PORs: Proofs of Retrievability for Large Files

Ari Juels[1] and Burton S. Kaliski Jr.[2]

[1] RSA Laboratories
Bedford, MA, USA
ajuels@rsa.com
[2] EMC Corporation
Hopkinton, MA, USA
kaliski_burt@emc.com

Abstract. In this paper, we define and explore *proofs of retrievability* (PORs). A POR scheme enables an archive or back-up service (prover) to produce a concise proof that a user (verifier) can retrieve a target file F, that is, that the archive retains and reliably transmits file data sufficient for the user to recover F in its entirety.

A POR may be viewed as a kind of cryptographic proof of knowledge (POK), but one specially designed to handle a *large* file (or bitstring) F. We explore POR protocols here in which the communication costs, number of memory accesses for the prover, and storage requirements of the user (verifier) are small parameters essentially independent of the length of F. In addition to proposing new, practical POR constructions, we explore implementation considerations and optimizations that bear on previously explored, related schemes.

In a POR, unlike a POK, neither the prover nor the verifier need actually have knowledge of F. PORs give rise to a new and unusual security definition whose formulation is another contribution of our work.

We view PORs as an important tool for semi-trusted online archives. Existing cryptographic techniques help users ensure the privacy and integrity of files they retrieve. It is also natural, however, for users to want to verify that archives do not delete or modify files prior to retrieval. The goal of a POR is to accomplish these checks *without users having to download the files themselves*. A POR can also provide quality-of-service guarantees, i.e., show that a file is retrievable within a certain time bound.

Key words: storage systems, storage security, proofs of retrievability, proofs of knowledge

1 Introduction

Several trends are opening up computing systems to new forms of outsourcing, that is, delegation of computing services to outside entities. Improving network bandwidth and reliability are reducing user reliance on local resources. Energy and labor costs as well as computing-system complexity are militating toward the centralized administration of hardware. Increasingly, users employ software and data that reside thousands of miles away on machines that they themselves do not own. Grid computing, the harnessing of disparate machines into a unified computing platform, has played a role in scientific computing for some years. Similarly, *software as a service (SaaS)*— loosely a throwback to terminal/mainframe computing architectures—is now a pillar in the internet-technology strategies of major companies.

Storage is no exception to the outsourcing trend. Online data-backup services abound for consumers and enterprises alike. Amazon Simple Storage Service (S3) [1], for example, offers an abstracted online-storage interface, allowing programmers to access data objects through web-service calls, with fees metered in gigabyte-months and data-transfer amounts. Researchers have investigated alternative service models, such as peer-to-peer data archiving [12].

As users and enterprises come to rely on diverse sets of data repositories, with variability in service guarantees and underlying hardware integrity, they will require new forms of assurance of

the integrity and accessibility of their data. Simple replication offers one avenue to higher-assurance data archiving, but at often unnecessarily and unsustainably high expense. (Indeed, a recent IDC report suggests that data-generation is outpacing storage availability [14].) Protocols like Rabin's data-dispersion scheme [33] are more efficient: They share data across multiple repositories with minimum redundancy, and ensure the availability of the data given the integrity of a quorum (k-out-of-n) of repositories. Such protocols, however, do not provide assurances about the state of *individual repositories*—a shortcoming that limits the assurance the protocols can provide to relying parties.

In this paper, we develop a new cryptographic building block known as a *proof of retrievability* (POR). A POR enables a user (verifier) to determine that an archive (prover) "possesses" a file or data object F. More precisely, a successfully executed POR assures a verifier that the prover presents a protocol interface through which the verifier can retrieve F in its entirety. Of course, a prover can refuse to release F even after successfully participating in a POR. A POR, however, provides the strongest possible assurance of file retrievability barring changes in prover behavior.

As we demonstrate in this paper, a POR can be efficient enough to provide regular checks of file retrievability. Consequently, as a general tool, a POR can complement and strengthen any of a variety of archiving architectures, including those that involve data dispersion.

1.1 A first approach

To illustrate the basic idea and operation of a POR, it is worth considering a straightforward design involving a keyed hash function $h_\kappa(F)$. In this scheme, prior to archiving a file F, the verifier computes and stores a hash value $r = h_\kappa(F)$ along with secret, random key κ. To check that the prover possesses F, the verifier releases κ and asks the prover to compute and return r. Provided that h is resistant to second-preimage attacks, this simple protocol provides a strong proof that the prover knows F. By storing multiple hash values over different keys, the verifier can initiate multiple, independent checks.

This keyed-hash approach, however, has an important drawback: High resource costs. The keyed-hash protocol requires that the verifier store a number of hash values linear in the number of checks it is to perform. This characteristic conflicts with the aim of enabling the verifier to offload its storage burden. More significantly, each protocol invocation requires that the prover process the *entire* file F. For large F, even a computationally lightweight operation like hashing can be highly burdensome. Furthermore, it requires that the prover read the entire file for every proof—a significant overhead for an archive whose intended load is only an occasional read per file, were every file to be tested frequently.

1.2 Our approach

We introduce a POR protocol in which the verifier stores only a single cryptographic key—irrespective of the size and number of the files whose retrievability it seeks to verify—as well as a small amount of dynamic state (some tens of bits) for each file. (One simple variant of our protocol allows for the storage of no dynamic state, but yields weaker security.) More strikingly, and somewhat counterintuitively, our scheme requires that the prover access only a small portion of a (large) file F in the course of a POR. In fact, the portion of F "touched" by the prover is essentially independent of the length of F and would, in a typical parameterization, include just hundreds or thousands of data blocks.

Briefly, our POR protocol encrypts F and randomly embeds a set of randomly-valued check blocks called *sentinels*. The use of encryption here renders the sentinels indistinguishable from other file blocks. The verifier challenges the prover by specifying the positions of a collection of sentinels and asking the prover to return the associated sentinel values. If the prover has modified or deleted a *substantial* portion of F, then with high probability it will also have suppressed a number of sentinels. It is therefore unlikely to respond correctly to the verifier. To protect against corruption

by the prover of a *small* portion of F, we also employ error-correcting codes. We let $\tilde{F}$ refer to the full, encoded file stored with the prover.

A drawback of our proposed POR scheme is the preprocessing / encoding of F required prior to storage with the prover. This step imposes some computational overhead—beyond that of simple encryption or hashing—as well as larger storage requirements on the prover. The sentinels may constitute a small fraction of the encoded $\tilde{F}$ (typically, say, 2%); the error-coding imposes the bulk of the storage overhead. For large files and practical protocol parameterizations, however, the associated expansion factor $|\tilde{F}|/|F|$ can be fairly modest, e.g., 15%.

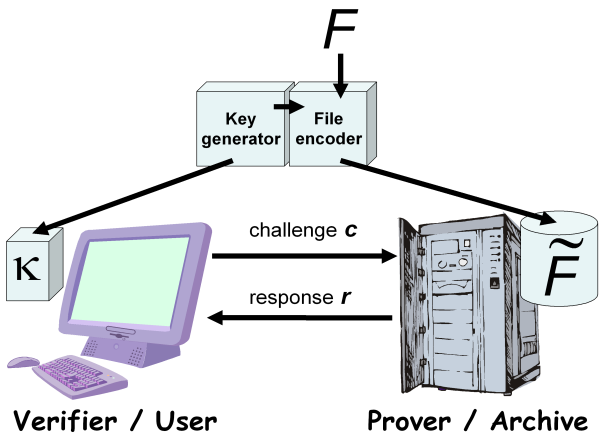

Fig. 1. Schematic of a POR system. An encoding algorithm transforms a raw file F into an encoded file $\tilde{F}$ to be stored with the prover / archive. A key generation algorithm produces a key κ stored by the verifier and used in encoding. (The key κ is independent of F in some PORs, as in our main scheme.) The verifier performs a challenge-response protocol with the prover to check that the verifier can retrieve F.

To illustrate the intuition behind our POR protocol a little better, we give two brief example scenarios.

Example 1. Suppose that the prover, on receiving an encoded file $\tilde{F}$, corrupts three randomly selected bits, $\beta_1, \beta_2, \beta_3$. These bits are unlikely to reside in sentinels, which constitute a small fraction of $\tilde{F}$. Thus, the verifier will probably not detect the corruption through POR execution. Thanks to the error-correction present in $\tilde{F}$, however, the verifier can recover the original file F completely intact.

Example 2. Suppose conversely that the prover corrupts many blocks in $\tilde{F}$, e.g., 20% of the file. In this case (absent very heavy error-coding), the verifier is unlikely to be able to recover the original file F. On the other hand, every sentinel that the verifier requests in a POR will detect the corruption with probability about 1/5. By requesting hundreds of sentinels, the verifier can detect the corruption with overwhelming probability.

We additionally consider schemes based on the use of message-authentication codes (MACs) applied to (selected) file blocks. The principle is much the same as in our sentinel-based scheme. The verifier performs spot-checks on elements of $\tilde{F}$. Error-coding ensures that if a sizeable fraction of $\tilde{F}$ is uncorrupted and available, as demonstrated by spot-checks, then the verifier can recover F with high probability.

1.3 Related work

Data-integrity protection is one of the fundamental goals of cryptography. Primitives such as digital signatures and message-authentication codes (MACs), when applied to a full file F, allow an entity in possession of F to verify that it has not been subjected to tampering.

A more challenging problem is to enable verification of the integrity of F without explicit knowledge of the full file. The problem was first described in broad generality by Blum et al. [8], who explored the task of efficiently checking the correctness of a memory-management program. Follow-on work has explored the problem of dynamic memory-checking in a range of settings. In recent work, for instance, Clarke et al. [11] consider the case of a trusted entity with a small amount of state, e.g., a trusted computing module, verifying the integrity of arbitrary blocks of untrusted, external, dynamically-changing memory. Their constructions employ a Merkle hash-tree over the contents of this memory, an approach with fruitful application elsewhere in the literature. In this paper, with our exploration of PORs, we focus on memory-integrity checking in the special case of a static file.

In networked storage environments, cryptographic file systems (CFSs) are the most common tool for system-level file-integrity assurance (see, e.g., [22] for a good, recent survey). In a CFS, one entity, referred to as a *security provider*, manages the encryption and/or integrity-protection of files in untrusted storage providers. The security provider may be either co-located with a physical storage device or architected as a virtual file system.

Cryptographic integrity assurance allows an entity to detect unauthorized modifications to portions of files upon their retrieval. Such integrity assurance in its basic form does not enable the detection of modification or deletion of files *prior* to their retrieval or on an ongoing basis. It is this higher degree of assurance that a POR aims to provide.

A POR permits detection of tampering or deletion of a remotely located file—or relegation of the file to storage with uncertain service quality. A POR does not by itself, however, protect against loss of file contents. File robustness requires some form of storage redundancy and, in the face of potential system failures, demands the distribution of a file across multiple systems. A substantial literature, e.g., [4, **?**,**?**], explores the problem of robust storage in a security model involving a collection of servers exhibiting Byzantine behavior. The goal is simulation of a trusted read/write memory register, as in the abstraction of Lamport [24]. In such distributed models, the robustness guarantees on the simulated memory register depend upon a quorum of honest servers.

While many storage systems operating in the Byzantine-failure model rely on storage duplication, an important recent thread of research involves the use of information dispersal [33] and error-coding to reduce the degree of file redundancy required to achieve robustness guarantees, as in [10]. Similarly, we use error-correction in our main POR construction to bound the effects of faults in a storage archive in our constructions.

Although a POR only aims at detection of file corruption or loss, and not prevention, it can work hand-in-hand with techniques for file robustness. For example, a user may choose to disperse a file across multiple service providers. By executing PORs with these providers, the user can detect faults or lapses in service quality. She can accordingly re-distribute her file across providers to strengthen its robustness and availability. In peer-to-peer environments, where service quality may be unreliable, such dynamic reallocation of resources can be particularly important.

As we explain in detail in section 2, a POR is loosely speaking a kind of proof of knowledge (POK) [5] conducted between a prover and a verifier on a file F. A proof of knowledge serves to demonstrate knowledge by the prover of some short secret y that satisfies a predicate specified by the verifier. Generally, as in an authentication protocol, the essential design property of a POK is to preserve the secrecy of y, i.e., not to reveal information about y to the verifier. The concept of zero-knowledge [17, 18] captures this requirement in a strict, formal sense. In a POR, the design challenge is different. The verifier has potentially already learned the value F whose knowledge the prover is demonstrating (as the verifier may have encoded the file to begin with). Since F is potentially quite large, the main challenge is to prove knowledge of F (or information from which F can be recovered) using computational and communication costs substantially smaller than $|F|$.

PORs are akin to other unorthodox cryptographic proof systems in the literature, such as proofs of computational ability [40] and proofs of work (POWs) [21]. Memory-bound POWs [13] are similar to the use of PORs for quality-of-service verification in that both types of proof aim to characterize memory use in terms of the latency of the storage employed by the prover. Very close in spirit to a POR is a construction of Golle, Jarecki, and Mironov [19], who investigate "storage-enforcing commitment schemes." Their schemes enable a prover to demonstrate that it is making use of storage space at least $|F|$. The prover does not prove directly that it is storing file F, but proves that it is has committed sufficient resources to do so.

The use of sentinels in our main scheme is similar is spirit to a number of other systems that rely on the embedding of secret check values in files, such as the "ringers" used in [20]. There the check values are easily verifiable computational tasks that provide evidence for the correct processing of accompanying tasks. PORs bear an important operational difference in that they involve "spot checks" or auditing, that is, the prover is challenged to reveal check values in isolation from the rest of the file. The distinguishing feature of the POR protocols we propose here is the way that they amplify the effectiveness of spot-checking for the special case of file-verification by combining cryptographic hiding of sentinels with error-correction.

The earliest POR-like protocol of which we are aware is one proposed by Lillibridge et al. [25]. Their goal differs somewhat from ours in that they look to achieve assurance of the availability of a file that is distributed across a set of servers in a peer relationship. To ensure that a file is intact, Lillibridge et al. propose application of error-coding to a file combined with spot-checks of file blocks conducted by system peers. Their approach assumes separate MACs on each block and does not directly address error-correction for the single-server case, , and the paper does not establish formal definitions or bounds on the verification procedure.

A more theoretical result of relevance is that of Naor and Rothblum (NR) [31]. They show that the existence of a sub-linear-size proof of file recoverability implies the existence of one-way functions.[1] NR propose a protocol in which an error-correcting code is applied to a file F and blocks are then MACed. By checking the integrity of a random subset of blocks, a verifier can obtain assurance that the file as a whole is subject to recovery. NR also provide a simple, formal security definition and prove security bounds on their construction. The NR security definition is similar to our formal POR definition and more general, but is asymptotic, rather than concrete. Thus, in their proposed scheme, NR consider encoding of an entire file as a single codeword in an error-correcting code. Such encoding is inefficient in practice, but yields good theoretical properties. For our purposes, the NR definition also omits some important elements. It assumes that the verifier has direct access to the encoded file $\tilde{F}$, in essence that $\tilde{F}$ is a fixed, published string. Thus the definition does not cover the case of a server that reports file blocks in $\tilde{F}$ inconsistently: In essence, the NR definition does not define an extractor for F. Additionally, the NR definition does not capture the possibility of a proof that relies on functional combination of file blocks, rather than direct reporting of file blocks. (We consider a POR scheme here, for instance, in which sentinels are XORed or hashed together to reduce bandwidth.)

More recent work has considered the application of RSA-based hashing as a tool for constructing proofs of recoverability. Filho and Barreto [16], for example, propose a scheme that makes indirect use of a homomorphic RSA-based hash introduced by Shamir [34], briefly as follows. Let N be an RSA modulus. The verifier stores $k = F \bmod \phi(N)$ for file F (suitably represented as an integer). To challenge the prover to demonstrate retrievability of F, the verifier transmits a random element $g \in \mathbb{Z}_N$. The prover returns $s = g^F \bmod N$, and the verifier checks that $g^k \bmod N = s$. This protocol has the drawback of requiring the prover to exponentiate over the entire file F. In work contemporaneous with our paper here, Ateniese et al. [3] have considered an elegant application of RSA-based hashing to individual file blocks. In their scheme, homomorphic composition of file-

[1] Note that our sentinel-based POR scheme interestingly does not require one-way functions, as sentinels may be randomly generated. The contradiction stems from the fact that our scheme requires a key with size linear in the number of protocol executions.

block check-values supports spot-checking of files and yields short proofs. As it relies on modular exponentiation over files, their approach is computationally intensive, and also relies on a somewhat lightly explored "knowledge-of-exponent" hardness assumption [6] adapted to the RSA setting. Their security definition hinges on the prover providing correct check values to the verifier, rather than directly characterizing bounds on file retrievability.

Shah et al. [37] also very recently proposed methods for auditing storage services. In their approach, a third-party auditor verifies a storage provider's possession of an encrypted file via a challenge-response MAC over the full (encrypted) file; the auditor also verifies the storage provider's possession of a previously committed decryption key via a conventional proof-of-knowledge protocol. This result is noteworthy for its detailed discussion of the role of auditing in a storage system, but again does not offer a formal security model.

1.4 Our contribution

We view our main contribution as threefold. First, we offer a formal, concrete security definition of PORs that we believe to be of general interest and applicability in practical settings. Second, we introduce a sentinel-based POR scheme with several interesting properties: Of theoretical significance, the data in sentinels, and thus the resulting PORs, can be made independent of the stored file; a strong proof can be very compact (on the order of 32 bytes in practice, with some caveats); the scheme supports hierarchical proofs; and the computational requirements for the prover and verifier are minimal. Our sentinel scheme highlights the benefits of pre-determined verifier queries in a POR—counterbalanced by a bound on the total number of such queries. We explore variations on our basic POR scheme with different sets of tradeoffs. As a final contribution, we offer concrete analysis, practical design guidance, and optimizations of general interest in POR construction.

Organization

In section 2, we introduce a formal definition of a POR, and explain how this definition differs from the standard cryptographic view of proofs of knowledge. We introduce our main POR scheme in section 3, briefly discuss its security, and describe several variants. We describe the adaptation and application of our POR scheme to the problem of secure archiving and quality-of-service checking in section 4. We conclude in section 5 with a brief discussion of future research directions. We prove our main theorem in appendix A.

2 Definitions

2.1 Standard proof-of-knowledge definitions and PORs

Bellare and Goldreich (BG) established a standard, widely referenced definition of proofs of knowledge in [5]. Their definition centers on a binary *relation* $R \subseteq \{0,1\}^* \times \{0,1\}^*$.

A language $L_R = \{x : \exists\, y \text{ s.t. } (x,y) \in R\}$ is defined as the set of values x that induce valid relations. The set $R(x) = \{y : (x,y) \in R\}$ defines the *witnesses* associated with a given x. Typically, relations of interest are polynomial, meaning that the bitlength $|y|$ of any witness is polynomial in $|x|$.

In the BG view, a proof of knowledge is a two-party protocol involving a prover P and a verifier V. Each player is a probabilistic, interactive function. The BG definition supposes that P and V share a common string x. A transcript includes the sequence of outputs of both players in a given interaction.

The BG definition relies upon an additional function, an *extractor* algorithm K that also takes x as input and has oracle access to P. Additionally, V has an associated *error function* $\kappa(x)$, essentially the probability that V accepts transcripts generated by a prover P that does not actually know (or

use its knowledge of) a witness for x. For every prover P, let $p(x)$ be the probability that on input x, prover P induces a set of transcripts that V accepts.

Briefly, then, in the BG definition, a poly-time verifier V characterizes a proof of knowledge if the following holds: There exists a polynomial $f(x)$ such that for all sufficiently large $|x|$, for every prover P, the extractor K outputs a witness $y \in R(x)$ in expected time bounded by $f(x)/(p(x) - \kappa(x))$. (The BG definition also has a non-triviality requirement: There must exist a legitimate prover P, i.e., a prover that causes V to accept with probability 1 for any $x \in L_R$.)

Intuitively, the BG definition states that if prover P can convince verifier V that $x \in L_R$, then P "knows" a witness y. The stronger P's ability to convince a verifier, the more efficiently a witness y can be extracted from P.

While very broad, the BG definition does not naturally capture the properties of POR protocols, which have several distinctive characteristics:

1. **No common string x:** In a POR, P and V may not share any common string x: P may merely have knowledge of some file F, while V possesses secret keys for verifying its ability to retrieve F from P and also for actually performing the retrieval.
2. **No natural relation R:** Since a *POR* aims to prove that the file F is subject to recovery from P, it would seem necessary to treat F as a witness, i.e., to let $y = F$, since F is precisely what we would like to extract. In this case, however, if we regard x as the input available to V, we find that there is no appropriate functional relation $R(x, y)$ over which to define a POR: In fact, x may be perfectly independent of F.
3. **Split verifier/extractor knowledge:** It is useful in our POR protocols to isolate the ability to verify from the ability to extract. Thus, K may take a secret input unknown to either P or V.

As we show, these peculiarities of PORs give rise to a security definition rather different than for ordinary POKs.

2.2 Defining a POR system

A *POR system* PORSYS comprises the six functions defined below. The function respond is the only one executed by the prover P. All others are executed by the verifier V. For a given verifier invocation in a POR system, it is intended that the set of verifier-executed functions share and implicitly modify some persistent state α. In other words, α represents the state of a given invocation of V; we assume α is initially null. We let π denote the full collection of system parameters. The only parameter we explicitly require for our system and security definitions is a security parameter j. (In practice, as will be seen in our main scheme in section 3, it is convenient for π also to include parameters specifying the length, formatting, and encoding of files, as well as challenge/response sizes.) On any failure, e.g., an invalid input or processing failure, we assume that a function outputs the special symbol $\perp$.

keygen$[\pi] \rightarrow \kappa$: The function keygen generates a secret key κ. (In a generalization of our protocol to a public-key setting, κ may be a public/private key pair. Additionally, for purposes of provability and privilege separation, we may choose to decompose κ into multiple keys.)

encode$(F; \kappa, \alpha)[\pi] \rightarrow (\tilde{F}_\eta, \eta)$: The function encode generates a file handle η that is unique to a given verifier invocation. The function also transforms F into an (enlarged) file $\tilde{F}_\eta$ and outputs the pair $(\tilde{F}_\eta, \eta)$.

Where appropriate, for a given invocation of verifier V, we let F_η denote the (unique) file whose input to encode has yielded handle η. Where this value is not well defined, i.e., where no call by verifier V to encode has yielded handle η, we let $F_\eta \stackrel{def}{=} \perp$.

$\mathsf{extract}(\eta; \kappa, \alpha)[\pi] \rightarrow F$: The function extract is an interactive one that governs the extraction by verifier V of a file from a prover P. In particular, extract determines a sequence of challenges that V sends to P, and processes the resulting responses. If successful, the function recovers and outputs F_η.

$\mathsf{challenge}(\eta; \kappa, \alpha)[\pi] \rightarrow c$. The function challenge takes secret key κ and a handle and accompanying state as input, along with system parameters. The function outputs a challenge value c for the file η.

$\mathsf{respond}(c, \eta) \rightarrow r$. The function respond is used by the prover P to generate a response to a challenge c. Note that in a POR system, a challenge c may originate either with challenge or extract.

$\mathsf{verify}((r, \eta); \kappa, \alpha) \rightarrow b \in \{0, 1\}$. The function verify determines whether r represents a valid response to challenge c. The challenge c does not constitute explicit input in our model; it is implied by η and the verifier state α. The function outputs a '1' bit if verification succeeds, and '0' otherwise.

2.3 POR security definition

We define the security of a POR protocol in terms of an experiment in which the adversary $\mathcal{A}$ plays the role of the prover P. Let us first give some preliminary explanation and intuition.

Definition overview The adversary $\mathcal{A}$ consists of two parts, $\mathcal{A}$("setup") and $\mathcal{A}$("respond"). The component $\mathcal{A}$("setup") may interact arbitrarily with the verifier; it may create files and cause the verifier to encode and extract them; it may also obtain challenges from the verifier. The purpose of $\mathcal{A}$("setup") is to create an archive on a special file F_{η^*}. This archive is embodied as the second component, $\mathcal{A}$("respond"). It is with $\mathcal{A}$("respond") that the verifier executes the POR and attempts to retrieve F_{η^*}.

In our model, an archive—whether honest or adversarial—performs only one function. It receives a challenge c and returns a response r. An honest archive returns the correct response for file $\tilde{F}_\eta$; an adversary may or may not do so. This challenge/response mechanism serves both as the foundation for proving retrievability in a POR and as the interface by which the function extract recovers a file F_η. In the normal course of operation, extract submits a sequence of challenges $c_1, c_2, c_3 \ldots$ to an archive, reconstructs $\tilde{F}_\eta$ from the corresponding responses, and then decodes $\tilde{F}_\eta$ to obtain the original file F_η.

In our security definition, we regard $\mathcal{A}$("respond") as a *stateless* entity. (That is, its state does not change after responding to a challenge, it has no "memory.") On any given challenge c, $\mathcal{A}$("respond") returns the correct response with some probability; otherwise, it returns an incorrect response according to some fixed probability distribution. These probabilities may be different from challenge to challenge, but because of our assumption that $\mathcal{A}$("respond") is stateless, the probabilities remain fixed for any given challenge value. Put another way, $\mathcal{A}$("respond") may be viewed as set of probability distributions over challenge values c.

It may seem at first that the assumption of statelessness in $\mathcal{A}$("respond") is too strong. In practice, after all, since an extractor must send many more queries than a verifier, a stateful adversary can distinguish between the two. Thus, by assuming that $\mathcal{A}$("respond") is stateless, our definition discounts the (quite real) possibility of a malicious archive that responds correctly to a verifier, but fails to respond to an extractor. Such a stateful adversary responds correctly to challenges but still fails to release a file.

We believe, however, that our POR definition is among the strongest possible in a real-world operational environment and that it captures a range of useful, practical assurances. There is in fact no meaningful way to define a POR without assuming some form of restriction on adversarial behavior. As we have explained, unless the POR protocol is indistinguishable from extract, a Byzantine

adversary can always fail when it detects an extraction attempt. Thus, the most appropriate security definition seems to be one that characterizes the ability of a verifier to extract a file F_η from a "snapshot," i.e., from the full (and, by assumption, unchanging) state of $\mathcal{A}$("respond"). The verifier effectively is able to "rewind" the adversary as desired during execution to preserve the adversary's lack of state. In a real-world environment, this ability corresponds to access to a memory dump or backup tape for an adversarial server.

For some applications, our modeling of $\mathcal{A}$("respond") may actually be too strong. For example, if the purpose of a POR is to ensure availability or quality-of-service in an archive, then there may be no reason to assume the possibility of adversarial corruption of a file. An adversary's only real economic incentive may be to minimize its storage cost, i.e., to delete file blocks or relegate them to slow storage. Our POR security definition may be modified to meet this weaker requirement, and we consider such an "erasing" adversary later in the paper. Our concern here, however, is to create a foundational definition with broad real-world applicability.

Briefly, our security definition involves a game in which the adversary $\mathcal{A}$ seeks to "cheat" a verifier V. $\mathcal{A}$ tries to create an environment in which V believes that it will be able to retrieve a given file F_{η^*} with overwhelming probability, yet cannot. Thus the aim of $\mathcal{A}$("setup") is to induce a verifier state α and create state (δ, η^*) in $\mathcal{A}$("respond") such that: (1) V accepts responses from $\mathcal{A}$("respond") to challenges with high probability and (2) V fails with non-negligible probability to retrieve F_{η^*} from $\mathcal{A}$("respond") on invoking $\mathsf{extract}$.

Definition details We let $\mathcal{O}_{\mathsf{encode}}$, $\mathcal{O}_{\mathsf{extract}}$, $\mathcal{O}_{\mathsf{challenge}}$, and $\mathcal{O}_{\mathsf{verify}}$ represent oracles respectively for functions encode, $\mathsf{extract}$, $\mathsf{challenge}$, verify in a single invocation of verifier V. These oracles take κ and α as implicit inputs, i.e., inputs not furnished by (or revealed to) the adversary. Additionally, these oracles may modify state α, which is initially null. We denote by the symbol '$\cdot$' those input values that the adversary has the freedom to specify in its oracle calls.

We let '*' designate protocol values created by $\mathcal{A}$ in the course of our experiment. We let δ denote adversarial state—in particular, the state information passed from $\mathcal{A}$("setup") to $\mathcal{A}$("respond"). As above, we let π denote the parameter set for a POR system PORSYS. Where appropriate for brevity, however, we drop π from our notation.

In our first experiment $\mathbf{Exp}^{\text{setup}}$, the adversary $\mathcal{A}$("setup") is permitted to interact arbitrarily with system oracles. At the end of the experiment $\mathcal{A}$("setup") specifies a file handle η^* and state δ as input to the adversarial function
$\mathcal{A}$("respond") for the next experiment.

Experiment $\mathbf{Exp}^{\text{setup}}_{\mathcal{A},\mathsf{PORSYS}}[\pi]$

$\kappa \leftarrow \mathsf{keygen}(j); \alpha \leftarrow \phi;$	% generate key, initialize oracle state
$(\delta, \eta^*) \leftarrow \mathcal{A}^{\mathcal{O}}(\text{"setup"});$	% accessing $\mathcal{O}$, $\mathcal{A}$ creates archive
output (α, δ, η^*)	% output full oracle and archive states

In our next experiment, the adversarial archive $\mathcal{A}$("respond") responds to a challenge issued by the verifier. The adversary is deemed successful if it generates a response accepted by the verifier.

Experiment $\mathbf{Exp}^{\text{chal}}_{\mathcal{A},\mathsf{PORSYS}}(\alpha, \delta, \eta^*)[\pi]$

$c^* \leftarrow \mathcal{O}_{\mathsf{challenge}}(\eta^*; \kappa, \alpha);$	% issue "challenge"
$r^* \leftarrow \mathcal{A}(\delta, c^*)(\text{"respond"});$	% adversary outputs response
$\beta \leftarrow \mathcal{O}_{\mathsf{verify}}((r^*, \eta^*); \kappa, \alpha);$	% verify adversarial response
output β	% output '1' if response correct, otherwise '0'

We define $\mathbf{Succ}^{\text{chal}}_{\mathcal{A},\mathsf{PORSYS}}(\alpha,\delta,\eta^*)[\pi] = \mathsf{pr}\big[\mathbf{Exp}^{\text{chal}}_{\mathcal{A},\mathsf{PORSYS}}(\alpha,\delta,\eta^*)[\pi] = 1\big]$, i.e., the probability that the adversarial archive succeeds in causing the verifier to accept.

Given these experiment specifications, we now specify our definition of security for a POR. Our definition aims to capture a key intuitive notion: That an adversary with high probability of success in $\mathbf{Exp}^{\text{chal}}$ must "possess" F_{η^*} in a form that may be retrieved by the verifier, i.e., by an entity with knowledge of κ and α. By analogy with security definitions for standard proofs of knowledge, we rely on the *extractor* function $\mathsf{extract}$. One special feature of a POR systems is that $\mathsf{extract}$ *is not just a component of our security proof.* As we have already seen, it is *also* a normal component of the POR system. (For this reason, $\mathcal{A}$ actually has oracle access to $\mathsf{extract}$ in $\mathbf{Exp}^{\text{setup}}$.) A priori, $\mathcal{A}(\text{"respond"})$ cannot distinguish between challenges issued by $\mathsf{challenge}$ and those issued by $\mathsf{extract}$.

In our security definition, the function $\mathsf{extract}$ is presumed to have oracle access to $\mathcal{A}(\delta,\cdot)(\text{"respond"})$. In other words, it can execute the adversarial archive on arbitrary challenges. Since $\mathcal{A}$ is cast simply as a function, we can think of $\mathsf{extract}$ as having the ability to rewind $\mathcal{A}$. The idea is that the file F_{η^*} is retrievable from $\mathcal{A}$ if $\mathsf{extract}$ can recover it. The $\mathsf{respond}$ function of the adversary is the interface by which $\mathsf{extract}$ recovers F.

We thus define

$$\mathbf{Succ}^{\text{extract}}_{\mathcal{A},\mathsf{PORSYS}}(\alpha,\delta,\eta^*)[\pi] = \mathsf{pr}\big[F = F_{\eta^*} \;\big|\; F \leftarrow \mathsf{extract}^{\mathcal{A}(\delta,\cdot)(\text{"respond"})}(\eta^*;\kappa,\alpha)[\pi]\big].$$

Let a poly-time algorithm $\mathcal{A}$ be one whose running time is bounded by a polynomial in security parameter j. Our main security definition is as follows.

Definition 1. *A poly-time POR system* $\mathsf{PORSYS}[\pi]$ *is a* (ρ,λ)-valid proof of retrievability (POR) *if for all poly-time* $\mathcal{A}$ *and for some* ζ *negligible in security parameter* j*,*

$$\mathsf{pr}\left[\begin{array}{l}\mathbf{Succ}^{\text{extract}}_{\mathcal{A},\mathsf{PORSYS}}(\alpha,\delta,\eta^*) < 1-\zeta,\\ \mathbf{Succ}^{\text{chal}}_{\mathcal{A},\mathsf{PORSYS}}(\alpha,\delta,\eta^*) \geq \lambda\end{array}\;\middle|\;\begin{array}{l}(\alpha,\delta,\eta^*)\\ \qquad\leftarrow \mathbf{Exp}^{\text{setup}}_{\mathcal{A},\mathsf{PORSYS}}\end{array}\right] \leq \rho.$$

At an intuitive level, our definition establishes an upper bound ρ on the probability that $\mathcal{A}(\text{"setup"})$ generates a "bad" environment—i.e., a "bad" adversarial archive (δ,η^*) in $\mathcal{A}(\text{"respond"})$ and system state α in the verifier. We regard an environment as "bad" if the verifier accepts adversarial responses with probability at least λ, but extraction nonetheless fails with non-negligible probability ζ. Note that we treat ζ asymptotically in our definition for simplicity: This treatment eliminates the need to consider ζ as a concrete parameter in our analyses.

Remarks

- We can also define a (ρ,λ)-valid proof of retrievability for an *erasing adversary.* Such an adversary is only permitted to reply to a challenge with either a correct response or a null one. In section 4, we consider an important practical setting for this variant.
- In our security definition, the adversary can make an arbitrary number of oracle calls in the setup phase of the experiment, prior to the challenge phase. Thus the adversary can "condition" the archive as desired, causing the verifier, for instance to issue an arbitrary number of queries prior to the challenge phase. In our sentinel-based POR protocol, if all sentinels are consumed prior to the challenge phase, then $\mathcal{O}_{\mathsf{challenge}}$ emits the special $\perp$, and the adversary fails to return a correct response. In this way, we model a bound t on the number of challenges our POR can support. An alternative approach is to define a (ρ,λ,t)-valid proof of retrievability, in which the adversary must make fewer than t calls to $\mathcal{O}_{\mathsf{challenge}}$. Most of the protocols we propose in this paper have bounded t, but POR schemes with unbounded t are desirable, of course.
- Note that we do not give $\mathcal{A}$ oracle access in $\mathbf{Exp}^{\text{chal}}$. This is a simplifying assumption: We rule out the possibility of $\mathcal{A}$ learning additional information from the verifier beyond what it may

have already learned in $\mathbf{Exp}^{\text{setup}}$. In $\mathbf{Exp}^{\text{chal}}$, we are only testing the ability to retrieve a file at a given point in time, after any corruptions or deletions have already occurred. Prior challenges are formally considered part of the setup when evaluating the bounds on the current challenge. The impact of additional oracle access during the challenge phase itself is worth further exploration.

3 Sentinel-Based POR Scheme

Our main POR scheme of interest is the sentinel-based one described in the introduction. Before giving details, we outline the general protocol structure.

Setup phase: The verifier V encrypts the file F. It then embeds sentinels in random positions in F, sentinels being randomly constructed check values. Let $\tilde{F}$ denote the file F with its embedded sentinels.

Verification phase: To ensure that the archive has retained F, V specifies the positions of some sentinels in $\tilde{F}$ and asks the archive to return the corresponding sentinel values.

Security: Because F is encrypted and the sentinels are randomly valued, the archive cannot feasibly distinguish *a priori* between sentinels and portions of the original file F. Thus we achieve the following property: If the archive deletes or modifies a substantial, ϵ-fraction of $\tilde{F}$, it will with high probability also change roughly an ϵ-fraction of sentinels. Provided that the verifier V requests and verifies enough sentinels, V can detect whether the archive has erased or altered a substantial fraction of $\tilde{F}$. (Individual sentinels are, however, only one-time verifiable.)

In practice, a verifier wants to ensure against change to *any portion of the file* F. Even a single missing or flipped bit can represent a semantically significant corruption. Thus, detection of ϵ-fraction modification alone is insufficient. With a simple improvement, however, we can ensure that even if the archive *does* change an ϵ-fraction (for arbitrarily large ϵ), the verifier can still recover its file. Very simply, before planting sentinels in the file F, the user applies an *error-correcting code* that tolerates corruption (or erasure, if appropriate) of an ϵ-fraction of data blocks in $\tilde{F}$. The verifier also permutes the file to ensure that the symbols of the (encrypted) code are randomly dispersed, and therefore that their positions are unknown to the archive.

We emphasize one strongly counterintuitive aspect of our POR scheme: The sentinels, which constitute the content of a POR proof, are generated *independently of the bitstring whose retrievability they are proving*. By contrast, as explained above, in an ordinary proof of knowledge (POK), the content of a proof depends on the values that are the subject of the proof, i.e., the witness.

3.1 Sentinel scheme details

We now describe our sentinel-based POR, which we call $\mathsf{Sentinel\text{-}PORSYS}[\pi]$.

We employ an l-bit *block* as the basic unit of storage in our scheme. We employ an error-correcting code that operates over l-bit symbols, a cipher that operates on l-bit blocks, and sentinels of l bits in length. While not required for our scheme, this choice of uniform parameterization has the benefit of conceptual simplicity. It is also viable in practice, as we demonstrate in our example parameter selections in section 3.4. We also assume for simplicity the use of an efficient (n, k, d)-error correcting code with even-valued d, and thus the ability to correct up to $d/2$ errors.

Suppose that the file F comprises b blocks, $F[1], \ldots, F[b]$. (We assume that b is a multiple of k, a coding parameter. In practice, we can pad out F if needed.) We also assume throughout that F contains a message-authentication code (MAC) value that allows the verifier to determine during retrieval if it has recovered F correctly.

The function encode entails four steps:

1. **Error correction:** We carve our file F into k-block "chunks." To each chunk we apply an (n, k, d)-error correcting code C over $GF[2^l]$. This operation expands each chunk into n blocks and therefore yields a file $F' = F'[1], \ldots, F'[b']$, with $b' = bn/k$ blocks.

2. **Encryption:** We apply a symmetric-key cipher E to F', yielding file F''. Our protocols require the ability to decrypt data blocks in isolation, as our aim is to recover F even when the archive deletes or corrupts blocks. Thus we require that the cipher E operate independently on plaintext blocks. One option is to use a l-bit block cipher. In this case, we require indistinguishability under a chosen-plaintext attack; it would be undesirable, for example, if an adversary in a position to influence F were able to distinguish the data contents of blocks.[2] In practice, an appropriate choice of cipher E would be a tweakable block cipher [27] such as XEX [35]. A second option is to employ a stream cipher E. On decryption, portions of the keystream corresponding to missing blocks may simply be discarded.
3. **Sentinel creation:** Let $f : \{0,1\}^j \times \{0,1\}^* \rightarrow \{0,1\}^l$ be a suitable one-way function. We compute a set of s sentinels $\{a_w\}_{w=1}^s$ as $a_w = f(\kappa, w)$. We append these sentinels to F'', yielding F'''. (Thus, we can accommodate up to $\lfloor s/q \rfloor$ challenges, each with q queries.)
4. **Permutation:** Let $g : \{0,1\}^j \times \{1,\ldots,b'+s\} \rightarrow \{1,\ldots,b'+s\}$ be a pseudorandom permutation (PRP) [28]. We apply g to permute the blocks of F''', yielding the output file $\tilde{F}$. In particular, we let $\tilde{F}[i] = F'''[g(\kappa, i)]$.

The function extract requests as many blocks of $\tilde{F}$ as possible. It then reverses the operations of encode. In particular, it permutes the ciphertext blocks under g^{-1}, strips away sentinels, decrypts, then applies error correction as needed to recover the original file F. Note that if the code C is *systematic*, i.e., a code word consists of the message followed by error-correction data, then error-correcting decoding is unnecessary when the archive provides an intact file.

To bolster the success probability of extract against probabilistic adversaries, i.e., adversaries that do not respond deterministically to a given challenge value, we do the following. If simple recovery fails, then extract makes an additional $\gamma - 1$ queries for each block and performs majority decoding over the resulting responses. Given sufficiently large γ, this approach recovers a given block with high probability provided that the adversary outputs a correct response for each block with probability non-negligibly greater than 1/2. (We assume the probabilities for each block are independent, as further discussed in appendix A.)

The function challenge takes as input state variable σ, a counter initially set to 1. It outputs the position of the σth sentinel by reference to g, i.e., it outputs $p = g(b' + \sigma)$ and increments σ; it repeats this process q times, i.e., generates positions for q different sentinels. The prover function respond takes as input a single challenge consisting of a set of q positions, determines the values of the q corresponding blocks (sentinels in this case), and returns the values. (See section 3.5 for some simple bandwidth optimizations.) The function verify works in the obvious manner, taking a challenge pair (σ, d) as input and verifying that the prover has returned the correct corresponding sentinel values.[3]

Purpose of the permutation step: The permutation step in our protocol serves two purposes. First, it randomizes the placement of sentinels such that they can be located in constant time and storage; only the sentinel generation key need be stored.

The second purpose relates to error correction. In principle, we could treat our entire file as a single message in an error-correcting code with a large minimum distance, e.g., a Reed-Solomon code. In practice, however, such coding can be challenging—even for erasure-coding. (See [15] on a recent effort to scale a Tornado code to large block sizes.) It is for this reason that we carve our file F into chunks. It is important to disperse the constituent blocks of these chunks in a secret, random manner. An adversary with knowledge of the location in $\tilde{F}$ of the blocks belonging to a particular chunk could excise the chunk without touching any sentinels, thereby defeating our POR scheme.

[2] In the case of re-use of a file-encryption key, which we deprecate here, it might be necessary to enforce security against chosen ciphertext attacks.

[3] Of course, it is possible for the verifier to pick σ at random from $\{1,\ldots,s\}$, rather than storing it as a counter value. In this case, by the Birthday Paradox, the power of the verifier degrades as the number of used sentinels approaches $\sqrt{s}$.

While pseudorandom-permutation primitives are most often designed to operate over bitstrings, and thus power-of-two-sized domains, Black and Rogaway [7] describe simple and efficient pseudorandom-permutation constructions over domains $\mathbb{Z}_k$ for arbitrary integers k. Their constructions are suitable for use in our POR scheme.

3.2 Security

We summarize our security results here; a formal analysis of the security of Sentinel-PORSYS$[\pi]$ may be found in appendix A. Let $C = b'/n$ be the number of constituent chunks (which include data, not sentinels). We define ϵ to be an upper bound on the fraction of data blocks and previously unused sentinels corrupted by the adversary. The total number of such blocks is at most $b' + s$, and decreases over time as sentinels are consumed in verifier challenges. As may be expected, the security of our POR system depends on q, the number of sentinels per challenge, not the total number of available sentinels. (The total number of challenges depends, of course, on the total number of sentinels.)

We make a "block isolation" assumption in appendix A—an extension of the general statelessness assumption —such that the probability distribution of responses to individual queries (i.e., blocks) are independent of one another.

In a simplified model that assumes ideal properties for our underlying cryptographic primitives (with little impact on practical parameterization), and under our block-isolation assumption, we prove the following:

Theorem 1. *Suppose that* $\gamma \geq 24(j \ln 2 + \ln b')$. *For all* $\epsilon \in (0, 1)$ *such that* $\mu < d/2$ *where* $\mu = n\epsilon(b' + s)/(b' - \epsilon(b' + s))$, Sentinel-PORSYS$[\pi]$ *is a* (ρ, λ)*-valid POR for* $\rho \geq Ce^{(d/2-\mu)}(d/2\mu)^{-d/2}$ *and* $\lambda \geq (1 - \epsilon/4)^q$.

As a technical aspect of our proof, we consider a block to be "corrupted" if $\mathcal{A}$("respond") returns it correctly with probability less than 3/4. (The constant 3/4 is arbitrary; our proofs work for any constant greater than 1/2, with changes to the constants in our theorem.) Recall that our security definition for a POR treats the extraction probability $1 - \zeta$ in an asymptotic sense for the sake of simplicity. We analyze γ—the number of queries made by extract on a given block—accordingly. Given the lower bound $\gamma \geq (j \ln 2 + \ln b')$, we can show that the verifier recovers all uncorrupted blocks from $\mathcal{A}$("respond") with overwhelming probability.[4]

The value ρ bounds the probability of more than $d/2$ corruptions in any chunk.

Our bound for λ simply reflects the probability of an adversary successfully returning q sentinels when it has corrupted an ϵ-fraction of blocks.

3.3 POR efficiency

Of course, application of an error-correcting (or erasure) code and insertion of sentinels enlarges $\tilde{F}$ beyond the original size of the file F. The expansion induced by our POR protocol, however, can be restricted to a modest percentage of the size of F. Importantly, the communication and computational costs of our protocol are low. As we mention below, the verifier can transmit a short (e.g., 128-bit) seed constituting a challenge over an arbitrary number of sentinels; the verifier can similarly achieve a high level of assurance on receiving a relatively compact (e.g., 256-bit) proof from the archive.

Perhaps the most resource-intensive part of our protocols in practice is the permutation step: This operation requires a large number of random accesses, which can be slow for a file stored on disk (but less so for random-access memory). Our POR construction requires only a single permutation pass, however, and it is possible in some measure to batch file accesses, that is, to precompute a

[4] Since extract needs to perform multiple queries *only* in the presumably rare case of a file-retrieval failure against a probabilistic adversary, we can make γ large if necessary in most practical settings, as when an adversarial archive is taken offline and "rewound" to extract block values.

sequence of accesses and partition them into localized groups as in batch sorting. Such detailed questions of system efficiency lie outside the scope of our investigation here.

3.4 An example parameterization

A block size of $l = 128$ is one natural choice; 128 bits is the size of an AES block and yields sentinels of sufficient size to protect against brute-force sentinel-guessing attacks. Let us consider use of the common $(255, 223, 32)$-Reed-Solomon code over $GF[2^8]$, i.e., with one-byte symbols. By means of the standard technique of "striping" (see, e.g., [9]), we can obtain a $(255, 223, 32)$-code over $GF[2^{128}]$, i.e., over file blocks, which is convenient for our parameterization in this example. A chunk consists then of $n = 255$ blocks.

Let us consider a file F with $b = 2^{27}$ blocks, i.e., a 2-gigabyte file. This file expands by just over 14% under error-coding to a size of $b' = 153,477,870$. Suppose that we add $s = 1,000,000$ sentinels. Thus the total number of blocks to be stored is $b' + s = 154,477,870$, the total number of blocks in the file $\tilde{F}$. The total file expansion is around 15%.

Consider $\epsilon = 0.005$, i.e., an adversary that has corrupted 1/2% of the data blocks and unused sentinels in $\tilde{F}$. Now $C = b'/n = 601,874$, and $\mu = n\epsilon(b' + s)/(b' - \epsilon(b' + s)) \approx 1.29$. (Recall μ is an upper bound on the mean number of corrupted blocks per chunk.) By Theorem 1, $\rho \geq Ce^{(d/2-\mu)}(d/2\mu)^{-d/2} \approx 601,874 \times e^{14.71}(12.41)^{-16} \approx 4.7 \times 10^{-6}$. In other words, the probability that the adversary renders the file unretrievable[5] —which is bounded above by the minimum ρ for this ϵ—is less than 1 in 200,000.

Suppose that we let $q = 1,000$, i.e., the verifier queries 1,000 sentinels with each challenge. Since the total number of sentinels is $s = 1,000,000$, the verifier can make 1,000 challenges over the life of the file (a challenge per day for about three years). The probability of detecting adversarial corruption of the file —which is bounded below by the maximum $1-\lambda$ for this ϵ—is at least $1-(1-\epsilon/4)^q \approx 71.3\%$ *per challenge*. This is not overwhelmingly large, of course, but probably suffices for most purposes, as detection of file-corruption is a cumulative process. A mere 12 challenges, for instance, provides detection-failure probability of less than 1 in 1,000,000.

Of course, for larger ϵ, the probability of file corruption is higher, but so too is that of detection by the verifier. We also believe that the bounds in our main theorem can be tightened through a more detailed proof.

3.5 Variant protocols

While we rely on our basic sentinel scheme as a conceptual starting point, there are a number of attractive variant protocols. We explore some of them here, giving brief overviews without accompanying formalism.

Erasure codes and erasing adversaries As we explain in section 4, in our envisaged real-world applications, the major concern is with erasing adversaries, rather than general ones. Moreover, we can appeal to erasure codes which are more efficient as a class than general error-correcting codes.

Modern erasure codes, e.g., fountain codes such as Raptor codes [2], operate in linear time and are amenable in some cases to practical application to fairly large files or file segments without any need for chunking [15]. Additionally, it is possible (if not generally practical) to treat a full file as a single message in an error-correcting code with large minimum distance. In such cases, we can obtain considerably tighter bounds on the security of our POR system.

Consider a system $\mathsf{Sentinel\text{-}PORSYS}[\pi]$ that is: (1) Implemented against an *erasing* adversary without chunking using an erasure code with minimum distance $d + 1$ or (2) Implemented against a fully capable adversary using an error-correcting code with minimum distance $2d$ and no chunking.

[5] We assume negligible ζ in this example. It may be seen, for instance, that $\gamma = 1800$ yields a majority-decoding failure probability $\zeta < 2^{-80}$.

In both cases, if $\epsilon \leq d/(b'+s)$, then the file F is fully recoverable. Additionally, we make the following observation (whose proof follows straightforwardly from the analysis underlying our main theorem):

Observation 1 *Suppose that $\epsilon \leq d/b'$. Then* Sentinel-PORSYS$[\pi]$ *is a (ρ, λ)-valid POR for $\rho \geq 0$ and $\lambda \geq (1-\epsilon/4)^q$ in the cases just noted.*

Erasure codes such as fountain codes by themselves, however, do not provide robust guarantees over an adversarial channel. Their strong resilience bounds apply only to erasures in a stochastic channel. Thus, to achieve the bounds given here in a POR, our encoding steps of encryption and permutation are still essential.[6] These steps effectively reduce an adversarial channel to a stochastic one. Additionally, for very large files, application of a fountain code across the entire file can be challenging, as such codes typically require repeated random accesses across the full file. Thus, chunking may still be desirable, and permutation can then provide enhanced resilience by eliminating chunk structure.

When file blocks are MACed, it is effectively possible to convert an erasure code into an error-correcting code. The decoding process simply discards corrupted blocks.

Bandwidth optimizations There are two types of bandwidth optimizations to consider:

Prover-to-verifier optimizations can reduce the size of the response transmitted by an archive to a verifier. In our basic sentinel POR, the archive can compress a sequence $a_1, \ldots, a_q$ of sentinels prior to transmission. One possibility is to hash them. While a useful heuristic, this approach introduces a problem: Without relying on a random oracle assumption, and/or assuming the oracle embodied in some trusted device, e.g., a TPM or remote server, it is unclear how to construct an efficient corresponding extract function.

Another appealing approach is for the archive to compute an XOR value, $\alpha = \oplus_{i=1}^{q} a_i$. This response format alone does not give rise to an efficient and robust extract function. Instead, it is helpful for the archive to transmit a second value α', an XOR over a random subset of $\{a_1, \ldots, a_q\}$ designated by the verifier. For the sake of efficiency, the verifier can specify this subset by means of a pseudorandom seed β. The function extract can thereby recover each data block by rewinding the archive and challenging it repeatedly with different values of β, for each set of block locations.

An interesting feature of XORing is that it can be employed for compression in a *hierarchical* POR setting. Suppose that an archive breaks $\tilde{F}$ into pieces and distributes the pieces among a collection of subordinate archives. On receiving a set of challenges, the primary archive can parcel them out appropriately to the subordinates. Each subordinate can return an XOR of its respective responses, which the primary archive itself can then XOR together as its response to the verifier. This process is transparent to the verifier and can operate recursively over a *tree* of archives.

Verifier-to-prover optimizations can reduce the size of the challenge transmitted by a verifier to an archive.

Rather than transmitting its ith challenge as a sequence of sentinel positions $W_i = \{w_{i,1}, \ldots, w_{i,q}\}$, the verifier could potentially transmit a pseudorandom seed $\kappa_{sentpos,i}$ from W_i is derived. The seed $\kappa_{sentpos,i}$ itself can be derived from a master seed $\kappa_{sentpos}$.

However, if sentinels are appended and permuted, as in our basic scheme, then it is not directly possible for the prover to derive W_i from $\kappa_{sentpos_i}$: The secret permutation g will disperse sentinels such that the prover cannot locate them. Instead, we can modify our scheme so that either (a) the sentinels are *inserted* into the designated positions after permutation or (b) the sentinels are *written over* the contents of the file in those positions. The former involves a serial merge operation; the

[6] Even though fountain codes can be keyed to operate over pseudorandomly selected file blocks, permutation still imparts stronger erasure resilience. That is because the code structure can be exploited by an adversary to delete pseudorandom *seeds* accompanying packets, without erasing other packet elements. Thus it is helpful to remove such local structure.

latter can be done in parallel, and thanks to the error-coding of the file, the overwriting can later be corrected (with appropriate adjustments to the parameters to accommodate the s additional "errors").

Turning data blocks into sentinels A particularly attractive variant scheme, given its minimal prover storage, is one in which data blocks effectively play the role of sentinels. When the file is encoded—as a last encoding step, for instance—the ith challenge is prepared as follows. A series of (pseudo)random data-block positions $W_i = \{w_{i,1}, \ldots, w_{i,q}\}$ is selected. A MAC M_i is computed over the corresponding data blocks $\alpha_i = \{a_{i,1}, \ldots, a_{i,q}\}$ using verifier key κ_{MAC}. The value M_i is stored with the file. A challenge takes the form of the set of positions W_i, and the position of M_i (if not known to the prover). The prover returns the pair (α_i, M_i), which the verifier may check quite inexpensively.

As an alternative, the verifier may store an encrypted version of the MAC, and send the MAC key to the prover for evaluation as in previous challenge-response schemes, except that here a subset of blocks is MACed.

In contrast to our basic sentinel scheme, which requires tq extra blocks of storage to support t queries, each over q sentinels, this "data-to-sentinels" scheme requires only $O(t)$ extra blocks of storage. With our proposed optimizations, challenges and responses may comprise just a small, constant number of data blocks.

Authenticated blocks All of the variants described above, as with our basic sentinel protocol, rely on challenge precomputation. They consequently "use up" challenges, and allow for only a bounded number t of challenge/response invocations. Using MACs, however, along the lines of the NR and Lillibridge et al. protocols, we can effectively eliminate this bound.

Building on our basic POR protocol, we might omit the sentinel insertion step from Sentinel-PORSYS, and add the following, final step after permutation. We partition the file $\tilde{F}$ into sequentially indexed segments of v blocks for appropriate parameter v (say, 5). To each segment we append a MAC under key κ of the contents of the blocks within the segment, the segment index, and the file handle. For the purposes here, the bit-length of a MAC can be small, e.g., 20 bits, since it is the aggregate effect on multiple blocks that is being measured. Thus, the resulting file expansion need not be prohibitive. For example, with 20-byte blocks, $v = 5$, and 20-bit MACs, the incremental file expansion due to MACing would be only 2.5%. As applied to our setting in Example 3.4, for instance, the total file expansion would be 16.5%, as opposed to 15% as parameterized in that example for sentinels.

This is essentially an adaptation of the NR / Lillibridge et al. schemes to our basic POR protocol structure. The steps of encryption and permutation—not present in the basic form of those schemes—play an important practical role. Given the need for chunking in our error-correcting code, these two operations hide local structure. In fact, though, even without the need for chunking, concealment of local structure still amplifies the robustness of the scheme. As an adversary cannot feasibly identify a single MACed segment, it is forced to spread corruptions or erasures uniformly over segments, increasing the probability of verifier detection. (Segment positions are revealed by verifier queries, but this causes only a gradual degradation in detection probability.)

This MAC-based approach is quite efficient in terms of file-expansion overhead, computational costs, and bandwidth. It has an important drawback, though: It does not permit the prover to return a digest of its responses, i.e., to hash or XOR them together. The MAC-based variant does have the interesting feature of permitting a model in which challenges derive from a (fresh) common reference string or public source of randomness. (Another possible but less efficient way to verify the correctness of file blocks is use of a Merkle tree in which each segment corresponds to a leaf, and the verifier stores the root.)

PIR schemes Another variant on Sentinel-PORSYS that allows for an unbounded number of queries involves the use of *private information retrieval* (PIR) [23]. In explicitly requesting the value of a

sentinel from the prover, the verifier discloses the location of the sentinel. A PIR scheme, in contrast, permits a verifier to retrieve a portion of a file $\tilde{F}$ from a prover without disclosing what it has retrieved. Thus, by retrieving sentinels using PIR, the verifier can re-use sentinels, i.e., let $q = s$, with no effective degradation in security.

While capable of communication costs of $O(\log^2(|\tilde{F}|))$ per retrieved sentinel bit [26], PIR schemes require access to all of $\tilde{F}$ and carry high computational costs. Recent work suggests that PIR schemes may be no more efficient in practice than transferring all of $\tilde{F}$ [39].

4 Practical Application to Storage Services

We now describe an application of our POR scheme to an archive service provided by a Storage Service Provider (SSP). Multiple service levels may be offered, corresponding to different storage "tiers" (disks of varying speeds, tape, etc.) or a combination (see, e.g., [38]). An SSP and a client typically operate under a *service level agreement* (SLA) specifying properties such as throughput, response time, availability, and recovery-time objectives [32]. We consider primarily the case where the SSP stores the file (or perhaps a share of it, as in [25]), but the client itself does not retain a copy; if the client did, it could just verify retrievability by sampling and comparing random blocks against its own copy, without the need for the POR *per se*.

The price of the service is set by the SSP at some profit margin above the cost of providing the service at a given level (equipment, maintenance, staff, facilities, etc.). An SSP is thus motivated legitimately to increase its profit margin by reducing cost while maintaining the same service level; in a competitive marketplace this will ultimately reduce the price, which is a benefit to clients as well. (Indeed, one of the reasons for outsourcing to an SSP is the client's belief that the SSP can reduce the cost more effectively than the client alone.)

Internet Service Providers (ISPs) and Application Service Providers (ASPs) follow a similar economic model, but with an important difference. An ISP or ASP's service levels are effectively tested continuously by clients for most functions as a part of their regular interactions with the services. An SSP's service levels, on the other hand, particularly for its retrieval service, are only tested when that function is actually run, which in general is infrequent. Furthermore, retrieval is the very reason for which the client is paying for service levels: The client does not (in general) pay a higher price to have archive data stored faster, but rather to ensure that it can be accessed faster.

Without a requirement to provide continuous service level assurances, an SSP may also be willing to take the risk of decreasing its cost by not maintaining an agreed service level. For instance, an SSP may move files it considers less likely to be accessed to a lower tier of storage than agreed. These lapses are exacerbated by the possibility that the SSP may itself rely on other SSPs to store files or parts of them. For instance, to meet an agreed availability level, an SSP may replicate data on geographically distributed sites, perhaps employing information dispersal techniques as suggested in section 1.3. Some of these sites may be operated by other SSPs, who in turn may have their own motivations to reduce cost, legitimate or otherwise. If a site knows that its occasional outage will be overlooked (indeed, planned for) due to the presence of its replication peers, it may opt to increase its frequency of "outages" by placing a fraction of files on lower tiers—or not storing them at all. (This is akin to the "freeloading" threat described by Lillibridge et al. for peer-to-peer storage systems.)

Another reason a malicious SSP may corrupt or delete certain files (or portions of them) is their content. Encryption partially mitigates this threat since an SSP does not directly know the content of encrypted files, but it may still be possible for other parties to inform the SSP by back channels of which files to "misplace," or to cause the misplacement themselves by physical attack. E-discovery of documents is one scenario motivating these concerns.

Equipment failures and configuration errors may also result in file placement that does not meet an SLA; the breach of agreement may simply be due to negligence, not malice.

One way for a client to obtain assurance that a file can be accessed at a given service level, of course, is for the client actually to access the file from time to time. Indeed, file access would be part of a typical "fire drill" operation for disaster recovery testing. If randomly chosen files are accessible at a given service level, then it is reasonable to assume that other files will be accessible as well. However, the highest assurance for a specific file requires access to the file itself.

We envision that a POR scheme would be applied to a storage service as follows. As part of its SLA, an SSP would offer periodic, unannounced execution of a POR for selected files. In the POR, a block would be considered to be an erasure if it cannot be read within the agreed response time (after accounting for variations in network latency, etc.). The client, taking the role of verifier, would thereby obtain (probabilistic) assurance that the agreed service level continues to be met for the file. If the SSP is trusted to provide file integrity, then an erasure code would be sufficient for error correction.

A POR scheme can also be applied by a third party to obtain assurance that files are accessible (as also observed in [37]). For instance, an auditor may wish to verify that an SSP is meeting its SLAs. To ensure that the POR corresponds to a file actually submitted for storage, the auditor would rely on the client to provide a storage "receipt" including the keys the verification operations. (The key for decrypting the file need not be provided—thus enforcing privilege separation between the auditor and the client.) As another example, one party's legal counsel may wish to verify that an archive stored at an SSP correctly corresponds to a document manifest submitted by another party. The separation of encryption and verification enables the legal counsel (and the court) to verify that the other party has met a requirement to archive a collection of files, without yet learning the content of those files—and, due to the POR, without having to access every block in every file.

5 Conclusion

Thanks to its basis in symmetric-key cryptography and efficient error-coding, we believe that our sentinel-based POR protocol is amenable to real-world application. As storage-as-a-service spreads and users rely on external agents to store critical information, the privacy and integrity guarantees of conventional cryptography will benefit from extension into POR-based assurances around data availability. Contractual and legal protections can, of course, play a valuable role in laying the foundations of secure storage infrastructure. We believe that the technical assurances provided by PORs, however, will permit even more rigorous and dynamic enforcement of service policies and ultimately enable more flexible and cost-effective storage architectures.

Our introduction of PORs in this paper leads to a number of possible directions for future research. One broad area of research stems from the fact that our main POR protocol is designed to protect a *static* archived file F. Any naïvely performed, partial updates to F would undermine the security guarantees of our protocol. For example, if the verifier were to modify a few data blocks (and accompanying error-correcting blocks), the archive could subsequently change or delete the set of modified blocks with (at least temporary) impunity, having learned that they are not sentinels. A natural question then is how to construct a POR that can accommodate partial file updates—perhaps through the dynamic addition of sentinels or MACs.

Another important vein of research lies with the implementation of PORs. We have described a host of design parameters, modeling choices, and protocol variants and tradeoffs. Sorting through these options to achieve an efficient, practical POR system with rigorous service assurances remains a problem of formidable dimensions.

Acknowledgments

Thanks to Guy Rothblum, Amin Shokrollahi, and Brent Waters for their helpful comments on this work.

References

1. Amazon.com. Amazon simple storage service (Amazon S3), 2007. Referenced 2007 at aws.amazon.com/s3.
2. A. Shokrollahi. Raptor codes. *IEEE Transactions on Information Theory*, 52(6):2551–2567, 2006.
3. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores, 2007. To appear.
4. R. Bazzi and Y. Ding. Non-skipping timestamps for Byzantine data storage systems. In R. Guerraoui, editor, *DISC '04*, pages 405–419. Springer, 2004. LNCS vol. 3274.
5. M. Bellare and O. Goldreich. On defining proofs of knowledge. In E.F. Brickell, editor, *CRYPTO '92*, pages 390–420. Springer, 1992. LNCS vol. 740.
6. M. Bellare and A. Palacio. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In M. Franklin, editor, *CRYPTO '04*, pages 273–289. Springer, 2004. LNCS vol. 3152.
7. J. Black and P. Rogaway. Ciphers with arbitrary finite domains. In B. Preneel, editor, *CT-RSA '02*, pages 114–130. Springer, 2002. LNCS vol. 2271.
8. M. Blum, W. S. Evans, P. Gemmell, S. Kannan, and M. Naor. Checking the correctness of memories. *Algorithmica*, 12(2/3):225–244, 1994.
9. C. Cachin and S. Tessaro. Asynchronous verifiable information dispersal. In *Reliable Distributed Systems (SRDS) '05*, pages 191–202, 2005.
10. C. Cachin and S. Tessaro. Optimal resilience for erasure-coded Byzantine distributed storage. In *DSN '06*, pages 115–124, 2006.
11. D.E. Clarke, G.E. Suh, B. Gassend, A. Sudan, M. van Dijk, and S. Devadas. Towards constant bandwidth overhead integrity checking of untrusted data. In *IEEE S & P '05*, pages 139–153, 2005.
12. B.F. Cooper and H. Garcia-Molina. Peer to peer data trading to preserve information. *ACM Trans. Inf. Syst.*, 20(2):133–170, April 2002.
13. C. Dwork, A. Goldberg, and M. Naor. On memory-bound functions for fighting spam. In D. Boneh, editor, *CRYPTO '03*, pages 426–444. Springer, 2003. LNCS vol. 2729.
14. IDC. J.F. Gantz et al. *The Expanding Digital Universe: A Forecast of Worldwide Information Growth through 2010*, March 2007. Whitepaper.
15. J. Feldman. Using many machines to handle an enormous error-correcting code. In *IEEE Information Theory Workshop (ITW)*, 2006. Referenced 2007 at http://www.columbia.edu/$\mathcal{S}$jf2189/pubs/bigcode.pdf.
16. D.L.G. Filho and P.S.L.M. Barreto. Demonstrating data possession and uncheatable data transfer, 2006. IACR eArchive 2006/150. Referenced 2007.
17. O. Goldreich. Randomness, interactive proofs, and zero-knowledge–a survey. In *A Half-Century Survey on The Universal Turing Machine*, pages 377–405. Oxford University Press, 1988.
18. S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. *SIAM J. Comput.*, 18(1):186–208, 1989.
19. P. Golle, S. Jarecki, and I. Mironov. Cryptographic primitives enforcing communication and storage complexity. In M. Blaze, editor, *Financial Cryptography '02*, pages 120–135. Springer, 2002. LNCS vol. 2357.
20. P. Golle and I. Mironov. Uncheatable distributed computations. In D. Naccache, editor, *CT-RSA '01*, pages 425–440. Springer, 2001. LNCS vol. 2020.
21. M. Jakobsson and A. Juels. Proofs of work and bread pudding protocols. In B. Preneel, editor, *Communications and Multimedia Security*, pages 258–272. Kluwer, 1999.
22. V. Kher and Y. Kim. Securing distributed storage: Challenges, techniques, and systems. In *StorageSS '05*, pages 9–25. ACM, 2005.
23. E. Kushilevitz and R. Ostrovsky. Replication is not needed: Single database, computationally-private information retrieval. In *FOCS '97*, pages 364–373. IEEE Computer Society, 1997.
24. L. Lamport. On interprocess communication. Part II: Algorithms. *Distributed Computing*, 1(2):86–101, 1986.
25. M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard. A cooperative Internet backup scheme. In *USENIX Annual Technical Conference, General Track 2003*, pages 29—41, 2003.
26. H. Lipmaa. An oblivious transfer protocol with log-squared communication. In J. Zhou and J. Lopez, editors, *Information Security Conference (ISC) '05*, pages 314–328. Springer, 2005. LNCS vol. 3650.
27. M. Liskov, R.L. Rivest, and D. Wagner. Tweakable block ciphers. In M. Yung, editor, *CRYPTO '02*, pages 31–46. Springer, 2002. LNCS vol. 2442.

28. M. Luby and C. Rackoff. How to construct pseudorandom permutations and pseudorandom functions. *SIAM J. Comput.*, 17:373–386, 1988.
29. D. Malkhi and M.K. Reiter. An architecture for survivable coordination in large distributed systems. *IEEE Transactions on Knowledge and Data Engineering*, 12(2):187–202, 2000.
30. J.-P. Martin, L. Alvisi, and M. Dahlin. Minimal Byzantine storage. In *DISC '02*, pages 311–325. Springer, 2002. LNCS vol. 2508.
31. M. Naor and G. N. Rothblum. The complexity of online memory checking. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 573–584, 2005.
32. E. St. Pierre. ILM: Tiered services and the need for classification. In *Storage Networking World (SNW) '07*, April 2007. Slide presentation.
33. M. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *JACM*, 36(2):335–348, April 1989.
34. R. Rivest. The pure crypto project's hash function. Cryptography Mailing List Posting. Referenced 2007 at http://diswww.mit.edu/bloom-picayune/crypto/13190.
35. P. Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In P.J. Lee, editor, *ASIACRYPT '04*, pages 16–31. Springer, 2004. LNCS vol. 3329.
36. K. Sakurai and T. Itoh. On the discrepancy between serial and parallel of zero-knowledge protocols (extended abstract). In E.F. Brickell, editor, *CRYPTO '92*, page 246259. Springer, 1992. LNCS vol. 740.
37. M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan. Auditing to keep online storage services honest, 2007. Presented at HotOS XI, May 2007. Referenced 2007 at http://www.hpl.hp.com/personal/Mehul_Shah/papers/hotos11_2007_shah.pdf.
38. X. Shen, A. Choudhary, C. Matarazzo, and P. Sinha. A multi-storage resource architecture and I/O performance prediction for scientific computing. *J. Cluster Computing*, 6(3):189–200, July 2003.
39. R. Sion and B. Carbunar. On the computational practicality of private information retrieval. In *Network and Distributed Systems Security Symposium (NDSS) '07*, 2007. To appear.
40. M. Yung. Zero-knowledge proofs of computational power (extended summary). In J.J. Quisquater and J. Vandewalle, editors, *EUROCRYPT '89*, pages 196–207. Springer, 1989. LNCS vol. 434.

A Proofs

For simplicity, we make ideal assumptions on our underlying cryptographic primitives. We assume an ideal cipher, a one-way permutation instantiated as a truly random permutation, and a PRNG instantiated with truly random outputs. Given well-constructed primitives, these ideal assumptions should not impact our security analysis in a practical sense. Viewed another way, we assume parameterizations of our cryptographic primitives such that the probability of an adversary distinguishing their outputs from suitable random distributions is negligible. The error terms in our theorems should therefore be small. (In a full-blown proof, we would create a series of games/simulators that replace primitives incrementally with random distributions.)

This ideal view yields a system in which block values are distributed uniformly at random in the view of the adversary. Thus the adversary cannot distinguish between blocks corresponding to message values and those corresponding to sentinels, and cannot determine which blocks are grouped in chunks more effectively than by guessing at random.

Additionally, in this model, because $\mathcal{A}$("respond") is assumed to be stateless, i.e., subject to rewinding, the verifier can make an arbitrary number of queries on a given block. These queries are independent events, i.e., for a given block at location i, the probability $p(i)$ that $\mathcal{A}$("respond") responds correctly is equal across queries. Hence we can model the adversary $\mathcal{A}$("respond") as a probability distribution $\{p(i)\}$ over blocks in the archived file.

We also, as explained above, adopt our simplifying block-isolation assumption for our proofs.

Furthermore, if $p(i)$ is non-negligibly greater than $1/2$ (for convenience, we choose $p(i) \geq 3/4$, but any bound $> 1/2$ would do), it is possible for an extractor to recover block i with overwhelming probability via majority decoding after a modest number of queries. Thus, we can simplify our model still further. Once we have bounded out the probability of the adversary failing to retrieve a block i with $p(i) \geq 3/4$, we may think effectively of $\mathcal{A}$("respond") in our ideal model as a collection of

"bins," each corresponding to a given block i. The adversary is modeled as corrupting a block by throwing a "ball" into the corresponding bin. If a bin contains a ball, then we assume $p(i) < 3/4$, and thus that the corresponding block is not retrievable. If a bin doesn't contain a ball, the corresponding block is retrievable. (If we restrict our attention to deterministic adversaries, then we have a further simplification: $p(i) = 1$ if the block is retrievable, $p(i) = 0$ if corrupted / deleted.)

Let us define b'' as the total number of data blocks and previously unused sentinels; thus, $b'+q \leq b'' \leq b'+s$. Recall that we define ϵ as the fraction of the b'' such blocks corrupted by the adversary. In the ball-and-bin view, therefore, the adversary throws a number of balls $\leq \epsilon b''$ into the b'' bins representing this aggregate of blocks. Provided that no chunk receives too many balls, i.e., provided that no chunk of n error-correcting blocks in a codeword has more than $d/2$ corruptions, extract can recover the file F completely. We use the ball-and-bin model to achieve bounds on the probability of success of extract. We also use the model to bound the probability of detecting adversarial corruption of F.

As the only adversarial function we refer to explicitly in our proofs is $\mathcal{A}$("respond"), we write $\mathcal{A}$ for conciseness.

Block-isolation assumption: We assume that, during the respond operation, the probabilities that the individual blocks returned by the prover are correct are independent of one another. For example, we exclude adversaries who return correct values for all the blocks simultaneously with some probability $p < 1/2$. In such a case, verification would succeed with probability p, but the file would almost always be unretrievable. This is a natural extension of the statelessness of the adversary: Not only does the adversary not remember from one challenge to the next, but it does not remember from one block to the next whether it has responded correctly. The extractor can thus "rewind" query by query within a challenge, as well as challenge by challenge. Put another way, we can assume that queries are made in serial, rather than in parallel, and that the adversary is rewound between each one. This brings to mind past discussions about the distinctions between serial and parallel zero-knowledge protocols (e.g., [36]). The block-isolation assumption is the basis for our use of the ball-and-bin model.

A.1 Bounding lemmas

We begin with some technical lemmas to establish bounds within our ball-and-bin model. The lynchpin of these lemmas is the well-known Chernoff probability bounds on independent Bernoulli random variables, as expressed in the following lemma.

Lemma 1 (Chernoff Bounds). *Let $X_1, X_2, \ldots, X_N$ be independent Bernoulli random variables with $\mathsf{pr}[X_i = 1] = p$. Then for $X = \sum_{i=1}^{N} X_i$ and $\mu = E[X] = pN$, and any $\delta \in (0, 1]$, it is the case that $\mathsf{pr}[X < (1-\delta)\mu] < e^{-\mu\delta^2/2}$ and for any $\delta > 0$, it is the case that $\mathsf{pr}[X > (1+\delta)\mu] < (e^{\delta}/(1+\delta)^{1+\delta})^{\mu}$.*

Now let us consider a simple algorithm that we refer to as a *γ-query majority decoder*. It operates in two steps: (1) The decoder queries $\mathcal{A}$ on a given block i a total of γ times, receiving a set R of responses and then (2) If there exists a majority value $r \in R$, the decoder outputs r; otherwise it outputs $\perp$. For simplicity of analysis, we exclude the possibility of ties; i.e., we assume that γ is odd.

We state the following lemma without proof, as it follows straightforwardly from Lemma 1.

Lemma 2. *Let γ be an odd integer ≥ 1. The probability that a γ-*query majority decoder *operating over b' blocks correctly outputs every block i for which $p(i) \geq 3/4$ is greater than $1 - b'e^{-3\gamma/72}$.*

Our next lemma bounds the probability, given $\epsilon b''$ bins with balls, i.e., corrupted blocks, that any chunk is corrupted irretrievably.

Lemma 3. *Suppose $\epsilon b''$ (for $\epsilon \in [0, 1]$) balls are thrown into $b' < b'' \leq b'+s$ bins without duplication, i.e., with at most one ball per bin. Suppose further that the bins partitioned randomly into $C = b'/n$*

chunks, each comprising n distinct bins. Let $\mu = n\epsilon(b' + s)/(b' - \epsilon(b' + s))$. If $\mu < d/2$, then the probability that any chunk receives more than $d/2$ balls is less than $Ce^{(d/2-\mu)}(d/2\mu)^{-d/2}$.

Proof: Since balls are thrown without duplication, the maximum probability that a given chunk receives a ball is achieved under the condition that $\epsilon b''-1$ balls have already landed outside the chunk. Thus, the probability that a ball lands in a given chunk is less than $p = n/(b'-\epsilon b'') \leq n/(b'-\epsilon(b'+s))$.

The number of balls that lands in a given chunk is therefore bounded above by a Bernoulli process in which X_i is the event that the ith ball lands in the chunk, $p_i = p$, and $X = \sum_{i=1}^{\epsilon b''} X_i$, which in turn is bounded above by a process with $E[X] = \mu < n\epsilon(b' + s)/(b' - \epsilon(b' + s))$.

Now $\mathsf{pr}[X > d/2] = \mathsf{pr}[X > (1 + \delta)\mu]$ for $\delta = d/2\mu - 1$. By Lemma 1, we have $\mathsf{pr}[X > d/2] < e^{(d/2-\mu)}(d/2\mu)^{-d/2}$. Since there are C chunks, the lemma follows. ∎

Our next lemma offers a lower bound on the probability that the verifier detects file-corruption by $\mathcal{A}$ when at least an ϵ-fraction of bins contain balls, i.e., $\mathcal{A}$ responds incorrectly with probability greater than $1/4$ in each of an ϵ-fraction of data blocks and unused sentinels.

Lemma 4. *Suppose that $\epsilon b''$ (for $\epsilon \in [0, 1]$) balls are thrown into b'' bins without duplication. Suppose that $\mathcal{A}$ is queried on q bins, each chosen uniformly at random (and independently) and that $\mathcal{A}$ provides an incorrect block with probability $> 1/4$ if a bin contains a ball. Then the probability that $\mathcal{A}$ provides at least one incorrect block is greater than $1 - (1 - \epsilon/4)^q$.*

Proof: Let X_i be a Bernoulli random variable s.t. $X_i = 1$ if $\mathcal{A}$ provides an incorrect block on the ith query. Since a bin contains a ball with probability ϵ, and a bin with a ball corresponds to a block incorrectly emitted by $\mathcal{A}$ with probability greater than $1/4$, $\mathsf{pr}[X_i = 0] < 1 - \epsilon/4$. It is easy to see that $\mathsf{pr}[X_i = 0 \mid X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_q = 0] \leq \mathsf{pr}[X_i = 0]$. Therefore $\mathsf{pr}[X = 0] < (1 - \epsilon/4)^q$. ∎

A.2 Main theorem

We state the following theorem about our sentinel-based practical scheme $\mathsf{Sentinel\text{-}PORSYS}[\pi]$:

Theorem 1. *Suppose that $\gamma \geq 24(j \ln 2 + \ln b')$. For any $\epsilon \in (0, 1)$ such that $\mu < d/2$ where $\mu = n\epsilon(b'+s)/(b'-\epsilon(b'+s))$, $\mathsf{Sentinel\text{-}PORSYS}[\pi]$ is a (ρ, λ)-valid POR for $\rho \geq Ce^{(d/2-\mu)}(d/2\mu)^{-d/2}$ and $\lambda \geq (1 - \epsilon/4)^q$.*

Proof: Consider a given value of ϵ in our balls-and-bins model. By Lemma 4, the probability for this value of ϵ that $\mathcal{A}$ causes the verifier to accept is less than $(1 - \epsilon/4)^q$. Accordingly, the POR is λ-valid for any $\lambda \geq (1 - \epsilon/4)^q$ for this ϵ. (To achieve a higher bound would require a smaller value of ϵ.)

Given this value of ϵ, by Lemma 2, the probability of recovering correct values for all blocks that have not received balls is at least $1 - \zeta$ for $\zeta < b'e^{-3\gamma/72}$. For $\gamma \geq 24(j \ln 2 + \ln b')$, we have $\zeta < 2^{-j}$, which is negligible (indeed, exponentially small) in j.

Assuming, then that no chunk has received more than $d/2$ balls, the verifier can recover data associated with every chunk of the file. By Lemma 3, this condition fails to hold with probability at most $Ce^{(d/2-\mu)}(d/2\mu)^{-d/2}$. (Lemma 3 assumes that the balls are thrown only at data blocks; this is the worst case for interdependence between ρ and λ, occurring when none of the balls hits sentinels.) Thus the POR is simultaneously ρ-valid for any $\rho < Ce^{(d/2-\mu)}(d/2\mu)^{-d/2}$ for this ϵ. ∎