Rerandomisable blind signatures without subliminal channels

Or: Strong anonymity in Smittestopp 2

Martin Strand
Forsvarets forskningsinstitutt
17 November 2021

Foto: AdobeStock

The Schnorr protocol

Public input: $G = \langle g \rangle, |G| = q$ and $B \in G$.
Private input to P: b such that $B = g^b$.

Prover		Verifier
$s \overset{\$}{\leftarrow} \mathbb{Z}_q$		
$R \leftarrow g^s$	$\xrightarrow{\quad R \quad}$	
	$\xleftarrow{\quad h \quad}$	$h \overset{\$}{\leftarrow} \mathbb{Z}_q$
$r \leftarrow bh + s$	$\xrightarrow{\quad r \quad}$	$g^r \overset{?}{=} RB^h$

Desirable properties

Handwavy edition

Completeness	If both the prover and the verifier are honest, the verifier will accept.
Soundness	If the prover is dishonest, the verifier will reject (with large probability)
Honest-Verifier Zero-Knowledge	(R, h, s) contains no information about b

Schnorr signatures

$$(G,*) = \langle g \rangle$$

$$H : G \times \mathcal{M} \rightarrow \mathbf{Z}_p^*$$

KeyGen

$b \stackrel{\$}{\leftarrow} \{1 \dots |G|\}$
$B \leftarrow g^b$
return $(sk = b, vk = B)$

Sign$(sk = b, M)$

$r \stackrel{\$}{\leftarrow} \{1 \dots |G|\}$
$R \leftarrow g^r$
$h \leftarrow H(R, M)$
$s \leftarrow r - bh \bmod p$
return $\sigma = (h, s)$

M, σ ←

Vrfy$\big(vk = B, M, \sigma = (h, s)\big)$

$R' \leftarrow g^s * B^h$
$h' \leftarrow H(R', M)$
if $h' = h$ **then**
    return 1
else
    return 0

Correctness: $\mathrm{Vrfy}\big(vk, M, \mathrm{Sign}(sk, M)\big) = 1$

$$h' = H(R', M) = H\big(g^s B^h, M\big) = H\big(g^{r-bh} g^{bh}, M\big) = H\big(g^{r-bh+bh}, M\big) = H(g^r, M) = H(R, M) = h$$

Schnorr signatures

$$(G,*) = \langle g \rangle$$

$$H : G \times \mathcal{M} \to \mathbf{Z}_p^*$$

KeyGen

$b \xleftarrow{\$} \{1 \ldots |G|\}$
$B \leftarrow g^b$
return $(sk = b, vk = B)$

Vrfy$(vk = B, M, \sigma = (h, s))$

$R' \leftarrow g^s * B^h$
$h' \leftarrow H(R', M)$
if $h' = h$ **then**
    return 1
else
    return 0

M, σ ⟵

Sign$(sk = b, M)$

$r \xleftarrow{\$} \{1 \ldots |G|\}$
$R \leftarrow g^r$
$h \leftarrow H(R, M)$
$s \leftarrow r - bh \bmod p$
return $\sigma = (h, s)$

Security:

- DLOG must be hard in G
- H must be collision-resistant, one-way, etc.
- Attacker must essentially solve $\quad g^r = g^s * g^{bh} \iff r = s + bh \iff s = r - bh$
- r must be picked new *every time*!

$$\sigma = (h, s), \quad \sigma' = (h', s') \quad \xRightarrow{\text{same } r} \quad s - s' = (r - bh) - (r - bh') = b \cdot (h' - h) \implies \underline{b} = (s - s') \cdot (h' - h)^{-1} \bmod p$$

Learned private long-term key!

Other properties of Schnorr signatures

Assume that the signer signs on behalf on someone else.

Subliminal channels The signature can contain a secret message

- $r \leftarrow \text{Enc}_k(\text{'don't trust them'})$
- $\ldots$
- $r' \leftarrow \text{Enc}_k(\text{'don't trust them'})$; if $g^{r'} = R, (\ldots)$

Not rerandomisable Adding fresh randomness will invalidate the signature

- "Hey, the identity of the bearer of signature ($M =$ 'has rare disease'$, \sigma$) is (...)"

Chaum-Pedersen proofs

Public input: $G = \langle g \rangle$, $|G| = q$ and $h, y, z \in G$.
Private input to P: x such that $h = g^x, y = z^x$.

Prover		Verifier
$s \xleftarrow{\$} \mathbb{Z}_q$		
$(a, b) \leftarrow (g^s, y^s)$	$\xrightarrow{(a, b)}$	
	$\xleftarrow{c}$	$c \xleftarrow{\$} \mathbb{Z}_q$
$r \leftarrow s + cx$	$\xrightarrow{r}$	$g^r \stackrel{?}{=} ah^c$
		$h^r \stackrel{?}{=} by^c$

David Chaum, Torben Pryds Pedersen: Wallet Databases with Observers (1992)

Blind RSA signatures

Textbook RSA signatures

$n = p \cdot q$

RSA.KeyGen

$p, q \xleftarrow{\$}$ two random prime numbers
$n \leftarrow p \cdot q$
$\phi(n) = (p-1)(q-1)$
choose e such that $\gcd(e, \phi(n)) = 1$
$d \leftarrow e^{-1} \bmod \phi(n)$
$sk \leftarrow (n, d) \qquad pk \leftarrow (n, e)$
return (sk, pk)

RSA.Vrfy$((n, e), M, \sigma)$

if $\sigma^e = M \bmod N$ **then**
  return 1
else
  return 0

$M, \ \sigma = M^d \bmod n$

RSA.Sign$((n, d), M)$

$\sigma \leftarrow M^d \bmod N$
return σ

Modification

- Choose r with corresponding r^{-1}
- $m' \leftarrow mr^e$
- Get signature $s' = (m'r^e)^d$ on m'
- Compute signature $s = r^{-1}s'$ on m

Smittestopp 2

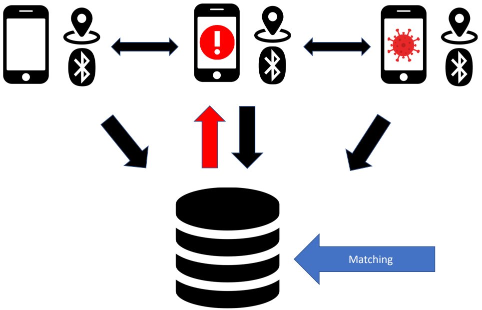
Digital contact tracing

Objective	Alert individuals that may have been around COVID-19 carriers
Proxy objective	Alert *phones* that may have been around *phones belonging to* COVID-19 carriers

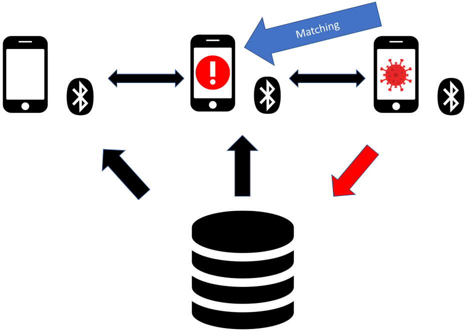
See also

Feretti, Wymant, Kendall, Zhao, Nurtay, Abeler-Dörner, Parker, Bonsall, Fraser: Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, vol 368, issue 6491.

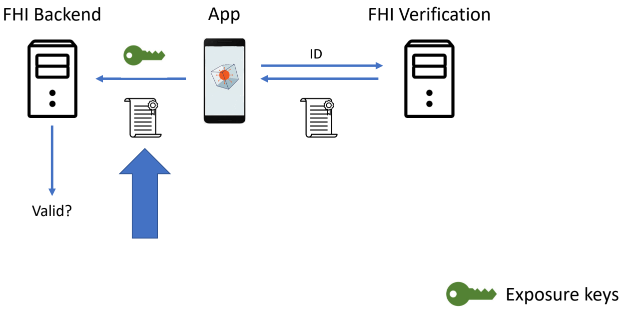
Strategy 1: Identifiable, centralised storage



Strategy ca. 37: dp^{3}t and ENS



Smittestopp 2: Initial plan



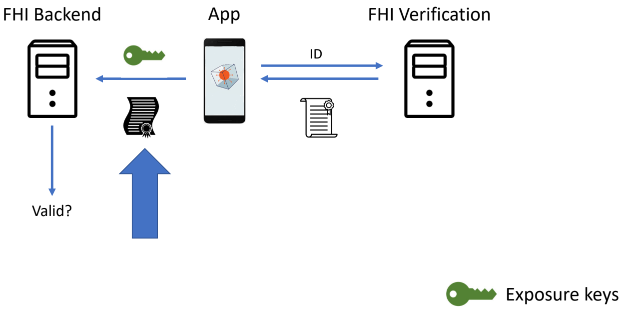
What is privacy here?

Rule of thumb

Cryptographers don't want to trust anyone

What if FHI Backend and FHI Verification collude to identify the user?

Smittestopp 2: Simple solution



How to solve this?

We need a signature scheme that is

- blinded
- single-use
- without subliminal channels
- rerandomisable for the user

</Martin’s knowledge in October 2020>

Privacy Pass

Privacy Pass: Bypassing Internet Challenges Anonymously — 171

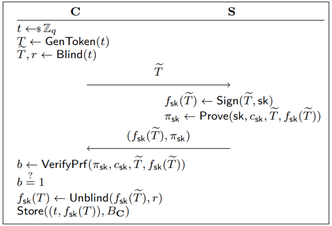


Fig. 2. An overview of the token signing protocol.

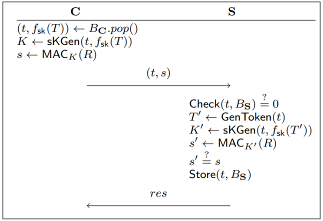


Fig. 3. An overview of the token redemption protocol.

Original publication

Davidson, Goldberg, Sullivan, Tankersley, Valsorda. Privacy Pass: Bypassing Internet Challenges Anonymously. *PETS 2018*.

VOPRF

Oblivious PRF

- A two-party protocol between a server and a client
- The server holds a PRF key k
- The client holds some input x
- Cooperate to compute $F(k, x)$ such that:
  — the client learns $F(k, x)$ without learning anything about k
  — the server does not learn anything about x or $F(k, x)$

VOPRF

Oblivious PRF

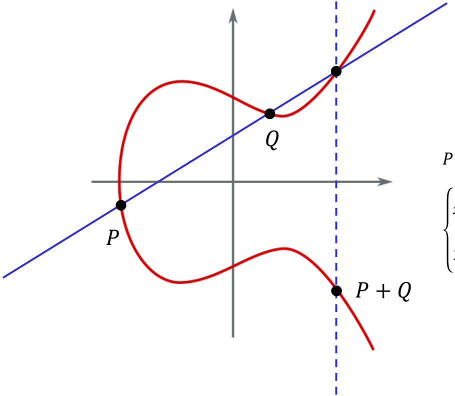
- A two-party protocol between a server and a client
- The server holds a PRF key k
- The client holds some input x
- Cooperate to compute $F(k, x)$ such that:
  - the client learns $F(k, x)$ without learning anything about k
  - the server does not learn anything about x or $F(k, x)$

Verifiable OPRF

A Verifiable OPRF (VOPRF) is an OPRF wherein the server can prove to the client that $F(k, x)$ was computed using the key k.

Elliptic curves

Theorem: the points on an elliptic curve, together with $\mathcal{O}$, is an abelian group under "geometric point addition"



$$y^2 = x^3 + ax + b$$

$$a, b, x, y \in \boldsymbol{R}$$

$$P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$\begin{cases} x_3 = \dfrac{(x_1x_2 - 2a)x_1x_2 - 4b(x_1 + x_2) + a^2}{(x_1x_2 + a)(x_1 + x_2) + 2y_1y_2 + 2b} \\ y_3 = \dfrac{x_1x_2(x_1 + x_2) - x_3\big((x_1 + x_2)^2 - x_1x_2 + a\big) - y_1y_2 - b}{y_1 + y_2} \end{cases}$$

Protocol details

Signing

User(K)		**Signer**(k)
$t \leftarrow\!\$\, \{0,1\}^\lambda$, $r \leftarrow\!\$\, \mathbb{Z}_p^*$		
$T \leftarrow \mathtt{H}_t(t)$		
$T' \leftarrow [r^{-1}]T$	$\xrightarrow{T'}$	$W' \leftarrow [k]T'$
	$\xleftarrow{W', \pi_{\mathtt{DLEQ}}}$	$\pi_{\mathtt{DLEQ}} \leftarrow \Pi_{\mathrm{DLEQ}}(G, T', K, W'; k)$
if not $\mathtt{V}(\pi_{\mathtt{DLEQ}})$:		
return $\perp$		
$W \leftarrow [r]W'$		
return (t, W)		

Redemption

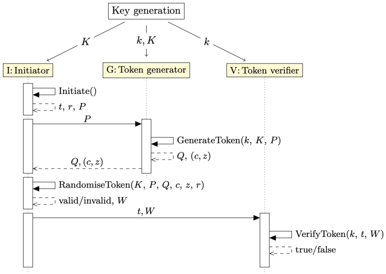
User(t, W)		**Verifier**(sk)
	$\xrightarrow{t, W}$	$T \leftarrow \mathtt{H}_t(t)$
		if $W = [k]T$:
		return true
		else :
		return false

Properties

Correctness	If the user, signer and verifier are honest, the verifier will accept
Unlinkability	$(T', W', \pi_{\mathrm{DLEQ}}, t, W)$ contains no information about the user
One-more unforgeability	If the user requests n valid tokens, the verifier should not later accept $n+1$ tokens

Implementation

- Henrik Walker Moe (Bekk)
- Tjerand Silde (NTNU)
- Martin Strand (FFI)



Public repository

https://github.com/HenrikWM/anonymous-tokens

Architecture

Integration choices

- Each public key is valid for 3 days
- Current keys can be retrieved from a public FHI endpoint
- Anonymous tokens enabled by a feature flag

Architecture

Integration choices

- Each public key is valid for 3 days
- Current keys can be retrieved from a public FHI endpoint
- Anonymous tokens enabled by a feature flag

Possible attacks

- Target custom keys to each individual
- Downgrade to JWS tokens for chosen user
- Network analysis

Anonymous tokens with public metadata

Signing

User(md)		**Signer**(md, sk)
$d \leftarrow \mathtt{H}_m(\text{md})$		$d \leftarrow \mathtt{H}_m(\text{md})$
$U \leftarrow [d]G + K$		$U \leftarrow [d+k]G$
$t \leftarrow\$ \{0,1\}^\lambda, r \leftarrow\$ \mathbb{Z}_p^*$		$e \leftarrow (d+k)^{-1}$
$T \leftarrow \mathtt{H}_t(t)$		
$T' \leftarrow [r^{-1}]T$	$\xrightarrow{T'}$	$W' \leftarrow [e]T'$
	$\xleftarrow{W', \pi_{\mathtt{DLEQ}}}$	$\pi_{\mathtt{DLEQ}} \leftarrow \Pi_{\mathrm{DLEQ}}(G, T', K, W'; e)$
if not $\mathtt{V}(\pi_{\mathtt{DLEQ}})$:		
return $\perp$		
$W \leftarrow [r]W'$		
return (t, md, W)		

Redemption

User(t, md, W)		**Verifier**(sk)
	$\xrightarrow{t, \text{md}, W}$	$T \leftarrow \mathtt{H}_t(t)$
		$e \leftarrow (\mathtt{H}_m(\text{md}) + k)^{-1}$
		if $W = [e]T$:
		return true
		else :
		return false

Anonymous Tokens with Public Metadata and Applications to Private Contact Tracing

Tjerand Silde[1] and Martin Strand[2]

[1] Department of Mathematical Sciences, Norwegian University of Science and Technology – NTNU, tjerand.silde@ntnu.no

[2] Norwegian Defence Research Establishment – FFI, martin.strand@ffi.no

Abstract. Anonymous tokens have recent applications in private Internet browsing and anonymous statistics collection. We develop new schemes in order to include public metadata such as expiration dates for tokens. This inclusion enables planned mass revocation of tokens without distributing new keys, which for natural instantiations can give 77–90 % amortized traffic savings compared to Privacy Pass (Davidson et al., 2018) and PrivateStats (Huang et al., 2021), respectively. By transforming the public key, we are able to append public metadata to several existing protocols without having to change the security proofs in any substantial way.
Additional contributions include expanded definitions and a description of how anonymous tokens can improve the privacy in dp[3]t-like digital contact tracing applications. We also show how to create efficient and conceptually simple tokens with public metadata and public verifiability from pairings.

Keywords: anonymous tokens, public metadata, elliptic curves, pairings, private contact tracing, cryptography

https://eprint.iacr.org/2021/203

Security proof

A Fast and Simple Partially Oblivious PRF, with Applications

Nirvan Tyagi, Cornell University
Sofía Celi, Cloudflare
Thomas Ristenpart, Cornell Tech
Nick Sullivan, Cloudflare
Stefano Tessaro, University of Washington
Christopher A. Wood, Cloudflare

Abstract

We build the first construction of a partially oblivious pseudorandom function (POPRF) that does not rely on bilinear pairings. Our construction can be viewed as combining elements of the 2HashDH OPRF of Jarecki, Kiayias, and Krawczyk with the Dodis-Yampolskiy PRF. We analyze our POPRF's security in the random oracle model via reduction to a new one-more gap strong Diffie-Hellman inversion assumption. The most significant technical challenge is establishing confidence in the new assumption, which requires new proof techniques that enable us to show that its hardness is implied by the q-DL assumption in the algebraic group model.

Our new construction is as fast as the current, standards-track OPRF 2HashDH protocol, yet provides a new degree of flexibility useful in a variety of applications. We show how POPRFs can be used to prevent token hoarding attacks against Privacy Pass, reduce key management complexity in the OPAQUE password authenticated key exchange protocol, and ensure stronger security for password breach alerting services.

`https://eprint.iacr.org/2021/864`

Security proof – sketch

- One-more unforgeability *if*

Security proof – sketch

- One-more unforgeability *if*
- (m, n)-OM-GAP-SDHI is hard, *if*

Security proof – sketch

- One-more unforgeability *if*
- (m, n)-OM-GAP-SDHI is hard, *if*
- m-UBER is hard, *if*

Security proof – sketch

- One-more unforgeability *if*
- (m, n)-OM-GAP-SDHI is hard, *if*
- m-UBER is hard, *if*
- q-discrete log is hard

Security proof – sketch

- One-more unforgeability *if*
- (m, n)-OM-GAP-SDHI is hard, *if*
- m-UBER is hard, *if*
- q-discrete log is hard

Security proof – sketch

- One-more unforgeability *if*
- (m, n)-OM-GAP-SDHI is hard, *if*
- m-UBER is hard, *if*
- q-discrete log is hard

q-Discrete Log Game

1. $x \xleftarrow{\$} \mathbb{Z}_q^*$
2. $z \leftarrow A(g^x, g^{x^2}, \ldots g^{x^q})$
3. return $z \stackrel{?}{=} x$

Public appreciation of some hardcore cryptography

Pris for innebygd personvern til Anonyme Tokens

Vinneren av innebygd personvernprisen 2020 er «Anonyme Tokens». Gruppen bak bidraget har utviklet en løsning som gir brukere med en positiv COVID-19-test økt anonymitet ved bruk av appen Smittestopp.

Publisert: 28.04.2021

Oppdatering: se teknisk presentasjon av Anonyme Tokens nederst i artikkelen.

«Anonyme Tokens» er dermed den fjerde vinneren av Datatilsynets konkurranse om *innebygd personvern*. Bak løsningen står Henrik Walker Moe i Bekk, Tjerand Silde ved NTNU og Martin Strand ved Forsvarets Forskningsinstitutt.

FFI
Forsvarets forskningsinstitutt

Vi gjør kunnskap og ideer til et effektivt forsvar