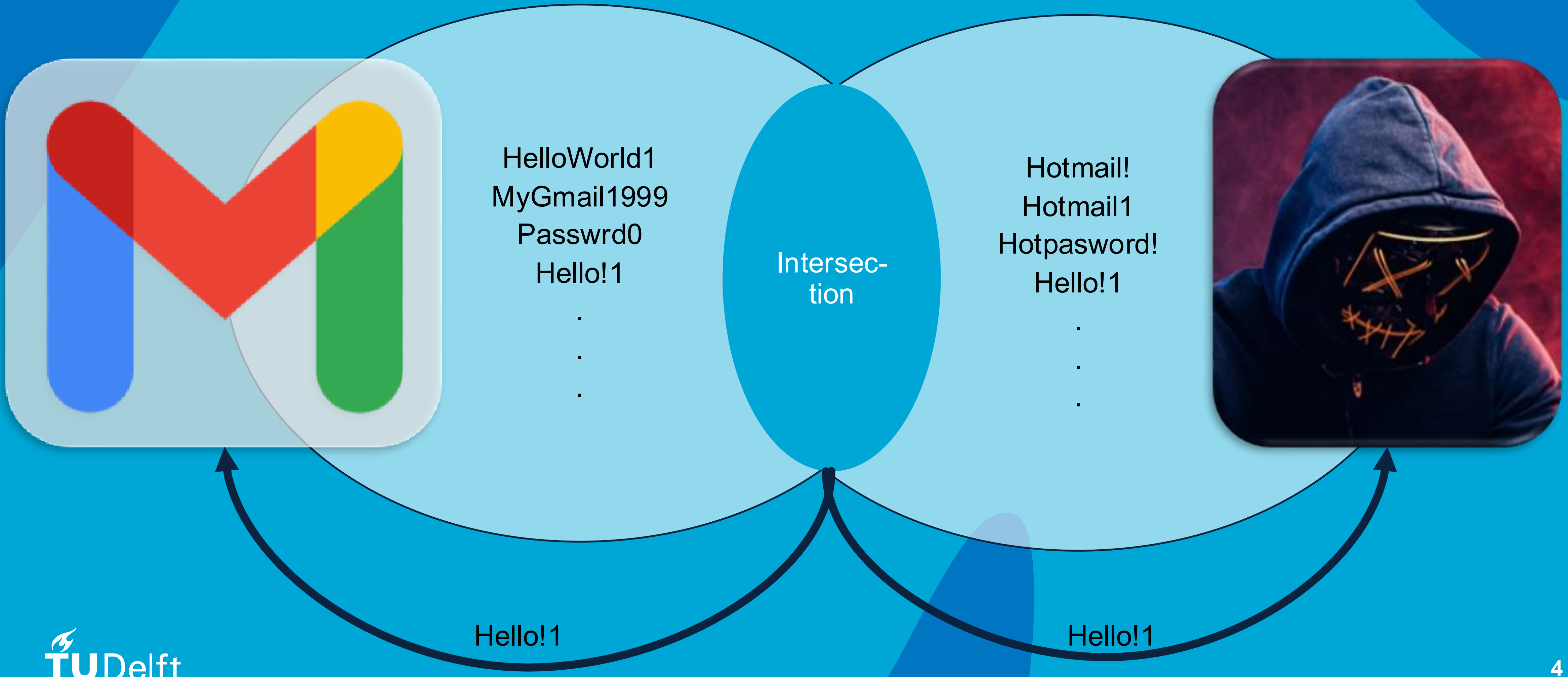
# Prevent malicious input in PSI

Partial Authorized Private Set Intersection as a solution | Tjitske Koster, PhD

Do my users use these passwords?
All passwords of Hotmail

I’m not crazy!
Let use PSI
Give your
passwords
and I’ll check
doubles!

# Private Set Intersection



HelloWorld1

MyGmail1999

Passwrd0

Hello!1

.

.

.

Intersec-
tion

Hotmail!

Hotmail1

Hotpasword!

Hello!1

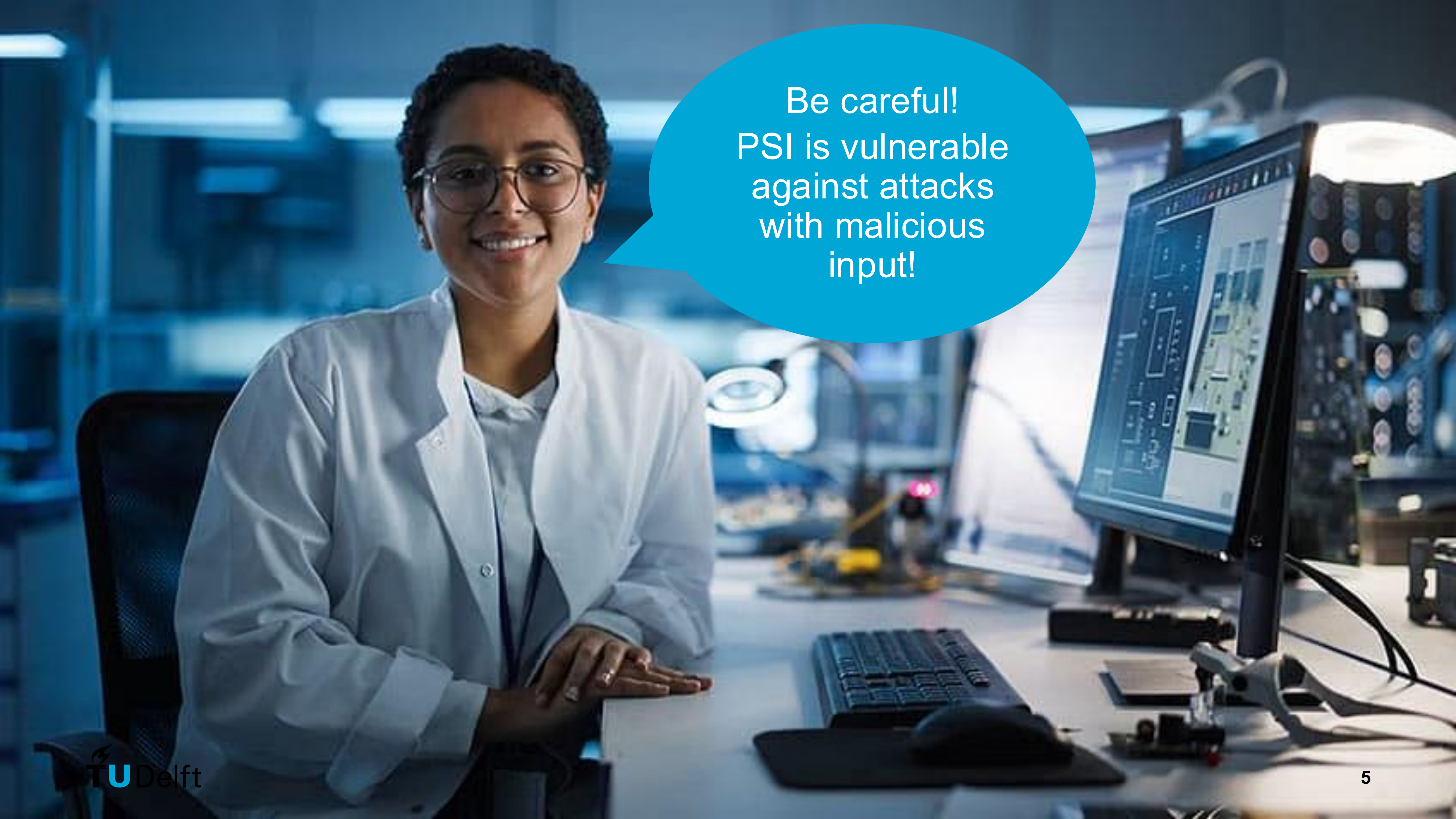
.

.

.

Hello!1

Hello!1



Be careful!

PSI is vulnerable against attacks with malicious input!

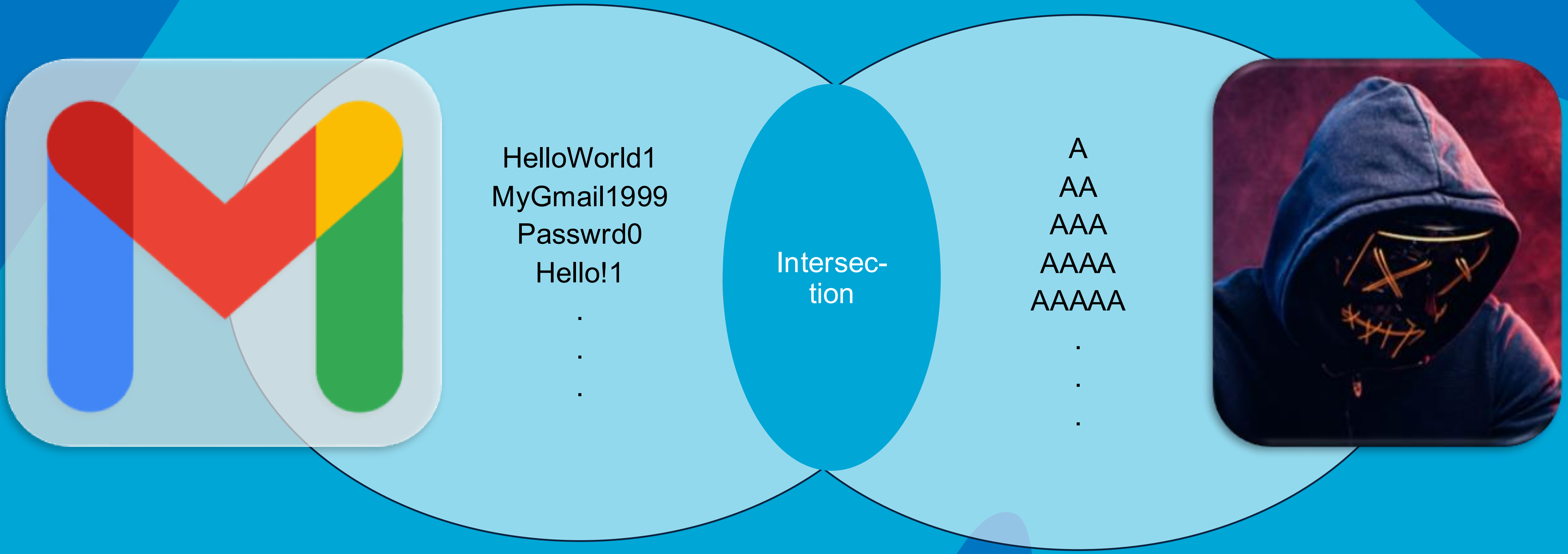
## Background

Authorized Private Set Intersection

## Problem and solution

## Compare with previous work

# Membership Inference Attack

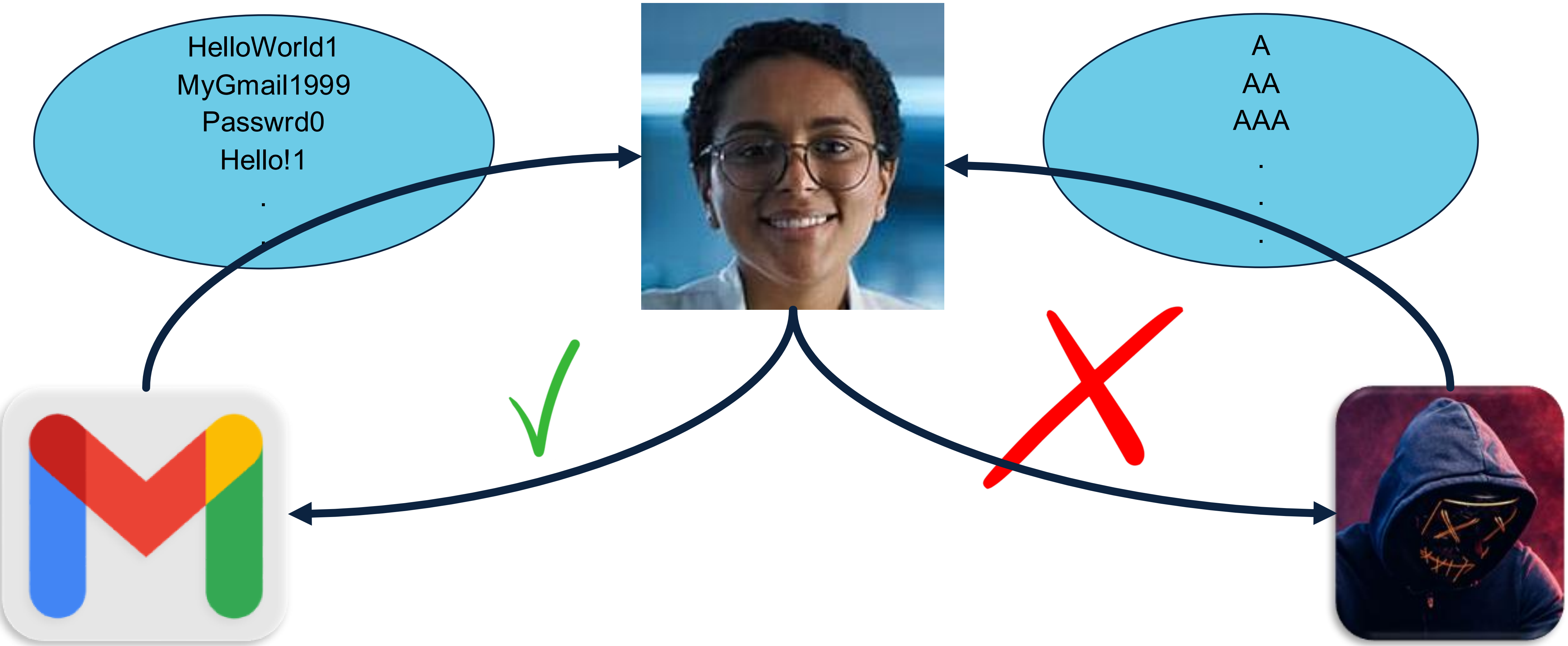


HelloWorld1
MyGmail1999
Passwrd0
Hello!1
.
.
.

Intersec-tion

A
AA
AAA
AAAA
AAAAA
.
.
.

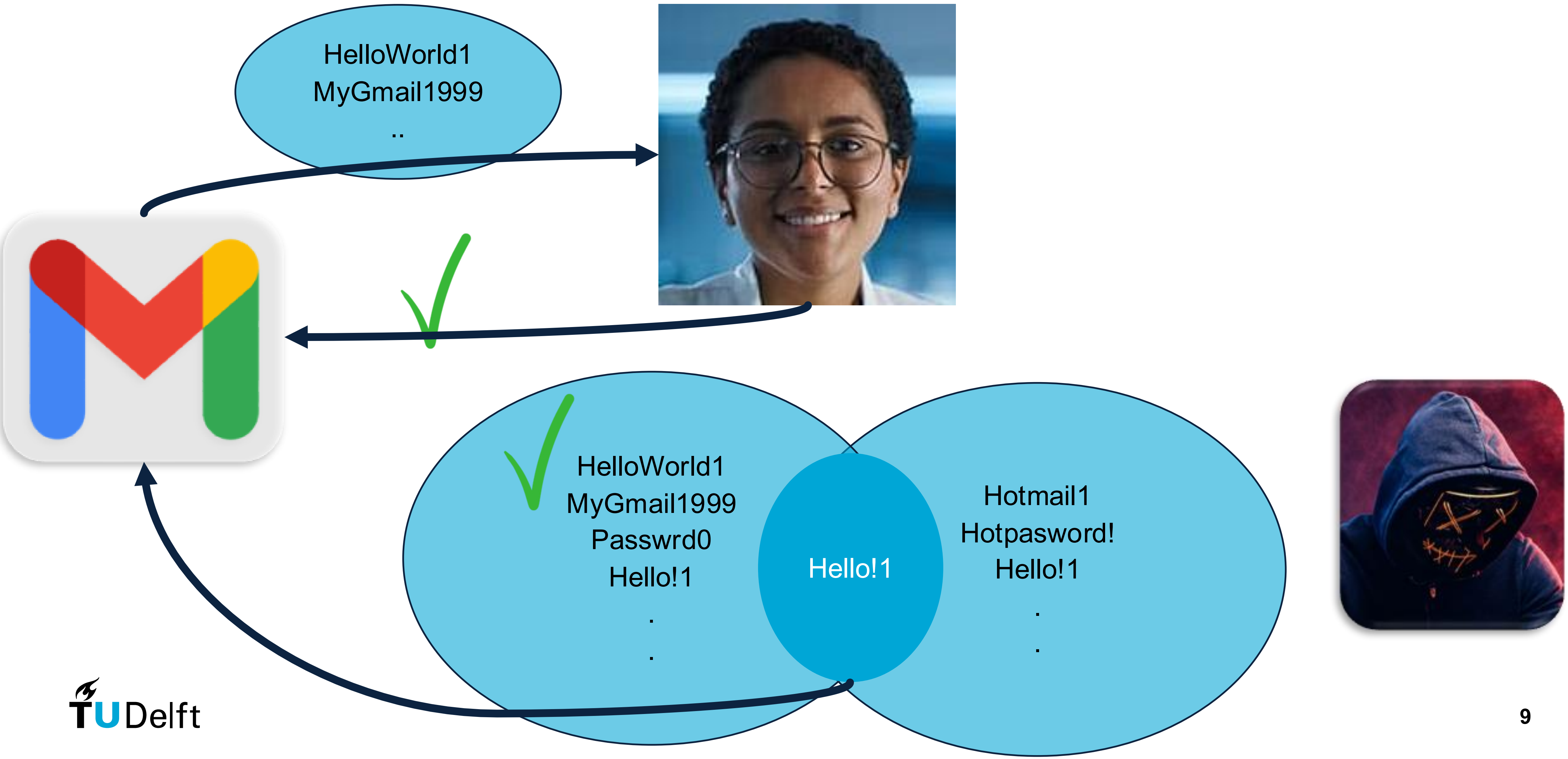
# Authorized Private Set Intersection



HelloWorld1
MyGmail1999
Passwrd0
Hello!1
.
.

A
AA
AAA
.
.
.

# Authorized Private Set Intersection



HelloWorld1
MyGmail1999
..

✓

✓

HelloWorld1
MyGmail1999
Passwrd0
Hello!1
.
.

Hello!1

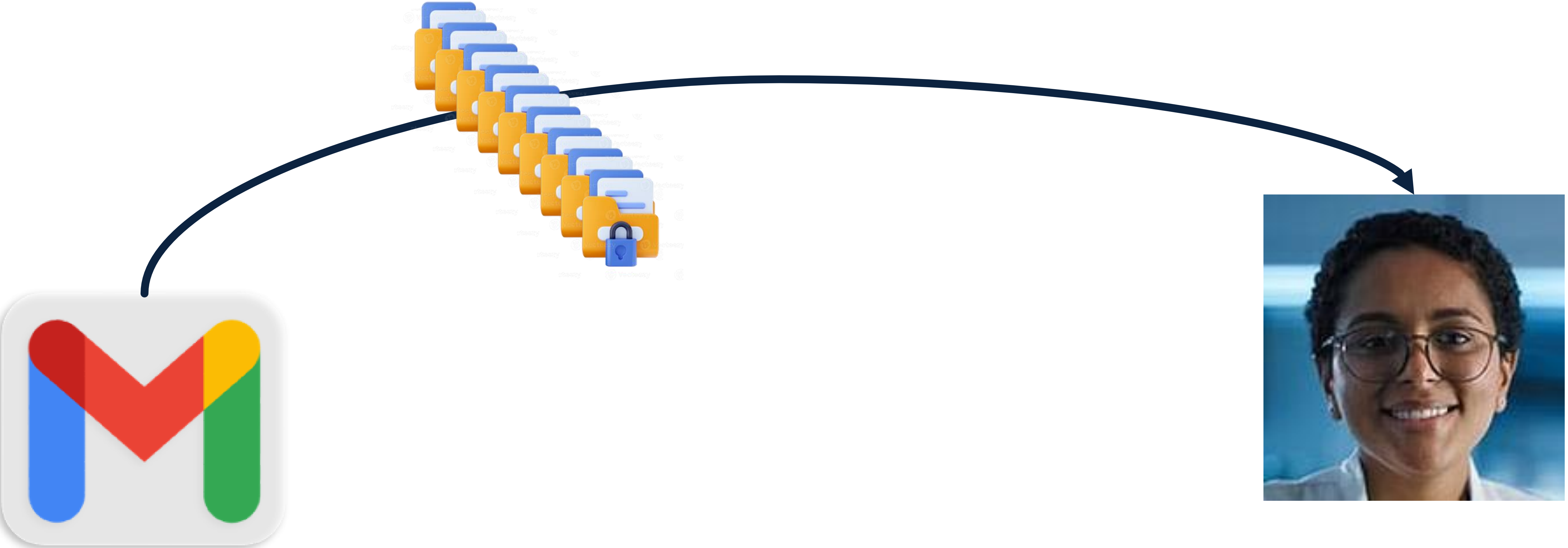
Hotmail1
Hotpasword!
Hello!1
.
.

# Problem!!!!

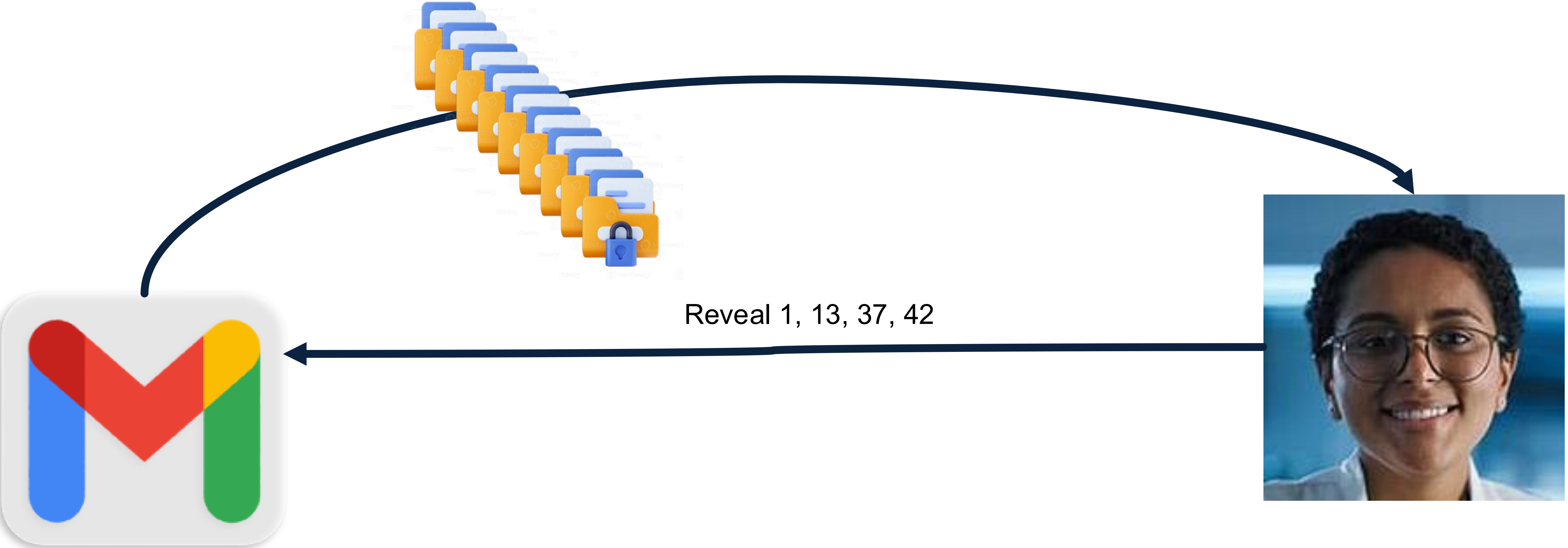
I don’t want to share all passwords!

# How to solve this? Previous work

# PARTIALLY Authorized Private Set Intersection

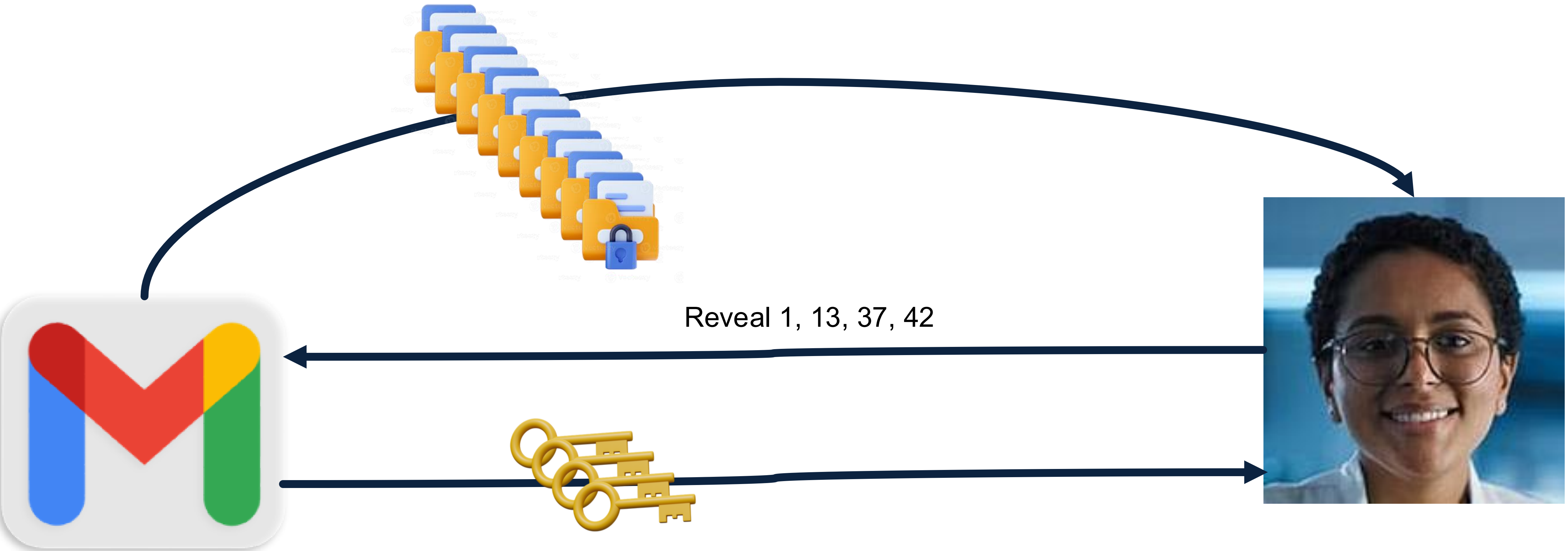


# PARTIALLY Authorized Private Set Intersection



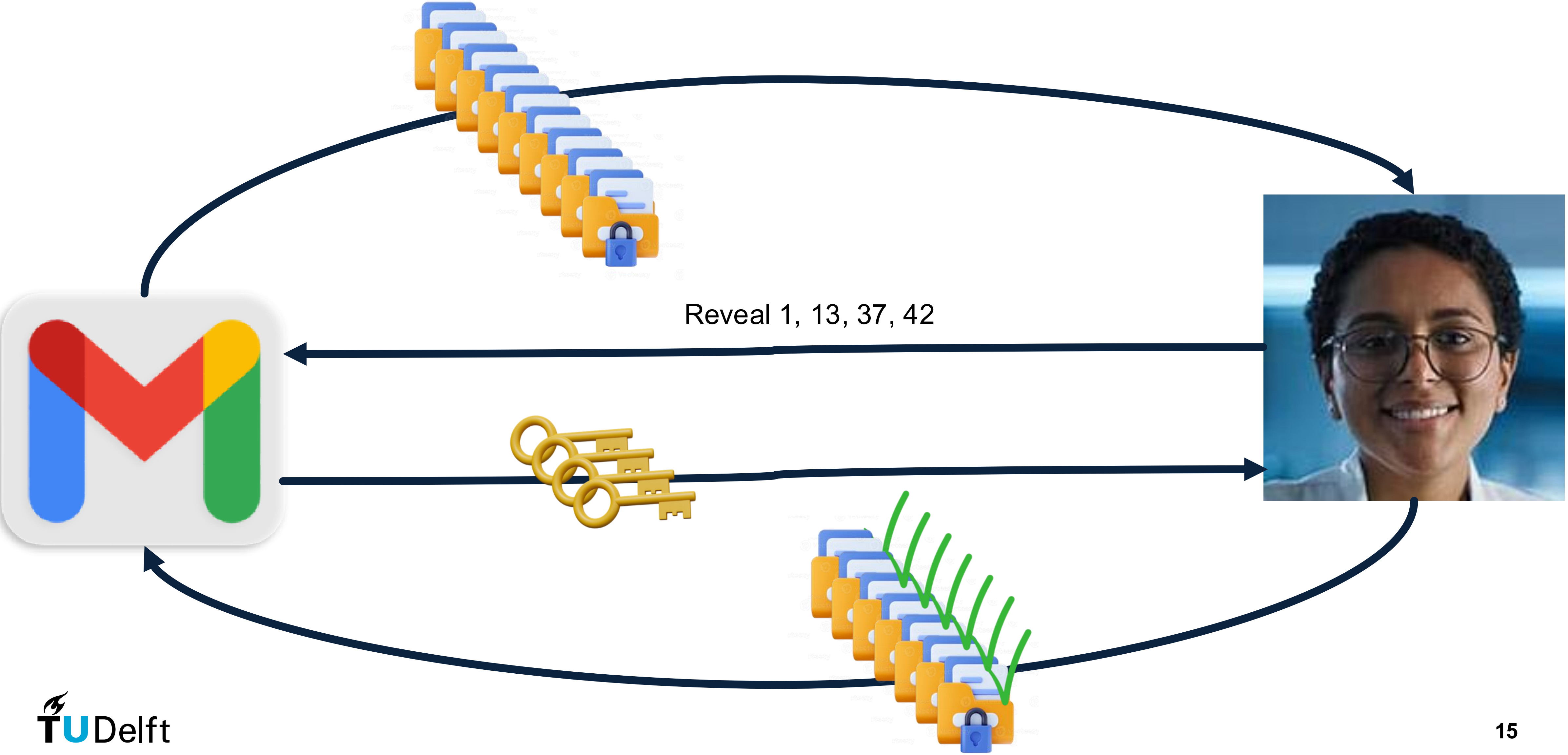
Reveal 1, 13, 37, 42

# PARTIALLY Authorized Private Set Intersection



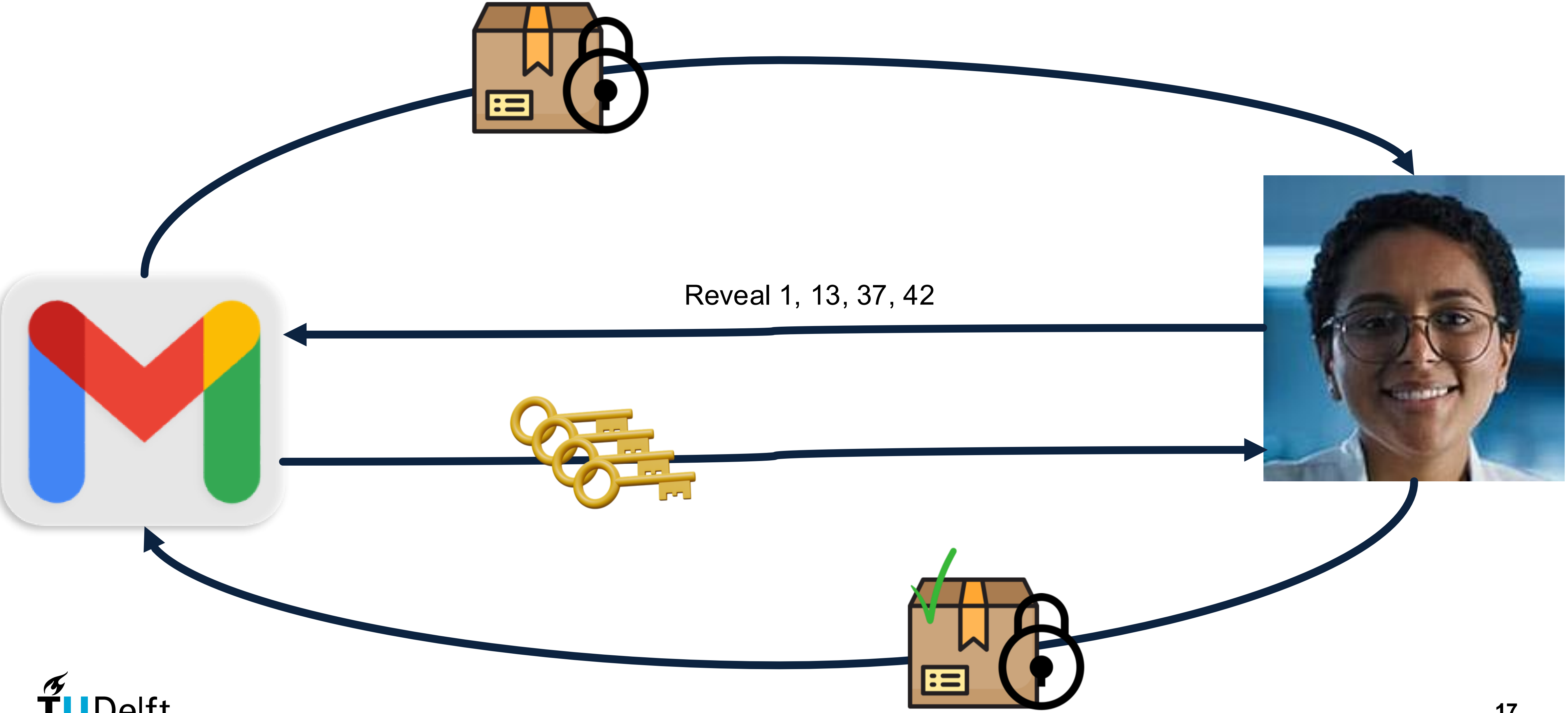
Reveal 1, 13, 37, 42

# PARTIALLY Authorized Private Set Intersection

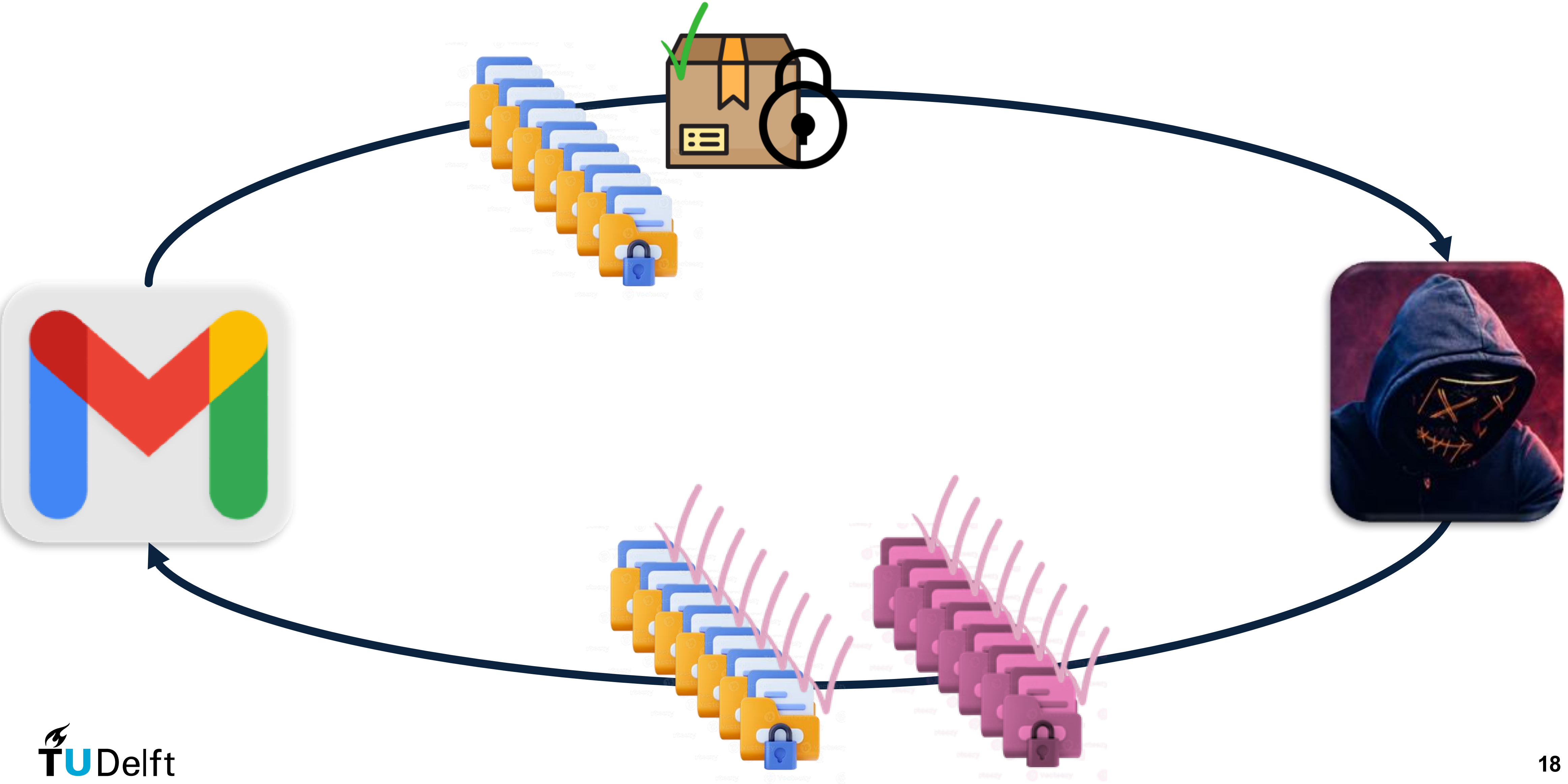


# That is a lot of documents… We can do this smarter! New work

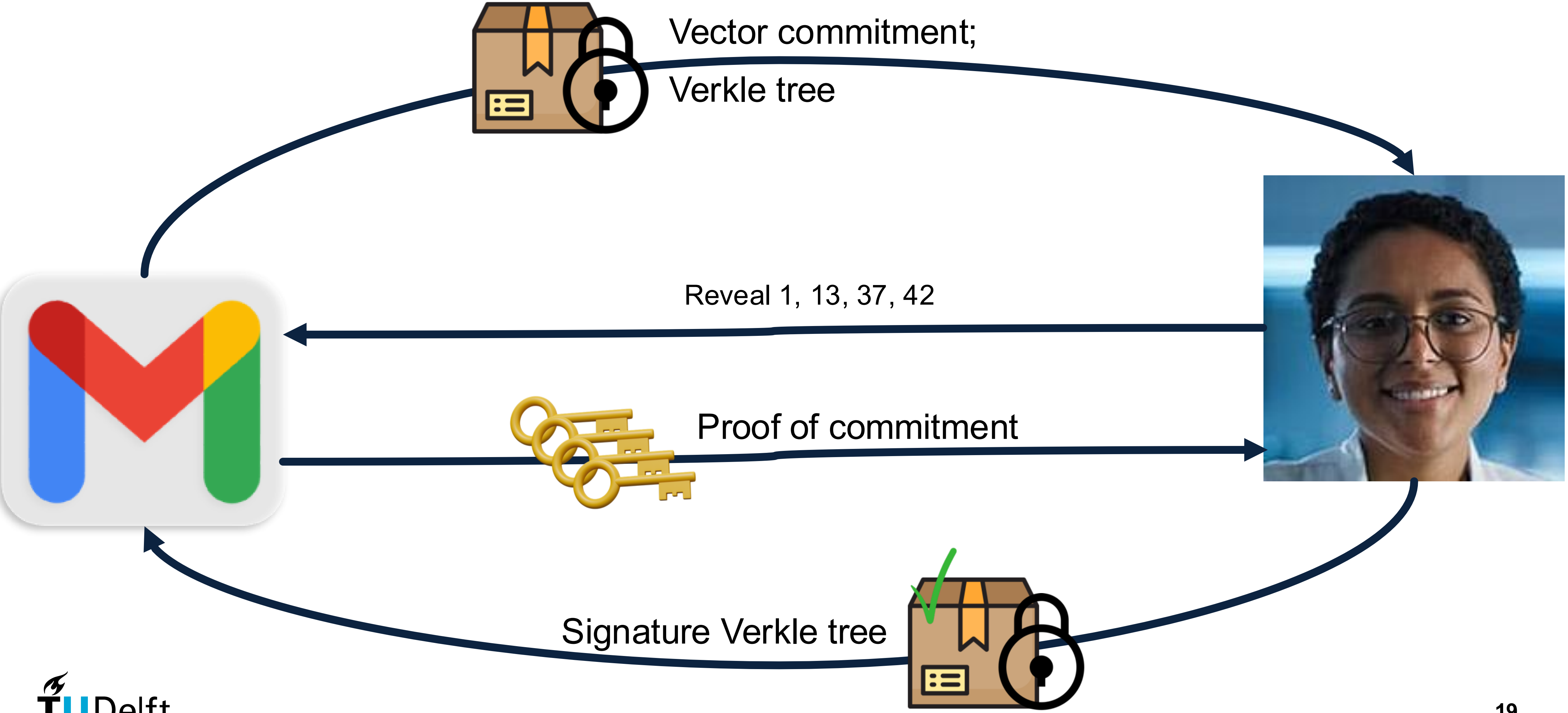
# IMPROVED Partial Authorized PSI



# IMPROVED Partial Authorized PSI - Intersection



# IMPROVED Partial Authorized PSI



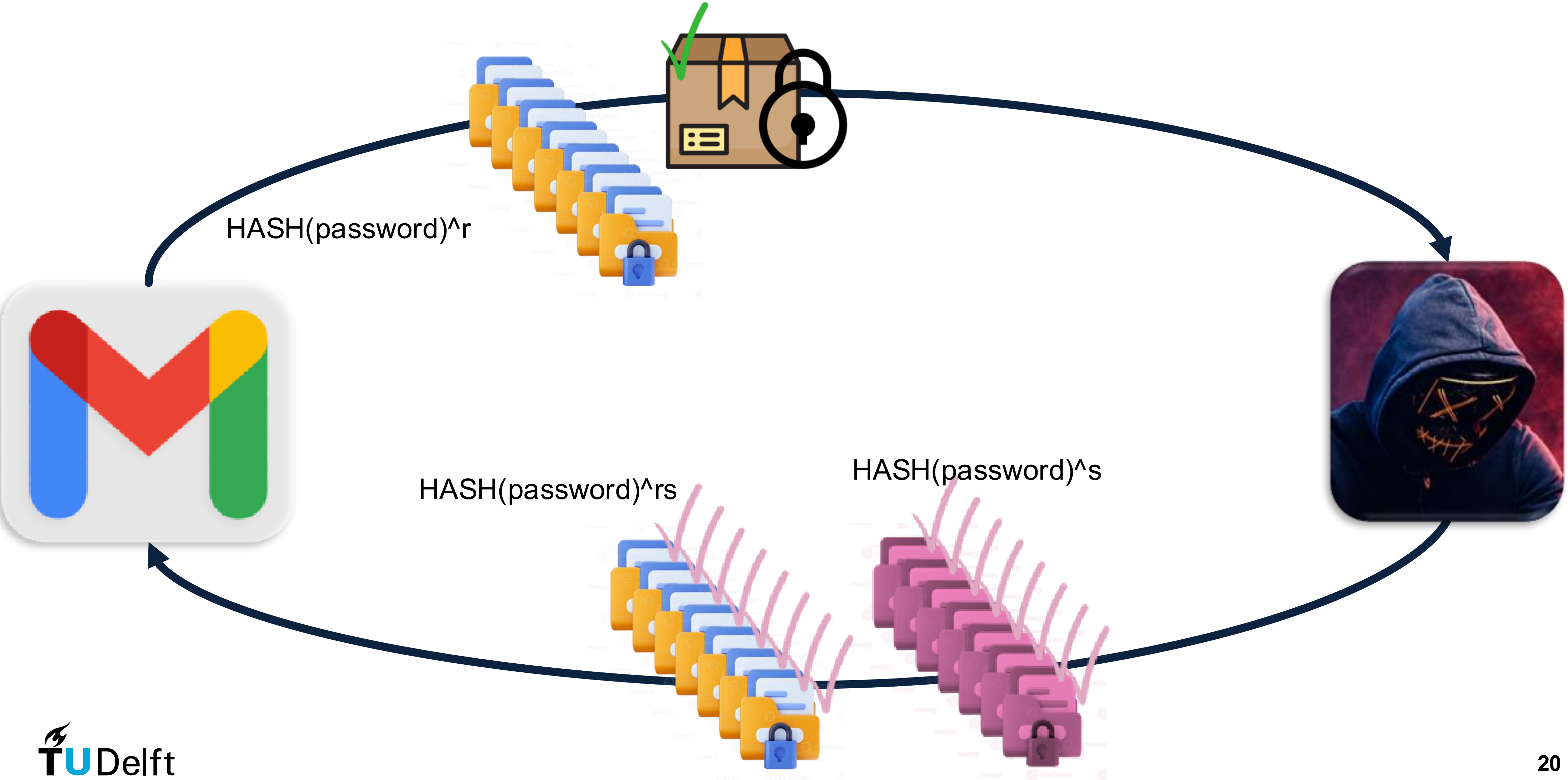
Vector commitment;
Verkle tree

Reveal 1, 13, 37, 42

Proof of commitment

Signature Verkle tree

# IMPROVED Partial Authorized PSI - Intersection

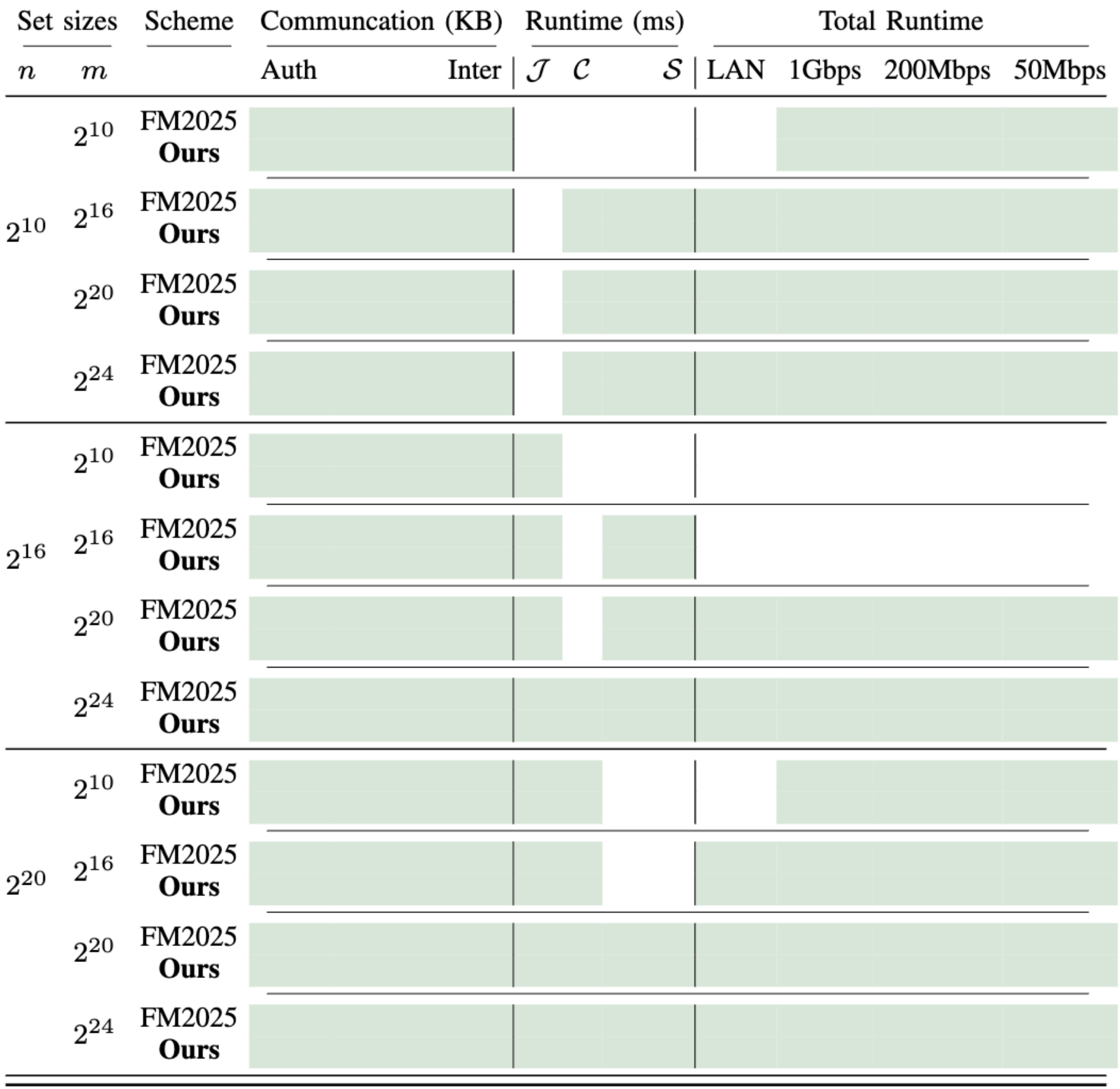


HASH(password)^r

HASH(password)^rs

HASH(password)^s

# Results



| Set sizes | | Scheme | Communcation (KB) | | Runtime (ms) | | | Total Runtime | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $n$ | $m$ | | Auth | Inter | $\mathcal{J}$ | $\mathcal{C}$ | $\mathcal{S}$ | LAN | 1Gbps | 200Mbps | 50Mbps |
| $2^{10}$ | $2^{10}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| | $2^{16}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| | $2^{20}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| | $2^{24}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| $2^{16}$ | $2^{10}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| | $2^{16}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| | $2^{20}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| | $2^{24}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| $2^{20}$ | $2^{10}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| | $2^{16}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| | $2^{20}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |
| | $2^{24}$ | FM2025 | | | | | | | | | |
| | | **Ours** | | | | | | | | | |

# To prevent Membership inference attacks in PSI use Partially Authorized PSI!

# Thanks for listening!

T.O.Koster@TUDelft.nl | Tjitske Koster