Norwegian University of Science and Technology

Anonymous Tokens and Private Contact Tracing

By Tjerand Silde. Joint work with Martin Strand.

Content

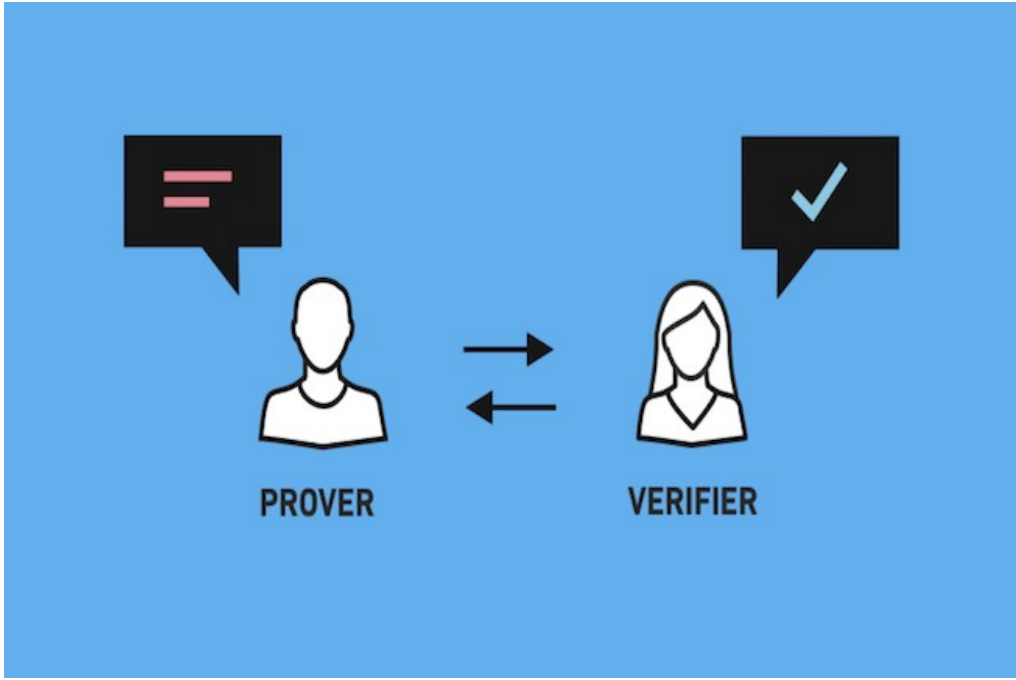
Verifiable Oblivious PRFs

Anonymous Tokens

Privacy Pass and PrivateStats

Anonymous Tokens for
Private Contact Tracing

Efficiently Revocable Tokens

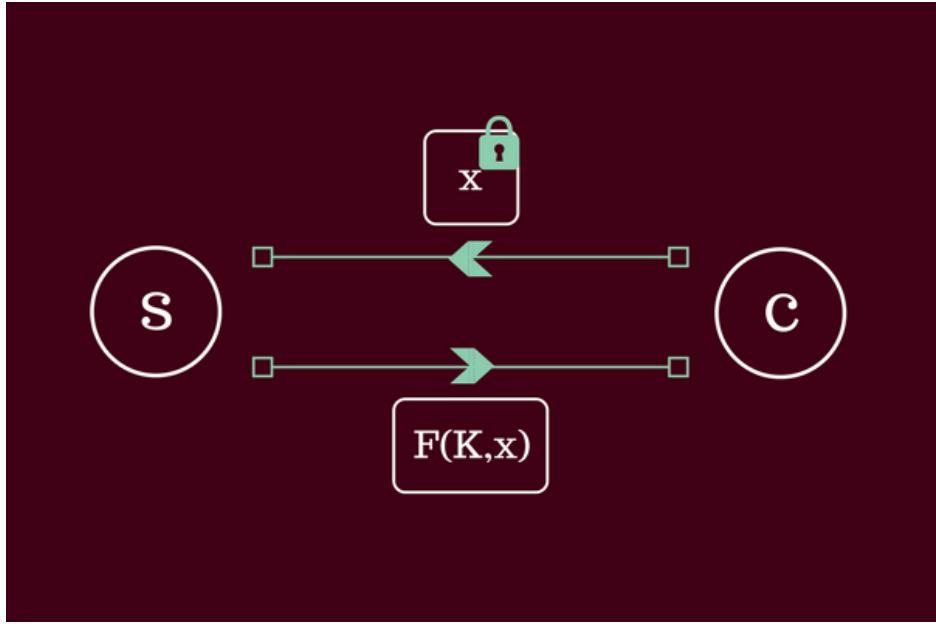


Verifiable Oblivious Pseudo-Random Functions

Two-party evaluation of a PRF.

Client learns the output of the PRF, but nothing about the key.

Server evaluates the PRF with a secret key, but learns nothing about the input or the output.



Verifiable Oblivious Pseudo-Random Functions

We make the OPRF verifiable to avoid subliminal channels.

We may get verifiability using zero-knowledge proofs or pairings.

EC-VOPRF with ZKPs:

$\underline{\text{Client}(t, K)}$		$\underline{\text{Server}(k, K)}$
$r \xleftarrow{\$} \mathbb{Z}_p^*, \quad T = \mathtt{H}(t)$		
$P = [r]T$	$\xrightarrow{P}$	$Q = [k]P$
If $\mathtt{Verify}((G, K), (P, Q), \pi) \stackrel{?}{=} 1$:	$\xleftarrow{Q, \pi}$	$\pi \leftarrow \mathtt{Prove}((G, K), (P, Q)); k)$
$W = [r^{-1}]Q$		
Store (t, W)		

Anonymous Tokens

Many flavors in literature: Anonymous Tokens, Anonymous Credentials, Blind Signatures, Partially Blind Signatures, …

Properties: unlinkability, unforgeability, public or designated verifiability, revocation, rounds of interaction, efficiency, …

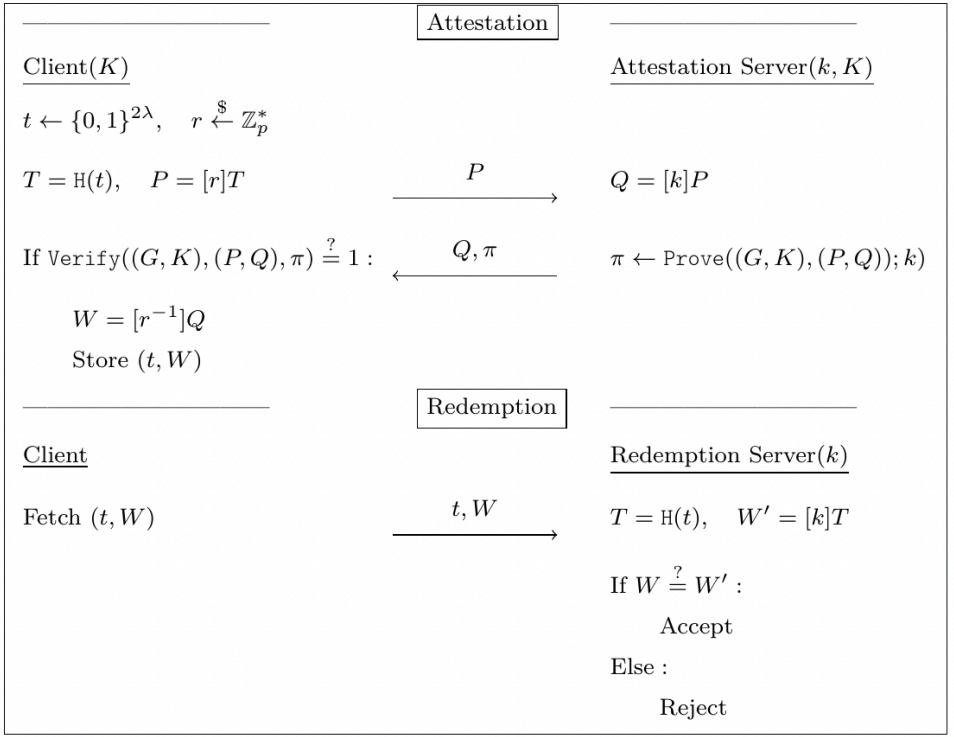
Underlying primitives: factoring, quadratic residues, (elliptic curve) discrete logarithms, bilinear pairings, …

Privacy Pass

Developed by Cloudflare.

Solve CAPTCHA, get batch of tokens. Redeem tokens later to avoid CAPTCHA.

Published at PETS 2018.

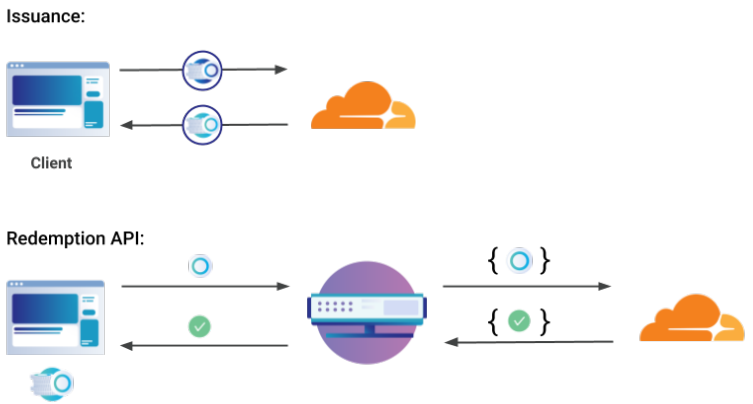


Privacy Pass

Use-case: Users should be able to use Tor without solving CAPTCHAs all the time.

Security: Should not track users, but also prevent DDOS.

Problem: Revocation of tokens.



PrivateStats

Developed by Facebook.

Used to collect anonymous statistics from WhatsApp.

Presented at RWC 2021 and AC Meeting 2021.

Use attributes and VOPRF based on Naor-Reingold to update the public key.

Solve revocation by updating the public key every day.

Adds overhead in signatures.

Anonymous Tokens for Private Contact Tracing

The Norwegian Institute of Public Health has developed an app “Smittestopp” to supplement traditional contact tracing.

The app sends you a notification if you have been close to someone that has tested positive for Covid 19.

The hope is that this may be faster and may notify contacts that you forgot about or didn’t know about.

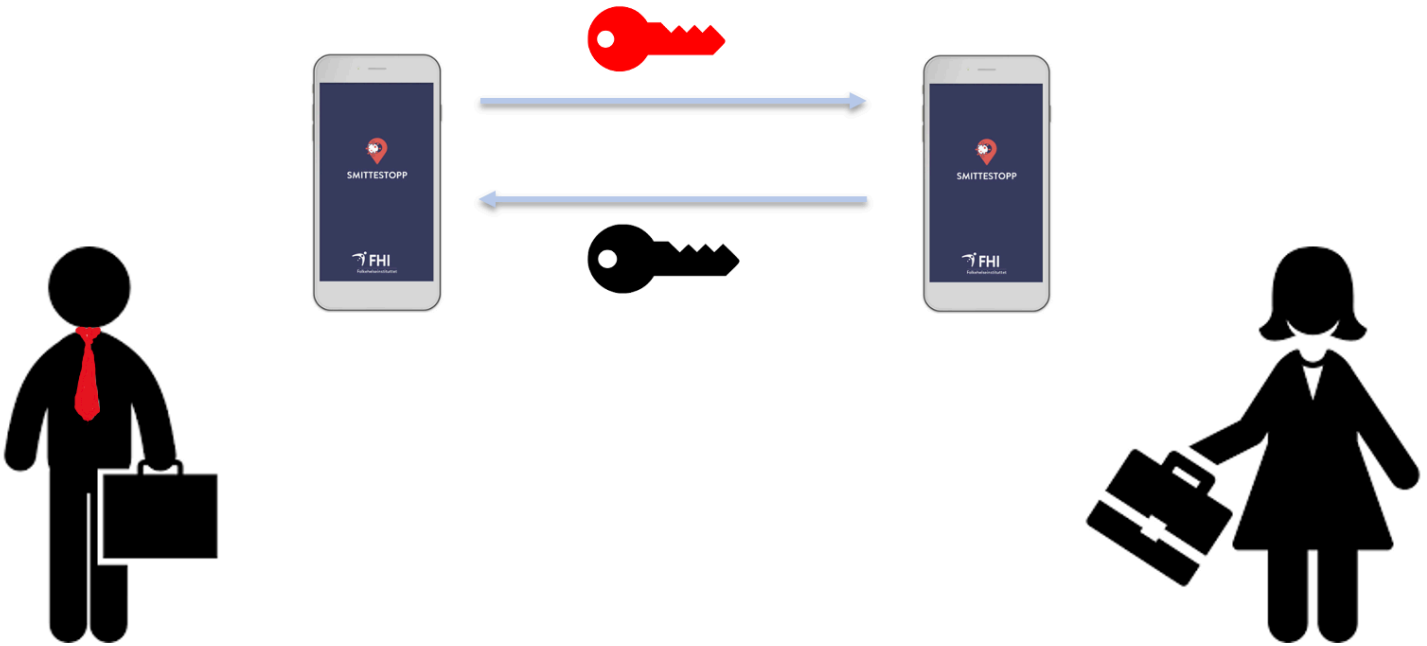
Anonymous Tokens for Private Contact Tracing

All data is stored on the user's phone. It uses Bluetooth for communication with other phones, but no GPS tracking.

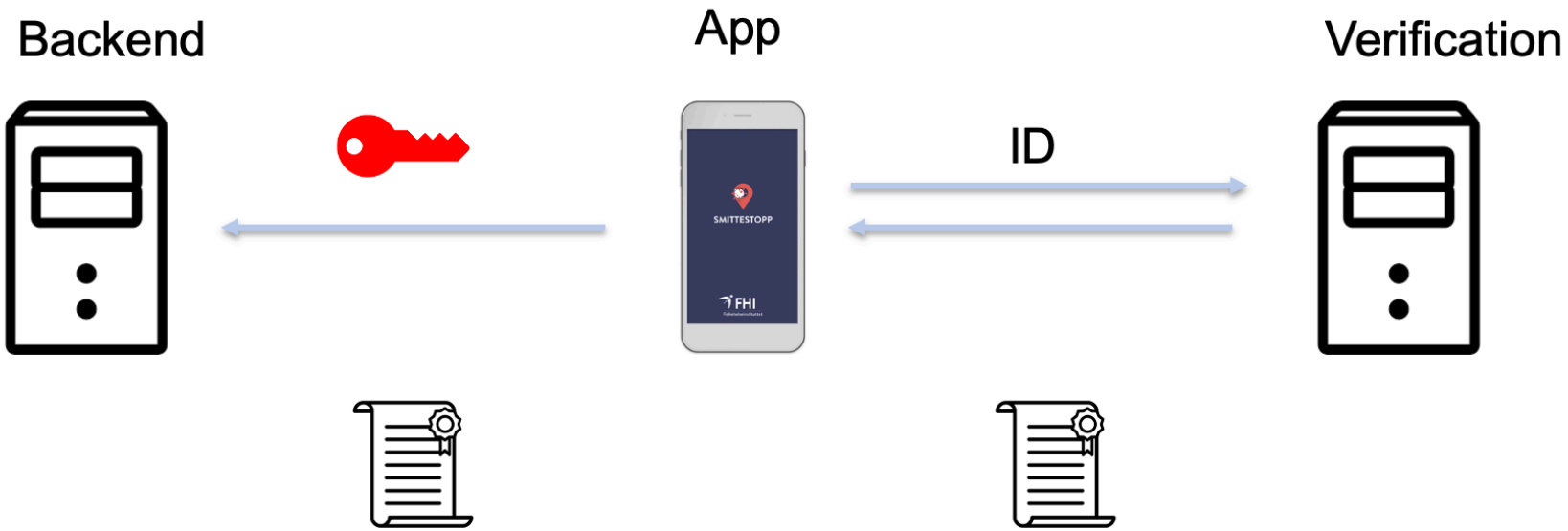
You only identify yourself to report a positive test, and then you upload the "infections keys" to the server.

The other users check locally if they have been in touch with someone who has uploaded their keys.

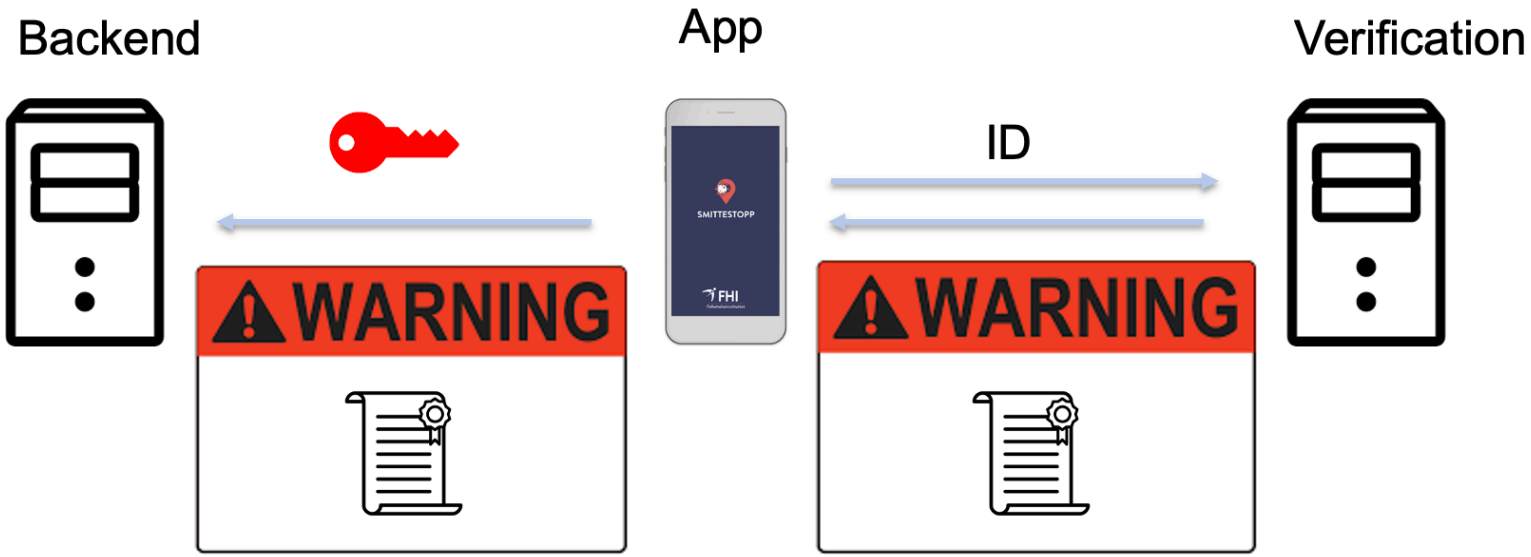
Anonymous Tokens for Private Contact Tracing



Anonymous Tokens for Private Contact Tracing

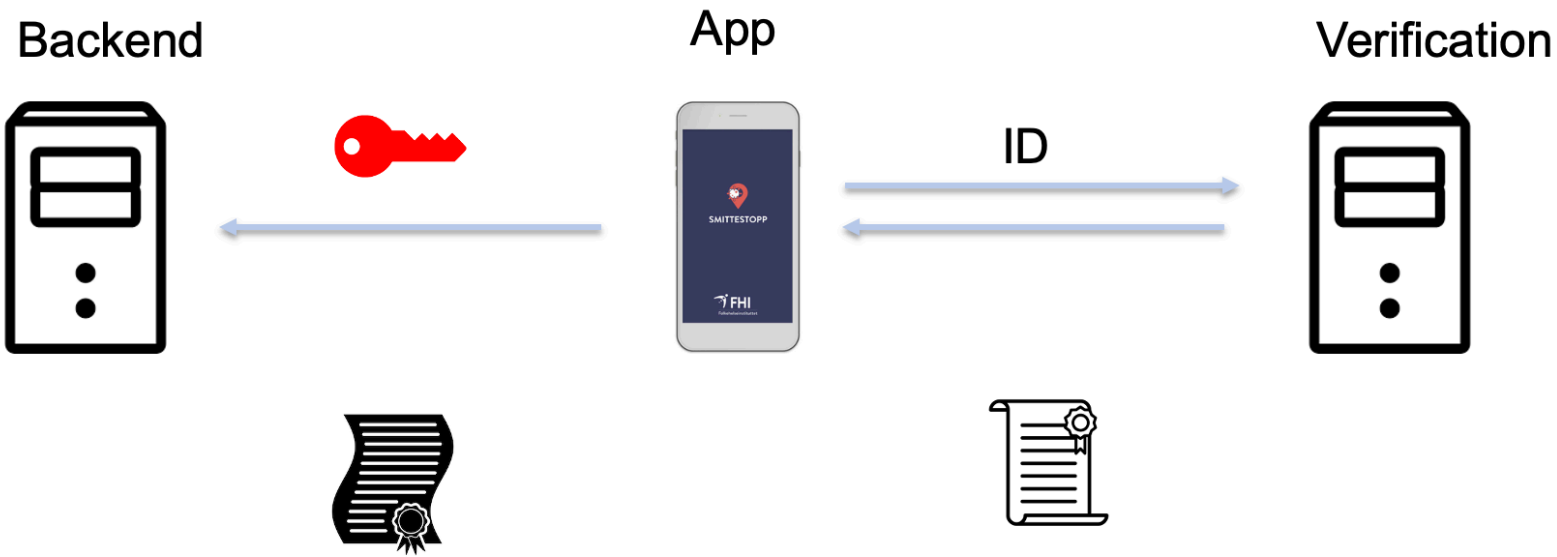


Anonymous Tokens for Private Contact Tracing



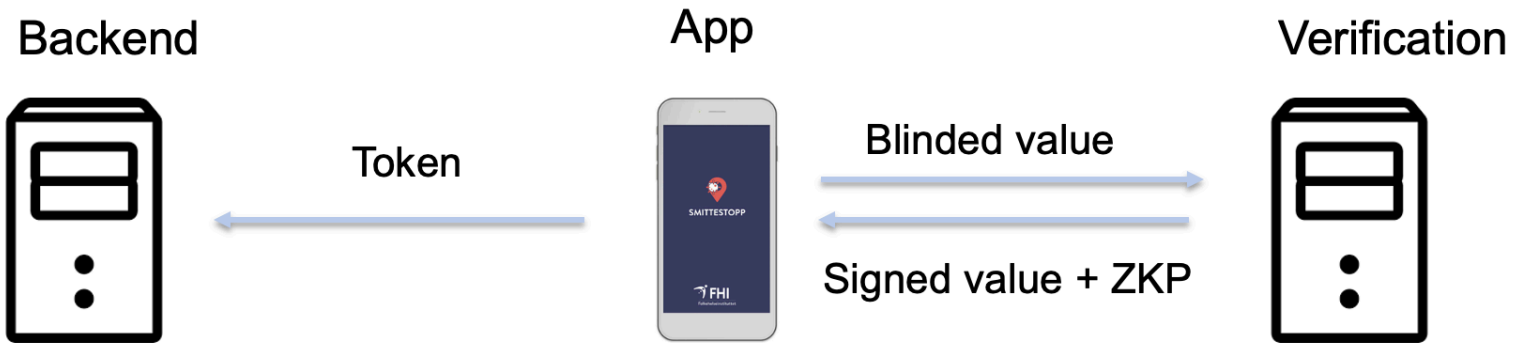
ID can be correlated with the “infection keys”!

Anonymous Tokens for Private Contact Tracing



Solution: The app randomizes the token before it is being forwarded.

Anonymous Tokens for Private Contact Tracing



4. Verify token

1. Choose a random and blinded value to be signed

3. Verify proof and unblind

2. Sign the value, and prove that it was correctly signed

Anonymous Tokens for Private Contact Tracing

Problem: Users should not be able to hold onto a token and upload later. We revoke all unspent tokens older than 3 days.

Solution: The client needs to download new public keys from a public API every time it wants to talk to the server. Impractical.

Note: Still possible to correlate identities with “infection keys” if the servers are logging IP-addresses and timestamps.

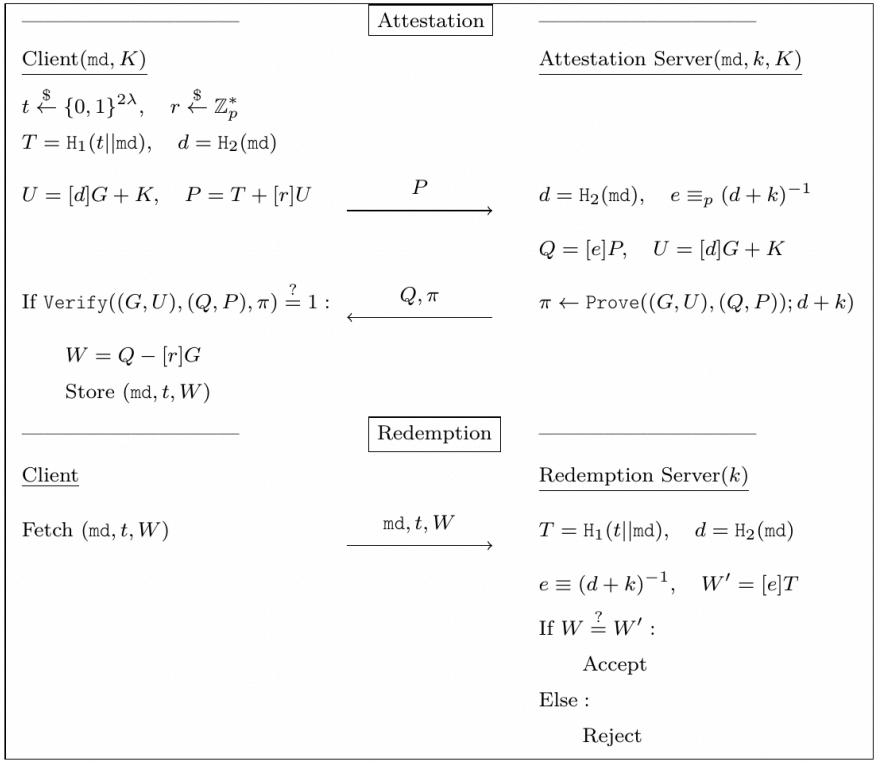
Efficiently Revocable Tokens

New anonymous token protocol with public metadata.

Based on ECC, avoids pairings.

Revocation based on metadata.

As efficient as plain Privacy Pass!



Efficiently Revocable Tokens

	PubKey	Request	Signature	Token
Privacy Pass [16]	2^N*257 bits	257 bits	769 bits	512 bits
PrivateStats [19]	(N+2)*257 bits	257 bits	(N+1)*769 bits	512 bits
Abe and Fujisaki [1]	3328 bits	3072 bits	3072 bits	3328 bits
Zhang et al. [26]	763 bits	382 bits	382 bits	638 bits
Our scheme (Fig 1)	257 bits	257 bits	769 bits	512 bits

Table 1. Comparison of the schemes allowing for 2^N rounds of batched token-revocations. Messages are of fixed size 256 bits, and metadata is implicit knowledge. Privacy Pass, PrivateStats and our scheme is instantiated with an elliptic curve over a 256 bits field, Abe and Fujisaki is instantiated with RSA-3072 and Zhang et al. is instantiated with BLS12-381. Additional signatures in Privacy Pass, PrivateStats and our protocol attested at the same time is only of size 257 bits because of batched proofs.

Thank you! Questions?

Slides: tjerandsilde.no/talks