Confirm Activity of Service-Providers in the NuCypher Network

Ghada Almashaqbeh

NuCypher
ghada@nucypher.com

Abstract. In this document we study the confirm activity problem in the NuCypher network. This problem is concerned with devising secure techniques that allow a service-provider, or Ursula, to prove being online and responsive during any time period. We consider two flavors of the problem based on the network operation stage, namely, confirm availability and confirm service activity. The former is about confirming that Ursula is available all the time and replies to all Bob requests, while the latter is about proving that an Ursula has served a specific number of distinct re-encryption requests within a given period. We present several potential solutions for each of these types, discuss the characteristics of these solutions with respect to their security guarantees and efficiency, and provide recommendations to when each of them should be used.

1 Introduction

The NuCypher network [1,2] is a decentralized key management system, encryption, and access control service. It uses threshold proxy re-encryption, namely, the Umbral scheme [3], to delegate access to encrypted data through a public network. This network is composed of semi-trusted re-encryption service-providers, or Ursulas, that implement access control policies created by data owners, or Alices. Alice supplies each Ursula with re-encryption keys allowing a quorum of Ursulas to transform ciphertexts encrypted under Alice's public key into ciphertexts encrypted under the delegatee's, or Bob's, public key. This enables the latter to decrypt the ciphertext without revealing anything about the decryption keys or the raw data to the intermediate service-providers.

Joining the NuCypher network is governed by consensus rules defining the service setup and the monetary incentives paid to provide the service. In order to join the system, Ursula needs to stake an amount of NU tokens (the native token of the network) for a specific period which will be released when the pre-specified staking period is over. Alice chooses an Ursula to hold an access control policy with a probability proportional to the stake this Ursula pledged in the system. Therefore, the stake value influences the service load an Ursula may receive. This stake is also used to punish Ursula financially, by forfeiting part of it for detectable malfeasance.

Alice uses the network by creating an access control policy to be implemented by a set of Ursulas. This policy specifies the re-encryption key fragments each

Ursula will need to answer requests coming from Bob(s), as well as the duration of the policy, which is basically the timeframe during which Bob is authorized to access Alice's data. Furthermore, the policy contract requires Alice to lock an amount of Ether that will be used by the network to pay Ursulas for providing the re-encryption service. As noted, Alice is not exposed to the NU token. All that she needs is an Ethereum wallet, awareness of the NuCypher network architecture to select Ursulas, and knowledge of the NuCypher rules with respect to preparing access control policies.

Bob, on the other hand, does not deal with currency in the system at all. He interacts with the storage network to retrieve the encrypted data, and with Ursulas in the NuCypher network to request the re-encryption service after which he will be able to access the raw data of interest.

Rewards and activity monitoring in the NuCypher network. Ursulas are rewarded for their re-encryption service by using two sources; the first is the service fees collected from the policy owner Alice, while the second is a subsidy in the form of newly minted NU tokens distributed on a schedule enforced by the NuCypher protocol. The latter will be provided during the early stage of the network operation to encourage Ursula's participation and sustain their operations in lieu of a mature fee market.

Currently, the subsidy size in each round or period is computed for each Ursula based on the size of her stake and duration of commitment to the network, and provided that she confirms to be online during this round. Confirming the status of being online is done by calling a simple function in one of the NuCypher contracts, which is like a signal that the calling Ursula is online. Similarly, for service fees, Ursula collects part of the Ether locked by Alice during the policy's duration in proportion to the number of periods up to that point in which Ursula has confirmed her online status.

Motivation. Although rewards computation and activity monitoring are reasonable for the first iteration of the network, we acknowledge that it suffers from two main problems:

- Confirming being online is flawed in the sense that the function call that Ursula makes does not require any input or proofs on providing the service, or even being online and responsive. Ursula can stay offline the majority of the time and not respond to Bobs' requests, then come online merely to call this function. This allows Ursula to collect both subsidy and fees without doing all (or even most) of the necessary work. Even worse, Ursula will be able to get her stake back once it unlocks.
- The revenue computation (both fees and subsidy) is agnostic to the number of requests Ursula serves. Thus, an active Ursula who may serve a huge number of re-encryption requests, and one who does not receive any requests (or more importantly, a malicious/lazy Ursula that does not answer Bob's requests), will both collect the same amount of revenue if they hold identical policies.

Therefore, we need to devise a secure, non-gameable technique that confirms Ursula's availability and service activity. Then we need to adapt the subsidy and fee computation accordingly to factor in the amount of delivered service, and potentially punish Ursulas if it is insufficient.

Problem statement. The confirm activity problem is defined differently based on the network operation stage. In the first 5 to 8 years after launch, when subsidy rewards are still distributed, we are concerned with the availability of Ursulas and their willingness to serve all requests coming from Bob. In other words, regardless of the number of requests served, the revenue total value (both subsidy and fees) will be computed based on the length of time during which Ursula is online and well-behaved.

On the other hand, in later stages, when subsidies disappear and the only revenue comes from fees, confirm activity will be tied to providing the re-encryption service, in the sense that the payment will be partially computed based on the amount of service provided. This requires Ursula to confirm its activity by proving that she served a given number of distinct re-encryption requests during a given period.

To make the distinction clear, we refer to the first as *confirm availability*, and for the second as *confirm service activity*.

Contributions. In this document, we introduce several solutions for both forms of confirming activity. These solutions differ in the trust, security guarantees, interactivity, and efficiency.

For confirming availability, we employ a detect-and-punish approach embedded within an optimistic service monitoring process. This means that it is only invoked when Bob complains that an Ursula is unresponsive. The proposed solution labels Ursulas as working and gateway Ursulas. The former are contacted in a regular way to handle the re-encryption service, while the latter act as challengers that are contacted only when there is a complaint from Bob so they will attest whether a working Ursula is indeed unavailable. If that is the case, a quorum of gateways (who have challenged the working Ursula and found her unresponsive) will collectively sign a proof-of-unavailability that will cost the misbehaving working Ursula part of her stake. We discuss several aspects related to gateway selection and a variety of potential attacks on this approach along with mitigation techniques.

For confirming service activity, we devise three solutions that allow producing a proof attesting to the statement *"An Ursula has served ω distinct requests correctly"* for some positive integer ω representing the number of served requests. These solutions are refereed to as zero knowledge proof-based (ZKP-based), committee-attestation, and commit/challenge/open-based.

For the *ZKP-based* approach, we utilize the fact that in our network each Ursula already produces a ZKP attesting to the correctness of each re-encryption request she performs [3]. Our solution is to aggregate the proofs of all served requests within a round into one proof attesting to the above statement. This accumulation can be done by using generic techniques like proof carrying data

(PCD) [4] or incrementally verifiable computation (IVC) [5]. An alternative, possibly more efficient approach, is to view the above statement as an instance of arithmetic circuit satisfiability problem and combine it a highly efficient ZKP system, e.g., [6]. That is, build a circuit that takes the set of correctness proofs and their count ω as inputs. If the number of correct distinct proofs equals to ω, i.e., the circuit output 1, then a valid proof will be produced. Ursula can submit this proof to the network to claim her payments.

As for the *committee-attestation* approach, it shares a similar theme to confirm availability solution mentioned previously. For each round, a committee of Ursulas (and possibly outsider verifiers) is elected to attest for the work load an Ursula served. In detail, the working Ursula sends all Bob requests she served along with the correctness proofs to this committee. After verifying all the proofs, the committee collectively signs the *"An Ursula has served ω distinct requests correctly"* statement, while replacing ω with the actual number of served requests. The committee (or the working Ursula) submits the signed statement to the network so the working Ursula can claim her payments.

For the *commit/challenge/open* approach, we introduce a mechanism inspired from the Merkle tree-based ZKP system proposed in [7]. For each round a working Ursula constructs a Merkle hash tree of all served requests and their correctness proofs. Then, she uses the root as a random beacon to be fed into an iterative hash process to select n leaf nodes at random to open them (i.e., these are the challenges). Ursula signs the Merkle tree root and the activity proof will be composed of the signed root, the challenge leaf nodes along with their openings, and membership paths of the challenge leaves. Ursula sends this proof to either a sidechain (maintained by round-selected committee) or to the main network to verify. Once verified, Ursula will be rewarded with the service payment.

Lastly, we discuss the trade-offs of each of these solutions in terms of security guarantees, assumptions, and efficiency. We also outline some recommendations regarding which solution should be used at what stage of the network operation.

Organization. We begin with outlining the adopted threat and network model, in Section 2, followed by an overview of some of the cryptographic primitives that we use in Section 3. Then, we present the proposed solutions for confirm availability in Section 4 and those for confirming service activity in Section 5. After that, we briefly discuss the trade-offs and requirements of each of these solutions along with some usage recommendations in Section 6. Lastly, in Section 7 we conclude with highlighting some of our future work directions.

2 Threat and Network Models

This section describes the network and threat models adopted by the proposed solutions. In particular, it introduces a modification for the network model of NuCypher, and it describes the security assumptions and attacker collusion cases considered in this work.

2.1 Network Model

In order for the proposed solutions to work, we need to ensure freshness, integrity, and authenticity of the re-encryption requests (as well as service complaints as we will see later) issued by Bob. This can be achieved by requiring Bob to include a timestamp, or sequence number, in each request to ensure freshness, and to sign the request to ensure integrity and authenticity. The keypair used for the signature should be separate from the keypair Bob uses for proxy re-encryption in the system.

2.2 Threat Model

The goal of this document is to address accounting attacks, namely, holding Ursula accountable for the service it provides and for claiming being available and responsive. In addressing this type of attacks we adopt a threat model that makes the following set of assumptions:

- **Self-interested parties:** We do not place trust in any party and we assume that all participants are self-interested. This means that a party may decide to follow the protocol or deviate from it, either on its own or by colluding with other attackers, and such decision is solely based on what maximizes the financial profits of this party.
- **Attackers' collusion:** If it is profitable, an Ursula may, for example, spin out her own Alice/Bob instances or collude with Alice or Bob. That is, by creating Alice/Bob instances (or colluding with them), Ursula will receive larger number of policies and re-encryption requests. Such a collusion case could be profitable if the subsidy size is influenced by the amount of service delivered. However, this is not the case in NuCypher as mentioned before. Thus, such a collusion scenario is not appealing to a rational Ursula.
  Moreover, we do not consider collusion between Bob and Ursula as a practical threat. This means that cases of Bob pretending that he obtained service from Ursula (while no service has been delivered) is not an issue. We do not suspect this will be of any importance and there is no motivation to do it given that the work Ursula does for any re-encryption request is minimal (as we will see shortly, the ciphertext size is very small since it encrypts a symmetric key instead of the whole data).
  We note that the above non-collusion assumption does not affect the solutions proposed to handle the confirm service activity (Section 5). This means that these solutions provide stronger security guarantees than the confirm availability solution (Section 4), where they address the issue of potential collusion between Bob and Ursula. In order to make an educated decision of the plausibility of this threat, we need more data about the system operation and the behavior of the participants once subsidies stop in the system.
- **Honest Ursulas:** We also assume that when sampling a subset of Ursulas in the network, at least one of them is honest. This assumption can be achieved by having a global assumption regarding the lower bound of the number of

honest Ursulas with respect to the total number of Ursulas in the NuCypher network. (Or it can be achieved by deploying a special entity like an external verifier, that changes on a periodic basis, or one by the NuCypher company, that is trusted to faithfully participate as a member of each samples set. This verifier does not provide any other services in the system.)
– **Efficient adversaries.**. We deal with computationally-bounded (or probabilistic polynomial time) adversaries that cannot break secure cryptographic primitives with non-negligible probability.

We also work in the random oracle model where hash functions are modeled as random oracles.

3 Preliminaries

This section provides an overview of two concepts that we use in the proposed solutions. These include the framework of proof carrying data (PCD) and the collective signing (CoSi) protocol.

3.1 Proof Carrying Data (PCD).

The paradigm of PCD [4] allows proving to the correctness of a distributed computation involving untrusted parties. It produces a single proof for the output that attests not only the correctness of the final result, but also the correctness of the entire history of intermediate computations that produced this result. Correctness here is defined as a polynomially computable predicate that abstracts the properties, or invariants, that must be satisfied.

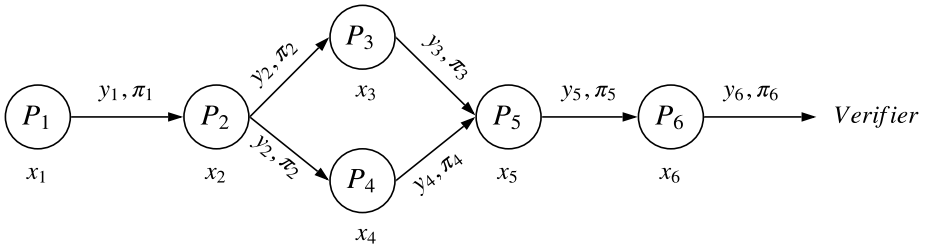

Fig. 1: An example of a PCD application. A distributed computation involving parties P_i, for $i \in \{1, \ldots, 6\}$, each of which has a local input x_i and produces an output y_i with a proof π_i.

To clarify how PDC works, consider a distributed computation task that involves the set of parties shown in Figure 1. Party P_1 starts the computation with its own input, produces an intermediate output with a proof saying that it performed the computation as defined by the protocol. It then sends both the

output and the proof to the next party, which is P_2 in this case. Here, P_2 will have its own input x_2, as well as everything it received from P_1 (including the proof) as input to the computation it will perform. Similarly, P_2 will produce another intermediate output and a proof. This proof not only attests to the correctness of the computation done by P_2, but also the history that lead to the result y_2. In other words, it implicitly includes the proof from P_1. The same process continues until the full computation is finished. Anyone can verify the correctness or compliance of the whole distributed protocol by only verifying the last proof π_6 produced by the exit party, which is P_6 in the figure.

As shown, PCDs enable untrusted parties to work with each other in a fully distributed fashion, without overwhelming the system with the storage and verification of individual proofs for each step of the performed protocol. Also, they attest to correctness or compliance to the prescribed protocol without re-executing any of the intermediate computations. Thus, they provide a promising paradigm for confirming service activity in a compact way.

3.2 Collective Signing (CoSi).

CoSi [8] is a protocol that enables a set of distributed parties to cosign a statement together in a way that produces a single signature. As such, both the verification time and the space requirements are just like having a single signer. The difference is that this signature attests that all parties agree with the signed statement instead of only one.

CoSi builds upon Schnorr multisignatures [9–11], but combines them with communication trees to speed up the signing process in case of a large number of cosigners. In what follows, we only present the protocol with a plain communication architecture as it suffices for the confirm service activity solution introduced in this document.

Schnorr signatures work in a group $\mathbb{G}$ of a prime order q and generator g, such that the discrete log is believed to be hard in this group. Take n parties that want to sign a statement together. Each of these parties has a secret $sk_i \in \mathbb{Z}_q$ and a public key $pk_i \in \mathbb{G}$ such that $pk_i = g^{sk_i}$. To sign a message m, one of these parties, let's say P_1, coordinates the signing process as follows:

1. P_1 prepares a message m and sends it to the rest of the signers.
2. Each party P_i, possibly after verifying m, selects a secret $\tau_i \in \mathbb{Z}_q$ and compute $V_i = g^{\tau_i}$, then it sends V_i back to P_1.
3. P_1 aggregates all random values received from the signers, and its own, by computing $V = \Pi_{i=1}^{n} V_i$.
4. P_1 then computes $c = H(V||m)$, where H is an appropriate hash function. P_1 then sends c to the rest of the parties.
5. Each party computes a response $r_i = \tau_i - sk_i \cdot c$ and sends it to P_1.
6. Lastly, P_1 computes $r = \sum_{i=1}^{n} r_i$, and outputs the collective signature over m as (c, r).

Verifying the signature proceeds as in classical Schnorr signatures [9] with one difference. An aggregated public key pk is used in the verification process, which is computed as $pk = \Pi_{i=1}^{n} pk_i$.

The work in [8] tackles several issues related to the availability of the signing parties, and optimizing the communication between them. We believe that such techniques can be used in the NuCypher network if we adopt the CoSi-based solution for the confirm service activity issue.

4 Confirm Availability Solution

In this section, we present a solution for confirming availability of Ursulas. As mentioned before, in the early operation stage of the network we only require Ursulas to be online and responsive to the re-encryption requests issued by Bob.

The proposed solution is called *Optimistic Challenge-based Approach*, which is centered around two important concepts: requiring minimal changes to the current network implementation, and minimizing the additional overhead.

We introduce the design details of our solution, after which we discuss some potential security attacks and how to address them.

Discovering working Ursulas. Recall that in the NuCypher network, Bob receives a map from Alice containing the set of Ursulas that has the key fragments needed to implement the access control policy. When issuing a re-encryption request, Bob uses this map (in association with the network discovery protocol) to reach each of these Ursulas and obtain the service.

In particular, in the NuCypher network there is a separation between the role of a staker and a working Ursula. All stakers' Ethereum addresses, along with their stake values, are recorded in one of the NuCypher network smart contracts, namely, the StakeEscrow contract. Each of these stakers will be tied, or bonded, to a working Ursula to provide the re-encryption service by having its address listed next to the staker's address.

The StakeEscrow contract does not contain any information about how to reach a specific working Ursula. Thus, the map that Bob receives includes only the Ethereum addresses of the working Ursulas. To allow the parties to communicate with each other, each participant, i.e., Alice, Bob, Ursula, employs a discovery protocol (more like a gossiping protocol) to discover the IP addresses and ports of the working Ursulas in the network.

The discovery process also includes retrieving the keypair a working Ursula uses for the re-encryption service purposes. We call this keypair a stamp, and we require an Ursula to use her stamp when signing all messages related to the proposed confirm availability protocol.

Optimistic Ursula challenging. Once Bob discovers the working Ursulas listed in the policy map, he can connect with each of them and start issuing service requests. As noted, this communication is one-to-one meaning that no other Ursulas (or any NuCypher network participant) mediates the communication between Bob and working Ursula. This in turn means that no one can attest to whether Ursula has responded if Bob complains later that he was not served.

The main idea is to add a mediator, or potentially a witness, in the service process (if needed) to monitor a specific working Ursula and challenge its responsiveness. Hence, it is an optimistic protocol invoked only when Bob complains about not receiving the service. In detail, for each round (where a round is the time needed to mine a block or several blocks on the blockchain) a set of Ursulas is selected at random. We call these gateway Ursulas. Bob contacts a working Ursula asking for the re-encryption service as usual. If this Ursula does not respond, Bob complains to a gateway about it. At this point, the gateway will act as an intermediary and forwards Bob's request to this working Ursula on behalf of Bob and waits for the answer. If no answer is received, this gateway will trigger other gateways to perform the same process, i.e., forward the request on behalf of Bob and wait for an answer. If the working Ursula is still unresponsive, these gateways will collectively sign a proof-of-unavailability, which is basically a statement saying that the working Ursula was contacted by these gateways and she did not respond, and publish it through the StakeEscrow contract (see Section 3.2 for an overview of collective signing). Once the proof-of-unavailability is verified, part of the working Ursula's stake will be slashed as a punishment.

Gateways Selection. For each round a set of n gateways Ursulas will be selected. A proof-of-unavailability will be accepted by the network if it is signed by at least t gateways among this set (this threshold is a relaxation of requiring all gateways to sign since it could be the case that not all of them are active).

A simple idea to select the gateways is to use a high entropy source of randomness to obtain a random beacon for each round. Then feed this beacon into an iterative hashing process. After each iteration, map the hash to a working Ursula index as listed in the StakeEscrow contract. That is, the working Ursula bonded with the first staker listed in the contract has index 0, the next has index 1, etc. Then, rehash the previous hash and map the output to an index, and so no. In case of a collision, i.e., an already selected index is produced again, discard it and proceed to the next hash iteration. This process is repeated until a set of distinct n indices is computed.

Note that the selection process may contain Ursulas for which Bob does not have a contact information. Hence, Bob has to discover these Ursulas before being able to submit a complaint. To reduce the delays, and as outlined earlier, Bob starts with complaining to one gateway and involves the rest if the working Ursula does not respond to the challenge from this gateway. Hence, Bob can start with a gateway that he already knows how to reach (if any) and in the meantime works on discovering the rest of the selected gateways (if he does not already have their contact information).

Furthermore, the above protocol assumes working in the random oracle model, meaning that hash functions are modeled as random oracles. Thus, the iterative hashing process selects at random the working Ursulas. Although, we believe this is sufficient for our purposes, this can be replaced with more sophisticated approaches to produce random strings (that are then mapped to indices), e.g., a verifiable random function [12]. We leave this as part of our future work in case we decide to pursue this path.

As for the high entropy source of randomness, there are several potential approaches here. We can rely on an external source, e.g., the NIST random beacon [13] or even a combination of multiple sources, for that. Or we can work also in the random oracle model and assume that block hashes are drawn from a uniform distribution, and thus, use the block hash as a random beacon. In particular, for the current round, the hash of the block that was mined y rounds ago is used (y is the confirmation interval in the underlying cryptocurrency system). Alternatively, and to avoid the random oracle assumption, we can use randomness extractors to produce a high entropy beacon from the block hashes which itself could be low entropy [14].

Proof-of-unavailability processing. As mentioned previously, a proof-of-unavailability against a working Ursula is a statement stating that this Ursula was unavailable during a specific round signed by at least t gateways out of the n gateways selected for that round. Such a proof is submitted to the StakeEscrow contract and is verified as follows:

- Produce the list of gateways selected for the current round. This is done by using the same process described previously.
- Verify the collective signature over the signed statement (see Section 3.2).
- If everything is fine, the StakeEscrow contract revokes part of the stake bonded to the working Ursula as a punishment.

Note that the above assumes that the StakeEscrow contract is aware of the gateways' stamps (or keys) that are used in signing the proof-of-unavailability. This can be done by either expanding the staker list in the contract to contain not only the Ethereum addresses of working Ursulas, but also their stamps. Another option is to piggyback the stamps (signed by using the key corresponding to the working Ursula's Ethereum address) with the proof-of-unavailability. A more simpler, and efficient, option is to sign the proof-of-unavailability by using the key corresponding to the working Ursula's Ethereum address in the first place, and thus, the StakeEscrow contract will not need an additional information. Which option to use depends merely on efficiency considerations.

Quantifying the Financial Punishment or Slashing Value. A question that comes to mind is how much should be revoked from Ursula's stake once a proof-of-unavailability is approved? Quantifying this amount should be driven by two factors; the unavailability duration and the utility gain (or profits) of this cheating behavior in terms of the collected fees and inflation rewards for that duration.

Accordingly, we can compute this value to be equal to the fees and inflation rewards that an Ursula is supposed to receive in a round (recall that a round is the time needed to mine a block or several blocks on the blockchain). Hence, the working Ursula will, first, lose her fees and inflation rewards from the network, and second, lose the same amount from her stake. Such a loss will take place even if a single proof-of-unavailability is received against a working Ursula within a round. In fact, the StakeEscrow contract will process only one proof against a working Ursula per round to reduce computational costs in the system.

Working Only During the Challenge Phase. A potential issue under the proposed optimistic scheme is that a working Ursula may operate only during the challenge phase. That is, she ignores any fresh request coming from Bob, and just replies afterwards when receiving the same request again (i.e., when it is forwarded by the gateways during the challenge phase).

We argue that such a behavior is not a practical issue since a rational Ursula will be online eitherway to monitor whether this is a challenge phase or not, and that the amount of work needed to respond to a re-encryption request is minimal. Hence, there is no incentive at all to follow this strategy, meaning that a rational Ursula will act honestly.

DoS Attacks. Another potential issue is exploiting the unavailability complaints to perform a DoS attack against the gateways and working Ursulas. In detail, Bob may lie and issue complaints against working Ursulas even though they are responsive just to slash their stakes. Or an attacker may replay these complaints, or issue them on behalf of Bob, to slash a working Ursula. Or the goal could be to overwhelm the gateways with the challenge process and make them unavailable to perform the re-encryption service (recall that the gateways are originally working Ursulas in the NuCypher network).

This issues can be handled using a collection of techniques as follows:

- Require Bob to sign all the complaints (so no one can impersonate Bob unless they know his signing key), and include a timestamp or a sequence number in each of them (to ensure freshness and prevent replay attacks).
- Increase the cost of issuing complaints. That is, require Bob to do some work in order to produce a valid complaint (in a similar way to proof-of-work, i.e., produce a hash over the complaint with specific number of leading zeros).

Unresponsive Gateways. A third issue that we may encounter in the proposed solution is that the gateways themselves could be unresponsive. This will stall the challenge phase and make it infeasible to prove that some working Ursula is unavailable. We believe that such an issue will be organically handled by the network. That is, the larger the number of Ursulas in the network, the higher the chances of having more honest Ursulas. By increasing the number of selected gateways n, and given that the selection process is random, the chances of having at least t honest gateways in a round will be high.

Another mechanism is to incentivize the gateways to do the work in the form of a small fee paid out of the revoked stake.

It could be the case that all gateways in a round are responsive (although we believe that the probability this happens is very low). In this case, it could be viable to perform the challenge phase in a recursive way. In other words, Bob can send an unavailability complaint against the gateways of the current round to the gateways of the previous round. The previous round gateways will in turn challenge the current round gateways by forwarding Bob's complaint to them and sign a proof-of-unavailability if no response is received.

5 Confirm Service Activity Solutions

In this section, we present potential solutions for the confirm service activity problem. The goal is to come up with provably secure solutions that allows an Ursula to prove that it has served a given number of distinct re-encryption requests within a given period.

The rest of this section discusses the proposed solutions along with an analysis of their security and efficiency aspects. Lastly, the section concludes with directions of future work on the confirm service activity issue.

5.1 PCD-based Scheme.

The main idea here is to adapt the PCD framework so that Ursula can combine the correctness proofs she computes for Bobs' requests in a single proof attesting to the following fact: "Ursula has served ω distinct re-encryption requests correctly."

Thus, in this setup, there is only one computation party, or prover, namely, Ursula. For each round, where a round could be the time needed to mine a block on the blockchain, Ursula starts with input x_1, which is a signed and fresh request from Bob. It answers this request with $cFrag_{x_1}$ and produces a correctness proof π_1 as defined in the Umbral scheme, in addition to another correctness proof $\hat{\pi}_1$ that will be used in the PCD composition. Then, when the next request x_2 arrives, which is the input for the next step in the computation, Ursula answers this request as before and produces $cFrag_{x_2}$ and a correctness proof π_2, then it uses $(x_2, cFrag_{x_2}, \pi_2)$ and the previous proof $\hat{\pi}_1$ to produce $\hat{\pi}_2$. $\hat{\pi}_2$ does not only attest to the correctness of $cFrag_{x_2}$, but also attests to the fact that Ursula has served two valid distinct requests until now. The same process is repeated until the end of the round to produce a single proof $\hat{\pi}_\omega$ along with the number of served requests ω. Figure 2 depicts this process pictorially.

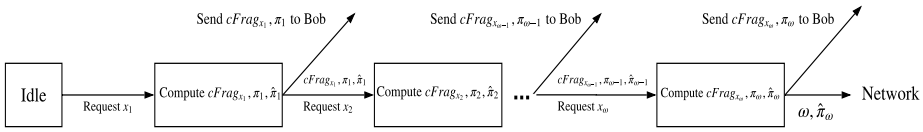

Fig. 2: PCD-based solution diagram. Ursula starts a round in the idle state. When the first request arrives, Ursula responds to the request and starts composing the proofs as new requests arrive. At the end of the round, Ursula announces the number of served requests and a single proof attesting to its claim to the network.

The final proof will be processed by the contract that governs Alice's policy. A valid proof allows Ursula to claim fees out of Alice's Ether escrow as a payment for ω re-encryption requests.

The above is a high level description of the idea. However, more time is need to understand PCD and SNARKs in order to come up with a concrete construction (if possible). Please see Section 7 for more information.

5.2 CoSi-based Scheme.

This solution utilizes the idea of collective signing by electing a committee that will sign a report submitted by a specific Ursula after verifying that the report supports the claim that "Ursula has served ω distinct re-encryption requests correctly."

At a high level, the scheme works as follows. For each round, a working Ursula keeps a full record of all the requests that she served during the round. These include the signed requests received from Bob(s), and the produced $cFrag$ and the correctness proof π (as in the Umbral scheme) for each request. At the end of the round, a committee of t Ursulas is elected, where t is a small integer, e.g., $t = 5$. The working Ursula initiates the CoSi protocol to sign the message m stated above while replacing ω with the actual number of served requests in the round. This Ursula sends m along with the full report to each member in the committee. Each member Ursula (i.e., member in the elected committee) verifies m by checking the report as follows:

1. Check that each request is distinct by checking the sequence number of the request (or any value that is used for freshaness), and valid by verifying Bob's signature over the request. (Here the policy will contain Bob's public key to allow the committee use the right verification key.)
2. Verify the correctness of each $cFrag$ as in the Umbral scheme.
3. Check that the value of ω inside m agrees with the record.

If everything is fine, each member of the committee and the working Ursula finalize the CoSi signing protocol as described in Section 3.2. At the end, the working Ursula publishes the collective signature, which can be verified using the accumulated public keys of the cosigning Ursulas.

On the committee election. This can be done by using some deterministic computation over a block hash and mapping the output to Ursulas' public keys. So the selection is not determined by the working Ursula to prevent any potential collusion. The selection may also take into account the presence and size of each Ursula's stake, to avoid an attacker spinning up enormous numbers of Ursulas in order to increase the chance of them controlling the entire committee.

The above scheme works under the assumption that at least one Ursula in the elected committee is honest, which pertains to an assumption on the least number of honest Ursulas in the network. If the latter assumption is under threat, one mitigating approach is to increase t (the committee size).

Another approach is to have a changing set of external verifiers, like trusted partners, that all working Ursulas must use for the CoSi signing of their records.

A third approach is to keep the deterministic selection of the committee but with an external member, e.g., either a trusted partner verifier or a special verifier

node deployed and maintained by the NuCypher company. Thus, achieving the assumption of at least one member of the elected committee is honest.

On the publicity of the signed records. Having a valid collective signature from a committee (that has at least one honest member) suffices for the correctness of the signed statement. However, it could be better to keep the records that produced the message m available for a while so that any party can verify them (the verifying parties could maintain such a public record for a given period after which the logs can be discarded).

We can resort to this option just at the beginning to convince the participants of the trustworthiness of the committee or the validity of the assumption that at least one Ursula in the elected committee is honest.

On compensating the committee. This solution may raise the question of why would the elected committee (especially if it is composed of other Ursulas in the system) participate in the CoSi process, which also involves verifying the full request record presented by the working Ursula. This can be pictured as a collaborative work, the committee does the work so that others will do the same when the committee members play the role of working Ursulas.

Another option is to pay the committee for their work, either as part of the inflation rewards, or by having working Ursulas pay for it (however, this may complicate the system operation).

5.3 Commit/Challenge/Open-based Scheme.

This solution utilizes the idea of commit/challenge/open protocols. In details, Ursula keeps track of the requests coming from Bob(s) during a time round and assign each of them a unique sequence number. That is, Ursula replies with $cFrag$ and the correctness proof along with a sequence number showing the order of the request within the batch of requests handled during a round. At the end of the round, Ursula constructs a Merkle tree of all requests, where the requests (and their replies) are the leaves of the tree ordered by the sequence numbers. Ursula signs the root of the tree, denoted as $root$ to produce a signature σ_{root}, then it publishes $(\omega, root, \sigma_{root})$ to the network (recall that ω is the number of served requests).

To prove correctness, Ursula will be challenged to open some leaves in the Merkle tree. This can be done by having the policy contract select at random (e.g. based on the block hash or any other mechanism) the leaf IDs to be opened. If Ursula fails to open them correctly within a predefined timeframe, she loses the whole fee she was supposed to collect for serving ω requests.

An alternative approach to the challenge/open scheme described above is to have Ursula publish the full Merkle tree on some known public space but not on the blockchain, and make the full record available online for a specific period to allow anyone to verify the work. If no one files a complaint about the tree (we still need to define correctness properties, like checking all Bob public keys are defined in the policy created by Alice, and that the response is valid by checking

the proof produced by Umbral), Ursula collects the fees for the provided service. On the other hand, a valid complaint or proof-of-cheating costs Ursula the full allocation of fees, or potentially involves slashing her stake.

6 Discussion and Analysis

Which solution to adopt will be based on benchmark testing and the development vision of the NuCypher network. The ZKP-based solution (the one utilizing bulletproofs) provides several advantages including non-interactivity (as opposed to the committee-attestation one that needs interaction with the committee). It also supports computational soundness as opposed to the statistical one of the commit/challenge/open solution. Nonetheless, it could be the case that the other solutions are more efficient especially if we incorporate committee attestation or sidechains to support other functionalities in the network.

Another issue pertains to the payment computation. During early stages when the network launches, we anticipate limited adoption and service demand. Thus, we reward Ursulas for just being online to encourage adoption. While in later stages, payments will be dispensed partially in proportion to the actual number of service requests an Ursula answers. This is due to the fact that later on the subsidies will effectively disappear, i.e., the majority of tokens in the network will be minted, and the service fees are the only source of income. To incentivize Ursula to provide a correct and timely service, these fees should be computed based on the actual amount of service. This shows how changes in incentive alignment lead to different views on how to distribute these incentives and ensure the security of the system.

Until now we assume that Alice pays for the service by using the Ether she locks in the policy contract. Other arrangement may emerge in the system like having Bob pay for each requests he issues. Such an arrangement and its implication on the confirm activity issue will be studied once it becomes part of the NuCypher network protocol.

7 Future Work

Most of the future work on the confirm service activity issue will be dedicated to construct a concrete PCD-based solution. This includes the following:

- Understand PCD and its applications in a greater depth. This also requires exploring NIZK in general and SNARKs in specific.
- Define an efficient output correctness predicate that characterizes the correctness of the statement that PCD will attest for. This could be hard for the confirm activity issue as the value of the output is dynamic based on the workload Ursula may receive.
- Define a way to compose the proofs efficiently and produce a single proof at the end. This will be tied to the formulated predicate.
- Argue about the correctness and security of the concrete scheme.

References

1. Nucypher. https://www.nucypher.com/.
2. Michael Egorov, MacLane Wilkison, and David Nuñez. Nucypher kms: decentralized key management system. *arXiv preprint arXiv:1707.06140*, 2017.
3. David Nuñez. Umbral: A threshold proxy re-encryption scheme. 2018. https://github.com/nucypher/umbral-doc/blob/master/umbral-doc.pdf.
4. Alessandro Chiesa and Eran Tromer. Proof-carrying data and hearsay arguments from signature cards. In *ICS*, volume 10, pages 310–331, 2010.
5. Paul Valiant. Incrementally verifiable computation or proofs of knowledge imply time/space efficiency. In *Theory of Cryptography Conference*, pages 1–18. Springer, 2008.
6. Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 315–334. IEEE, 2018.
7. Nico Döttling, Russell WF Lai, and Giulio Malavolta. Incremental proofs of sequential work. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 292–323. Springer, 2019.
8. Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, and Bryan Ford. Keeping authorities" honest or bust" with decentralized witness cosigning. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 526–545. Ieee, 2016.
9. Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of cryptology*, 4(3):161–174, 1991.
10. Mihir Bellare and Gregory Neven. Multi-signatures in the plain public-key model and a general forking lemma. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 390–399, 2006.
11. Silvio Micali, Kazuo Ohta, and Leonid Reyzin. Accountable-subgroup multisignatures. In *Proceedings of the 8th ACM conference on Computer and Communications Security*, pages 245–254, 2001.
12. Silvio Micali, Michael Rabin, and Salil Vadhan. Verifiable random functions. In *40th annual symposium on foundations of computer science (cat. No. 99CB37039)*, pages 120–130. IEEE, 1999.
13. *NIST Random Beacon*. https://beacon.nist.gov/home.
14. Joseph Bonneau, Jeremy Clark, and Steven Goldfeder. On bitcoin as a public randomness source. *IACR Cryptology ePrint Archive*, 2015:1015, 2015.