Anonymous Tokens with Private Metadata Bit Report

Julian Levkov
julian.levkov@epfl.ch
EPFL

Jonas Sulzer
jonas.sulzer@epfl.ch
EPFL

Abstract

This report summarizes the paper *Anonymous Tokens with Private Metadata Bit* [2] by Ben Kreuter et al., which introduces PMBTokens—a cryptographic primitive enabling the issuance of anonymous, single-use tokens embedding a private metadata bit. The construction enhances the Privacy Pass protocol by allowing issuers to embed a secret bit into tokens, accessible only to the issuer, while preserving unlinkability of the tokens. The paper furthermore presents a technique to guarantee unlinkability of Privacy Pass tokens, and in extension of PMBTokens, without the need for NIZK zero-knowledge proofs. The construction is based on the Decisional Diffie-Hellman (DDH) and chosen-target Diffie–Hellman (CTDH) assumptions in the random oracle model, achieving unforgeability, unlinkability, and privacy for the metadata bit.

1 Introduction & Motivation

The protection of online services necessitates mechanisms to distinguish honest from malicious content requests. Traditional methods often rely on IP reputation combined with user tracking. Those methods compromise user privacy and lead to false positives for VPN, Tor or I2P users, because they rely on shared IP use. This motivates the development of anonymous one-time-use tokens. Privacy Pass is one such protocol, allowing users to obtain anonymous tokens from an issuer after being verified as legitimate and later redeem the token without revealing their identity. Privacy Pass however has a major flaw: whether a user is deemed legitimate or not is revealed at issuance time; the user receives the tokens or not. This information however can be abused e.g. by training a machine model to differentiate which malicious behaviour gets noticed and which doesn't. This paper extends PP by introducing a private metadata bit indicating the legitimacy of the user without revealing it at issuance time.

2 Background

Privacy Pass [1], introduced in PETS 2018, enables users to obtain anonymous tokens from an issuer and redeem them with a verifier. Privacy Pass satisfies both unforgeability and unlinkability.

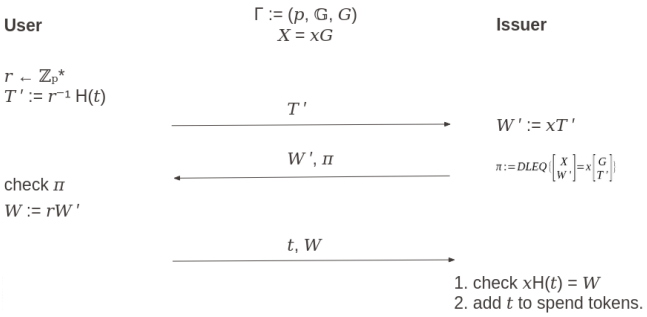

Figure 1: Privacy Pass protocol

The first step consists of the user blinding his nonce t by a factor r and sending it to the issuer. The issuer then multiplies it by his secret key x and provides a NIZK prove, to ensure that he indeed used his private key x corresponding to X and not a random x'. This is necessary since otherwise the issuer could use x' to recognize and link the issued token at redemption time. Finally the user unblinds the token using r again and sends the obtained signature as well as t for verification at the time of redemption. Note that PP is deterministic, i.e., the will be a unique token corresponding to a string nonce t. This characteristic will complicate the direct extension to include a private metadata bits.

3 Contributions

The key contributions include:

- PBMTokens which extends Privacy Pass by a private metadata bit

- A technique that removes the NIZKs from PP and PMBTokens while preserving unlinkability.
- An implementation demonstrating the practicality and efficiency of the proposed construction.

3.1 From Privacy Pass to PMBTokens

3.1.1 Naive Construction

To extend PP to include a private metadata bit, one could naively think of using different secret keys for the bit value correspondingly at issuance. Using an OR zero-knowledge proof, it could still be guaranteed, that one of the two secrets was used without disclosing which one. However, this would compromise the privacy of the metadata bit since a malicious user (attacker) could run two token issuances with the same nonce t, unblind both credentials and compare them. Since Privacy Pass is deterministic in terms of the nonce t, checking if they're different is equivalent to checking if the private metadata bit has changed. This allows an attacker to distinguish between tokens which ruins the privacy of the metadata bit.

3.1.2 Okamoto-Schnorr Privacy Pass

We introduce an extension to PP that allows for randomized tokens. In this construction we will issue tokens under two generators (G,H), in a similar way to Okamoto–Schnorr signatures [3]. The issuer adds randomness s to the token, which counteracts the mentioned attack in section 3.1.1.

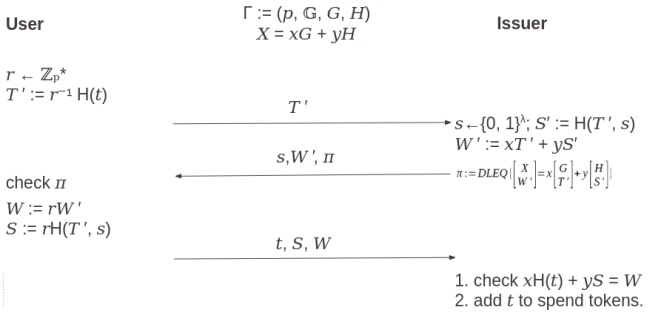

Figure 2: Okamoto-Schnorr Privacy Pass protocol

3.1.3 PMBTokens

To construct the protocol of the PMBTokens, the Okamoto-Schnorr approach from section 3.1.2 is extended by using two different secrets (see section 3.1.1 depending on the metadata bit to encode. Since there are two generators G and H and correspondingly two secret values x_b and y_b, four secret values have to be generated during the key generation for x_0, x_1, y_0 and y_1 accordingly. To accomodate for the two different secrate values determining the metadata bit, a OR zero-knowledge proof needs to be used again.

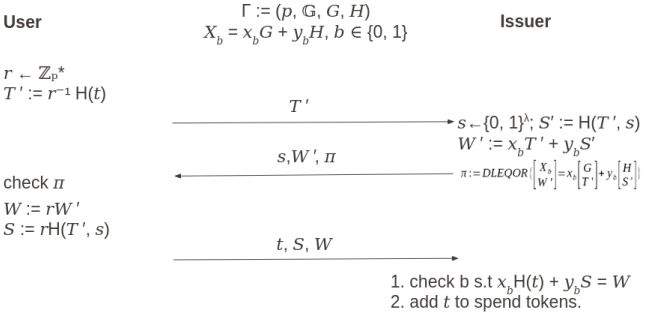

Figure 3: PMBTokens protocol

3.2 Removing the need for NIZK proofs

The second contribution made by the paper is an approach to remove the need for the zero-knowledge proofs in the described protocols. We recall that the role of the NIZK is to provide unlinkability for the user, as they can check that the tokens received are consistent with the issuer's public parameters. However NIZKs are expensive and make up for approximately two thirds of the computational overhead (see section 5). Thus the goal is to remove the need for NIZKs while still preserving unlinkability.

3.2.1 ... from Privacy Pass

The change proposed is that the user blinds their token hash $H(t)$ using both multiplicative and additive blinding instead of just multiplicative blinding. The additive part can be removed during the unblinding only if the issuer used the correct secret key. Otherwise the generated token will be random and invalid.

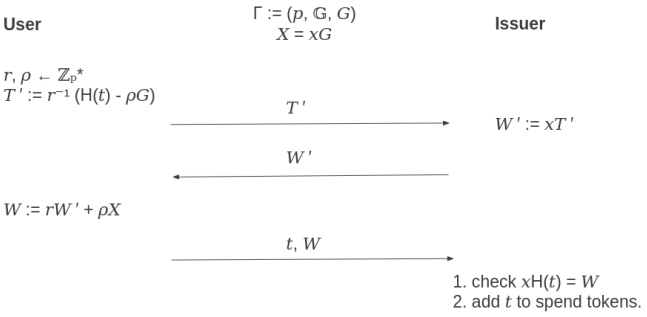

Figure 4: Privacy Pass with removed ZK proof

3.2.2 ... from PMBTokens

The challenge in adapting the PP construction for private metadata is ensuring the user does not learn the issuer's metadata

bit value. The proposed solution is to have the user unblind with both public keys X_b, resulting in one valid token for the bit value and one random value.

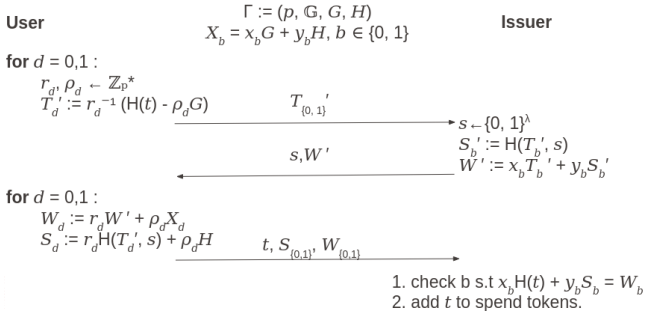

Figure 5: PMBTokens without NIZK proof protocol

4 Security Analysis

The proposed protocols achieves the following security properties:

- **Unforgeability**: guarantees that nobody but the issuer can generate new valid tokens
- **Unlinkability**: guarantees that the tokens that were issued with the same private metadata bit are indistinguishable to the issuer when redeemed.
- **Metadata Privacy**: states that no party that does not have the secret key can distinguish any two tokens, including tokens issued with different metadata bits.

These security properties are proven in the paper for all constructions under the chosen-target gap Diffie-Hellman (CT-GDH) assumption which is introduced in the paper and based on the CTDH and the gap CDH assumptions.

5 Performance Evaluation

The authors implemented the constructions in Rust using the Ristretto group10 on the Curve25519. PPB and PMBTB stand for Privacy Pass and PMBTokens without the NIZK prove respectively.

Constructions	DLEQ/DLEQOR		User		Issuer		
	Prove	Verify	Token Gen.	Unblinding Key	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

Table 1: Benchmarks

6 Conclusion

PMBTokens enhance the Privacy Pass protocol by enabling the embedding of private metadata within anonymous tokens. The authors' technique for maintaining unlinkability without relying on NIZK zero-knowledge proofs enables better performance and therefore reduces the overhead of using a private metadata bit significantly. The paper provides proves that the proposed protocols achieves the key security properties; unforgeability, unlinkability, and privacy for the embedded metadata.

References

[1] 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.

[2] Ben Kreuter, Tancrède Lepoint, Michele Orrù, and Mariana Raykova. Anonymous tokens with private metadata bit, 2020. https://eprint.iacr.org/2020/072.

[3] 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.