Anonymous, Timed and Revocable Proxy Signatures

Ghada Almashaqbeh[1] and Anca Nitulescu[2]

[1] University of Connecticut, {ghada@uconn.edu
[2] IOG, anca.nitulescu@iohk.io

Abstract. A proxy signature enables a party to delegate her signing power to another. This is useful in practice to achieve goals related to robustness, crowd-sourcing, and workload sharing. Such applications, especially in the blockchain model, usually require delegation to satisfy several properties, including time bounds, anonymity, revocability, and policy enforcement. Despite the large amount of work on proxy signatures in the literature, none of the existing schemes satisfy all these properties; even there is no unified formal notion that captures them.

In this work, we close this gap and propose RelaySchnorr, an anonymous, timed, and revocable proxy signature scheme. We achieve this in two steps: First, we introduce a tokenizable digital signature based on Schnorr signature allowing for secure distribution of signing tokens. Second, we utilize a public bulletin board, instantiated as a blockchain, and timelock encryption to support: (1) one-time usage of the signing tokens by tracking tokens used so far based on unique values associated to them, (2) timed delegation so that a proxy signer cannot sign outside a given period, and (3) delegation revocation allowing the original signer to end a delegation earlier than provisioned. All of these are done in a decentralized and anonymous way so that no one can tell that someone else signed on behalf of the original signer or even that a delegation took place. We define a formal notion for proxy signatures capturing all these properties, and prove that our construction realizes this notion. We also discuss several design considerations addressing issues related to deployment in practice.

1 Introduction

Proxy signatures allow one user (the original signer) to delegate their signing right to another party (the proxy signer). The proxy signer can generate signatures that are verified using the original signer's certified public key.[3] Proxy signatures are useful in many applications related to distributed systems, e-cash using smart cards, grid computing, and workload sharing [33, 52, 54, 64]. For example, Alice can let her assistant (Bob) reply to (and sign) emails on her behalf while on a vacation, or simply she can share the workload of handling emails with Bob.

[3] This is not to be confused with proxy re-signatures [6, 13], in which Alice gives a trusted third party a secret key $sk_{b\to a}$ that is used to transform Bob's signature into Alice's signature. Our focus in this work is on signature delegation.

Anonymous delegation guarantees that no one can tell that the task was delegated. Alice may further limit the delegation rights to a certain task or period of time, and may retain the ability to revoke the delegation at any moment of her choice.

The concept of proxy signatures was first introduced in [51], where several types of delegation were presented: full delegation—the original and proxy signers share the same secret key, partial delegation—the original signer generates a delegation key for the proxy signer to use, and delegation by warrant—the original signer specifies a policy that restricts which messages the proxy signer can sign. Since then, a large number of followup works emerged analyzing security and efficiency of older schemes, and devising new constructions, e.g., [7, 29, 42, 44, 45, 52, 65]. Other foundational works focused on formulating and unifying the security requirements of proxy signatures, and strengthening the adversary model [16, 50, 60]. Furthermore, several works focused on extending proxy signatures to handle different settings and support new features, such as threshold proxy signatures [41, 62], blind proxy signatures [68], and anonymous proxy signatures [35].

Motivation. Our motivation stems from recent advances in distributed systems and Web 3.0 applications, and their need for delegation of signing rights. The continuous emergence of such applications raises the question of whether we can realize many of the robustness, user-control, and flexible-configuration features (facilitated by trusted banks/financial institutions) in the trustless blockchain model. This model also introduced new needs that did not exist before, such as managing hot and old wallets and targeted attacks against consensus. Having cryptographic schemes that cover various properties is valuable as these can always become off-the-shelf solutions for new needs arising in this active area. In this work, we identify the properties and capabilities that decentralized applications require from signature delegation, and how to realize them. Towards this, we discuss two motivating applications, and we explain how existing solutions are not suitable as there is no single scheme that supports *all* the required properties.

Application 1: Decentralized Finance (DeFi) and wallet management. In DeFi, blockchains are used to facilitate financial services. There is always the question of whether DeFi can replace traditional banking systems. For example, can Alice allow a family member to spend currency from her Ethereum account in a controlled way without giving away her secret key? (in a similar way to issuing a credit card to a family member while the original account owner controls the credit limit and activation period of the new card.) Delegated signatures can easily enable that: Alice delegates signing rights to her sister Eve, under a *policy* ensuring that, e.g., only transactions with capped values can be issued, and that delegation is valid only for a *given period*. Alice can also end, or *revoke*, the delegation earlier if desired. Given the decentralized nature of blockchains, Alice wants to do all of that in a *decentralized* way.

Another use case is related to cold and hot cryptocurrency wallets. Cold wallets are used to store most of the funds and are not connected to the Internet. It happens that the hot wallet (e.g., a mobile application) may need more funds for a particular activity than what was originally anticipated. Transferring funds between the two wallets requires the cold wallet to be connected to the network,

which is risky. By delegating the signing capability to the hot wallet, it can *non-interactively* transfer funds out of the cold wallet, reducing security risks.

Application 2: System robustness. Another important application is related to system robustness and addressing targeted attacks. Take Byzantine agreement-based consensus as an example. For each round, a committee will agree on the next block. A party, say Alice, can designate a few other parties as backups to sign on her behalf. If Alice's machine is down, Bob can sign on Alice's behalf after a preset timeout. So, even if Alice is a victim of a targeted attack, Bob will do the work until she recovers. Here *anonymity* is a key; backups must be anonymous to avoid targeted attacks against them as part of attacking Alice. The same analogy can be applied to any system in which designated parties must be available to perform particular functionalities.

These applications outline several desired properties. *Delegation anonymity* hides that a delegation took place and the identities of the proxies, ensuring that to an outsider everything appears to be done by the original signer. Also, delegation should be of an *ephemeral nature* so it can be exercised during a preset time period. Another feature is *revocability*, which could be automatic when the delegation period is over, or on-demand due to unforeseen circumstances. Moreover, *policy enforcement* allows restricting the proxy signer's power, e.g., signing messages that belong to a certain class. Furthermore, *decentralization and non-interactivity* are important features especially for large-scale distributed systems. That is, all delegation information are generated by the original signer and can be sent to the proxy signer in one shot; no further interaction with the original signer and no trusted third party are needed when the proxy generates signatures. This promotes scalability and agrees with the spirit of delegation—the original signer can go offline once the delegation is created.

Despite the large amount of work around signature delegation, there is no single proxy signature scheme that achieves all the properties mentioned above, and there is no formal notion that covers all these properties. Full delegation, by giving away the signing key, offers anonymity but at the price of losing control over the delegation. Many schemes allow some fine-grained control [29,39,51], but violate anonymity. Others [7,35] support controlled and anonymous delegation, but without any revocation capability or timed notion. At the same time, schemes that support timed delegation and/or revocation [48,49,61,67] either do not offer anonymity, require interaction between the original and proxy signers, rely on trusted/semi-trusted third party, or do not have formal security analysis.

These observations raise the following question: *Can we construct a decentralized and non-interactive proxy signature scheme that is anonymous, timed and revocable? and how to formally define its security?*

1.1 Contributions

In this paper, we answer this question in the affirmative by defining a formal notion for anonymous, timed and revocable proxy signatures, and constructing a proxy signature scheme, called RelaySchnorr, that satisfies all the properties discussed above.

Formal modeling. Our notion builds on previous proxy signature definitions [16, 35, 50] and defines the additional properties that we require. We generalize the notion to produce generic delegation information rather than restricting that to be tokens or delegation keys. We also introduce a revocation algorithm covering automatic and on-demand revocability. For policy enforcement, we view it as two parts: a policy over time encapsulating the delegation period, and a policy over the message specifying which messages can be signed. To support delegation anonymity, verification of all signatures is done under the original signer's public key without involving the proxy signers' identities. We formally define correctness and security, where the latter covers unforgeability under chosen message attacks, anonymity, revocability, and policy enforcement. We note that none of the existing definitions covered all these properties at once, and none of them defined a time policy or revocation.

Construction. We introduce a new proxy signature scheme, RelaySchnorr, that realizes our notion. RelaySchnorr combines Schnorr signature, timelock encryption, and a public bulletin board to support token-based delegation that is anonymous and revocable, and enforces time and message policies.[4] We introduce a *one-time tokenizable digital signature scheme* based on Schnorr signatures. This is done via a *two-layered approach*: the first layer produces a token, while the second layer produces a signature over the intended message using this token. The original signer can produce tokens on her own and communicate them securely to the proxy signer. Signature verification is done against the public key of the original signer, and the signature structure is identical whether it is generated by the original or proxy signer. In terms of size, a signature consists of four field elements and one group element, so the cost of delegation consists of one group element and two field elements compared to original Schnorr signatures.

We enforce *one-time use* of a token by publishing its unique value (i.e., a unique random element k) on the bulletin board. Any signature with an already published k value will be rejected, and upon accepting a valid signature, the verifier publishes the corresponding k value on the board, preventing the proxy signer from reusing a token. This differs from conventional one-time signatures, where if a signer signs more than one message her signing key will be revealed. A proxy signer would attempt to reveal the original signer's signing key, and hence the conventional notion does not work in our setting. Our approach does not reveal the key even if a proxy signer (locally) uses a token to sign several messages, and still only one of these signatures will be accepted. As noted, verifiers are trusted to publish the k values of the signatures they accept. In blockchain applications (our main target) signed transactions are verified by the miners/validators, so consensus honest majority guarantees this behavior.

For the *timed delegation*, we achieve that in a decentralized way without involving a time server or public warrants that compromise anonymity. We utilize

[4]We assume a secure bulletin board that is an append-only, publicly-accessible log instantiated in a decentralized way as a blockchain maintained by a set of miners (we refer to the miners as validators). Any secure bulletin board (that satisfies persistence and liveness) can be used whether it is based on proof-of-work, proof-of-stake, etc.

the bulletin board along with timelock encryption [37]. In timelock encryption, a ciphertext is locked to a time ρ so that when time ρ comes, some public information will become available allowing for decryption. To enforce a proxy signer to exercise the delegation within a time period $[\rho_a, \rho_b]$, where ρ is a round number from the board, the original signer encrypts the delegation tokens locked to time ρ_a and privately sends them to the proxy signer. Only at time ρ_a the proxy signer can access the tokens. To enforce the end of the period, or *automatic revocation of delegation*, the original signer encrypts all unique k values of these tokens in another ciphertext locked to time ρ_b and publishes that on the board. When time ρ_b comes, the board validators will decrypt and publish all unused k values preventing the proxy signer from using any unused tokens after ρ_b.

For *on-demand revocation*, we do that in a similar way to automatic revocation. The difference is that the original signer publishes the unused k values of the delegated tokens before time ρ_b. To the best of our knowledge, we are the first to support revocability and the timed notion in an anonymous and decentralized way. For *policy enforcement over messages*, we follow generic approaches [35, 39] for two cases: public policy (using the warrant approach) and private one (using non-interactive zero knowledge proofs—NIZKs).

A few challenges arise when deploying our scheme in practice. Examples include synchronization issues of the board, denial of service (DoS) attacks, and anonymity concerns related to mass publication of k values during revocation. We discuss these and other challenges, along with solutions, in our construction.

Security. We formally prove security of RelaySchnorr based on our notion. Unforgeability relies on the unforgeability of Schnorr signatures in the random oracle model [57], and the Schnorr knowledge of exponent assumption [8, 27]. Anonymity is achieved by having identical signature structure and behavior (i.e., with respect to any information published on the board) for the original and proxy signers. Revocability relies on the security of timelock encryption and the bulletin board. Policy enforcement relies on the security of digital signatures (for public warrants) or NIZKs (for private policies), as well as security of timelock encryption and the bulletin board.

Lastly, we note that the techniques we devise to support the timed/revocability notion could be of independent interest; they could be used to support these features for other cryptographic functionalities. Furthermore, the reliance on Schnorr signature, which is a widely studied and used cryptographic primitive, favors construction simplicity. This could also make it easier for our construction to be adopted in practice by systems that use Schnorr signatures (e.g., Bitcoin is awaiting the adoption of Schnorr signatures as proposed in BIP 340 [66]).

1.2 Related Work

We review existing proxy signature schemes in terms of the properties they support (based on the list of properties that we aim to achieve), showing that none of them support all these properties. Then we review works on relevant notions, including one-time signatures and timed cryptographic primitives, and discuss how our work is positioned with respect to these efforts.

1.2.1 Proxy signatures

Anonymity. Anonymity is usually not supported since the proxy signer's key is public and needed for verification, e.g., [51]. Fuchsbauer et al. [35,36] address this issue by unifying the notion of proxy and group signatures, and they consider traceability with a trusted authority holding a trapdoor that can compromise anonymity if needed. Beside introducing a centralized entity, this scheme does not support revocation or timed delegation. Functional signatures [21] allow deriving a secret key sk_f, from the original signer's key, so a proxy signer can sign a message m only if $f(m) = 1$ (where f represents the policy). Delegatable functional signatures [7] utilize signature malleability to allow delegation. Both notions support anonymity but not timed or revocable delegation.

Time-bounded delegation. The few works on timed notion for delegation are limited. Lu et al. [49] add the delegation period to the public warrant, and relies on a trusted server to issue a timestamp for each signature a proxy signer wants to generate. Sun et al. [61] adopt an interactive delegation process; a verifier asks the proxy signer to sign a message, and one of these parties generates a timestamp that the other verifies. Beside being interactive and involving a trusted server, these schemes violate anonymity and do not have formal security.

Revocation. Techniques for revoking delegation rights [51, 67] are based on changing the original signer's key, so all delegated signatures will be rejected, or on creating a public list of revoked proxy signers' keys. The scheme in [67] uses revocation epochs, where for each signature, the proxy signer generates a proof that her key is not on the epoch revocation list, so anonymity is not supported. Others [28, 48, 49] rely on a (semi-)trusted server, where the proxy signer must contact this server when generating a signature: the original signer updates the server with all revoked proxy signers to deny their requests. This approach introduces centralization and trust issues, which we avoid in our scheme.

Policy enforcement. Warrants are used to enforce a policy over delegation, and are usually public—a verifier rejects any signature over a message that violates the warrant [16, 50]. Private warrant approaches either rely on NIZKs to show that a signed message belongs to a hidden (committed) set of messages [40], on polynomial commitments to restrict the proxy signer to sign messages following a specific template [39], or on anonymous non-interactive credentials [29]. However, none of these schemes offer anonymity. Functional (delegatable) signatures [7, 21] and traceable policy-based signatures [3] support private policy and proxy anonymity using NIZKs, but without any timed notion for the delegation (and the latter requires interaction between the proxy and the tracing authority). In terms of message policy enforcement, we use these generic approaches, while we leave traceability for future work as we do not to involve a trusted entity.

1.3 One-time Signatures

One-time signatures are schemes that allow signing only one message using a given signing key [2, 31, 43]. The one-time notion is enforced by the fact that if more than one signature is produced, these signatures can be used to reveal the

signing secret key. Such a notion does not work in the anonymous delegation setting: the signing keys are tied to their own public keys (that are used in verification) rather than to the original signer's public key. Even if there is a way to produce tokens tied to the original signer public key, under this one-time security guarantee, a proxy signer could reuse a token in order to reveal the original signer's signing key.

One-time signatures have also been investigated in the quantum model [4, 12, 26] and permit signature tokenization; the original signer generates a signing token that a proxy signer can use to sign a message m. The one-time is achieved by generating an unclonable (quantum state) token that self-destructs once it is used. Our goal is to support delegatable one-time signing tokens in the classical model. Furthermore, none of these schemes support timed delegation; a proxy signer can use the token at anytime. While some of these works discuss a limited notion of revocability that is interactive; the original signer notifies the proxy signer that she wants to revoke, and the proxy signer has to produce a proof that the token has been used or simply return the physical token. Our revocation notion does not require any interaction with the proxy signer.

1.4 Timed Cryptographic Primitives

There are many versions of conventional cryptographic primitives that support a time notion (we briefly review some of them here). These started with time capsules and timed commitments [9,20,58], which can be opened after performing a sequential computation for a preset time period. More recent notions include, for example, short lived proofs and signatures [5] that support deniability. That is, a proof or signature is valid for a time period—the time needed to open the capsule—after which it can be forged. Timed signatures [38, 55, 63] allow locking a signature on a known message for a given amount of time through means of times capsules (or timed commitments) as well. That is, the signature cannot be verified (or even produced) until the time needed to open the capsule/commitment elapses. Time-release encryption allows encrypting messages to the future such that before that time even the designated recipient cannot decrypt. Generally, existing constructions either relied on time capsules, e.g. [58], or involved a trusted time server, e.g. [24]. Others provided a pre-open capability through a trapdoor allowing for decryption before the designated time, e.g., [25].

Timelock encryption (TLE) aims to avoid the high cost of opening the capsules and the server trust assumption. TLE constructions rely on a reference time realized by a blockchain. Liu et al. [47] use a blockchain along with witness encryption to build a TLE scheme. In encryption to the future [22] similar tools are used to encrypt messages that can be decrypted by a future committee to be elected. McFLY [30] uses signature-based witness encryption combined with a BFT (Byzantine fault tolerant) blockchain, so the decryption of the message is piggypacked on the tasks a blockchain committee (elected at a certain time) is doing. Another timelock encryption scheme is proposed in [37] that relies on a (threshold) random beacon to produce decryption information at certain time

allowing anyone to decrypt. Lastly, Abadi et al. [1] uses publicly verifiable random beacons to realize the notion of timestamping for signatures and zero-knowledge proofs. Our work extends these efforts to involve a timed notion for delegation using means of TLE that also enables us to support decentralized revocation.

2 Preliminaries

We provide an overview of Schnorr signatures (where we adopt the formulation from [53] that mitigates related key attacks), and timelock encryption (TLE) that we utilize in our construction.

Notation. We denote the natural numbers by $\mathbb{N}$, the integers by $\mathbb{Z}$, and the integers modulo some q by $\mathbb{Z}_q$. Elements of $\mathbb{Z}_q$ are lowercase, and elements of a multiplicative group $\mathbb{G}$ of order q generated by generator $G \in \mathbb{G}$ are uppercase. λ denotes the security parameter, pp denotes the public parameters, $\mathsf{negl}(\lambda)$ denotes a function negligible in λ, and PPT stands for probabilistic polynomial time.

2.1 The Schnorr Digital Signature Scheme

Schnorr signature is obtained by applying the Fiat-Shamir transform [32] to the Schnorr identification scheme [59]. We adopt the formulation from [53] that mitigates related key attacks.

Related key attacks. In related key attacks (RKA), that were formalized by Bellare and Kohno [10], an adversary may alter a (hardware-stored) secret key and obtain signatures under the modified key. This notion captures security against practical attacks such as tampering or fault injection. Morita et al. [53] showed that the original version of Schnorr signature is vulnerable to related key attacks, and proposed an easy fix: include the public verification key in the challenge c component as shown below.

For a security parameter λ, let $\mathbb{G}$ be a cyclic group of a prime order q and a generator G, and $\mathsf{H} : \{0,1\}^* \times \mathbb{G}^2 \to \mathbb{Z}_q$ be a hash function. The Schnorr signature scheme is a tuple of three algorithms $\Sigma_{\mathsf{Schnorr}} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ defined as follows:

- $\mathsf{Schnorr.KeyGen}(1^\lambda)$: On input the security parameter λ, choose uniform $x \in \mathbb{Z}_q$ and compute $X = G^x$. Set the secret signing key $\mathsf{sk} = x$ and the public verification key $\mathsf{vk} = X$.
- $\mathsf{Schnorr.Sign}(\mathsf{sk}, m)$: On input the secret key $\mathsf{sk} = x$ and the message m, choose uniform $k \in \mathbb{Z}_q$. Compute $K = G^k$, $X = G^x$, $c = \mathsf{H}(m, X, K)$, and $s = k + cx \mod q$. Output the signature $\sigma = (c, s)$.
- $\mathsf{Schnorr.Verify}(\mathsf{vk}, m, \sigma)$: On input the public key $\mathsf{vk} = X$, the message m, and signature $\sigma = (c, s)$ over m, compute $K = G^s \cdot X^{-c}$ and $c' = \mathsf{H}(m, X, K)$, then output 1 if $c = c'$.

Correctness and security. It is easy to see that for any correctly generated signature, Verify will always output 1. Existential unforgeability against adaptive chosen message attacks (EUF-CMA) in the random oracle model has been formally proved in [57] under the Discrete Logarithm assumption by relying on the forking lemma.

2.2 Timelock Encryption (TLE)

TLE enables encrypting messages towards a time ρ (which is a round number from the bulletin board) such that they can be decrypted only after that time. Thus, for each ρ, a round-related information π_ρ is published on the board to enable decryption. We adopt the definition in [37] with a more generalized time information production algorithm as shown below.

Definition 1 (Timelock Encryption (TLE)). *A Timelock encryption scheme $\mathcal{E}$ is a tuple of five* PPT *algorithms defined as follows:*

$\mathsf{TLE.Setup}(1^\lambda) \to (\mathsf{pp}, s)$**:** *Takes as input the security parameter λ, and outputs public parameters* pp *and a private key s.*[5]

$\mathsf{TLE.RoundBroadcast}(s, \rho) \to \pi_\rho$**:** *Takes as input the round number ρ and a private key s, and outputs the round-related decryption information π_ρ.*

$\mathsf{TLE.Enc}(\rho, m) \to (\mathsf{ct}_\rho, \tau)$**:** *Takes as input the round number ρ and a message m, and outputs a round-encrypted ciphertext ct_ρ, and trapdoor τ for pre-opening.*

$\mathsf{TLE.Dec}(\pi_\rho, \mathsf{ct}_\rho) \to m'$**:** *Takes as input the round-related decryption information π_ρ and a ciphertext ct_ρ, and outputs a message m'.*

$\mathsf{TLE.PreOpen}(\mathsf{ct}_\rho, \tau) \to m'$**:** *Takes as input a ciphertext ct_ρ and a trapdoor τ, and outputs a message m'.*

We use TLE in a blackbox way by invoking the algorithms defined above. We leave any details of, e.g., model and security of the blockchain and time information, to the concrete instantiation (which we require to be fully decentralized and publicly verifiable).

Correctness of TLE (based on the notion presented in Section 2) requires that for all λ, all $(\mathsf{pp}, s) \leftarrow \mathsf{Setup}(1^\lambda)$, all ρ and all m, if $(\mathsf{ct}_\rho, \tau) \leftarrow \mathsf{Enc}(\rho, m)$ and $\pi_\rho \leftarrow \mathsf{RoundBroadcast}(s, \rho)$, then:

$$\mathsf{Dec}\big(\pi_\rho, \mathsf{ct}_\rho\big) = \mathsf{PreOpen}\big(\mathsf{ct}_\rho, \tau\big) = m$$

That is, decrypting ct_ρ using the public round information π_ρ, or pre-opening it using the trapdoor τ associated to this particular ciphertext, will produce the original plaintext message m that was encrypted.

For security, various security models have been proposed and analyzed in [23] including CPA (chosen-plaintext attacks) and CCA (chosen-ciphertext attacks where the adversary has access to the decryption oracle). We require a TLE scheme to be secure against CCA attackers; given that anyone who has the ciphertext ct_ρ can decrypt once the public decryption information π_ρ becomes available, this implies that the attacker has access to the decryption oracle.

In terms of concrete constructions, as mentioned earlier, we require an instantiation that is fully decentralized and publicly verifiable. Gailly et al. [37] develop a CCA-secure TLE scheme that realizes the notion presented in Section 2 with these requirements. Their construction combines Boneh and Franklin's identity based encryption (IBE) scheme [18] with a threshold network implementing

[5] The public parameters pp are implicitly input to all subsequent algorithms.

Boneh-Lynn-Shacha (BLS) signatures [15, 19]. So the secret key s is shared among several parties that collectively produce the decryption information for each round. Furthermore, McFly [30] in a way can be used to realize this notion as well: the committee elected at round ρ will decrypt the ciphertext making it available to everyone, and the original signer who knows the plaintext in our setup can execute the $\mathsf{PreOpen}$ by simply revealing that plaintext. This can be used to decrypt ciphertexts that are published, but not the delegation information that we have in our construction (which is encrypted as ct_a) that only the proxy signer knows. So an additional modification is required to allow revealing some key at time ρ_a that the proxy signer can use to decrypt ct_a (as in encrypting this key to time ρ_a and the committee will decrypt it at time ρ_a. Since only the proxy signer knows the ciphertext ct_a, she is the only one who can decrypt). As a result, we favor scheme in [37] since it does not require these extra modifications.[6]

3 Definitions

In this section, we formulate a notion for anonymous, timed and revocable proxy signature scheme. We build on previous definitions for proxy signatures [16,35,50] and extend them to cover the additional properties we require.

Definition 2. *An anonymous, timed and revocable proxy signature scheme Σ is a tuple of seven* PPT *algorithms defined as follows:*

$\mathsf{Setup}(1^\lambda) \to \mathsf{pp}$**:** *Takes the security parameter λ as input, and outputs a set of public parameters* pp.[5]

$\mathsf{KeyGen}(1^\lambda) \to (\mathsf{sk}, \mathsf{vk})$**:** *Takes the security parameter λ as input, and outputs a signing key* sk *and a verification key* vk.

$\mathsf{Sign}(\mathsf{sk}, m, \mathsf{policy}) \to \sigma$**:** *Takes the signing key* sk*, a message m, and a policy* policy *as inputs, and outputs a signature σ over m.*

$\mathsf{Delegate}(\mathsf{sk}, \mathsf{vk}, \mathsf{degspec}) \to (\mathsf{degInfo}, \mathsf{rk})$**:** *Takes as inputs the signing and verification keys* $(\mathsf{sk}, \mathsf{vk})$*, and delegation specifications* $\mathsf{degspec}$ *(i.e., any auxiliary information and the policies over the time period and the messages that can be signed). It outputs delegation information* $\mathsf{degInfo}$ *and a revocation key* rk.

$\mathsf{DegSign}(m, \mathsf{degInfo}) \to \sigma$**:** *Takes a message m and the delegation information* $\mathsf{degInfo}$ *as inputs. It outputs a signature σ over m.*

$\mathsf{Revoke}(\mathsf{degInfo}, \mathsf{rk}, \mathsf{revState}[\mathsf{vk}]) \to \mathsf{revState}[\mathsf{vk}]'$**:** *Takes* $\mathsf{degInfo}$*, the revocation key* rk*, and the revocation state associated to* vk *as inputs, and outputs an updated revocation state* $\mathsf{revState}[\mathsf{vk}]'$.

$\mathsf{Verify}(\mathsf{vk}, m, \sigma, \mathsf{revState}[\mathsf{vk}]) \to 1/0$**:** *Takes as inputs the verification key* vk*, a message m, a signature σ over m, and the revocation state* $\mathsf{revState}$ *of* vk*. It outputs 1 if the signature is accepted, and 0 otherwise.*

We require the scheme Σ to satisfy the following properties: correctness, existential unforgeability under chosen message attacks, anonymity, revocability, and policy enforcement, which we define below.

[6] This scheme satisfies CCA under the co-Bilinear Diffie-Hellman (co-BDH) assumption for asymmetric bilinear groups introduced by Boneh and Franklin [18] in the random oracle model.

As shown above, the inputs for Sign include the policy, which we view to be composed of two sub-policies: policy_m determines which messages can be signed, and policy_t determines the time period so that a signature produced and verified outside this period will be rejected. Although the latter is needed for the timed delegation but we include it here to satisfy anonymity. That is, all signatures whether produced by the original or proxy signer will have the same structure. The term policy is general and could be extended to include additional polices if desired. Also, policy is configured by the original signer; the proxy signer cannot change it. For delegation, Delegate takes as input the delegation specifications degspec, which includes all auxiliary information needed for delegation configuration, such as number of signing tokens in token-based schemes, and the policy policy to be enforced. The produced degInfo that will be sent to the proxy signer will include the same policy found in degspec and all information a proxy signer needs to sign.

Our definition contains one verify algorithm used for all signatures whether produced by the original or proxy signer. Verify will reject any signature that does not satisfy the policy, and checks that the signature is not revoked (based on the revocation state revState associated with vk that is publicly available).[7]

Lastly, note that when Revoke is invoked, it updates the revocation state of vk to which the delegation is associated. This update is simply a concatenation operation that appends the new revocation information. Furthermore, this is a revocation of a delegation so the proxy signature cannot exercise the delegation anymore. It is not about revoking signatures that were already accepted.

Now we define the properties listed in Definition 2. We use code-based games [11] to formulate our security notions; an experiment $\mathsf{Exp}^{\mathsf{sec}}_{\Sigma,\mathcal{A}}$ is played with respect to a security notion sec and an adversary $\mathcal{A}$ against a scheme Σ. Furthermore, and similar to [14], we define the following helper functions that are not available in the actual scheme, but only for the challenger in the experiments.

$\mathsf{SimSetup}(1^\lambda) \rightarrow (\mathsf{pp}, \tau)$: Receives the security parameter λ, and outputs the public parameters pp whose distribution is computationally indistinguishable from what is produced by Setup, and a trapdoor τ.

$\mathsf{ExtDeg}(\tau, \sigma, \{\mathsf{degInfo}\}) \rightarrow 1/0$: Receives a trapdoor τ, a valid signature σ, and a set of delegation information $\{\mathsf{degInfo}\}$. It returns 1 if any of the degInfo in this set was used to generate σ, and 0 otherwise.

As shown, ExtDeg determines if a forgery signature was generated via a delegation based on hidden values in the signature. We resort to the use of such help function, as in [14], since this check cannot be performed on the available

[7] In our construction, Verify takes the current revocation state of vk (retrieved from the bulletin board) as input; it uses this state to check the freshness of the signature and then updates this state to include the unique value of the accepted signature to enforce one-time usage. One may argue that the definition of Verify should output an updated state revState to reflect that. However, we did not incorporate that to keep the definition general so it can be used by future constructions that may not rely on a bulletin board to enforce the one-time property.

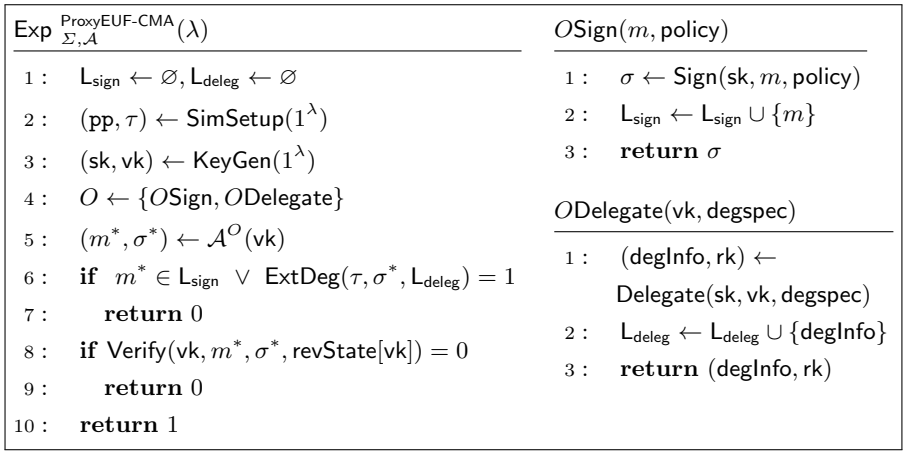

Fig. 1: Existential unforgeability under chosen message attacks.

public signature values without a special extractor, since that would break the anonymity property of the scheme.

Correctness. Informally, correctness implies that a signer holding a valid secret key or delegation information can always produce a valid signature σ over a message m such that Verify will accept that signature if: the signature verifies correctly against vk; it is not revoked based on the latest version of $\mathsf{revState}[\mathsf{vk}]$; and that it does not violate the specified policy.

Formally, for all λ, all $m \in \{0,1\}^*$, any policy $\mathsf{policy} = (\mathsf{policy}_m, \mathsf{policy}_t)$ such that m satisfies policy_m and the time of signing/verification is within policy_t, any delegation specifications $\mathsf{degspec}$ and delegation information for this specifications $\mathsf{degInfo}$ such that $\mathsf{policy} = \mathsf{degspec.policy} = \mathsf{degInfo.policy}$, and the latest public revocation state $\mathsf{revState}$ based on which the signature σ is not revoked, the following probability is 1:

$$\Pr\left[\mathsf{Verify}(\mathsf{vk}, m, \sigma, \mathsf{revState}[\mathsf{vk}]) = 1 \;\middle|\; \begin{array}{c} \mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda) \\ (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ (\mathsf{degInfo}, \mathsf{rk}) \leftarrow \mathsf{Delegate}(\mathsf{sk}, \mathsf{vk}, \mathsf{degspec}) \\ \sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m, \mathsf{policy}) \ \vee \\ \sigma \leftarrow \mathsf{DegSign}(m, \mathsf{degInfo}) \end{array}\right]$$

Existential unforgeability. This property states that no adversary can produce a valid signature without the knowledge of the signing key sk or a delegation information $\mathsf{degInfo}$ created with respect to $(\mathsf{sk}, \mathsf{vk})$. Formally, for all λ, all $m \in \{0,1\}^*$, and any PPT adversary $\mathcal{A}$, there exists a negligible function negl such that $\Pr[\mathsf{Exp}^{\mathsf{ProxyEUF\text{-}CMA}}_{\Sigma,\mathcal{A}}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$, where $\mathsf{Exp}^{\mathsf{ProxyEUF\text{-}CMA}}_{\Sigma,\mathcal{A}}$ is the experiment of existential unforgeability under chosen message attacks defined in Figure 1, and the probability is taken over all randomness used in the experiment.

We note the following in the description of $\mathsf{Exp}^{\mathsf{ProxyEUF\text{-}CMA}}_{\Sigma,\mathcal{A}}$. Checking if the forged signature has been produced using a delegation obtained through

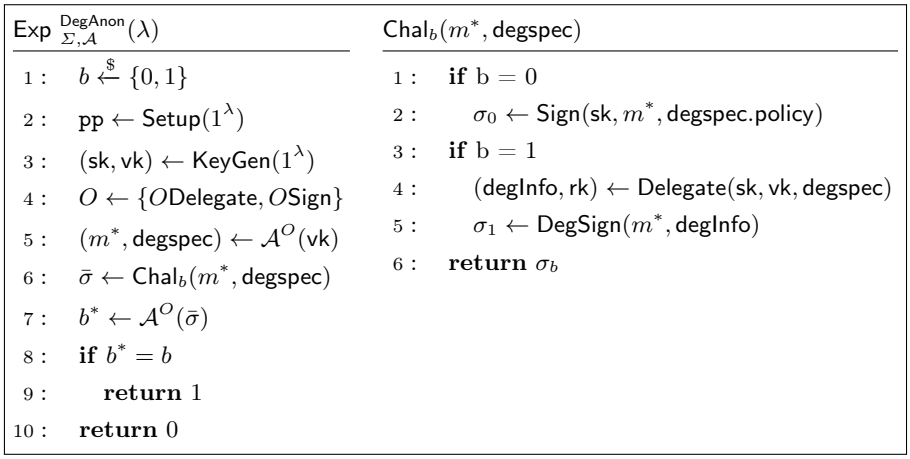

Fig. 2: Anonymity for delegation (OSign and ODelegate are as defined in Figure 1).

ODelegate is done by invoking ExtDeg over the signature and $\mathsf{L}_{\mathsf{deleg}}$ (with the trapdoor τ) which will decide if this signature was produced using any of the degInfo in $\mathsf{L}_{\mathsf{deleg}}$. Note that this helper function is not part of the actual scheme, and that τ is secret. Thus, seeing a signature does not reveal that a signature was produced by the original or proxy signer, thus compromising anonymity.

Delegation anonymity. This implies that the verifier, or any adversary, will not be able to infer any information about a delegation (one that he does not know its degInfo). That is, all signatures will appear as if they were produced by the original signer—they do not reveal anything about the identity of the proxy signers or even that there are delegations in the first place. Thus, all signatures are indistinguishable (in terms of structure and behavior) and all are verified against the original signer's verification key vk. Also, the produced degInfo is transmitted to the proxy signer over a secure channel, thus outside these two parties, no one will be able to tell that such information was produced.

Formally, for all λ, all $m \in \{0,1\}^*$, and any PPT adversary $\mathcal{A}$, there exists a negligible function negl such that $\Pr[\mathsf{Exp}^{\mathsf{DegAnon}}_{\Sigma,\mathcal{A}}(\lambda) = 1] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$, where $\mathsf{Exp}^{\mathsf{DegAnon}}_{\Sigma,\mathcal{A}}$ is the experiment of delegation anonymity defined in Figure 2, and the probability is taken over all randomness used in the experiment.

As shown in the figure, the adversary $\mathcal{A}$ will choose a message m^* and delegation specifications degspec (where the latter includes a policy policy). The challenger, based on the value of b, signs m^* using either delegation information degInfo generated based on degspec, or the signing key sk (hence, no delegation) and returns the signature to $\mathcal{A}$. The adversary $\mathcal{A}$ is challenged to tell which method was used for signing.

Revocability. This implies that an adversary $\mathcal{A}$ cannot produce a valid signature that will convince the verifier using a revoked delegation. Formally, for all λ, all $m \in \{0,1\}^*$, and any PPT adversary $\mathcal{A}$, there exists a negligible function negl

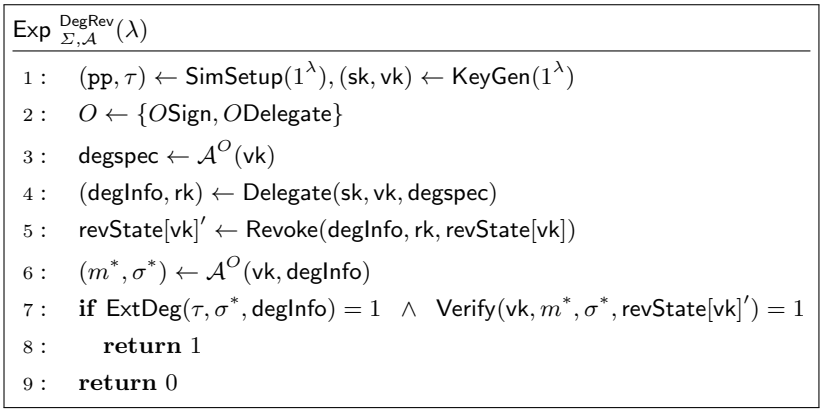

Fig. 3: Delegation revocation ($O\mathsf{Sign}$ and $O\mathsf{Delegate}$ are as defined in Figure 1).

such that $\Pr[\mathsf{Exp}^{\mathsf{DegRev}}_{\Sigma,\mathcal{A}}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$, where $\mathsf{Exp}^{\mathsf{DegRev}}_{\Sigma,\mathcal{A}}$ is the experiment of delegation revocation defined in Figure 3, and the probability is taken over all randomness used in the experiment.

As shown in the figure, $\mathcal{A}$ is challenged to produce a valid signature (that will be accepted) using the revoked delegation. Thus, the game checks that indeed the signature σ^* is produced using the revoked $\mathsf{degInfo}$ as done before. This check is needed to rule out the following trivial attack: $\mathcal{A}$, who has access to $O\mathsf{Delegate}$, can produce a valid signature that verifies under vk using a different delegation from the one in the challenge that is not revoked, thus always winning the game.

Policy enforcement. Informally, this implies that an adversary holding a valid delegation cannot produce a signature, that will be accepted, such that policy is not satisfied. This covers violating the policy over the message or the time.

Formally, for all λ, all $m \in \{0,1\}^*$, and any PPT adversary $\mathcal{A}$, there exists a negligible function negl such that $\Pr[\mathsf{Exp}^{\mathsf{DegPolicy}}_{\Sigma,\mathcal{A}}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$, where $\mathsf{Exp}^{\mathsf{DegPolicy}}_{\Sigma,\mathcal{A}}$ is the experiment of delegation policy enforcement defined in Figure 4, and the probability is taken over all randomness used in the experiment. As shown in the figure, we use the variable now to refer to the current time, which is publicly accessible in the system. Thus, to check that the time policy is violated we check that now is outside the time period specified in policy_t. Also, the notion $m^* \notin \mathsf{policy}_m$ represents checking that m^* does not satisfy policy_m.

4 Construction

We present $\mathsf{RelaySchnorr}$, a construction for an anonymous, timed and revocable proxy signature scheme that realizes the notion defined in the previous section. It relies on distributing one-time signing tokens to the proxy signers. Towards that, we introduce a tokenizable version of Schnorr signature, and employ a public bulletin board (an immutable, append-only log maintained by a set of validators

$\mathsf{Exp}^{\mathsf{DegPolicy}}_{\Sigma,\mathcal{A}}(\lambda)$

$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda), (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$O \leftarrow \{O\mathsf{Sign}, O\mathsf{Delegate}\}$

$\mathsf{degspec} \leftarrow \mathcal{A}^O(\mathsf{vk})$

$(\mathsf{degInfo}, \mathsf{rk}) \leftarrow \mathsf{Delegate}(\mathsf{sk}, \mathsf{vk}, \mathsf{degspec})$

$(m^*, \sigma^*) \leftarrow \mathcal{A}^O(\mathsf{vk}, \mathsf{degInfo})$

Parse $\mathsf{degspec.policy}$ as $(\mathsf{policy}_m, \mathsf{policy}_t)$

if $\mathsf{Verify}(\mathsf{vk}, m^*, \sigma^*, \mathsf{revState}[\mathsf{vk}]) = 1 \ \wedge \ (m^* \notin \mathsf{policy}_m \vee \mathsf{now} \notin \mathsf{policy}_t)$

  return 1

return 0

Fig. 4: Policy enforcement ($O\mathsf{Sign}$ and $O\mathsf{Delegate}$ are as defined in Figure 1).

with an honest majority, which can be instantiated as a blockchain), and timelock encryption to enforce the one-time use of signing tokens as well as the timed and revocable properties. The full construction is shown in Figures 5 and 6. To simplify the discussion, we present our scheme with only the time policy, and we assume full synchrony with the bulletin board (i.e., any message that is sent appears immediately there). Toward the end of the section, we discuss enforcing a policy over the messages and handling synchrony of the board, as well as issues related to reducing the storage and information lookup on this board.

As mentioned before, the board state state is public and accessible by all parties. The time notion we use is in term of rounds derived from this board (in a similar way as done in blockchains). That is, a round is a block index from the board, which we denote as $\mathsf{state.round}$. We also use the notation $\mathsf{state}[\mathsf{vk}]$ to access the revocation state associated with vk, and $\mathsf{state.roundInfo}(\rho)$ to access the TLE decryption information published on the board for round ρ.

One-time tokenizable signature scheme. This is based on Schnorr signatures, and done via a two-layered approach; layer 1 produces a token, while layer 2 produces a signature over m using the token.

For the signing algorithm, as shown in Figure 5, we first generate a token using the signing key $\mathsf{sk} = x$, that is actually a Schnorr signature over a random element k with a secret randomness r. In particular, the signature requires computing $w = \mathsf{H}(k, X, R)$, where $R = G^r$. Looking ahead, the tuple (z, w, k) will be the token given to the proxy signer. To sign a message m, the original signer uses z as a secret key and produces another Schnorr signature over m with randomness e (note that the value z is also a random element in $\mathbb{Z}_p$). So this signature will be over the value $c = \mathsf{H}(m, Z, E)$, where $Z = G^z$. The output signature is $\sigma = (w, c, s, k, Z)$. The verification algorithm uses the public key $\mathsf{vk} = X$ to verify a signature by verifying the two layers of the Schnorr signature. As shown in Figure 6, this is done by computing the randomness R and E and

Let λ be a security parameter, S be the original signer, P be the proxy signer, and TLE be a timelock encryption scheme as defined in Definition 1. Construct an anonymous, timed and revocable proxy signature scheme $\Sigma = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Delegate}, \mathsf{DegSign}, \mathsf{Revoke}, \mathsf{Verify})$ as follows:

$\mathsf{Setup}(1^\lambda)$: On input the security parameter λ, set $\mathbb{G}$ to be a cyclic group of a prime order q with a generator $G \in \mathbb{G}$ and $\mathsf{H} : \{0,1\}^* \times \mathbb{G}^2 \to \mathbb{Z}_q$ to be a hash function, initialize $\mathsf{state} = \{\}$, and invoke $\mathsf{TLE.Setup}(1^\lambda)$. Output $\mathsf{pp} = (\mathsf{TLE.pp}, \mathsf{H}, \mathbb{G}, G, q, \mathsf{state})$.

$\mathsf{KeyGen}(1^\lambda)$: On input the security parameter λ, choose uniform $x \in \mathbb{Z}_q$, then compute $X = G^x$. Output the signing key $\mathsf{sk} = x$ and the verification key $\mathsf{vk} = X$.

$\mathsf{Sign}(\mathsf{sk}, m)$: On input the signing key $\mathsf{sk} = x$ and some message m, do:

1. Choose uniform $k, r, e \in \mathbb{Z}_q$, compute $R = G^r,\ E = G^e$
2. Compute $w = \mathsf{H}(k, X, R)$, $z = (r + wx) \mod q$, and $Z = G^z$
3. Compute $c = \mathsf{H}(m, Z, E)$ and $s = (e + cz) \mod q$ (if $z = 0$ or $s = 0$ start again with fresh r and e)
4. Output the signature $\sigma = (w, c, s, k, Z)$

Every now and then, S either (1) populates a set klist from the stored k values and fresh ones, encrypts it as $(\mathsf{ct}_b, \tau_b) = \mathsf{TLE.Enc}(\mathsf{klist}, \rho_b)$, where ρ_b is some future round number, and posts (ρ_b, ct_b) on the board (resulting in $\mathsf{state}'[\mathsf{vk}] = \mathsf{state}[\mathsf{vk}] \| (\rho_b, \mathsf{ct}_b)$), or (2) posts a fresh klist on the board (resulting in $\mathsf{state}'[\mathsf{vk}] = \mathsf{state}[\mathsf{vk}] \parallel \mathsf{klist}$).

$\mathsf{Delegate}(\mathsf{sk}, \mathsf{vk}, \mathsf{degspec})$: On input the keypair $(\mathsf{sk} = x, \mathsf{vk} = X)$ and delegation specifications $\mathsf{degspec} = (u, [\rho_a, \rho_b])$, where $u \in \mathbb{N}$ and $[\rho_a, \rho_b]$ is the delegation period, do the following:

1. Set $\mathsf{klist} = \{\}$
2. Do the following for $i \in \{1, \ldots, u\}$:
   (a) Choose uniform $k_i, r_i \in \mathbb{Z}_q$
   (b) Compute $R_i = G^{r_i}$ and $w_i = \mathsf{H}(k_i, X, R_i)$
   (c) Compute $z_i = (r_i + w_i x) \mod q$ (if $z_i = 0$ start again with fresh r_i)
   (d) Set $t_i = (z_i, w_i, k_i)$ and $\mathsf{klist} = \mathsf{klist} \cup \{k_i\}$
3. Compute two ciphertexts: $(\mathsf{ct}_a, \tau_a) = \mathsf{TLE.Enc}(t_1 \parallel \cdots \parallel t_u, \rho_a)$ and $(\mathsf{ct}_b, \tau_b) = \mathsf{TLE.Enc}(\mathsf{klist}, \rho_b)$ (where τ_b is the revocation key rk).
4. Set $\mathsf{degInfo} = (\rho_a, \rho_b, \mathsf{ct}_a)$
5. Output $(\mathsf{degInfo}, \mathsf{ct}_b \parallel \tau_b)$

S stores ciphertext ct_b and trapdoor τ_b to be used for revocation if needed (τ_a is dropped as it is not needed), posts (ρ_b, ct_b) on the board (resulting in $\mathsf{state}'[\mathsf{vk}] = \mathsf{state}[\mathsf{vk}] \parallel (\rho_b, \mathsf{ct}_b)$), and sends $\mathsf{degInfo}$ to P.

Fig. 5: RelaySchnorr—continued in Figure 6.

then verifying that the signed hashes, w and c, are indeed correct hashes based on the computed randomness.

The one-time property is enforced as follows. Each new signature contains a unique, freshly generated value k. When receiving a valid signature, the verifier checks that k is not on the board state associated to vk, namely $\mathsf{state}[\mathsf{vk}]$, and if

$\mathsf{DegSign}(m, \mathsf{degInfo})$: On input a message m and delegation information $\mathsf{degInfo}$, P does the following (let $\rho_{now} = \mathsf{state.round}$ be the current round number):

1. If $\rho_{now} < \rho_a$ or $\rho_{now} > \rho_b$, then do nothing
2. If $\rho_a \leq \rho_{now} \leq \rho_b$, then:
   (a) If $\mathsf{degInfo} = (\rho_a, \rho_b, \mathsf{ct}_a)$, then retrieve π_{ρ_a} from the board ($\pi_{\rho_a} = \mathsf{state.roundInfo}(\rho_a)$) and set $\mathsf{degInfo} = (\rho_a, \rho_b, \mathsf{TLE.Dec}(\pi_{\rho_a}, \mathsf{ct}_a))$
   (b) Pick an unused signing token $t = (z, w, k)$ from $\mathsf{degInfo}$
   (c) Compute $Z = G^z$
   (d) Choose uniform $e \in \mathbb{Z}_q$ and compute $E = G^e$
   (e) Compute $c = \mathsf{H}(m, Z, E)$, and $s = e + cz \mod q$ (if $s = 0$ start again with a fresh e)
   (f) Output the signature $\sigma = (w, c, s, k, Z)$

$\mathsf{Revoke}(\mathsf{degInfo}, \mathsf{rk}, \mathsf{state}[\mathsf{vk}])$: On input $\mathsf{degInfo} = (\rho_b, \mathsf{ct}_b)$, revocation key rk, and revocation state $\mathsf{state}[\mathsf{vk}]$, do (let $\rho_{now} = \mathsf{state.round}$ be the current round number):

1. If $\rho_{now} \geq \rho_b$, then retrieve π_{ρ_b} from the board ($\pi_{\rho_b} = \mathsf{state.roundInfo}(\rho_b)$) and compute $\mathsf{klist} = \mathsf{TLE.Dec}(\pi_{\rho_b}, \mathsf{ct}_b)$
2. If $\rho_{now} < \rho_b$, then use $\mathsf{rk} = \tau_b$ to compute $\mathsf{klist} = \mathsf{TLE.PreOpen}(\mathsf{ct}_b, \tau_b)$
3. Add all k values such that $k \in \mathsf{klist} \ \wedge k \notin \mathsf{state}[\mathsf{vk}]$ to the board state $\mathsf{state}[\mathsf{vk}]$ associated with vk resulting in an updated state $\mathsf{state}[\mathsf{vk}]'$.

$\mathsf{Verify}(\mathsf{vk}, m, \sigma = (w, c, s, k, Z), \mathsf{revState} = \mathsf{state}[\mathsf{vk}])$: On input the verification key $\mathsf{vk} = X$, the message m, signature $\sigma = (w, c, s, k, Z)$ over m, and the revocation state $\mathsf{state}[\mathsf{vk}]$, if $k \in \mathsf{state}[\mathsf{vk}]$, then output 0. Else, add k to $\mathsf{state}[\mathsf{vk}]$ (resulting in $\mathsf{state}'[\mathsf{vk}] = \mathsf{state}[\mathsf{vk}] \parallel k$) and do the following:

1. Compute $R = Z \cdot X^{-w}$ and $E = G^s \cdot Z^{-c}$
2. Output 1 if and only if $w = \mathsf{H}(k, X, R) \ \wedge \ c = \mathsf{H}(m, Z, E)$.

Fig. 6: RelaySchnorr (cont.).

so, the signature will be accepted and the verifier posts the k value on the board to be appended to $\mathsf{state}[\mathsf{vk}]$.[8] Any signature with an already-published k will be rejected. Looking ahead, this will enable one-time use of delegated tokens. As noted, verifiers are trusted to behave as prescribed by publishing the k values of the signatures they accept. In blockchain applications (our main target) signed transactions are verified by the miners who publish valid signed transactions (that include the k values) on the blockchain, so consensus honest majority guarantees this behavior (hence, it is not a trust in a single entity). Also, as shown, due to the reliance on the updated bulletin board state to enforce the one-time property, our construction is stateful (in practice, updating the state is done automatically

[8]The verifier sends k to the board validators who will update the state $\mathsf{state}[\mathsf{vk}]$ when publishing a new block.

in blockchain applications since accepting a valid transaction means that this transaction and its signature—including k—will be published on the board).[9]

To preserve delegation anonymity, the original signer must mimic the behavior of signatures produced by delegation (which we will see shortly). As shown in Figure 5, every now and then the original signer will publish on the board a TLE ciphertext of a list of fresh and previously-used k values (locked to a future time). This is done to mimic having ct_b associated with a delegation (and so the automatic revocation). Also, every now and then, the original signer will generate a fresh list of k values and publish the list itself on the board. This is done to mimic the mass publishing of k values associated with on-demand revocation.

Timed delegation. To delegate signing, i.e., the Delegate algorithm in Figure 5, the original signer chooses the delegation specifications including the number of signing tokens and the delegation period. The original signer uses her signing key $\mathsf{sk} = x$ to generate u fresh signing tokens, denoted as $t_1, \ldots, t_u$. Each of these tokens contains z (first layer Schnorr signature over a fresh k), and the corresponding w and k values.

Our goal is to enforce a time period over the delegation in a decentralized way and without violating anonymity. To do that, we utilize a recent notion of timelock encryption TLE (defined in Section 2) in the blockchain model (again, we view the bulletin board as a blockchain). We represent the time period $[a, b]$ in terms of block indices, or rounds, covering the intended period. That is, this period will be $[\rho_a, \rho_b]$, where ρ_a (respectively ρ_b) is the round number during which the block with index a (respectively index b) is mined. To force a proxy signer to use the signing tokens only during $[\rho_a, \rho_b]$, we propose the following. The original signer uses TLE to encrypt the tokens in a ciphertext ct_a such that when ρ_a comes, and so the decryption information π_{ρ_a} becomes publicly available, the proxy signer can decrypt ct_a to retrieve the tokens. To enforce the end of the period, recall that any signature with a k value that appears on the board state state will be rejected. Thus, the original signer uses TLE to produce another ciphertext ct_b for time ρ_b encrypting klist (the list of k values of the delegated tokens) and posts ct_b on the board. When time ρ_b comes, and so π_{ρ_b} becomes publicly available, the board validators will decrypt ct_b and publish all unused k values in klist on the board (this is included under Revoke in Figure 6). This will prevent the proxy signer from using the unused tokens after time ρ_b.

The original signer stores ct_b and its secret trapdoor τ_b that can be used for early revocation (if needed) as we explain shortly. He then sends the delegation information $\mathsf{degInfo} = (\rho_a, \rho_b, \mathsf{ct}_a)$ to the proxy signer over a secure channel since this is secret information, and posts (ρ_b, ct_b) on the board.

Delegated signing. As shown in Figure 6, at time ρ_a, the proxy signer decrypts ct_a using the decryption information π_{ρ_a} that will become available on the board at that time. This will reveal degInfo containing the signing tokens. The proxy signer can use any of these tokens to sign a message m as follows: it chooses a

[9] Having a bulletin board does not introduce direct interaction between the original and proxy signers; an original signer produces degInfo and sends it in one shot to the proxy signer who can exercise delegation without any help from the original signer.

random e and computes a signature using any of the unused (k, w, z) in $\mathsf{degInfo}$, which produces the second layer Schnorr signature. This signature has the same structure as the signatures that the original signer would produce, and will be verified using the same Verify algorithm against the original signer's verification key $\mathsf{vk} = X$, thus preserving anonymity of the proxy signer.

Revocation. We support decentralized and anonymous two types of revocation: automatic, when the delegation period is over enforced by the timed property discussed above, and on-demand allowing the original signer to end the delegation before time ρ_b. Both are done by decrypting ct_b and publishing all unused k values on the board, preventing the proxy signer from using the tokens tied to them. The difference is that for automatic revocation, decryption is done using π_{ρ_b} that will become publicly available at time ρ_b. While for on-demand revocation, that only the original signer can execute, the trapdoor τ_b of $\mathsf{degInfo}$ (in particular ct_b) is used to $\mathsf{PreOpen}$ ct_b.

As mentioned in Section 2, we employ a decentralized TLE scheme in our construction. The decryption information is produced using $\mathsf{RoundBroadcast}$ for each round (either by relying on a period random beacon as in [37] or a committee that will be elected at round ρ as in [30]). This information will be published on the board. For the decryption of ct_b and publishing all unused k values, we piggyback that on the tasks that the board validators do. Thus, the validators keep a record of all ct_b for each round ρ, and when π_ρ becomes available, they decrypt ct_b and post all unused k values on the board. Furthermore, $\mathsf{RoundBroadcast}$ as defined in Definition 1 involves a secret value s that is used to produce the round decryption information. This value (and whether it is needed) is based on the concrete instantiation of the TLE scheme (e.g., using the scheme in [37], s will be shared among the producers of the threshold random beacon).

As noted, during revocation or when the delegation period ends, multiple k values will be published on the board. One may argue that such mass production, or even the existence of ct_b, may violate delegation anonymity. However, this is not the case since: (1) this information does not contain anything about the identity of the proxy signer or which delegation it is tied to, and (2) the original signer will mimic a similar behavior (i.e., periodic publishing of multiple k values and ct_b) for her own signatures as outlined in the Sign algorithm in Figure 5.

Policy enforcement. The construction above enforces only a time policy. To restrict the proxy signer to sign messages that satisfy certain policy policy_m, we can adopt two generic approaches from the literature [35, 39].

Public policy. If policy_m is public, we use the warrant approach. The original signer encodes the conditions that message m must satisfy in policy_m, and signs it using a separate signing key from the one used in the delegation (to prevent a proxy signer from using one of the signing tokens to sign any policy she wishes). The signature scheme used to sign policy_m could be any secure signature scheme; no need to be a proxy scheme. As a result, each original signer in the system will be known using two public keys: the one used for signing the policy and the one used for the proxy signature. Within a delegation, the original signer sends the signed policy as part of policy found inside $\mathsf{degInfo}$ as discussed previously. For

Sign, the original signer can pick any policy_m. Both Sign and $\mathsf{DegSign}$ will output this public policy_m as part of output signature structure σ. Verifying a signature will then be modified to include an additional check; verifying that policy_m is signed by the original signer, and that the signed message satisfies this policy.

Private policy. For private policy policy_m, we employ a NIZK proof system, so that a signature includes a proof π attesting that m satisfies policy_m and that this private policy is signed by the original signer as above. policy_m is basically encoded as a function f (or a circuit that encodes the required conditions). Also, the public parameters of the system will include any public parameters needed for the NIZK proof system. In terms of signing, σ will be computed over $m \parallel \pi$ to preserve the proof integrity. Verifying a signature will involve verifying π to ensure that the private policy_m is satisfied.

Denial of service (DoS) attacks against signers. A signature will be directly rejected if its k value is already published on the board. Earlier we state that the k values are either published by the verifiers (after accepting a valid signature), by the original signer (when executing an early revocation), or by the board validators (when a delegation period ends after decrypting ct_b). However, in practice an attacker may perform a DoS attack against the original or proxy signers by intercepting a signature (before being verified) and publishing its k value on the board to invalidate the signature.

We can address this attack as follows: instead of just logging only the k value of a signature, we publish *the whole signature and the hash of the signed message.* Thus, a signature will be rejected if another valid signature (with the same k value) over a *different message* is already on the board. This also means that ct_b will contain valid signatures over random hashes using the tokens instead of just a list of the k values of these tokens. Thus, when we say a k value, we implicitly refer to a valid signature tied to this k value and the component c in the signature (based on construction) is computed over the hash of m rather than m itself. In blockchain applications, our main target, this is not an issue; either way transactions are already published on the chain with their signatures, which will prevent DoS attacks against signers.

Remark 1 (Validity of accepted signatures outside the delegation period). A valid signature produced during the delegation period will stay valid outside that period since the verifier can easily check that it is for the same message in hand and can be verified as many times as desired. A signature over a different message means a reuse of a token and either way will be rejected.

Bulletin board synchronization and off-chain processing issues. In presenting our construction earlier, we assumed that the board is instantly synced. That is, any information sent to the board will appear directly and all parties will see the updated board state instantly. However, this is not the case in practice; propagation delays and other factors may prevent that. So a verifier might be checking an old state that does not contain the updated list of k values/signatures, which allows a proxy signer to use a token several times (with several verifiers) during this period.

Furthermore, our scheme is similar to off-chain processing in blockchains. That is, a signature is handed directly to verifiers who rely on the current state of the board during verification. Similar to the concept of double spending in off-chain payments, a malicious proxy signer may reuse a token to generate several valid signatures each of which is handed to a different verifier at the same time. All these verifiers will accept these signatures since none of these signatures is published on the board yet.

We handle both issues by introducing the concept of *delayed signature acceptance*. A verifier will verify the signature as before, then publish it on the board as above, but will not take any action based on this valid signature—which is basically based on the content of the signed message—until later, e.g., a few rounds later. If at that time this verifier finds out that more than one valid signature (over different messages than what she has) using the same k value appeared on the board, they will reject the signature. Note that in blockchain applications, the signature is destined to the board validators, e.g., it is a signature over transactions to be posted on the board. Hence, this issue is resolved by consensus itself. That is, only one valid signature associated with a given k value will be accepted and parties act based on the confirmed state of the blockchain.

Reducing information lookup time. As noted, a verifier has to check that the k value (or basically the signature) is not already published on the board (under the revocation state associated to vk, namely, $\mathsf{state}[\mathsf{vk}]$) before accepting a valid signature. The cost of information lookup grows linearly with the number of signatures produced under a given original signer's key. This cost can be reduced by using, e.g., universal accumulators [17, 46] that are dynamic and allow for non-membership proofs. So for each original signer's public key vk, the board validators compute an accumulator of all its k values and they update it as more k values are published. A signature now will be accompanied with a non-membership proof proving that its k value is not published on the board. Thus, a verifier just needs to verify the validity of this proof without doing a linear search over $\mathsf{state}[\mathsf{vk}]$ as before. Updating the state with new k value proceeds as before; the verifier publishes the new k value (by sending this information to the board validators), but the validators now will update the accumulator representing $\mathsf{state}[\mathsf{vk}]$.

5 Security

We prove the following theorem (where $\mathsf{schnorr\text{-}koe}$ is the Schnorr knowledge of exponent assumption [8, 27]).

Theorem 1. *Assuming EUF-CMA security of Schnorr signatures, the* $\mathsf{schnorr\text{-}koe}$ *assumption, a secure bulletin board, a CCA-secure TLE scheme, an EUF-CMA secure signature scheme, and a secure NIZK proof system,* $\mathsf{RelaySchnorr}$ *is an anonymous, timed and revocable proxy signature scheme (cf. Definition 2).*

Before providing the main result that states the security of our construction, we discuss the choice of the security model and some considerations raised by

prior work. We also recall the security notions of the bulletin board and the NIZK scheme needed to prove security of revocability, timed delegation, and policy enforcement. This is in addition to the definition of the Schnorr knowledge of exponent assumption that we rely on while proving unforgeability of our proxy signature scheme.

As we aim to have our scheme usable by open-access distributed systems that do not assume a public key infrastructure (PKI), we account for eventual related key attacks (RKA) on Schnorr signatures and use the solution proposed in [53] as discussed in Section 2. Since RKA considers a broader class of attacks than ordinary attacks, security against RKA implies strong unforgeability for our resulting proxy signature.

Below we informally recall the security properties we require from the underlying public bulletin board and the NIZK system (the former is based on the security notion of blockchains, e.g., [56]).

Definition 3 (Security of the bulletin board). *A public bulletin board is secure if it satisfies two properties: persistence and liveness, which are (informally) defined as follows:*

Persistence. *For any two honest parties P_1 and P_2, and any two time rounds ρ_1 and ρ_2 such that $\rho_1 \leq \rho_2$, with overwhelming probability the confirmed state of the board maintained by party P_1 at time ρ_1 is a prefix of the confirmed state of the board maintained by party P_2 at time ρ_2.*

Liveness. *If information* info *is broadcast at time round ρ (to be published on the board), then with overwhelming probability* info *will be recorded on the board at time at most $\rho + v$, where v is the liveness parameter.*

Note that liveness includes growth and availability, i.e., new data is being added to the bulletin board and, this board is accessible by any party at any time. Also, the board protocol is parameterized by predicates to ensure that the board records only valid information.

Definition 4 (Security of NIZK). *Let $\mathcal{R}$ be an efficiently computable binary relation which consists of pairs of the form (x, w), and let $L_{\mathcal{R}}$ be the language associated with $\mathcal{R}$. A secure non-interactive zero-knowledge proof system (NIZK) for $\mathcal{R}$ must satisfy three properties: completeness, computational soundness, and zero-knowledge, which are (informally) defined as follows:*

Completeness. *An honest verifier always accepts a proof generated by an honest prover for a valid statement x using a valid witness w.*

Soundness. *A* PPT *adversary can convince an honest verifier to accept a proof of an invalid statement x (i.e., an x that is not in $L_{\mathcal{R}}$) with at most a negligible probability.*

Zero-knowledge. *It is possible to simulate (in polynomial time) the honest prover for any instance $x \in \mathcal{L}_{\mathcal{R}}$ without knowing a witness w. This insures that a NIZK proof does not reveal any information about the witness beyond the validity of the statement.*

In our proof of ProxyEUF-CMA of our scheme, we rely on the EUF-CMA security of Schnorr signature (which holds under the discrete logarithm assumption in the random oracle model), and on the Schnorr knowledge of exponent assumption (denoted as schnorr-koe) introduced in [8, 27]. The schnorr-koe assumption states that an adversary $\mathcal{A}$ that forges a Schnorr signature with respect to a public key of her choice must know the corresponding secret key. In other words, there exists an extractor Ext that when given the signature, the public key, and the random coins of $\mathcal{A}$, can extract the corresponding secret key which is basically computing the discrete logarithm of the public key. Crites et al. show that this assumption is true under the discrete logarithm assumption in the algebraic group model [34]. They define a security game for schnorr-koe, denoted as $\mathsf{Exp}^{\mathsf{schnorr\text{-}koe}}_{\mathcal{A},\mathsf{Ext}}(\lambda)$, in which the adversary is challenged to produce a valid Schnorr signature under a public key of her choice, and the adversary wins the game if the extractor fails in extracting the secret key corresponding to this public key. We informally recall the definition of the schnorr-koe assumption below while full details can be found in [8, 27].

Definition 5 (The schnorr-koe Assumption). *Let $\mathbb{G}$ by a cyclic group of order q and generator G in which the discrete logarithm assumption holds. The schnorr-koe assumption holds with respect to $\mathbb{G}$ if for any* PPT *adversary $\mathcal{A}$, there exists a* PPT *extractor Ext and a negligible function* negl *such that* $\Pr[\mathsf{Exp}^{\mathsf{schnorr\text{-}koe}}_{\mathcal{A},\mathsf{Ext}}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$.

Proof of Theorem 1. Correctness is immediate by the correctness of the Schnorr signature scheme, correctness and availability of the bulletin board, correctness of TLE (that allows the proxy signer to correctly decrypt degInfo), and correctness of the building blocks used for policy enforcement.

For security, we show that our construction satisfies the security properties defined in Section 3. Thus, the proof of Theorem 1 follows by the correctness argument above, and Lemmas 1, 2, 3, and 4 shown below. We construct the helper functions SimSetup and ExtDeg used in our security games as follows:

$\mathsf{SimSetup}(1^\lambda) \rightarrow (\mathsf{pp}, \tau)$: Runs $\mathsf{Setup}(1^\lambda)$ to obtain pp and s that is output by $\mathsf{TLE.Setup}(1^\lambda)$, set $\tau = s$ and outputs (pp, τ).

$\mathsf{ExtDeg}(\tau, \sigma, \{\mathsf{degInfo}\}) \rightarrow 1/0$: Parse σ as (w, c, s, k, Z), and each degInfo in the set as $(\rho_a, \rho_b, \mathsf{ct}_a)$. Then use τ to obtain the round decryption information π_{ρ_a} by invoking $\mathsf{TLE.RoundBroadcast}(\tau, \rho_a)$, then decrypt ct_a by invoking $\mathsf{TLE.Dec}(\pi_{\rho_a}, \mathsf{ct}_a)$ to obtain a list of signing tokens $\{t\} = \{(w, k, z)\}$ (the full list $\{t\}$ will be the union of all of these lists). Compute a list $\{t'\}$ such that $\{t'\} = \{(w, k, G^z)\}$ for all tuples obtained from the decryption output. If (w, k, Z) from σ is in the list $\{t'\}$ output 1, otherwise output 0.

Lemma 1 (Unforgeability). *Assuming EUF-CMA security of Schnorr signature scheme and the schnorr-koe assumption,* RelaySchnorr *satisfies ProxyEUF-CMA security as defined in Figure 1 in the random oracle model.*

Proof. Let $\mathcal{A}$ be a PPT adversary attempting to break the ProxyEUF-CMA security (based on the game defined in Figure 1) of our construction. For the sake of contradiction, consider that $\mathcal{A}$ can break ProxyEUF-CMA security with non-negligible probability. This means that $\mathcal{A}$ can produce a valid proxy signature $\sigma^* = (w^*, c^*, s^*, k^*, Z^*)$ over m^* such that $O\mathsf{Sign}$ was not queried over m^*, and $O\mathsf{Delegate}$ did not produce the token (w^*, k^*, z^*) where z^* is such that $Z^* = G^{z^*}$.

In a nutshell, the success of this forgery means that $\mathcal{A}$ is able to output a valid token, i.e., layer 1 Schnorr signature, and use this token to produce a valid proxy signature, i.e., layer 2 Schnorr signature. Thus, for the latter there exists an Ext that can extract z^* from this signature and the public key Z^* such that $Z^* = G^{z^*}$, if not, this means that $\mathcal{A}$ is able to break the schnorr-koe assumption (which is a contradiction). Then, if extraction succeeds, we have that (z^*, w^*) is a forgery for the message k^* with respect to layer 1, breaking the EUF-CMA security of Schnorr signature with respect to the original signer's key vk (which is also a contradiction).

More formally, we construct two PPT adversaries $\mathcal{B}_1$ and $\mathcal{B}_2$. $\mathcal{B}_1$ attempts to break the EUF-CMA security of Schnorr signature with respect to vk, while $\mathcal{B}_2$ attempts to break the schnorr-koe assumption with respect to Z^* produced by $\mathcal{A}$. As a result, let the advantage of $\mathcal{B}_1$ be $\mathsf{Adv}_{\mathcal{B}_1} = \Pr[\mathsf{Exp}^{\mathsf{EUF\text{-}CMA}}_{\mathsf{Schnorr},\mathcal{B}_1}(\lambda) = 1]$ and the advantage of $\mathcal{B}_2$ be $\mathsf{Adv}_{\mathcal{B}_2} = \Pr[\mathsf{Exp}^{\mathsf{schnorr\text{-}koe}}_{\mathsf{Schnorr},\mathcal{B}_2}(\lambda) = 1]$, we have:

$$\Pr[\mathsf{Exp}^{\mathsf{ProxyEUF\text{-}CMA}}_{\Sigma,\mathcal{A}}(\lambda) = 1] \leq \mathsf{Adv}_{\mathcal{B}_1} + \mathsf{Adv}_{\mathcal{B}_2}$$

Adversary $\mathcal{B}_1$ has access to the signing oracle $O\mathsf{Sign}^{\mathsf{Schnorr}}_{\mathsf{vk}}(\cdot)$ and should produce a forgery on a new message $m^* \notin \mathsf{L}^{\mathsf{Schnorr}}_{\mathsf{sign}}$, i.e., not queried before through the signing oracle. It does that by invoking $\mathcal{A}$ to produce a forged proxy signature (based on the game defined in Figure 1), then it invokes the extractor Ext in the schnorr-koe game that $\mathcal{B}_2$ is attempting to break to extract z^* from the Z^* part in the forged proxy signature. This z^* serves as a forged Schnorr signature over message k^* against vk. If the extractor fails, i.e., it cannot compute the discrete logarithm z^* of Z^*, this means that $\mathcal{B}_2$ can use $\mathcal{A}$'s output to break the schnorr-koe assumption.

$\mathcal{B}_1$ simulates $\mathcal{A}$ oracle queries in Figure 1 as follows. When $\mathcal{A}$ requests $O\mathsf{Sign}(m)$, $\mathcal{B}_1$ answers as follows:

1. Update list $\mathsf{L}_{\mathsf{sign}} \leftarrow \mathsf{L}_{\mathsf{sign}} \cup \{m\}$
2. Sample a random $k \in \mathbb{Z}_q$
3. Query $(z, w) \leftarrow O\mathsf{Sign}^{\mathsf{Schnorr}}_{\mathsf{vk}}(k)$
4. Add k to $\mathsf{L}^{\mathsf{Schnorr}}_{\mathsf{sign}}$
5. Sample a random $e \in \mathbb{Z}_q$
6. Compute $E = G^e, Z = G^z$
7. Compute $c = \mathsf{H}(m, Z, E)$
8. Compute $s = (e + cz) \mod q$
9. Return $\sigma = (w, c, s, k, Z)$

When $\mathcal{A}$ requests $O\mathsf{Delegate}(\mathsf{vk})$, $\mathcal{B}_1$ answers as follows:[10]

[10]Note that, to simplify the presentation and without loss of generality, we let $O\mathsf{Delegate}$ generate one signing token for every query instead of generating several

1. Sample a random $k \in \mathbb{Z}_q$
2. Query $(z, w) \leftarrow O\mathsf{Sign}_{\mathsf{vk}}^{\mathsf{Schnorr}}(k)$
3. Update list $\mathsf{L}_{\mathsf{deleg}} \leftarrow \mathsf{L}_{\mathsf{deleg}} \cup \{(\mathsf{degInfo} = (z, w, k)\}$
4. Return $\mathsf{degInfo} = (z, w, k)$

The adversary $\mathcal{A}$ produces a forgery $\sigma^* = (w^*, c^*, s^*, k^*, Z^*)$ on a new message $m^* \notin \mathsf{L}_{\mathsf{sign}}$ and new (z^*, w^*, k^*) that is not $\mathsf{L}_{\mathsf{deleg}}$. By the security of the schnorr-koe assumption, $\mathcal{B}_1$ can obtain the discrete log z^* of Z^* found in the forged signature. This holds since the second layer of our proxy signature, namely (c^*, s^*) is a Schnorr signature over m^* with respect to the key Z^* that the adversary $\mathcal{A}$ chooses. Otherwise, meaning that if extraction fails, then $\mathcal{B}_2$ can use (c^*, s^*, Z^*) to break the schnorr-koe assumption, which is a contradiction as the advantage of $\mathcal{B}_2$ in doing that is negligible.

Now, since the extractor will succeed, $\mathcal{B}_1$ outputs the message k^* and the signature $\sigma^* = (z^*, w^*)$ as a valid forgery to Schnorr signature for the verification key vk. Given that Schnorr signature is EUF-CMA secure, the advantage of $\mathcal{B}_1$ is also negligible. Thus, $\mathcal{A}$'s advantage in producing a valid forgery against our scheme is negligible.

Lemma 2 (Anonymity). RelaySchnorr *satisfies the anonymity property defined in Figure 2.*

Proof. In the DegAnon security game, defined in Figure 2, $\mathcal{A}$ may rely on the following to distinguish the challenge signature:

1. **Case 1: signature structure.** $\mathcal{A}$ tries to use $\bar{\sigma}$ to infer any information on whether the original or proxy signer has produced this signature.
2. **Case 2: bulletin board state.** $\mathcal{A}$ monitors the bulletin board to tell if a new delegation has been created, and thus case $b = 0$ was executed by the challenger. This allows $\mathcal{A}$ to guess correctly that $\bar{\sigma}$ was produced by a proxy signer.

For case 1, note that in our construction the two signatures σ_0 and σ_1 are identically distributed, and hence, indistinguishable for an outsider. Both have an identical structure and are verified in the same way against the original signer's verification key vk. Thus, $\bar{\sigma}$ will not provide $\mathcal{A}$ with any information on whether this signature was produced by Sign or DegSign.

For case 2, note that degInfo in our construction, in particular the portion of the time policy published on the board—(ρ_b, ct_b), does not reveal any information about the signing tokens, which delegation they are tied to (if any), or the identity of the proxy signer. Moreover, the *indistinguishable behaviour* of the original signer ensures hiding that a delegation took place. That is, the original signer simulates a "self-delegation" and behaves in a similar way to the case of delegation even when generating signatures using her signing key—by posting dummy (ρ_b, ct_b) simulating a timed delegation or fresh klist simulating a delegation revocation.

tokens based on degspec that $\mathcal{A}$ can choose. We also do not include a time policy, which is also a part of degspec, since we prove security of our timed notion when proving the policy enforcement property in Lemma 4.

The original signer will also include policy policy_m with her signatures. This will make Sign and DegSign follow the same behavior. Thus, seeing time policies on the board, or published k values, or signatures with policies over the signed messages, will not give the adversary $\mathcal{A}$ any additional advantage in distinguishing the signatures.

This is in addition to the fact that delegation in our construction is generated in a non-interactive way (by the original signer). Also, the generated delegation information is sent securely to the proxy signer. So, only these two parties are aware that a delegation took place while any information posted publicly on the board does not reveal that.

As a result, the two strategies above will not give $\mathcal{A}$ any additional advantage, over just random guessing, in winning the DegAnon.

Lemma 3 (Revocability). *Assuming a secure bulletin board and a CCA secure TLE scheme, then* RelaySchnorr *satisfies the revocability property defined in Figure 3.*

Proof. Security of both automatic and on-demand revocability relies on the security of the bulletin board and the TLE scheme used in our construction. A verifier will check the board to validate the $\mathsf{revState}[\mathsf{vk}]$ before accepting a valid signature, and will reject any signature that is already revoked. An adversary $\mathcal{A}$ who tries to break the revocability of our construction can do that by: (1) manipulating the bulletin board (i.e., prevent publishing revState on the board, control the verifier's view of the board—so the verifier sees the old state that does not contain the updated revState, or even rewrite the board to omit already recorded revState), or (2) maul (ρ_b, ct_b) to produce different revState (or k values) from those produced by the original signer.

By the assumption that the bulletin board is secure (cf. Definition 3), the first strategy succeeds with negligible probability. Also, by the assumption that the TLE scheme we use in our construction is CCA secure, the second strategy succeeds with negligible probability. Thus, $\mathcal{A}$'s advantage in breaking the revocability property of our scheme is negligible.

Lemma 4 (Policy enforcement). *Assuming a secure bulletin board, a CCA secure TLE scheme, an EUF-CMA secure signature scheme Π, and a secure NIZK system Σ, then* RelaySchnorr *—with the policy enforcement techniques described in Section 4—satisfies the policy enforcement property defined in Figure 4.*

Proof. Recall that in our scheme a policy is composed of two parts: $\mathsf{policy} = (\mathsf{policy}_t, \mathsf{policy}_m)$. We show that our construction satisfies policy enforcement for both of them.

For the time policy policy_t, security relies on the security of the bulletin board and the TLE scheme. By the correctness of the TLE scheme, the valid decryption information will be produced at times ρ_a and ρ_b. Thus, the proxy signer can reveal the degInfo only when time ρ_a comes, and the board validators can decrypt ct_b only when time ρ_b comes. By Lemma 3, an adversary $\mathcal{A}$ cannot prevent automatic revocation, which ends the delegation time period at time ρ_b.

In other words, an adversary that can violate policy_t can be used to build another adversary $\mathcal{B}$ that can break the security of the TLE scheme and the revocability of our construction, which is a contradiction.

For the message policy policy_m, we discuss both public and private policy options in our construction. For public policy_m, its security relies on the EUF-CMA security of the signature scheme Π that the original signer uses to sign the public warrant. A verifier will verify this signature first before checking that $m \in \mathsf{policy}_m$. An adversary $\mathcal{A}$ cannot forge a valid signature over a policy of her choice with non-negligible probability. For private policy_m, using a similar argument, an adversary $\mathcal{A}$ cannot forge a signature over a policy_m of her choice to produce a valid NIZK. And by the security of the NIZK system (cf. Definition 4), $\mathcal{A}$ cannot produce a valid proof that convinces the verifier of accepting a signature over a message $m \notin \mathsf{policy}_m$ (where here policy_m is a valid policy produced by the original signer). Furthermore, the integrity of a valid NIZK proof π is preserved since in our construction the produced signature in case of private message policy is over $m \parallel \pi$, which completes the proof.

Acknowledgements

We thank Yolan Romailler for insightful discussions about timelock encryption and drand. The work of G.A. is supported by Protocol Labs grant program RFP-013: Cryptonet network grants, and in part by NSF Grant No. CNS-2226932.

References

1. Abadi, A., Ciampi, M., Kiayias, A., Zikas, V.: Timed signatures and zero-knowledge proofs—timestamping in the blockchain era—. In: International Conference on Applied Cryptography and Network Security. pp. 335–354. Springer (2020)
2. Abe, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Tagged one-time signatures: Tight security and optimal tag size. In: The 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC). pp. 312–331. Springer (2013)
3. Afia, I., AlTawy, R.: Traceable policy-based signatures with delegation. Cryptology ePrint Archive (2023)
4. Amos, R., Georgiou, M., Kiayias, A., Zhandry, M.: One-shot signatures and applications to hybrid quantum/classical authentication. In: Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing. pp. 255–268 (2020)
5. Arun, A., Bonneau, J., Clark, J.: Short-lived zero-knowledge proofs and signatures. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 487–516. Springer (2022)
6. Ateniese, G., Hohenberger, S.: Proxy re-signatures: new definitions, algorithms, and applications. In: CCS (2005)
7. Backes, M., Meiser, S., Schröder, D.: Delegatable functional signatures. In: Public-Key Cryptography–PKC (2016)
8. Bellare, M., Crites, E., Komlo, C., Maller, M., Tessaro, S., Zhu, C.: Better than advertised security for non-interactive threshold signatures. In: CRYPTO (2022)

9. Bellare, M., Goldwasser, S.: Encapsulated key escrow (1996)
10. Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: Rka-prps, rka-prfs, and applications. In: EUROCRYPT (2003)
11. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: EUROCRYPT (2006)
12. Ben-David, S., Sattath, O.: Quantum tokens for digital signatures. arXiv preprint arXiv:1609.09047 (2016)
13. Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy cryptography. In: EUROCRYPT (1998)
14. Bobolz, J., Diaz, J., Kohlweiss, M.: Foundations of anonymous signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In: Financial Cryptography and Data Security (2024)
15. Boldyreva, A.: Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In: International Workshop on Public Key Cryptography. pp. 31–46. Springer (2002)
16. Boldyreva, A., Palacio, A., Warinschi, B.: Secure proxy signature schemes for delegation of signing rights. Journal of Cryptology **25**(1), 57–115 (2012)
17. Boneh, D., Bünz, B., Fisch, B.: Batching techniques for accumulators with applications to iops and stateless blockchains. In: CRYPTO (2019)
18. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: CRYPTO (2001)
19. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: International conference on the theory and application of cryptology and information security. pp. 514–532. Springer (2001)
20. Boneh, D., Naor, M.: Timed commitments. In: The 20th Annual International Cryptology Conference (CRYPTO). pp. 236–254. Springer (2000)
21. Boyle, E., Goldwasser, S., Ivan, I.: Functional signatures and pseudorandom functions. In: PKC (2014)
22. Campanelli, M., David, B., Khoshakhlagh, H., Konring, A., Nielsen, J.B.: Encryption to the future: a paradigm for sending secret messages to future (anonymous) committees. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 151–180. Springer (2022)
23. Choi, G., Vaudenay, S.: Timed-release encryption with master time bound key (full version). Cryptology ePrint Archive (2019)
24. Chow, S.S., Roth, V., Rieffel, E.G.: General certificateless encryption and timed-release encryption. In: SCN (2008)
25. Chow, S.S., Yiu, S.M.: Timed-release encryption revisited. In: Provable Security: Second International Conference, ProvSec (2008)
26. Coladangelo, A., Liu, J., Liu, Q., Zhandry, M.: Hidden cosets and applications to unclonable cryptography. In: CRYPTO (2021)
27. Crites, E., Komlo, C., Maller, M.: How to prove schnorr assuming schnorr: security of multi-and threshold signatures. Cryptology ePrint Archive (2021)
28. Das, M.L., Saxena, A., Gulati, V.P.: An efficient proxy signature scheme with revocation. Informatica **15**(4), 455–464 (2004)
29. Derler, D., Hanser, C., Slamanig, D.: Privacy-enhancing proxy signatures from non-interactive anonymous credentials. In: IFIP Annual Conference on Data and Applications Security and Privacy (2014)
30. Döttling, N., Hanzlik, L., Magri, B., Wohnig, S.: Mcfly: verifiable encryption to the future made practical. In: Financial Cryptography and Data Security (2023)
31. Even, S., Goldreich, O., Micali, S.: On-line/off-line digital signatures. In: Advances in Cryptology—CRYPTO. pp. 263–275. Springer (1990)

32. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Advances in Cryptology—CRYPTO. vol. 86, pp. 186–194. Springer (1986)
33. Foster, I., Kesselman, C., Tsudik, G., Tuecke, S.: A security architecture for computational grids. In: CCS (1998)
34. Fuchsbauer, G., Kiltz, E., Loss, J.: The algebraic group model and its applications. In: The 38th Annual International Cryptology Conference (CRYPTO) (2018)
35. Fuchsbauer, G., Pointcheval, D.: Anonymous proxy signatures. In: SCN (2008)
36. Fuchsbauer, G., Pointcheval, D.: Anonymous consecutive delegation of signing rights: Unifying group and proxy signatures. Formal to Practical Security pp. 95–115 (2009)
37. Gailly, N., Melissaris, K., Romailler, Y.: tlock: Practical timelock encryption from threshold bls. Cryptology ePrint Archive, Paper 2023/189 (2023)
38. Garay, J.A., Jakobsson, M.: Timed release of standard digital signatures. In: The 6th International Conference on Financial Cryptography and Data Security. pp. 168–182. Springer (2003)
39. Hanser, C., Slamanig, D.: Blank digital signatures. In: ASIA CCS (2013)
40. Hanser, C., Slamanig, D.: Warrant-hiding delegation-by-certificate proxy signature schemes. In: INDOCRYPT (2013)
41. Herranz, J., Sáez, G.: Verifiable secret sharing for general access structures, with application to fully distributed proxy signatures. In: Financial Cryptography and Data Security (2003)
42. Kim, S., Park, S., Won, D.: Proxy signatures, revisited. In: International Conference on Information and Communications Security (1997)
43. Lamport, L.: Constructing digital signatures from a one way function (1979)
44. Lee, B., Kim, H., Kim, K.: Strong proxy signature and its applications. In: Proceedings of SCIS. vol. 2001 (2001)
45. Lee, J.Y., Cheon, J.H., Kim, S.: An analysis of proxy signatures: Is a secure channel necessary? In: CT-RSA (2003)
46. Li, J., Li, N., Xue, R.: Universal accumulators with efficient nonmembership proofs. In: ACNS (2007)
47. Liu, J., Jager, T., Kakvi, S.A., Warinschi, B.: How to build time-lock encryption. Designs, Codes and Cryptography **86**, 2549–2586 (2018)
48. Liu, Z., Hu, Y., Zhang, X., Ma, H.: Provably secure multi-proxy signature scheme with revocation in the standard model. Computer Communications **34**(3), 494–501 (2011)
49. Lu, E.J.L., Hwang, M.S., Huang, C.J.: A new proxy signature scheme with revocation. Applied mathematics and Computation **161**(3), 799–806 (2005)
50. Malkin, T., Obana, S., Yung, M.: The hierarchy of key evolving signatures and a characterization of proxy signatures. In: EUROCRYPT (2004)
51. Mambo, M., Usuda, K., Okamoto, E.: Proxy signatures for delegating signing operation. In: CCS (1996)
52. Mambo, M., Zheng, Y., Okamoto, T., Tada, M., Okamoto, E.: Extended proxy signatures for smart cards. In: Information Security Workshop, ISW (1999)
53. Morita, H., Schuldt, J.C., Matsuda, T., Hanaoka, G., Iwata, T.: On the security of the schnorr signature scheme and dsa against related-key attacks. In: ICISC (2016)
54. Neuman, B.: Proxy-based authorization and accounting for distributed systems. In: International Conference on Distributed Computing Systems (1993)
55. Ozden, D., Yayla, O.: Verifiable timed proxy signatures and multi-signatures. Cryptology ePrint Archive (2023)

56. Pass, R., Seeman, L., Shelat, A.: Analysis of the blockchain protocol in asynchronous networks. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 643–673. Springer (2017)
57. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. Journal of cryptology **13**(3), 361–396 (2000)
58. Rivest, R.L., Shamir, A., Wagner, D.A.: Time-lock puzzles and timed-release crypto (1996)
59. Schnorr, C.P.: Efficient identification and signatures for smart cards. In: Advances in Cryptology—CRYPTO. pp. 239–252. Springer (1990)
60. Schuldt, J.C., Matsuura, K., Paterson, K.G.: Proxy signatures secure against proxy key exposure. In: PKC (2008)
61. Sun, H.M.: Design of time-stamped proxy signatures with traceable receivers. IEE Proceedings-Computers and Digital Techniques **147**(6), 462–466 (2000)
62. Sun, H.M., Lee, N.Y., Hwang, T.: Threshold proxy signatures. IEE Proceedings-Computers and Digital Techniques **146**(5), 259–263 (1999)
63. Thyagarajan, S.A., Malavolta, G., Schmid, F., Schröder, D.: Verifiable timed linkable ring signatures for scalable payments for monero. In: The 27th European Symposium on Research in Computer Security (ESORICS). pp. 467–486. Springer (2022)
64. Varadharajan, V., Allen, P., Black, S.: An analysis of the proxy problem in distributed systems. In: IEEE Computer Society Symposium on Research in Security and Privacy (1991)
65. Wang, H., Pieprzyk, J.: Efficient one-time proxy signatures. In: ASIACRYPT (2003)
66. Wuille, P., Nick, J., Ruffing, T.: Schnorr signatures for secp256k1. Bitcoin Improvement Proposal 340 (2020), `https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki`
67. Xu, S., Yang, G., Mu, Y., Ma, S.: Proxy signature with revocation. In: Australasian Conference on Information Security and Privacy (2016)
68. Zhang, F., Kim, K.: Efficient id-based blind signature and proxy signature from bilinear pairings. In: Australasian Conference on Information Security and Privacy (2003)