user sends malformed message to corrupt mailbox?

Malformed DPFs

A user could send malformed DPF, such that every value has a entry.

x	$f(x)$
0	”28f912”
1	”dd2df$”
2	”Pf!TZ”
$\cdots$	$\cdots$
N	”rAUcH*?”

Table 1: Malformed DPF

How filter out malformed DPFs?

Filteringout malformed DPFs

Solution

Server blindly audit all incoming write requests

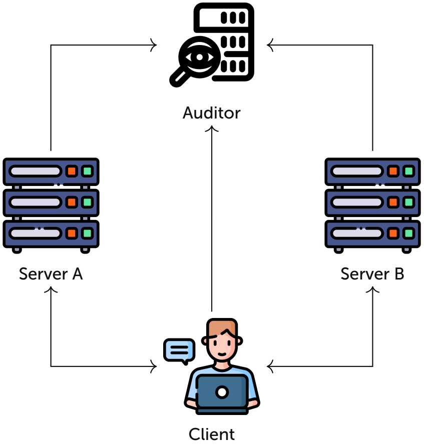


Figure 6: Schema of Express

Performance of auditor

Performance

Cost	Riposte	Express' Audit
Communcation	$\mathcal{O}(\sqrt{N})$	$\mathcal{O}(1)$
Client/auditor computation	$\mathcal{O}(\sqrt{N})$	$\mathcal{O}(1)$

Auditor Issue

Issue: Because of semihonest solution!

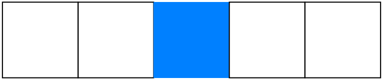


Figure 7: Server A

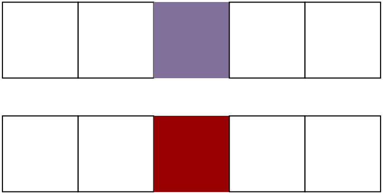


Figure 8: Server B, Malicious attack

Issue: Malicous server can guess the mailbox destination, and corrupts the entry in the guessed mailbox. If the protocol still accepts then its correct, if not it is not the right mailbox! They must jave differed at the one point that the person was trying to write to!

Protocol Issue - Solution using SNIP

To solve this issue, the clients sends a secret-shared non-interactiove proofs (SNIPs) to servers that honest evaluation of the semihonest protocol accepts.