

Prevent malicious input in PSI

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





Do my
users use
these
passwords?



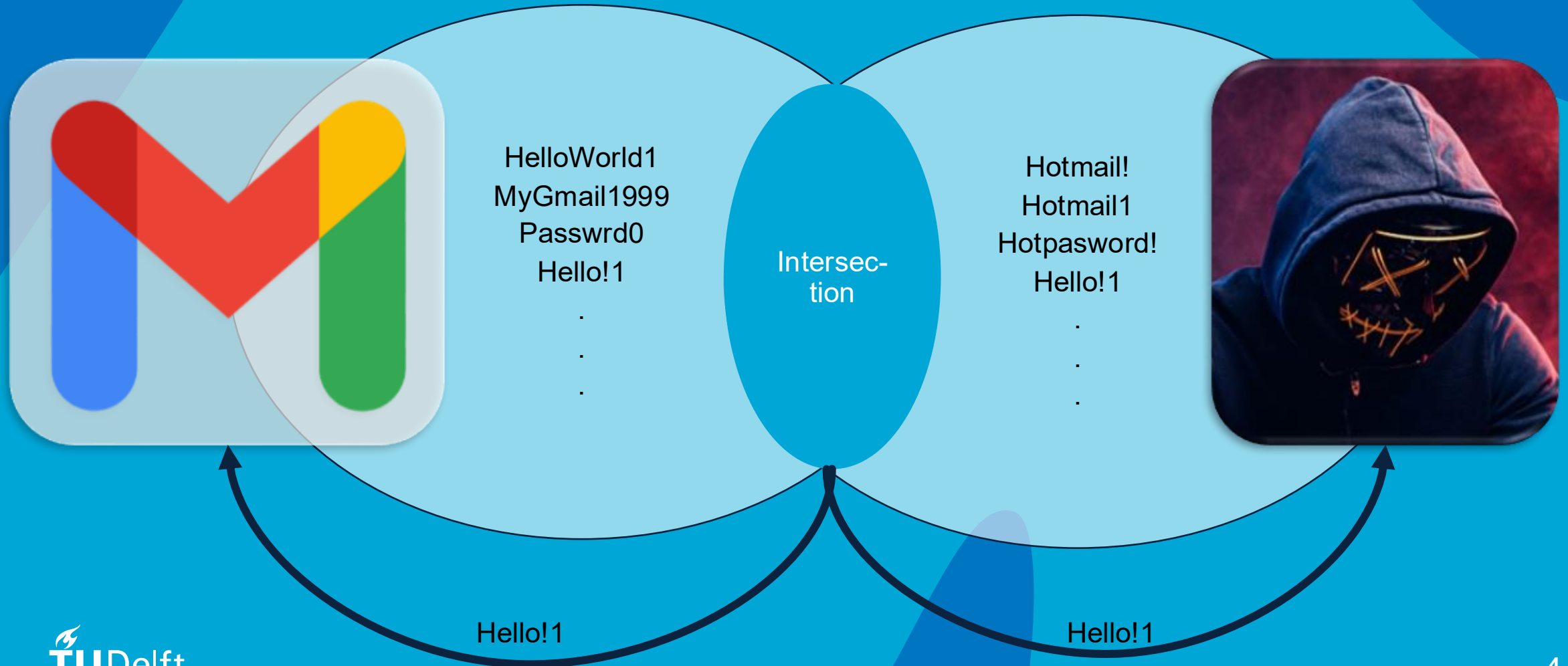
All passwords
of Hotmail

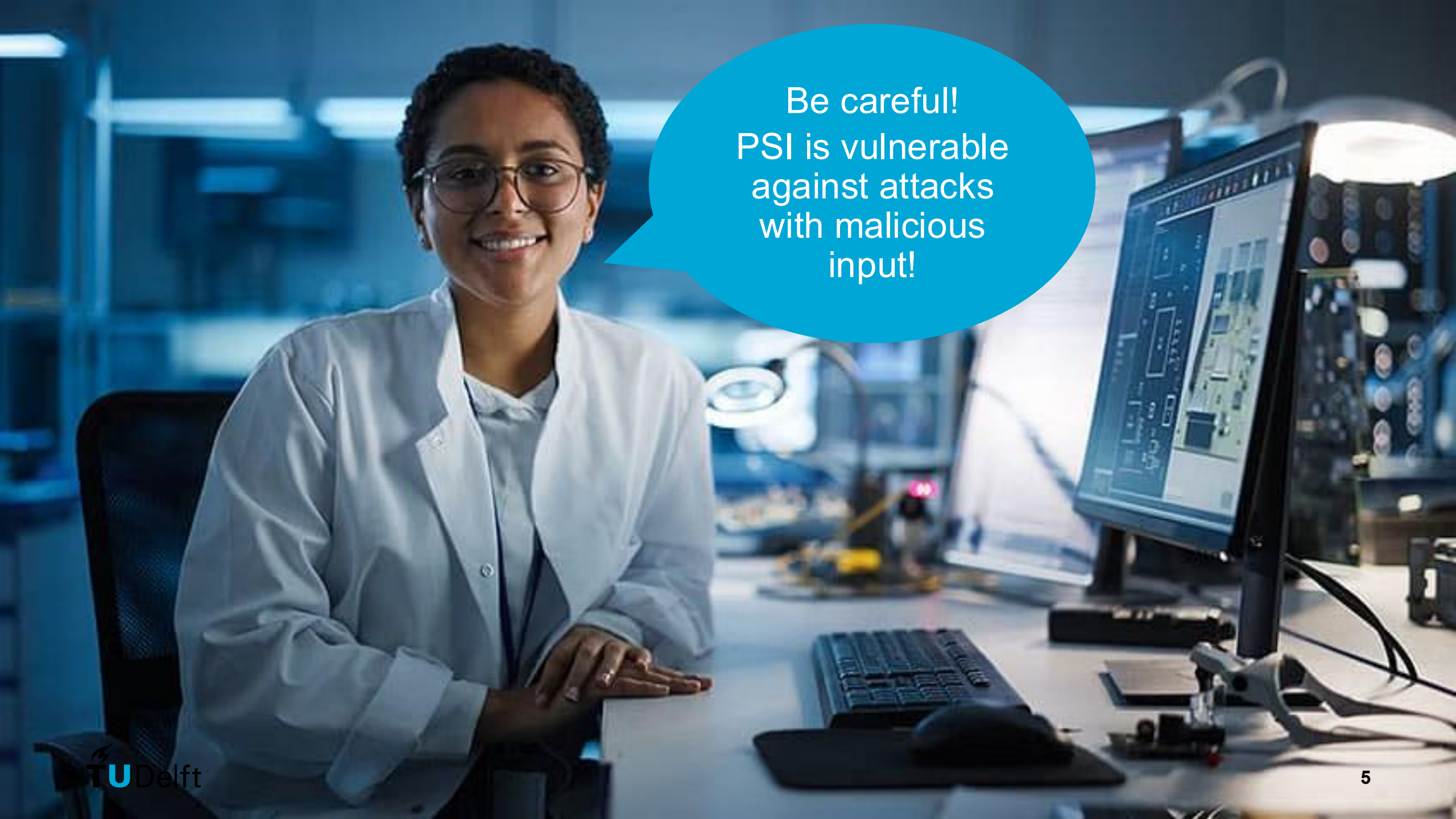
I'm not crazy!
Let use PSI

Give your
passwords
and I'll check
doubles!



Private Set Intersection



A woman with short dark hair and glasses, wearing a white lab coat over a light blue shirt, is sitting at a desk in a laboratory or office. She is smiling and looking towards the camera. Her hands are resting on the desk. In front of her is a computer monitor displaying a technical diagram, a keyboard, and a mouse. The background is a blurred laboratory setting with various equipment and lights.

Be careful!
PSI is vulnerable
against attacks
with malicious
input!



Background

Authorized Private Set
Intersection

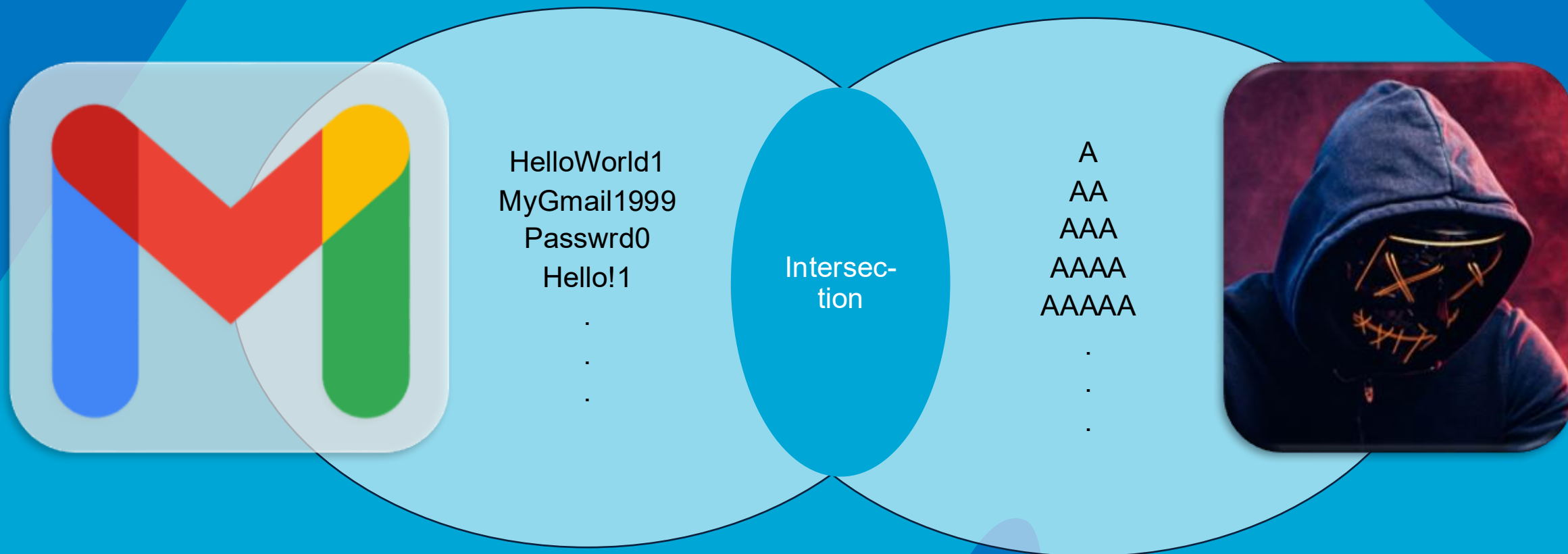


Problem and solution

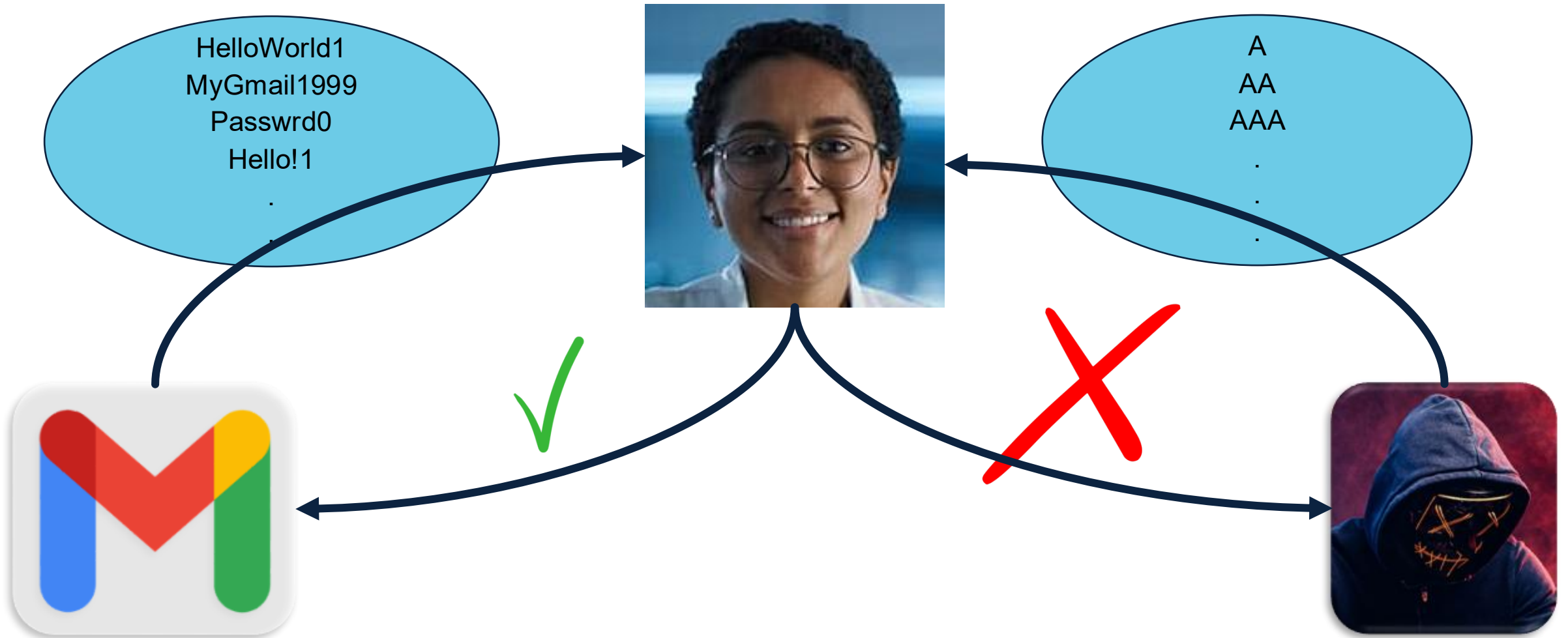


Compare with previous work

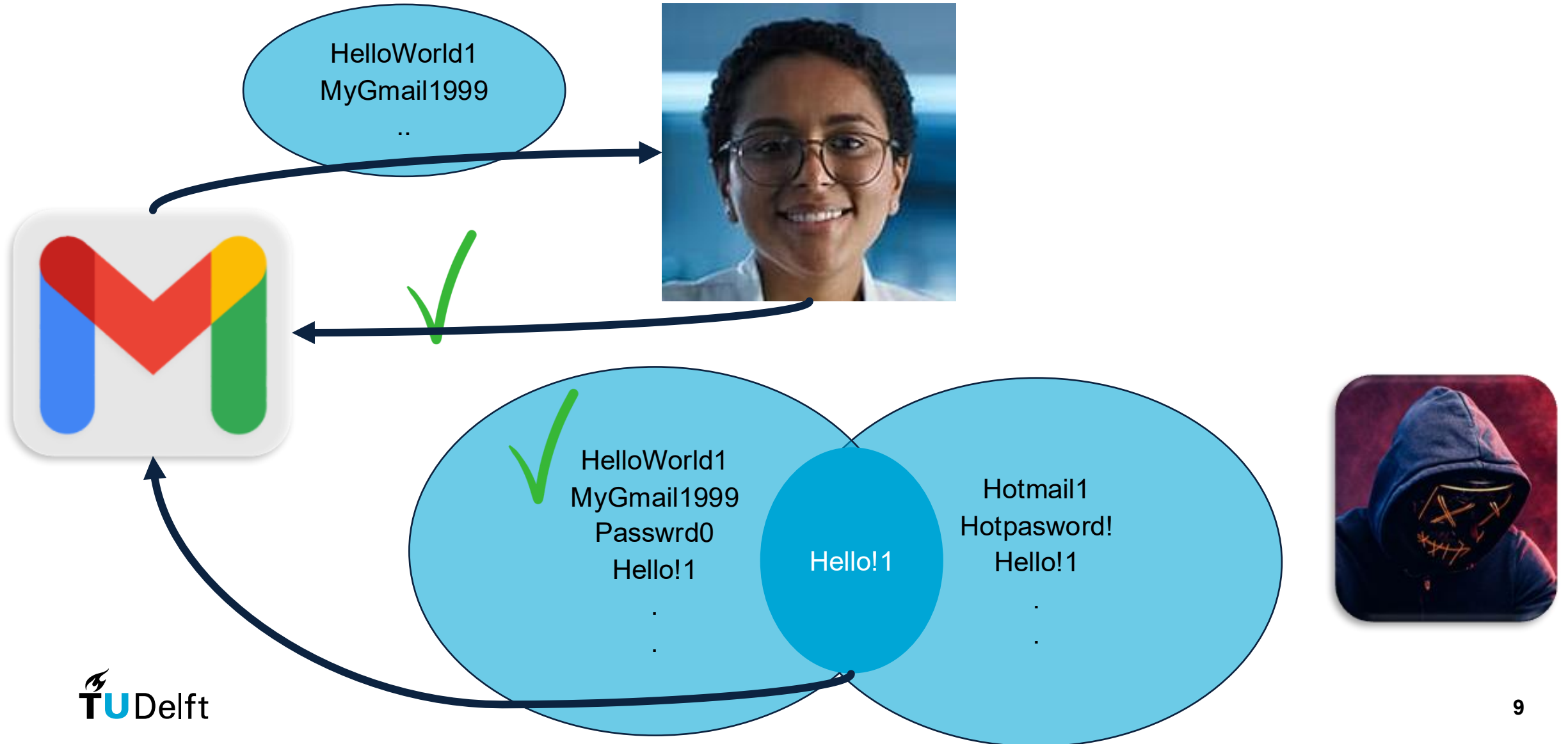
Membership Inference Attack



Authorized Private Set Intersection



Authorized Private Set Intersection



Problem!!!!

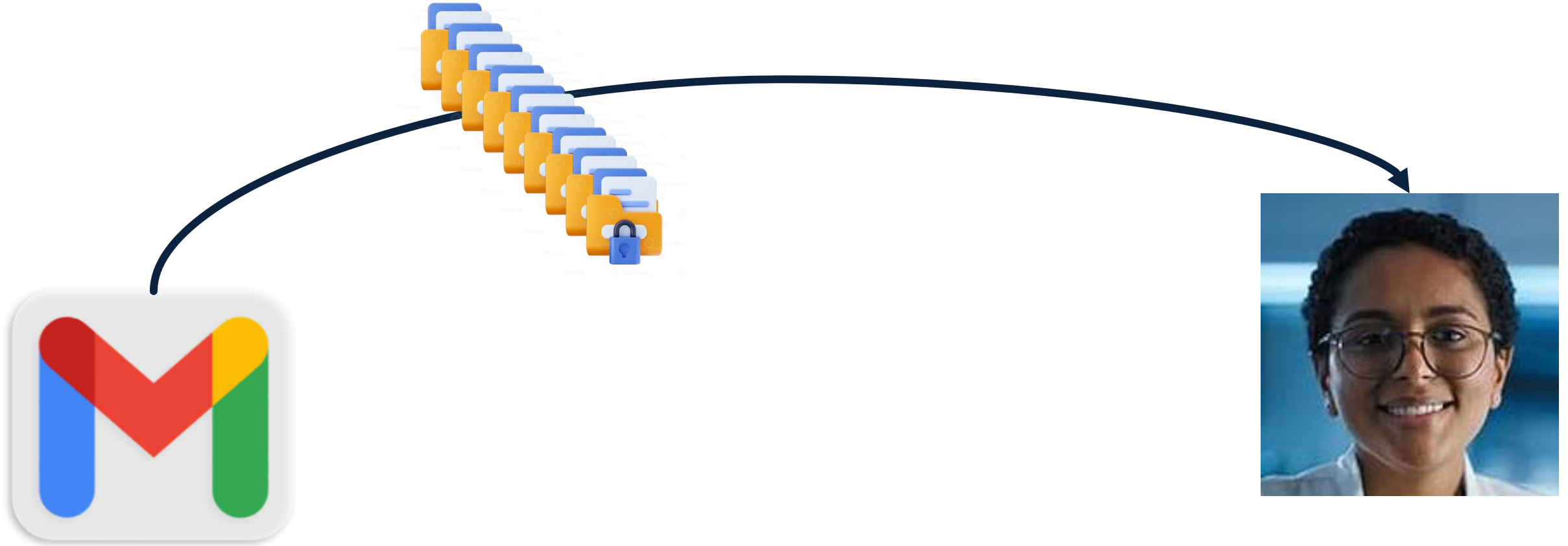


I don't want to share all
passwords!

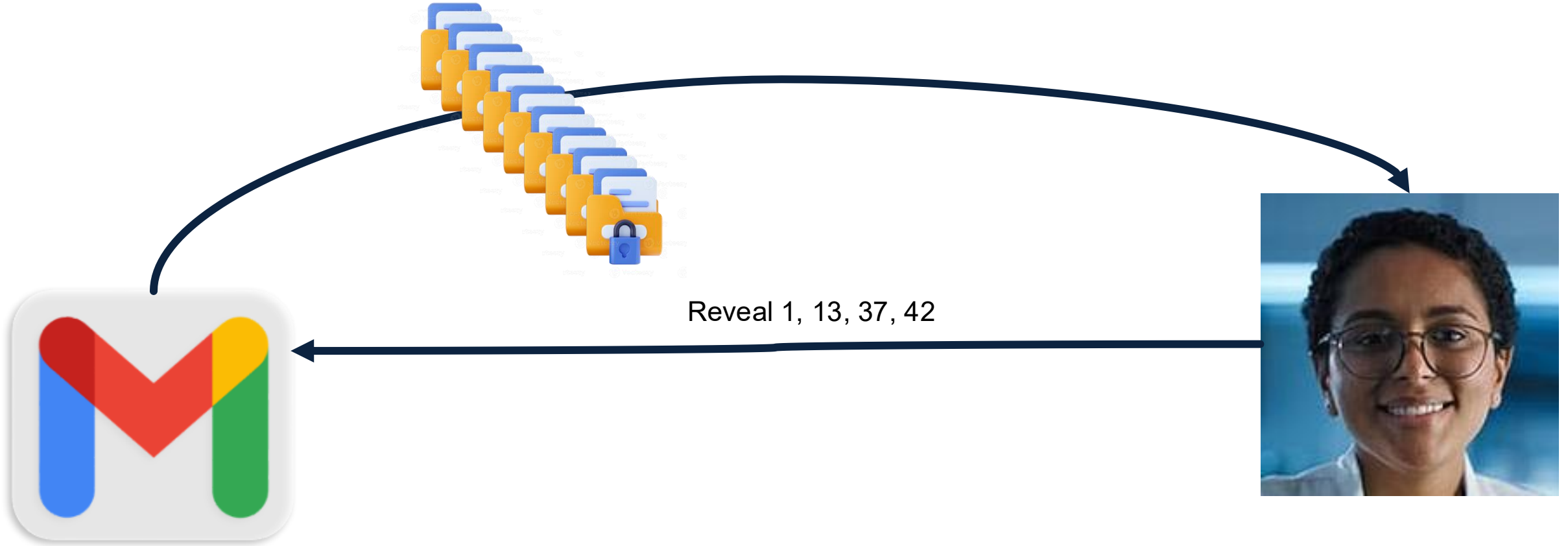


How to solve
this? Previous
work

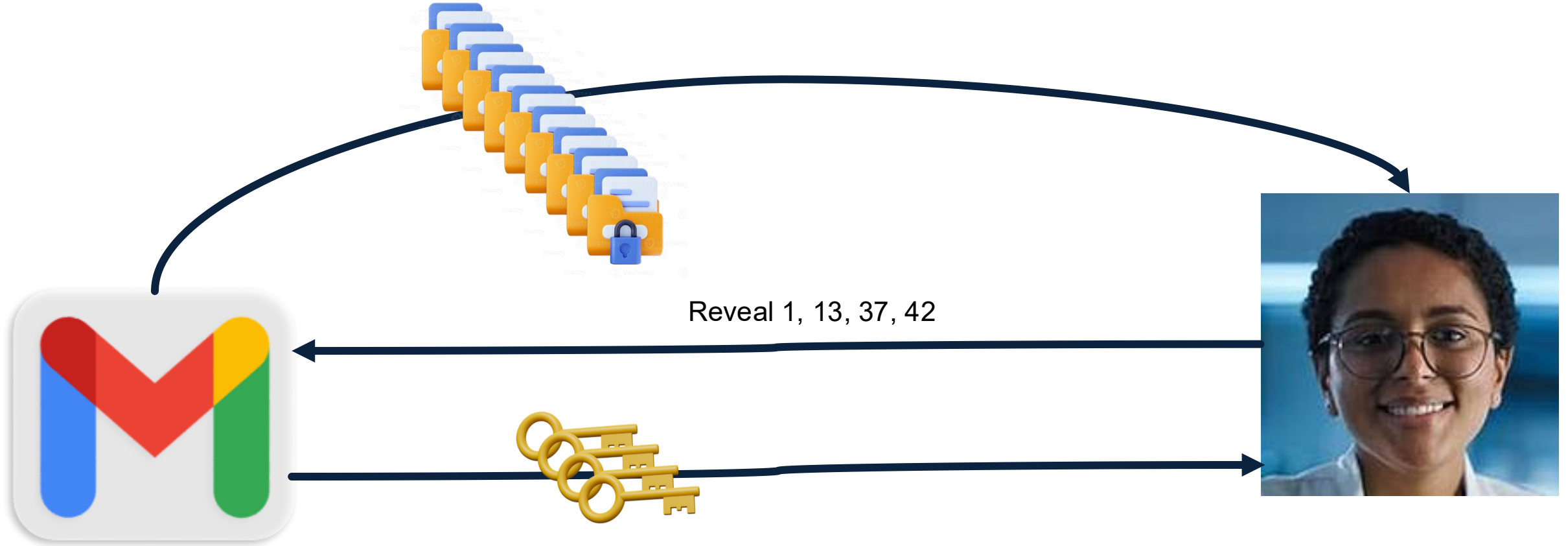
PARTIALLY Authorized Private Set Intersection



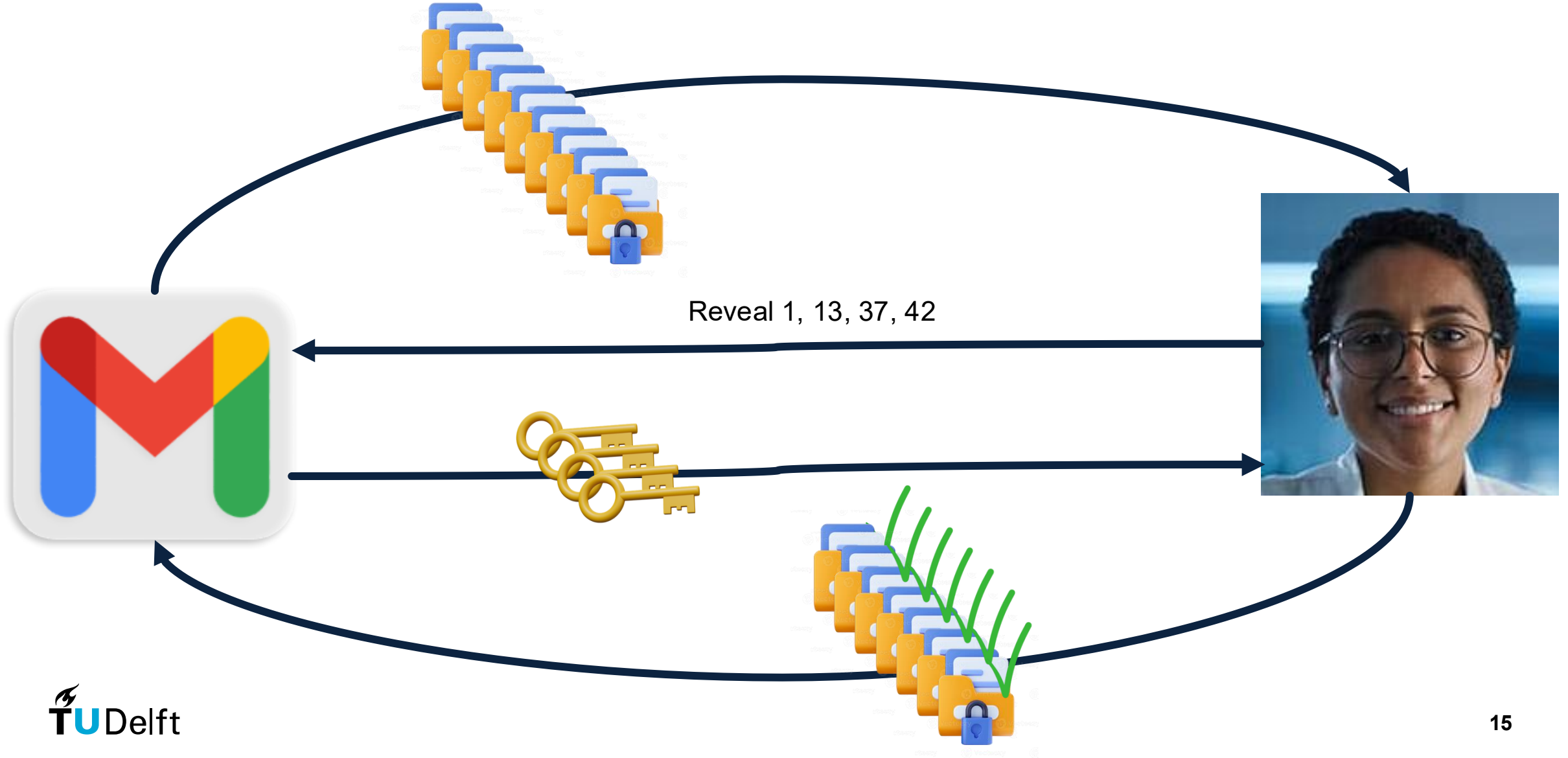
PARTIALLY Authorized Private Set Intersection



PARTIALLY Authorized Private Set Intersection



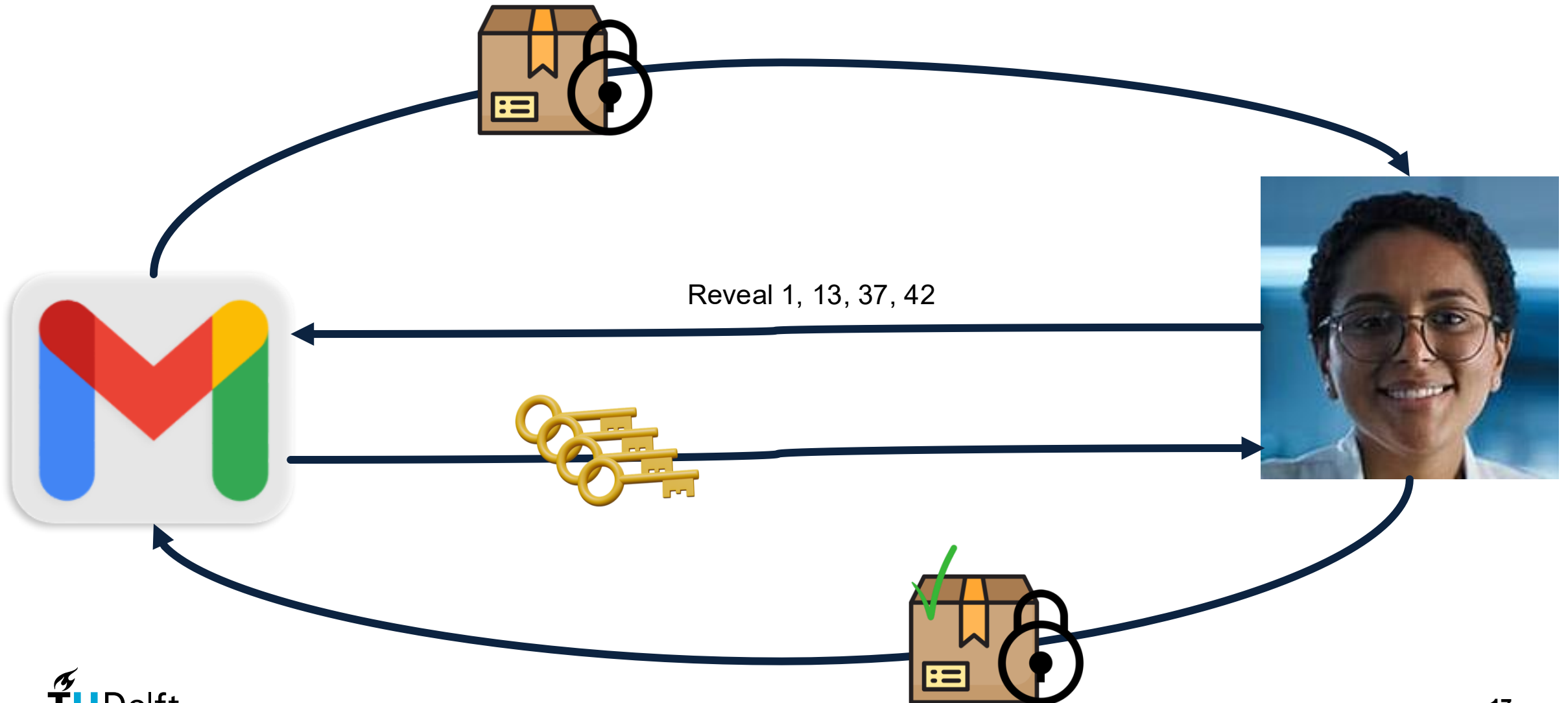
PARTIALLY Authorized Private Set Intersection



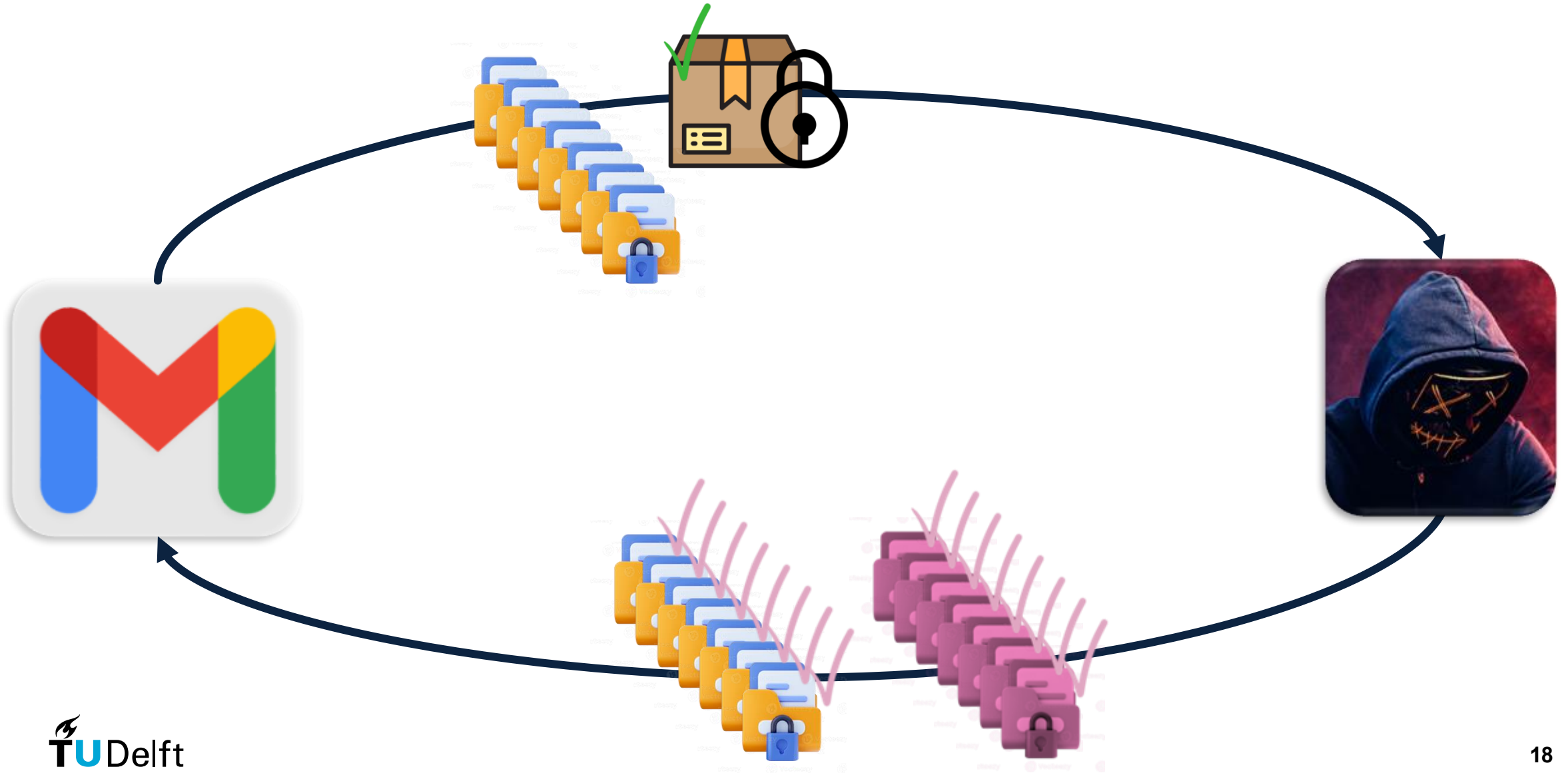


That is a lot of
documents...
We can do this
smarter! **New
work**

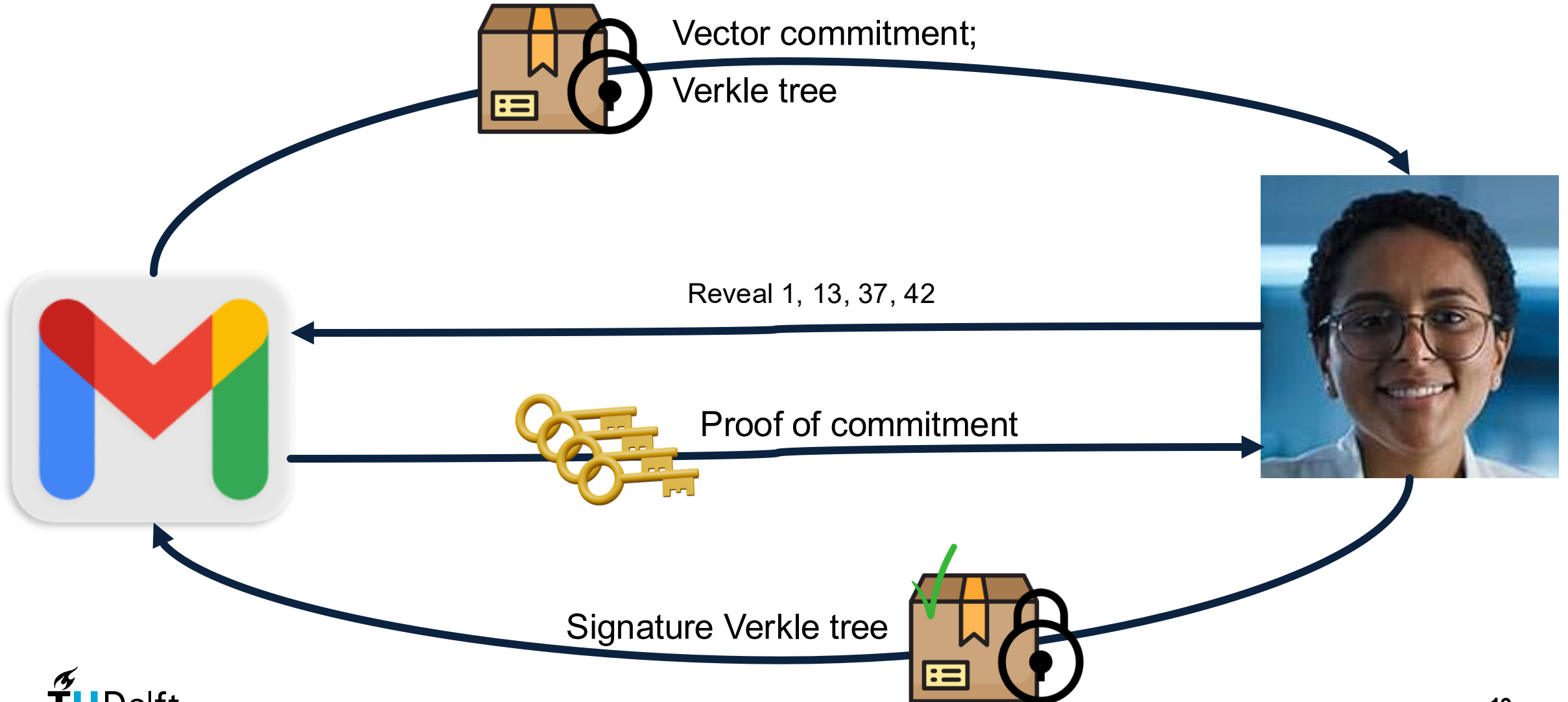
IMPROVED Partial Authorized PSI



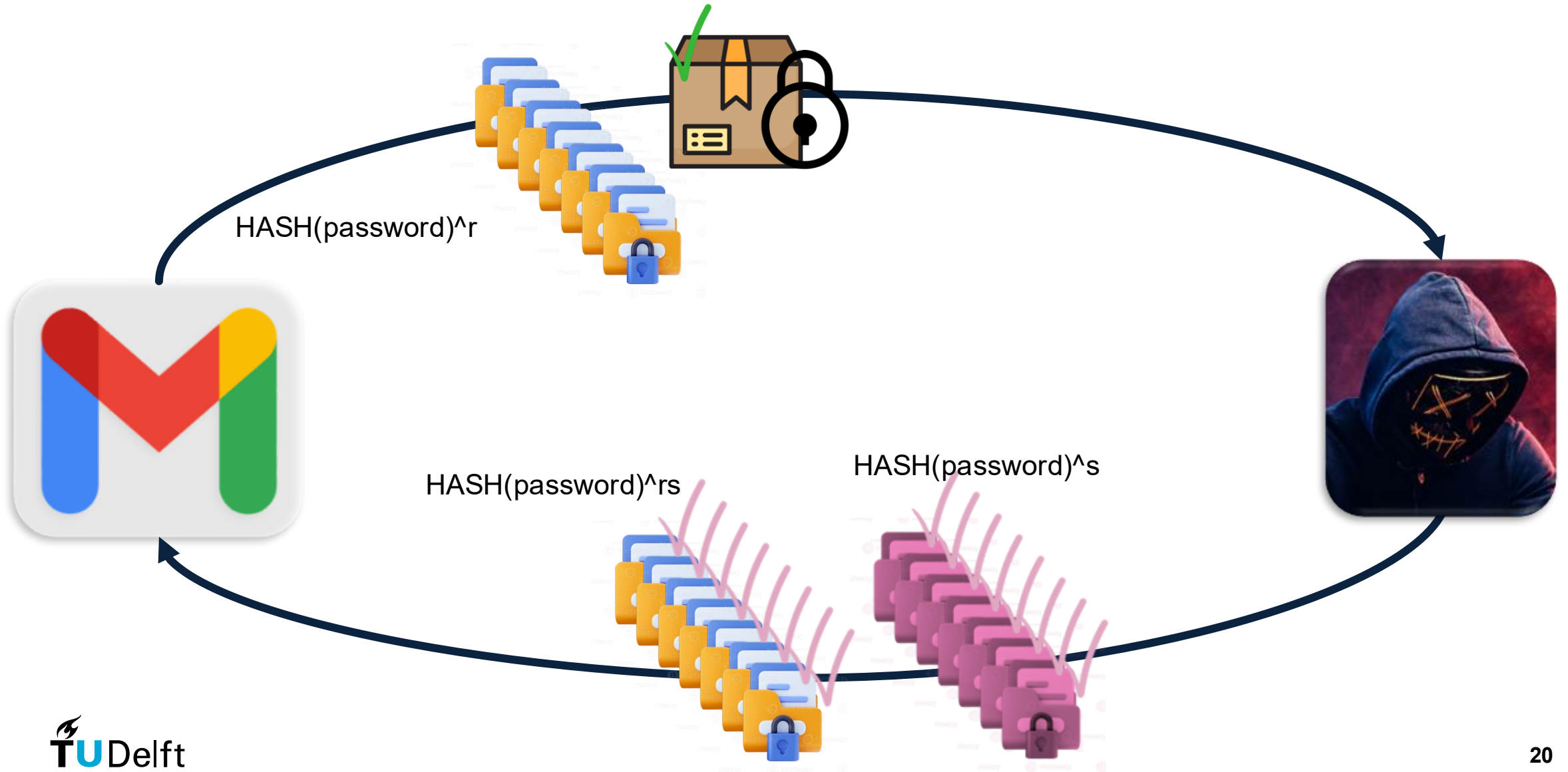
IMPROVED Partial Authorized PSI - Intersection



IMPROVED Partial Authorized PSI



IMPROVED Partial Authorized PSI - Intersection



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!