Anonymous Tokens with Private Metadata Bit

COM-506 Student seminar: security protocols and applications

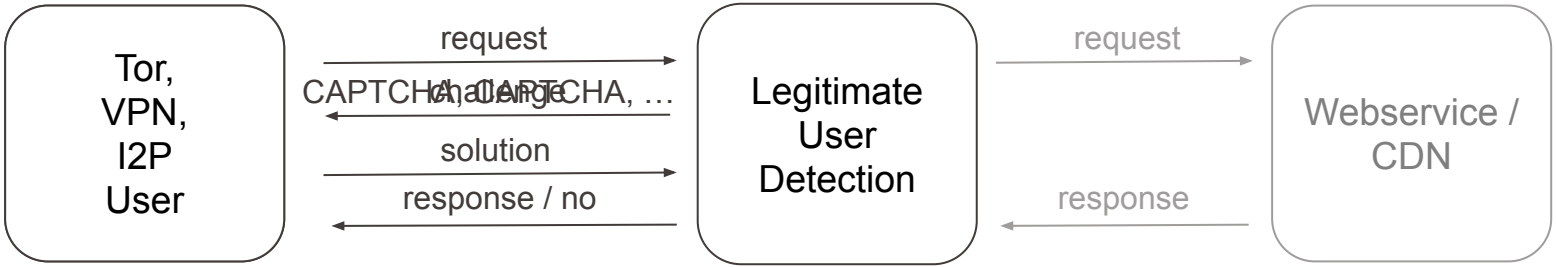
https://eprint.iacr.org/2020/072

Julian Levkov & Jonas Sulzer

Motivation

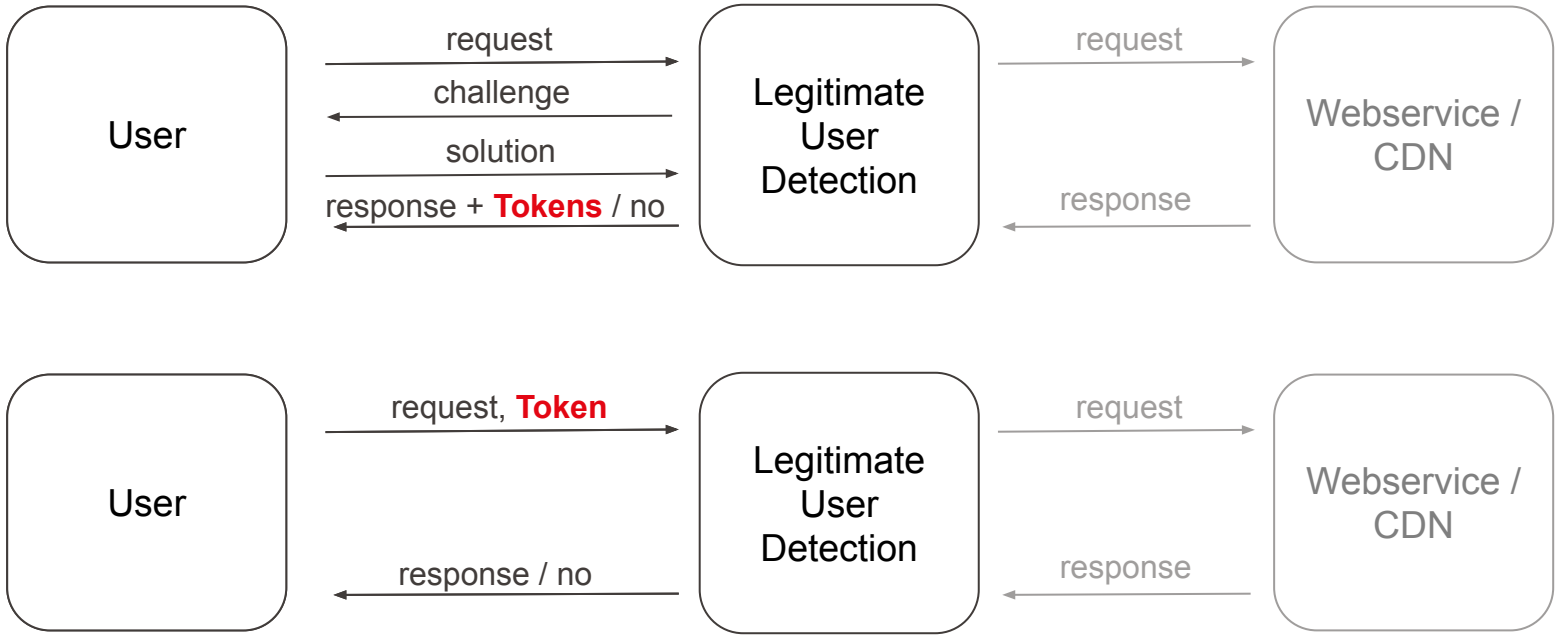
- *"On the Internet, nobody knows you're a dog."*

Website protection

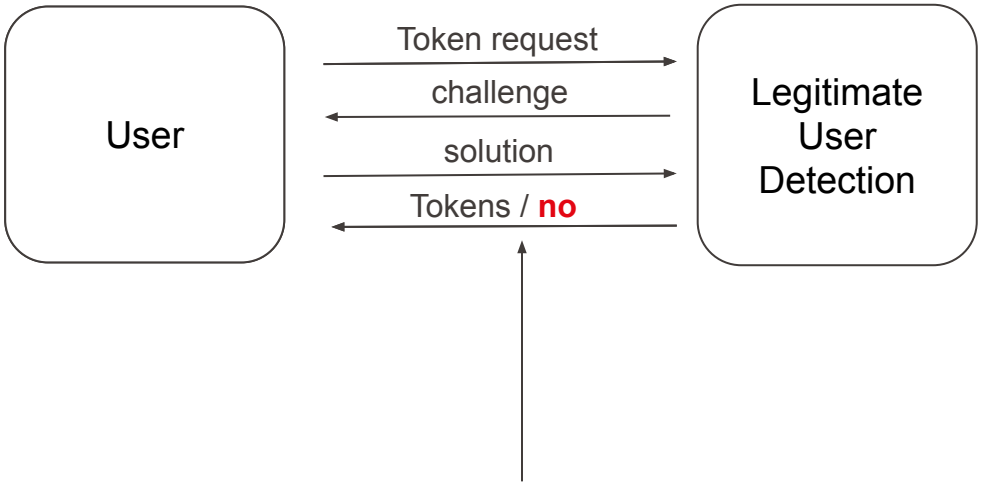


Previous Solutions: IP reputation

Solution: Privacy Pass

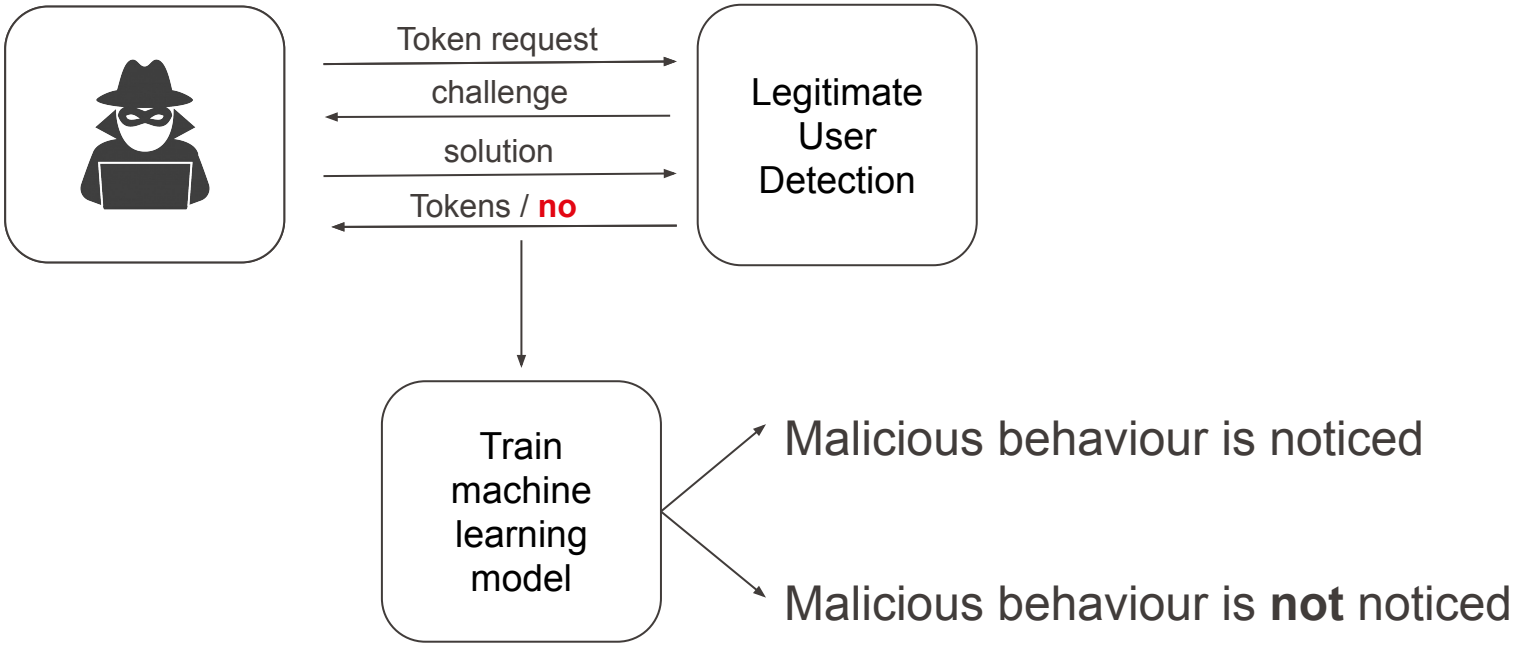


Problem with Privacy Pass

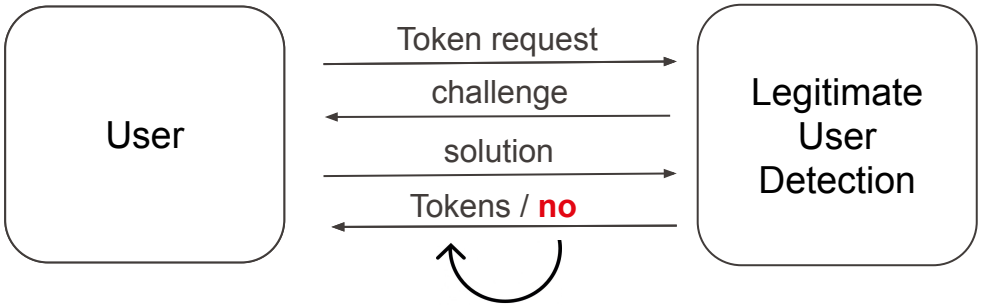


no reveals service denial at request time

Problem with Privacy Pass



PMBTokens



Hide denial in private metadata bit inside token

PMBTokens

Anonymous Token with private metadata bit

PMBTokens

- Lightweight, single-use anonymous trust token
- Private metadata bit can only be read by the authority
- Extension of Privacy Pass
- Technique to remove the need for NIZKs

Security notions

- Unlinkability
- One-more unforgeability
- Privacy of the metadata bit

From Privacy Pass To PMBTokens

Privacy Pass Recap

$\Gamma := (p, \mathbb{G}, G)$
$X = xG$

User

$r \leftarrow \mathbb{Z}_p^*$
$T' := r^{-1}\,\mathrm{H}(t)$

T'

$W' := xT'$

W', π

$\pi := DLEQ\{\begin{bmatrix} X \\ W' \end{bmatrix} = x\begin{bmatrix} G \\ T' \end{bmatrix}\}$

check π

$W := rW'$

t, W

1. check $x\mathrm{H}(t) = W$
2. add t to spend tokens.

Issuer

Private Metadata Bit ?

$\Gamma := (p, \mathbb{G}, G)$

$X_b = x_b G,\ b \in \{0, 1\}$

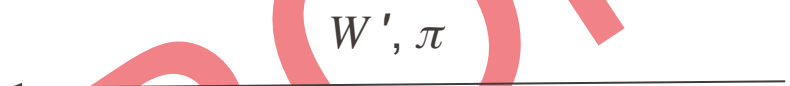
User

Issuer

$r \leftarrow \mathbb{Z}_p^*$

$T' := r^{-1} \mathrm{H}(t)$

$W' := x_b T'$



$\pi := DLEQOR\left\{\begin{bmatrix} X_b \\ W' \end{bmatrix} = x_b \begin{bmatrix} G \\ T' \end{bmatrix}\right\}$

check π

$W := rW'$

1. check b s.t $x_b \mathrm{H}(t) = W$
2. add t to spend tokens.

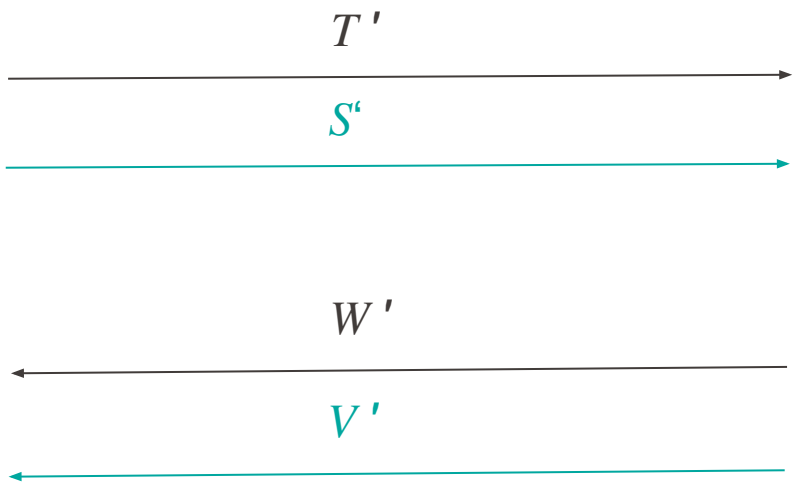
Attack

$\Gamma := (p, \mathbb{G}, G)$
$X = x_b G,\ b \in \{0, 1\}$

User

$r, s \leftarrow \mathbb{Z}_p^*$
$T' := r^{-1} H(t)$
$S' := s^{-1} H(t)$

Issuer



$rW' \stackrel{?}{=} sV$

Okamoto-Schnorr Privacy Pass

$\Gamma := (p, \mathbb{G}, G, H)$
$X = xG + yH$

User

Issuer

$r \leftarrow \mathbb{Z}_p^*$
$T' := r^{-1}\,\mathrm{H}(t)$

T' →

$s \leftarrow \{0,1\}^\lambda$; $S' := \mathrm{H}(T', s)$
$W' := xT' + yS'$

← s, W', π

$\pi := DLEQ\left\{\begin{bmatrix} X \\ W' \end{bmatrix} = x\begin{bmatrix} G \\ T' \end{bmatrix} + y\begin{bmatrix} H \\ S' \end{bmatrix}\right\}$

check π

$W := rW'$
$S := r\mathrm{H}(T', s)$

t, S, W →

1. check $x\mathrm{H}(t) + yS = W$
2. add t to spend tokens.

PMBTokens

$\Gamma := (p, \mathbb{G}, G, H)$

$X_b = x_b G + y_b H,\ b \in \{0, 1\}$

User

Issuer

$r \leftarrow \mathbb{Z}_p^*$

$T' := r^{-1}\, \mathrm{H}(t)$

T' →

$s \leftarrow \{0, 1\}^\lambda$; $S' := \mathrm{H}(T', s)$

$W' := x_b T' + y_b S'$

← s, W', π

$\pi := DLEQOR\left\{ \begin{bmatrix} X_b \\ W' \end{bmatrix} = x_b \begin{bmatrix} G \\ T' \end{bmatrix} + y_b \begin{bmatrix} H \\ S' \end{bmatrix} \right\}$

check π

$W := rW'$

$S := r\mathrm{H}(T', s)$

t, S, W →

1. check b s.t $x_b \mathrm{H}(t) + y_b S = W$
2. add t to spend tokens.

Removing the ZK proof in Privacy Pass

$\Gamma := (p, \mathbb{G}, G)$
$X = xG$

User

Issuer

$r, \varrho \leftarrow \mathbb{Z}_p^*$
$T' := r^{-1}(\mathsf{H}(t) - \varrho G)$

T' →

$W' := xT'$

← W'

$W := rW' + \varrho X$

t, W →

1. check $x\mathsf{H}(t) = W$
2. add t to spend tokens.

Removing the ZK proof in PMBTokens

User

$\Gamma := (p, \mathbb{G}, G, H)$

$X_b = x_b G + y_b H,\ b \in \{0, 1\}$

Issuer

for $d = 0,1$:

$r_d, \varrho_d \leftarrow \mathbb{Z}_p^*$

$T_d' := r_d^{-1}(\mathrm{H}(t) - \varrho_d G)$

$T_{\{0,1\}}'$ →

$s \leftarrow \{0, 1\}^\lambda$

$S_b' := \mathrm{H}(T_b', s)$

$W' := x_b T_b' + y_b S_b'$

← s, W'

for $d = 0,1$:

$W_d := r_d W' + \varrho_d X_d$

$S_d := r_d \mathrm{H}(T_d', s) + \varrho_d H$

$t, S_{\{0,1\}}, W_{\{0,1\}}$ →

1. check b s.t $x_b \mathrm{H}(t) + y_b S_b = W_b$
2. add t to spend tokens.

Security notions

- Unlinkability
- One-more unforgeability
- Privacy of the metadata bit

Implementation & Performance

Implementation & Performance

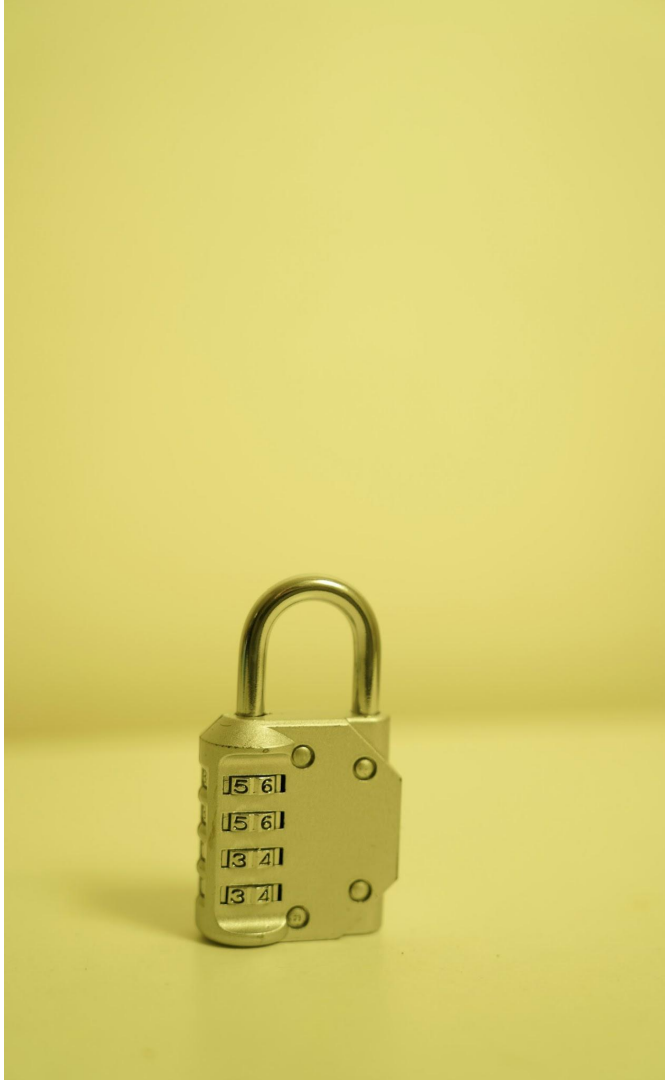
- Implemented using Rust
- Using the Ristretto group
- Using EC Curve25519

Constructions	DLEQ/DLEQOR		User		Issuer		
	Prove	Verify	Token Gen.	Unblinding	Key Gen.	Signing	Redemption
PP [DGS+18]	212 µs	181 µs	111 µs	286 µs	84 µs	303 µs	95 µs
PMBT	576 µs	666 µs	135 µs	844 µs	234 µs	845 µs	235 µs
PPB	–	–	197 µs	164 µs	190 µs	87 µs	95 µs
PMBTB	–	–	368 µs	678 µs	512 µs	155 µs	247 µs

Summary

- PMBTokens extend Privacy Pass with a private metadata bit

- Technique to remove NIZK for PP and PMBTokens enhancing performance



Bibliography

- Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda. Privacy pass: Bypassing internet challenges anonymously. Proceedings on Privacy Enhancing Technologies (PoPETs), 2018(3):164–180, 2018.
- Ben Kreuter, Tancrède Lepoint, Michele Orrù, and Mari-ana Raykova. Anonymous tokens with private metadata bit, 2020. https://eprint.iacr.org/2020/072.
- Claus Peter Schnorr. Security of blind discrete log signatures against interactive attacks. In Sihan Qing, Tatsuaki Okamoto, and Jianying Zhou, editors, Information and Communications Security, volume 2229 of Lecture Notes in Computer Science, pages 1–12. Springer, 2001.
- Michele Orrù. Annymous tokens with privat metadaa bit, 2020. https://www.youtube.com/watch?v=uk3WOFaasCQ.