Reimagining Secret Sharing: Creating a Safer and More Versatile Primitive by Adding Authenticity, Correcting Errors, and Reducing Randomness Requirements

Abstract:
Aiming to strengthen classical secret-sharing to make it a more directly useful primitive for human end-users, we develop definitions, theorems, and efficient constructions for what we call adept secret-sharing. Our primary concerns are the properties we call privacy, authenticity, and error correction. Privacy strengthens the classical requirement by ensuring maximal confidentiality even if the dealer does not employ fresh, uniformly random coins with each sharing. That might happen either intentionally—to enable reproducible secret-sharing—or unintentionally, when an entropy source fails. Authenticity is a shareholder’s guarantee that a secret recovered using his or her share will coincide with the value the dealer committed to at the time the secret was shared. Error correction is the guarantee that recovery of a secret will succeed, also identifying the valid shares, exactly when there is a unique explanation as to which shares implicate what secret. These concerns arise organically from a desire to create general-purpose libraries and apps for secret sharing that can withstand both strong adversaries and routine operational errors.

Keywords: Adept secret-sharing, computational secret sharing, cryptographic definitions, secret sharing

DOI 10.2478/popets-2020-0082
Received 2020-02-29; revised 2020-06-15; accepted 2020-06-16.

1 Introduction

Overview. This paper strengthens classical secret-sharing [17, 40] to obtain a primitive we call adept secret-sharing (ADSS). Our initial reason for developing ADSS was to address use cases involving journalists and whistleblowers. We were motivated by a conversation with journalist Laurent Richard [22, 36], by the Snowden revelations [24], and by the development of Sunder [39]. We recognized that unadorned Shamir secret-sharing [40] wouldn’t do; for example, garbage would be recovered if a share got accidentally corrupted, and a strong adversary could force recovery of whatever secret it wanted by adjusting a single share. We set out to develop a primitive that would guarantee more. It would need to be versatile, easy to understand, and support efficient and provably secure realizations.

Our approach is definitionally focused. Modern cryptography has taught that stronger definitions lead to conforming schemes that are easier to correctly use, so less prone to misuse. Our definitions are motivated by use cases, although no one use case fully motivates all of our demands. This is customary. By way of analogy, no application we know requires the full strength of IND-CCA public-key encryption [34], yet this has become the accepted definitional target because it implies other properties, such as nonmalleability [19], that are useful in numerous settings. We strive to create definitions that can play the same role for secret sharing that IND-CCA plays for public-key encryption.

Sample use case. To start to appreciate why new definitions are needed, let us consider a realistic but fictitious use case. German journalist D is visiting New York when a source hands him a thumb drive of shocking, classified files. D transfers the archive to his laptop, encrypts it with a strong passphrase, and destroys the thumb drive. D now wants to return to Berlin with these materials, but fears he will be detained, or worse, before he can publish. D mustn’t have the sensitive plaintext on him at border crossings, where phone and laptop contents may be copied by authorities.

To ensure that the material gets out no matter what, D decides to give the encrypted archive and a share of its decryption key to colleagues A, B, and C. He intends that any two parties can reconstruct the archive. D decides it would be safest to meet A at the Newark airport, B at the Icelandair lounge where D will transit, and to send C her materials over Signal.

To begin, D needs to generate a share \( c \) of his passphrase for C. But the way secret-sharing schemes generate shares is probabilistic: fresh coins are chosen
Reimagining Secret Sharing

with each sharing. So it would seem that D will need to retain A’s share $a$ until he meets A in Newark, and must retain B’s share $b$ all the way to Iceland. But this is no good, for keeping $a$ and $b$ on the laptop along with the encrypted achieve is equivalent to keeping the archive as plaintext. A better choice might be to retain the coins that generated the shares, using them, and the passphrase, to regenerate $a$ or $b$ only when they are needed. But it is unclear what security properties secret sharing will have if an attacker learns retained coins. With Shamir secret-sharing, acquiring them (e.g., by confiscating the device) along with any one share (say $c$) enables reconstruction of the secret. In any case, D needs to use off-the-shelf tools, which, quite correctly, do not support the retention of coins used for share generation.

The scenario motivates reproducible secret-sharing: the ability to recompute a share, or a vector of shares, as long as you still have the secret.

Continuing our example, we must report that, soon after his arrival, D mysteriously vanished in Berlin. Meanwhile, A fell ill with COVID-19. Parties B and C nervously converge in Iceland. Unfortunately, C’s smartphone had already been hacked by a state intelligence agency, her share $c$ quietly replaced by $\tilde{c}$. When B and C reconstruct the passphrase and use it to decrypt, the plaintext looks fine—parties B and C don’t know that anything is wrong—but the archive is less important than they anticipated. It is not the original one. This is possible, at least in principle, because, with classical secret-sharing, if someone can control a single share, they may be able to control the secret that is recovered, even without knowing other shares. Nothing in the classical secret-sharing definition excludes this. This possibility motivates another non-standard aim: authenticity.

It guarantees that recovery using a share either fails or recovers the secret originally associated to it. Schemes like Shamir’s achieve nothing like this.

Finally, as an alternative continuation of our story, party A, now recovered, meets up with B and C in Iceland. Party C’s share is still wrong. When A, B, and C contribute their shares $a, b, \tilde{c}$ for recovery, a classical secret-sharing scheme (like Shamir’s) will recover something—but something wrong. This time, the recovered archive looks like random bits. The shareholders know that something went wrong, but they don’t know what. If they had the insight to try recovery again without using C’s share $\tilde{c}$ they would recover the correct secret. But they don’t know to do this. How much nicer it would be if the recovery algorithm itself would have said: “look, share $\tilde{c}$ was bad, but shares $a$ and $b$ were fine, and implicated the following passphrase.” A scheme like that enjoys error correction. Our formalization strengthens robustness [15, 31], which would actually be sufficient for this example (but not, say, for 2-of-4 secret sharing).

We use the labels Auth (authenticity), Errx (error correction), and Priv (privacy) for our main goals (the last of these encompassing reproducibility). Fig. 1 provides a single-sentence description of each. Fig. 2 summarizes definitional choices and their rationale more broadly. As that figure makes clear, we have taken clues from multiple directions—not just use cases—as to what characteristics an ADSS scheme should enjoy.

Enhanced syntax. ADSS begins with an enriched syntax, over which the security notions above can be defined. Let us start by taking a look at the new syntax.

Unlike a classical secret-sharing scheme, the sharing algorithm of an ADSS scheme is deterministic, surfacing an input $R$ that captures the provided coins. This enables reproducibility (described above) and hedging (described later). The sharing algorithm also takes in a description of an access structure—the specification of which sets of shareholders are authorized—rather than being specific to one. This enables runtime selection of the access structure and for the access structure itself to be authenticated being crucial for security. Finally, the sharing algorithm now takes in a string of associated data (AD), analogous to that seen in schemes for authenticated encryption. Moving on, the recovery algorithm of an ADSS scheme no longer operates on vectors of shares, but on sets of shares [2]. This better models the coming together of human participants who have only their shares. And the algorithm not only returns the original secret, but also identifies which shares were deemed to be valid. This allows a shareholder to reject...
a recovered secret if she has confidence in her own share but it was not deemed valid. As for the shares themselves, the access structure and AD must be encoded in each, to ensure that no side information needs be known by the recovering party. And shares can have separate secret and non-secret parts, so that shareholders need only keep the first in private storage. This enables the sharing of arbitrarily long secrets even when shareholders are only able to privately store a limited amount. The syntactic changes just sketched may seem low-level but are fundamental in enabling the capabilities we seek.

**Enhanced security.** A journalist could certainly share her documents using Shamir secret-sharing [40]. This provides privacy. But as our extended example illustrates, the adversary may have other goals in mind, like disrupting recovery, either by making it fail or by making shareholders recover something other than that which the dealer shared. The adversary can attempt to achieve this goal by infiltrating a shareholder’s system (something nation-state adversaries are good at) and changing her share. It can create entirely new shareholders that show-up for reconstruction. We want to defend against such attacks to the maximal extent possible. To do so, we develop Auth and Errx.

**Authenticity (Auth),** which we alternatively term binding, ensures that when a user is given a share $S$, ...
there is at most one secret \( M \) for which it might be a share. The share is effectively a commitment to that secret. A shareholder can thus regard her share as a locked box containing some well-defined secret that she does not yet know. (We do allow that if the dealer was dishonest then nothing might be in that box.) In short, authenticity concretizes the basic intuition that a share is associated to some one particular thing.

Error correction (Errx) ensures that if some shares from a sharing of a secret get corrupted, or new shares are added, but there remains a single nontrivial explanation as to what the secret must have been before the shares got messed up, then the recovery process must identify that one correct secret. It must also indicate which shares implicate it. Recovery must fail if there is no authorized subset of shares, or if there are two or more explanations for what got corrupted. In short, an Errx-secure scheme must fix what is fixable, and must indicate if shares irreparably messed up.

Auth and Errx are different from verifiable secret-sharing (VSS) [18]. VSS requires a reliable broadcast channel, which may not be available; Auth and Errx do not. Errx is related to but different from robustness [15, 31], which aims to guarantee message recovery despite the presence of some bad shares shuffled in among an authorized collection of good ones. Errx formalizes different intuition: that recovery does the best job possible with whatever is presented. For this reason, Errx is achievable for any access structure, while robustness is achievable for threshold schemes with honest majority, but little more. Errx demands that nothing be recovered when there is no authorized subset of shares, will robustness requires nothing. All of that said, Errx security does imply robustness whenever the latter can be achieved. Auth and Errx have little in common with repairable threshold schemes [25, 32], which allow a party to reconstruct a missing share by interacting with fellow shareholders. In scenarios we care about, shareholders may not have the ability to interact with one another prior to recovery. See Section A for fuller comparisons with VSS, robustness, and repairability.

Enhanced usability. Our ADSS schemes employ hedging [5], using the anticipated unpredictability of the secret itself, together with the entropy in the provided coins, to provide as much privacy as possible. This means that privacy is maintained, to the extent possible, in settings where high-quality randomness is unavailable or was inadequately harvested. At the same time, the approach provides for reproducibility, enabling the dealer, if it so arranges, to re-share a secret \( M \) and get the same shares as before. Other ADSS elements that enhance usability include: the ability to handle AD, having the recover algorithm operate on sets instead of vectors of shares; and the capacity to deal with enormous secrets, as we now discuss.

Protocols and proofs. We construct simple, efficient, and provably secure ADSS schemes for arbitrary access structures. Our schemes can be used for splitting anything from a PIN code to a huge archive of files (the Panama papers were 2.6 terabytes [26]). In sharing out a large archive one needn’t encrypt it and then share out the key; the user can regard the archive itself as the secret, which is conceptually and operationally simpler.

Our constructions begin with a scheme \( S_1 \) that satisfies our ADSS syntax but only achieves Priv\$ security with uniformly random coins—what we call classical privacy, or Priv\$\$. The scheme only works for threshold access structures. It is basically just Shamir’s scheme [40], but adapted to our syntax. Scheme \( S_2 \) still achieves only Priv\$ privacy, but can handle any access structure, now presented as a circuit of threshold gates. Despite the classical aim, we could find no full exposition or proof on how to carry out secret sharing for arbitrary access structures; our paper fills this gap.

Our main construction is the transformation AX that converts a secret-sharing scheme \( S \) that achieves only classical (Priv\$) privacy to a scheme \( SS = AX[S] \) that achieves Priv and Auth security. This can then be composed with a further transformation, EX, to achieve Errx security. Rather roughly, AX starts by symmetrically encrypting the secret \( M \) to the ciphertext \( C \), which is put in the public portion of each share. The key \( K \) for this encryption is determined by applying a hash function to all inputs the sharing algorithm gets. The hash function is here used as a randomness extractor [33]. The lower-level secret-sharing scheme \( S \) shares out \( K \) using randomness that is again extracted from the inputs to \( S \). When speculative values are recovered, a correctness check is done to see if re-sharing \( M \) with the recovered randomness \( R \) gives rise to a superset of the shares received. Schemes \( SS_1 \) and \( SS_2 \) are the result of applying AX and then EX to \( S_1 \) and \( S_2 \). They are the concrete ADSS schemes that we propose.

Discussion. Kacsmar, Komlo, Kerschbaum, and Goldberg [29] also address gaps between the formulation and use of secret sharing. Their motivations are similar to ours: closing the theory/practice gulf in this domain. They employ the idea of ceremonies [20] and design a proactive VSS scheme [27] to achieve goals that they call
integrity and availability. Our work is more formal, and, in carrying it out, we have insisted on retaining the fundamental elements of the classical model: ADSS abides no broadcast channels, no interaction among shareholders, no preprocessing, no PKI (public-key infrastructure), and no algorithms but Share and Recover.

Secret sharing can be viewed as a flavor of encryption [15]: sharing corresponds to encryption; recovery corresponds to decryption. From this vantage, the move from classical to adept secret-sharing mirrors the move from semantically secure to authenticated encryption [11, 13, 30], as well as the move from probabilistic to deterministic [4, 8] and hedged [5] public-key encryption. Strengthening of secret sharing that begins by surfacing for format-preserving encryption [12]. In addition, the ministic and searchable public-key encryption [4] and ministic scheme. Similar tradeoffs are present for deter-

reproducibility; we merely enable it. If the dealer uses privacy for low-entropy secrets. But we never mandate randomness. We trade internal randomness for an externally supplied input [38]. We add in AD [37]. Of course there are spots where the analogy breaks down: secret sharing involves no keys, while access structures were outside the ambit of encryption prior to ABE [23]. Still, the analogy explains many aspects of our work.

Reproducibility comes at the price of diminished privacy for low-entropy secrets. But we never mandate reproducibility; we merely enable it. If the dealer uses random coins she gets classical privacy; if she wires in a constant, she gets best possible privacy for a deterministic scheme. Similar tradeoffs are present for deterministic and searchable public-key encryption [4] and for format-preserving encryption [12]. In addition, the strengthening of secret sharing that begins by surfaced the coins includes other benefits, like hedging.

The value of new definitions is always somewhat speculative. Our definitional choices have been guided by uses cases, by analogies, and by conversations with developers, journalists, whistleblowers, and cryptographers. But only time will tell if we have identified the secret-sharing aims that can precipitate a flourishing.

2 Preliminaries

Notation. Fig. 3 summarizes the most frequently used notation in this paper. The table may serve as a reference or overview of things to come.

Access structures. We need a way to specify which parties are authorized to reconstruct the secret. Number parties $1, 2, \ldots, n$. We then define an access structure $A$ as a set of sets of positive numbers. It must be finite, nonempty, and exclude the empty set. Define $n(A)$,

the number of parties in $A$, as the least $n$ such that $U \subseteq [1..n]$ for all $U \in A$. We say that $U \subseteq [1..n(A)]$ is authorized if $U \in A$ and unauthorized if $U \not\in A$. We re-

\[
\begin{align*}
\{0, 1\}^* & \quad \text{Set of all strings over } \{0, 1\} \\
\{0, 1\}^{\geq} & \quad \text{Set of all vectors (lists) of strings} \\
\{\ldots\} & \quad \text{A string encoding of what’s in the brackets} \\
1..n & \quad \text{Indicates invalidity: no secret can be recovered} \\
\text{Integers between } 1 \text{ and } n \text{ inclusive} & \quad \text{Integers between } 1 \text{ and } n \text{ inclusive} \\
\text{Sample, then assign. Uniform dist if } X \text{ a set} & \quad \text{Sample, then assign. Uniform dist if } X \text{ a set} \\
A & \quad \text{A string that names an access structure} \\
\text{An access structure: a set of subsets of } [1..n(A)] & \quad \text{An access structure: a set of subsets of } [1..n(A)] \\
\text{An adversary} & \quad \text{An adversary} \\
\text{Access-structure naming function} & \quad \text{Access-structure naming function} \\
\text{Set of strings that name access structures} & \quad \text{Set of strings that name access structures} \\
\text{A’s advantage breaking Auth-security of } S & \quad \text{A’s advantage breaking Auth-security of } S \\
\text{A’s advantage breaking Erx-security of } S & \quad \text{A’s advantage breaking Erx-security of } S \\
\text{A’s advantage breaking Priv-security of } S & \quad \text{A’s advantage breaking Priv-security of } S \\
\{\text{The set of all possible access structures}\} & \quad \{\text{The set of all possible access structures}\} \\
\text{Main authenticity property we formalize} & \quad \text{Main authenticity property we formalize} \\
\text{Transform to get } \text{Auth + Priv from Priv}$ & \quad \text{Transform to get } \text{Auth + Priv from Priv}$ \\
\text{The empty string} & \quad \text{The empty string} \\
\text{The error-correction property we formalize} & \quad \text{The error-correction property we formalize} \\
\text{Transform to get Erx security} & \quad \text{Transform to get Erx security} \\
\text{Set of things the recovering party might be sure of} & \quad \text{Set of things the recovering party might be sure of} \\
\text{Hash function, modeled as a random oracle} & \quad \text{Hash function, modeled as a random oracle} \\
\text{A secret shared out in a secret-sharing scheme} & \quad \text{A secret shared out in a secret-sharing scheme} \\
\text{Length of the string } M \text{ (in bits)} & \quad \text{Length of the string } M \text{ (in bits)} \\
\text{The set of possible secrets (messages)} & \quad \text{The set of possible secrets (messages)} \\
\text{Number of parties in the access structure } A & \quad \text{Number of parties in the access structure } A \\
\text{Set of all finite subsets of the set } X & \quad \text{Set of all finite subsets of the set } X \\
\text{The new privacy property we formalize} & \quad \text{The new privacy property we formalize} \\
\text{Classical privacy property. Weaker than Priv} & \quad \text{Classical privacy property. Weaker than Priv} \\
\text{Randomness / coins given to Share} & \quad \text{Randomness / coins given to Share} \\
\text{All possible coins (randomness)} & \quad \text{All possible coins (randomness)} \\
\text{A share. String-valued and have several parts} & \quad \text{A share. String-valued and have several parts} \\
\text{A vector of shares, } S = (S_1, \ldots, S_n) & \quad \text{A vector of shares, } S = (S_1, \ldots, S_n) \\
\text{The i-th entry of vector } S & \quad \text{The i-th entry of vector } S = (S[1], \ldots, S[i]) \\
\text{A set of shares, } S = \{S_1, \ldots, S_t\} & \quad \text{A set of shares, } S = \{S_1, \ldots, S_t\} \\
\text{Generic ADSS scheme } S = (\text{Access, Share, Recover}) & \quad \text{Generic ADSS scheme } S = (\text{Access, Share, Recover}) \\
\text{Access structure associated to share } S & \quad \text{Access structure associated to share } S \\
\text{Identity of party associated to share } S & \quad \text{Identity of party associated to share } S \\
\text{Non-secret part of share } S & \quad \text{Non-secret part of share } S \\
\text{Secret part of share } S & \quad \text{Secret part of share } S \\
\text{Tag (AD) part of share } S & \quad \text{Tag (AD) part of share } S \\
\text{Shamir-like SS scheme. Achieves Priv$} & \quad \text{Shamir-like SS scheme. Achieves Priv$} \\
\text{Yao-like SS scheme. Achieves Priv$} & \quad \text{Yao-like SS scheme. Achieves Priv$} \\
\text{Algorithm that recovers a secret} & \quad \text{Algorithm that recovers a secret} \\
\text{Algorithm that shares a secret} & \quad \text{Algorithm that shares a secret} \\
\text{All possible shares (which are strings)} & \quad \text{All possible shares (which are strings)} \\
\text{All possible vectors of shares} & \quad \text{All possible vectors of shares} \\
\text{All possible sets of shares} & \quad \text{All possible sets of shares} \\
\text{Tag (associated data) (a string)} & \quad \text{Tag (associated data) (a string)} \\
\text{The set of all possible tags (AD values)} & \quad \text{The set of all possible tags (AD values)} \\
\text{Maximal set of valid shares, } V \subseteq B & \quad \text{Maximal set of valid shares, } V \subseteq B
\end{align*}
\]

Fig. 3. Frequently used notation. Note that font styles for a given letter are routinely differentiated.
quire access structures be monotone, which means that an authorized set stays authorized if you add in parties: if $U \in A$ and $U \subseteq V \subseteq [1..n(A)]$ then $V \in A$.

An example access structures is the 2-out-of-3 one $A_{2,3} = \{(1,2), \{1,3\}, \{2,3\}, \{1,2,3\}\}$. More generally, for $1 \leq t \leq n$ the threshold access-structure $A_{n,t}$ is $\{U \subseteq [1..n] : |U| \geq t\}$. A secret-sharing scheme for such access structures is called a threshold scheme. A simple non-threshold access-structure is $A_{12,13} = \{(1,2), \{1,3\}, \{1,2,3\}\}$: party 1 and either party 2 or 3.

Classical secret-sharing. Let us briefly review the classical notion of a secret-sharing scheme—what a scheme like Shamir’s targets [17, 40]. One can formalize a classical secret-sharing scheme as a pair of algorithms $S = (Share, Recover)$ along with an associated access structure $A$, as follows:

- **Share** The sharing algorithm $Share$ probabilistically maps a message $M \in \text{Msg}$ to a vector (or list) of $n = n(A)$ shares, each of them a string: $S \leftarrow Share(M)$.
- **Recover** The recovery algorithm $Recover$ is a deterministic algorithm that takes in an $n$-vector of values, $n = n(A)$, each being either a string or the special symbol $\Diamond$, which is used to indicate that the share is missing. It returns a string $M \leftarrow Recover(S)$.

If $S = (S_1, \ldots, S_n)$ is an $n$-vector of strings and $U \subseteq [1..n]$, let $S_U$ be the $n$-vector with $i$th component $S_i$ if $i \in U$, and $\Diamond$ otherwise. So $S_U$ is $S$ with $\Diamond$-symbols shuffled in at positions outside of $U$. Then we require the following: if $S \leftarrow Share(M)$ and $U \in A$ then $Recover(S_U) = M$. In words: you can recover the secret from an authorized subvector of shares.

For any $M, M' \in \text{Msg}$ and any $U \not\in A$, we can regard $(Share(M))_U$ as a distribution on vectors of shares, the underlying randomness that of Share. The security notion for a classical secret-sharing scheme can then be formalized by asking that distributions $(Share(M))_U$ and $(Share(M'))_U$ be identical. In words: unauthorized subvectors of shares reveal nothing about the secret. If desired, this condition can be relaxed to computational indistinguishability or formalized in other ways [15, 31].

### 3 Syntax

**Changes.** We enrich the syntax of a classical secret-sharing scheme in multiple directions. First, the access structure $A$ won’t be fixed, but, instead, the party who shares a secret, the dealer, will be able to specify the access structure it wants. A string $A$ will denote the desired access structure, a function Acc specifying its interpretation. For example, the string “2,3” might denote the threshold access-structure $A_{2,3}$. Second, our sharing algorithm Share will have still more inputs. Beyond the access structure and the secret, the dealer will provide coins and associated data. With coins now an explicit input, the algorithm will be deterministic. Finally, the recovery algorithm Recover will output more: not only will it return the recovered secret, but also the shares that were used. Alternatively, it may recover nothing, outputting a special I-can’t-recover-anything symbol. We now make all of this precise.

**Formal definition.** We define a scheme for adept secret-sharing (ADSS) as a triple of deterministic functions $S = (Acc, Share, Recover)$, as follows.

- **Acc:** The access-structure naming function $Acc : Access \to A$ associates an access structure $A = Acc(A)$ with each string $A \in Access$. Here $Access = \{0,1\}^*$ (Kleene star) is the set of all binary strings, while $A$ is the set of all possible access structures. Note that there may be multiple ways to name an access structure under Acc: distinct strings $A$ and $A'$ such that $Acc(A) = Acc(A')$. Also, some access structures might be impossible to name using Acc: for some $A \in A$ there might be no $A \in Access$ with $Acc(A) = A$. For example, a secret-sharing scheme designed for threshold access structures won’t be able to request $\{(1,2), \{1,3\}, \{1,2,3\}\}$ (i.e., “1 and (2 or 3”).

- **Share:** The sharing algorithm $Share : Access \times \text{Msg} \times \text{Rand} \times \text{Tag} \to \text{Share}^*$ takes in a description $A \in Access$ of an access structure, a message (or secret) $M \in \text{Msg}$, some coins $R \in \text{Rand}$, and a tag (or associated data) $T \in \text{Tag}$. It outputs a vector of shares. Here $Msg, Access, Rand, Tag, Share \subseteq \{0,1\}^*$ are binary strings. We require that $M \in \text{Msg}$ implies $\{0,1\}^{|M|} \subseteq \text{Msg}$ and $R \in \text{Rand}$ implies $\{0,1\}^{|R|} \subseteq \text{Rand}$. The sharing algorithm must generate the appropriate number of shares for the specified access structure: $|Share(A, M, R, T)| = n(A)$ for all $A \in Access, M \in \text{Msg}, R \in \text{Rand},$ and $T \in \text{Tag}$: By $|\cdot|$ we denote the length, cardinality, or number of components for string, set, or vector.

- **Recover:** The message-recovery algorithm $Recover : \text{Shares} \to \text{Msg} \times \text{Shares} \cup \{\bot\}$ maps a set of shares $S \in \text{Shares} = \text{P}(\text{Share})$ to a message $M \in \text{Msg}$ and a set of valid shares $V \subseteq S$. Alternatively, the algorithm can decline to produce such a pair and
return \bot instead. By \( \mathcal{P}(X) \) we mean the finite power set of \( X \), the set of all finite subsets of \( X \). (The traditional power set of an infinite set such as \( \text{Share} = \{0, 1\}^* \) includes infinite subsets. We don’t want that, as one provide Recover, like any algorithm, a finite set of strings.) Note that Share returns a list of shares while Recover takes in a set of shares.

**Parts of a share.** We establish the convention that each share \( S \in \text{Share} \) is actually the encoding of five strings, \( S = (S.\text{id}, S.\text{as}, S.\text{sec}, S.\text{pub}, S.\text{tag}) \). We call the parts of a share its identity, access structure, secret portion, public portion, and \( \text{AD} \). We extend the \text{sec} and \text{pub} operators to vectors, defining \( S.\text{sec} = (S_1.\text{sec}, \ldots, S_n.\text{sec}) \) and \( S.\text{pub} = (S_1.\text{pub}, \ldots, S_n.\text{pub}) \) when \( S = (S_1, \ldots, S_n) \). We extend the \text{id} operator to sets, defining \( S.\text{id} = \{S.\text{id} : S \in \mathcal{S}\} \). We extend the access operator to sets, so that \( S.\text{as} = A \) if \( S.\text{as} = A \) for all \( S \in \mathcal{S} \), and \( S.\text{as} = \bot \) otherwise. We insist that \( S = \text{Share}(A, M, R, T) = (S_1, \ldots, S_n) \) implies that \( S_i.\text{tag} = T \) and \( S_i.\text{as} = A \) and \( S_i.\text{id} = i \) for all \( i \). Whenever Recover(\( S \)) returns a pair \((M, V)\) we demand that all shares in \( S \in \mathcal{V} \) share the same \text{as} component \( A \), the same \text{tag} component \( T \), and that \( V.\text{id} \in \text{Acc}(A) \), meaning the set of shareholders underlying \( V \) is authorized.

**Random oracles.** We allow the Share and Recover algorithms of an ADSS scheme may call an oracle hash that realizes a function \( H : \Omega \to \Omega \), where \( \Omega \) the set of all functions \( H : \mathbb{N} \times \{0, 1\}^* \to \{0, 1\}^* \) such that \( |H(t, X)| = t \). By \( \{0, 1\}^* = (\{0, 1\}^*)^* \) we denotes the space of vectors of strings. We can explicitly indicate the presence of the oracle or hash function that Share and Recover may access by writing it as a superscript.

**Basic correctness.** An ADSS scheme \( S = (\text{Acc}, \text{Share}, \text{Recover}) \) enjoys basic correctness if for all \( A \in \text{Access}, M \in \text{Msg}, R \in \text{Rand}, T \in \text{Tag}, H \in \Omega, S \leftrightarrow \text{Share}^H(A, M, R, T) \), and \( U \subseteq [1..n(\text{Acc}(A))] \),

- if \( U \in \text{Acc}(A) \) then Recover\(^H\)(\( S[U] \)) = \((M, S[U]) \),
- while if \( U \notin \text{Acc}(A) \) then Recover\(^H\)(\( S[U] \)) = \bot .

Here \( S[U] = \{S[i] : i \in U\} \) is the set of shares from parties \( U \). In words: applying Recover to a subset of shares obtained by sharing out \( M \) gives \( M \) if the subset is authorized and \( \bot \) if it is not. We henceforth require that all ADSS schemes satisfy basic correctness.

**Notation.** We write \( S.\text{Access} \), \( S.\text{Share} \), and \( S.\text{Recover} \) for the components of \( S \). In the same way, we write \( S.\text{Access} \), \( S.\text{Msg} \), \( S.\text{Rand} \), and \( S.\text{Tag} \).

**Discussion.** Once the decision has been reached to provide the access structure to Share it is tempting to just say that it’s encoded as a string \((A)\) and leave it at that. But more care needs to be taken because what access structures can be named, and how compactly, are central concerns of secret sharing. This is what motivates making \( \text{Acc} \) a first-class component of an ADSS scheme.

Let us give some examples of access-structure naming functions \( \text{Acc} \). For threshold schemes, a string \((n, t)\) encoding numbers \( n \) and \( t \) could name \( A_{n,t} \). It would be equally permissible, but less compact and convenient, to have \( \text{Acc} \) expect a string listing authorized sets, like \("\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\)". For a representation that is compact and expressive, the string \( A \) could encode a Boolean circuit of threshold gates having a single output wire and input wires \( 1, \ldots, n \). We’d say that \( U \in \text{Acc}(A) \) if the circuit named by \( A \) evaluates to true when its \( n \) inputs indicate if a party is present (that bit is 1) or absent (it is 0).

Having Recover take in a subset instead of a vector relieves shareholders of having to know their “position” in line. It also opens the door to authenticity notions where multiple parties can impersonate some shareholder.

While the \( \text{AD} \) of an ADSS scheme is analogous to that of an authenticated-encryption (AE) scheme, there are important differences. Our \( \text{AD} \) values are not assumed to be known by the party recovering a secret; an AE scheme’s \( \text{AD} \) value is. This follows the philosophical view that for secret sharing one should not require the receiver to know anything beyond what is in the shares.

The “public” portion of a share need not be public; we only mean that it is not a secret. The secret/public distinction matters most when the message being shared is long. We anticipate that most or all of the public portion of shares would be the same across all shares. When this is true, the public potion of shares might be kept in some highly available repository, rather than stored with each share.

Extensions to the syntax of Recover are described in Section 6, where we allow a priori information \( K \in \text{Known} \) to be input to Recover, and allow coins \( R \in \text{Rand} \) to be output by Recover.

A paper on VSS by Bai, Damgård, Orlandi, and Xia [2] employed some related syntactic choice. In particular, their Share algorithm takes in an access structure, assumed to be described by a circuit. But it is not authenticated, returned during recovery, or guaranteed to be dropped into shares. The “public share” \( S_0 \) that their Share algorithm outputs resembles the public portion of a share from our own treatment. But the former was ac-
The idea. One way to formalize privacy for a classical secret-sharing scheme captures this idea: if an adversary obtains an unauthorized set of shares, this will tell it nothing about the message beyond that which it already knows [15]. Achieving this requires fresh, high-entropy coins with each sharing. In their absence, all bets are off. Our formulation generalizes this idea, following the idea of hedging [5], so that the guarantee above continues to hold, to the maximum extent possible, even when the coins are not good. We ask that if an adversary obtains an unauthorized set of shares, this will tell it nothing about the message \( M \) as long as the \((M, R)\) pair was drawn from a set too large for the adversary to exhaust. Intuitively, this is the best possible, because if the adversary could exhaust this set then it could violate privacy by running the sharing algorithm on each candidate \((M, R)\) to see which results are consistent with the shares it has seen.

What is the benefit of all of this? First, it enables reproducible secret-sharing with meaningful privacy guarantees. For example, the random input \( R \) might be chosen at software-installation time, then supplemented by a counter with each sharing. Share regeneration is now possible, but even if the adversary does get hold of the device containing \( R \), privacy will be preserved as long as \( M \) itself is unpredictable and the adversary obtains only an unauthorized set of shares. For a classical secret-sharing scheme like Shamir’s that wouldn’t be true. A related benefit is for the sharing algorithm to work as well as possible in the presence of imperfect randomness. A cryptographic technique becomes safer to use when you can prove that it does not catastrophically fail when the randomness isn’t perfect.

**Definition.** Fix an adept secret-sharing scheme \( S \), an algorithm \( I \) called the input-selector, and an adversary \( A \) called the privacy adversary. Consider the \( G_{\mathbb{S}_1}^{\mathsf{Priv}}(A) \) game of Fig. 4. The Priv advantage of \( A \) relative to \( I \) is defined by

\[
\text{Adv}_{\mathbb{S}_1}^{\mathsf{Priv}}(A) = 2 \Pr[G_{\mathbb{S}_1}^{\mathsf{Priv}}(A)] - 1.
\]

We first explain the broad elements of the game, and then its fine points. The game picks a challenge bit \( c \) at random. The input-selector represents the dealer. It has a \( \text{Deal} \) oracle via which it provides a pair of message \( M_0, M_1 \in S.\text{Msg} \) that are required to be of the same length. It also provides an access-structure description \( A \in S.\text{Access} \) and a tag \( T \in S.\text{Tag} \). More unusually, it provides a string \( R \in S.\text{Rand} \) that will be the randomness used by \( S.\text{Share} \). The randomness is chosen by the input-selector, not the game. In response to a query \((A, M_0, M_1, T, R)\), oracle \( \text{Deal} \) creates a vector \( S_t \) of shares by running \( S.\text{Share} \), the message being either \( M_0 \) or \( M_1 \) depending on the challenge bit \( c \). The access structure and AD, and also the randomness, are taken from the query. The oracle may be called as often as the input-selector likes, but with the following non-repetition condition: if \((A, M_{0,1}, M_{1,1}, R_{1,1}T_{1})\), \ldots, \((A_{q}, M_{q,0}, M_{q,1}, R_q, T_q)\) are the queries made, then the tuples \((A_{1}, M_{1,0}, R_{1,1}T_{1})\), \ldots, \((A_{q}, M_{q,0}, R_q, T_q)\) are all distinct, and also the tuples \((A_{1}, M_{1,1}, R_{1,1}T_{1})\), \ldots, \((A_{q}, M_{q,1}, R_q, T_q)\) are all distinct. So for both \( c = 0 \) and \( c = 1 \), the inputs provided to Share will be distinct. This is necessary because, otherwise, Share being deterministic, an adversary could trivially discover the challenge bit \( c \).
The number of calls made is recorded in the variable \( q \). As per line 29, nothing is returned to the adversary in response to a DEAL query. This ensures that the inputs to DEAL are chosen non-adaptively, a choice we will discuss later. The output of \( I \) consists of state information \( St \), to be passed to its accomplice \( A \), and a \( q \)-vector \( B \) whose \( j \)-th component \( B[j] \) \( \subseteq [1..n(\text{Acc}(A[j]))] \), for each \( j \in [1..q] \), is a set of parties that the input-selector is corrupting, meaning \( I \) is requesting the corresponding set of shares \( S_1[B[j]], \ldots, S_q[B[q]] \) of the corrupted parties, as well as the public parts of all shares dealt. It also gets the random oracle \( H \), which was denied to \( I \). The privacy adversary returns its guess \( c' \) for the challenge bit \( c \) and wins (the game returns true) if this guess is correct.

Priv security is achievable only when the \((M_0, R)\), \((M_1, R)\) pairs in the DEAL queries of \( I \) are unpredictable, as we now formalize, following [4, 5, 8]. Game \( G_{1}^{\text{pred}}(P) \) of Fig. 4 measures the predictability of an input-selector \( I \) via another adversary \( P \) called a predictor. The input-selector \( I \) is executed with its DEAL oracle, the latter now simply recording the adversary queries: no secret sharing is done, and nothing is returned to the adversary. The predictor wins if it can predict (output) some secret-randomness pair that was returned by the adversary. Its input is that which we allow secret sharing to leak to the second stage: the access structures, tags, message lengths, which parties are corrupted, and the state returned by \( A \) in its first stage. The privacy-adversary \( A \) is not relevant here; unpredictability is a metric on the input-selector alone. We let

\[
\text{Adv}_{I}^{\text{pred}}(P) = \Pr[G_{1}^{\text{pred}}(P)] \quad \text{and} \quad \text{pred}(I) = \max_{P} \left\{ \text{Adv}_{I}^{\text{pred}}(P) \right\} .
\]

The notation reflects that \( I \) is the object whose security (in the sense of unpredictability) is being measured and \( P \) is the adversary. The max is over all predictor adversaries \( P \), regardless of their running time or the number of \( H \) queries they make. Thus \( \text{pred}(I) \) measures the information-theoretic guessing probability. The min-entropy of \( I \) could be defined as the negative log of this probability, but we do not need this.

Recovering classical privacy. Classical privacy corresponds to Priv security restricted to a class of input-selectors denoted \( \text{I}^{\text{priv}} \). An input-selector \( I \) is in this class if there is an input-selector \( I_{1} \) and an integer \( r \) such that \( I \) is defined as follows: it lets \((St, B) \leftarrow \text{DEAL}^{*} \) and returns \((St, B)\). Here \( \text{DEAL}^{*} \) is a subroutine defined by \( I \) as follows: On input a query \((A, M_0, M_1, R, T)\) made by \( I_{1} \), input-selector \( I \) picks \( R^{*} \leftarrow \{0,1\}^{T} \), queries its own DEAL oracle with \((A, M_0, M_1, R^{*}, T)\), and returns.

For such an input-selector, we drop the non-repeating requirement; we expect that \( r \) is large, in which case non-repetition holds with high probability. For emphasis, we can in this case write \( \text{Adv}_{I_{1}}^{\text{priv}}(A) \) in place of \( \text{Adv}_{I_{1}}^{\text{priv}}(A) \). Note that \( \text{pred}(I) \leq q \cdot 2^{-r} \) where \( q \) is the number of DEAL queries of \( I \).

Discussion. In an asymptotic-security setting, where all advantages are functions of a security parameter, we would say that I is unpredictable if \( \text{pred}(I) \) is negligible. Then we would say that \( S \) is Priv-secure if \( \text{Adv}_{S}^{\text{priv}}(A) \) is negligible for every polynomial-time, unpredictable I and every polynomial-time A. In our concrete-security setting, we will informally use the terms in italics above with the understanding that polynomial-time means “efficient” and negligible means “small.” Results will make this precise via concrete bounds on advantage. For example, Theorem 1 upper-bounds \( \text{Adv}_{S_{1,1}}^{\text{priv}}(A) \) as a function of \( \text{pred}(I) \), so that if the latter is small (\( I \) is unpredictable) then the former is too (\( S \) is Priv-secure). Unpredictability is necessary for Priv security in the same way that it is necessary for the privacy of deterministic public-key encryption [4].

Denying I access to the hash function \( H \) is necessary to achieve Priv for the same reason that messages in deterministic public-key encryption cannot depend on the public key [4] and in message-locked encryption cannot depend on the parameters [10]. From a usage perspective, this models dealers (users) picking the inputs to S.Share independently of \( H \), which is what we expect real users to do. This is analogous to the argument that users of deterministic public-key encryption will not usually encrypt messages that depend on the public key of the recipient [4]. For both deterministic public-key encryption and message-locked encryption, allowing messages to depend on the public key or parameters (respectively) has been considered [1, 7, 35]. Doing the same here is an open question.

Our formalizations capture non-adaptive privacy, meaning that secrets (as well as the access structure, set of corrupted parties and the randomness) are not chosen as a function of the shares the adversary sees of previously shared secrets. This is in general necessary for Priv. In the case that the randomness is true and independent across sharing, stronger privacy (adaptive and with I allowed access to Hash) is possible and in fact
achieved by our schemes. But we prefer the simplicity of a single definition to pursuing this because in usage, inputs to $S$ are chosen by users who are unlikely to pick them adaptively or in a way depending on $H$.

Usage scenarios and their privacy. Different choices of randomness, made by a combination of user and scheme choices, are captured by different classes of input-selectors. We discuss a few.

The $S$.Share interface of an implementation could give the caller options with regard to $R$, effectively asking: do you want to pick the coins, or do you want the implementation to? If the user selects the latter, the implementation could pick $R$ uniformly random from a large space for each invocation of Share. This would be captured as the class of input-selectors that pick $R$ in this way, and, for that class, achieving the definition confers the standard indistinguishability-style privacy. However, it precludes reproducibility. A user desiring the latter could select the option of itself providing $R$, and then has various choices of how to do so. It may omit it altogether, setting $R$ to the empty string, corresponding to an `I` that does the same, so that privacy is provided as long as the message alone is unpredictable, as is possible if it is a good passphrase. To strengthen privacy in the case the message may lack entropy, the user could maintain a separate, long-term, high quality password, always using this in the role of $R$. Finally, the input-selector could choose such a long-lived $R$, but then append a counter. All of these possibilities are modeled as different choices of $I$.

## 5 Authenticity

Authenticity captures the immutability of what is shared: if a dealer shares out $M$, then nothing else can be recovered, even if some shares are changed. One could call the desired aim a binding property—one of the goals of a commitment scheme.

We give two notions of authenticity, Auth0 and Auth. The former assumes an honest dealer. For the use cases we have considered, it is sufficient. The Auth notion is simpler and implies Auth0. It does not assume an honest dealer. We take Auth as our main definitional target, but retain Auth0 to clarify the key security aim that Auth ensures.

The Auth0 goal. Our first notion for authenticity, Auth0, says that if you receive a share from an honest dealer, contribute it to Recover, and a secret is recovered using your share, then that secret must be what the dealer originally shared. In brief, a valid share is a commitment to the secret that was shared at that time. This holds no matter what other parties do.

The definition of Auth0 employs the game $G^\text{auth0}_S$ defined in Fig. 5. An adversary $A$ attacking Auth0 security runs a first stage to pick $(A, M, T)$. The sharing algorithm is then run on these values, along with uniformly random coins $R$, to produce a vector of shares $S$. The adversary, given $S$ (and whatever state she wants to retain from her first stage of execution, $St$), must now find a set of shares $S'$ that has some share $S$ in common with those in $S$. It wins if recovering a secret from $S'$ results in some message $M'$ distinct from $M$ and employing the share $S$. Formally, we define $\text{Adv}^\text{auth0}_S(A) = \Pr[G^\text{auth0}_S(A)]$ as the probability that the specified game returns true. Note that the game depends on the selection of a random oracle $H$, which we let $A$ query. Note that the common share $S$ of our English exposition is not explicit in the game, but is an arbitrary element of $V \cap V'$. Recall that the second argument $(M, V)$ returned by a call to Recover is the set of shares deemed valid.

The Auth goal. There is a natural way to strengthen and simplify Auth0. A game that does so is again defined in Fig. 5. Rather than insisting that shares arise from honestly sharing out a secret, we let the adversary name two sets of shares, $S$ and $S'$, in whatever way it likes. Recovery is then performed on both sets of shares. The adversary wins if the two sets of shares have at least
one share $S$ in common, that share is used in recovery operations, but the messages recovered differ. Note that strings are recovered if the adversary wins (that is, $M \neq \perp \neq M'$), because $V \neq \perp \neq V'$. We let $\text{Adv}_S^{\text{auth}}(A) = \Pr[\text{G}_S^{\text{auth}}(A)]$ be the probability that the game returns true.

Auth implies is stronger than Auth0, as the adversary certainly has the option of creating $S$ by sharing out some $(A, M, T)$ of its choice.

We can summarize the difference between Auth0 and Auth by saying that, in the former, a good share commits the dealer to at most one $M$, while in the latter, any share, good or bogus, commits to at most one $M$. Auth0 speaks to what a party can believe if it gets a share from an honest dealer; Auth speaks to what can be believed if the share is of unknown provenance.

We prefer Auth to Auth0 because it is simpler and stronger. For applications the extra strength would usually be irrelevant: in our motivating use cases, legitimate shareholders are assumed to hold valid shares.

We comment that having Recover identify which shares are good is important to making the authenticity guarantee meaningful. In particular, a party holding a share $S$ it believes to be valid and who recovers a message $M$ should only accept $M$ as the underlying secret if her share $S$ was identified as one of the good shares.

### 6 Error Correction

**Informal description.** Basic correctness demands that Recover($S$) return $(M, S)$ when $S$ is an authorized subset of some sharing of $M$. But what should Recover do when $S$ is not an authorized subset of any sharing of $M$? One possibility is to have it return $\perp$, thereby signaling that something is wrong. One might call such a scheme error-detecting.

Error-detection comes with a liability: it enables the adversary to thwart message recovery by changing a single share. There is no attempt to fix any problem. Error correction (Errx) goes to the opposite extreme: we seek to recover from errors whenever we can.

Error correction can be regarded as an exercise in explanation seeking. The Recover algorithm is presented with a set of shares. If there is a unique explanation for how they arose, we demand that Recover find this explanation. Given shares $S$, the explanation will say: “Here is the message $M$ that was previously shared out to give a subset $V \neq \emptyset$ of the shares $S$. The remaining shares from $S$ are all bad.” If there is no unique explanation like this, then an Errx-secure scheme must say so. Note that we disregard the degenerate explanation in which all shares are bad. That explanation is always a possibility, so an uninteresting one.

In this section we formalize Errx security. In Section 7 we show how to achieve Errx security, while in Appendix A.2 we compare it to robustness [15, 31].

**Enriching the Syntax.** For ADSS schemes that target error correction we enrich the syntax for the Recover algorithm in two directions.

First, we allow known information to be identified in Recover’s input. This information $K \in \text{Known} = \text{Access \cup Shares}$ is either an access structure $K = A \in \text{Access}$ that the recovering party somehow knows to be the operative one, or it is the subset $K \in \text{Shares}$ of the shares $S$ given to Recover know to be valid.

Second, we demand that the recovery process identify not only the message $M$ and the valid shares $V \subseteq S$ but also the randomness $R$ that was used in the sharing.

Formally, we will say that an enriched ADSS scheme $\Pi = (\text{Acc}, \text{Share}, \text{Recover})$ has Acc and Share as before but the message-recovery algorithm Recover: $\text{Known \times Shares} \rightarrow \text{Msg \times Rand} \times \text{Shares} \cup \{ \perp \}$ gets the indicated domain and range. We demand that Recover respects the known information: if $A \in \text{Access \cap Known}$ and Recover$(A, S) = (M, R, V)$ then $V = S = A$; and if $\emptyset \in \text{Shares \cap Known}$ and Recover$(\emptyset, S) = (M, R, V)$ then $\emptyset \subseteq V$. If the recovering party has no a priori information, select $K = \emptyset$.

As before, if Recover$(K, S) = (M, R, V)$ then $V \subseteq S$ and all shares from $V$ have the same .as component and the same .tag component. As for the return value $R$, we now describe our expectations.

**Full correctness.** For $\Pi = (\text{Acc}, \text{Share}, \text{Recover})$ an enriched ADSS scheme, we adjust basic correctness to demand that the identified coins are right: for all $A \in \text{Access}$, $H \in \Omega$, $I \subseteq [1..n(\text{Acc}(A))]$, $M \in \text{Msg}$, $R \in \text{Rand}$, $T \in \text{Tag}$, $S \leftarrow \text{Share}^H(A, M, R, T)$, $S = S[I]$, and $K \in \{A\} \cup \mathcal{P}(S)$ (where $\mathcal{P}(S)$ is all subsets of the components of $S$): (1) if $I \in \text{Acc}(A)$ then Recover$^H(K, S) = (M, R, S)$, and (2) if $I \notin \text{Acc}(A)$ then Recover$^H(K, S) = \perp$. If all you are worried about is vanishing shares then Recover returns the right thing.

The following validity requirement for an enriched ADSS scheme $\Pi = (\text{Acc}, \text{Share}, \text{Recover})$ can be considered a converse to basic correctness: when Recover$(K, S) = (M, R, V)$ and $S = \text{Share}(V.as, M, R, V.tag)$ then $V$ is an authorized subset of $S$, meaning that $V = S[G]$ for some $G \in \text{Acc}(A)$,
The error-correction game is structured in a way to directly reflect the intended intuition. The adversary wins if it forces Recover to recover something wrong—something other than the unique explanation, when there is one, for the provided shares. We carry out the thought experiment of looking at all plausible explanations for the shares, and see if one is unique. At the lowest level, at lines 78–7A, the plausible explanations are indicated by the Recover procedure itself.

**ALTERNATIVE ERRX DEFINITION.** There is an equivalent way to define Errx security: one defines the plausible explanations for a set of shares according to the Share procedure instead of the Recover procedures. Specifically, lines 78–7A of Fig. 6 can be replaced by the following:

\[78' \text{ procedure } \text{Explanations}^H(K, S)\]
\[79' \text{ if } K \in \text{Access} \text{ then return } \{(A, M, R, V): \text{ } G \in \text{Acc}(K), R \in \text{Rand}, T \in \text{Tag}, S = \text{Share}^H(K, M, R, T, V) \}\]
\[79' \text{ else return } \{(A, M, R, V): A \in \text{Access}, G \in \text{Acc}(A), R \in \text{Rand}, T \in \text{Tag}, S = \text{Share}^H(A, M, R, T, V) \}\]
\[7A' \text{ return } \{ \langle V, \text{as}, M, R, V \rangle: (V, \text{as}, M, R, V) \text{ is qualified}, \text{or } \text{Tag} \}\]

No other changes are made. We justify the equivalence of the definitions in Appendix C.2.

**DISCUSSION.** We defined ADSS in such a way that the reconstructing party is not required to know the operative access structure; rather, it recovers this from the valid shares. This choice interacts badly with use of an expressive access-structure naming function. Suppose, for example, that Acc supports the 1-out-of-1 threshold scheme. Then an adversary can replace a single share \(S\) from a deal \(S\) with a share \(S_1\) for a message \(M_1\), the share asserting the 1-out-of-1 access structure. Message recovery will either be thwarted by the presence of this one bogus share (when \(S \setminus \{S\}\) is qualified), or \((M_1, \{S_1\})\) will be recovered (when \(S \setminus \{S\}\) is not qualified). Neither outcome is good.

The underlying problem is a failure to distinguish between the access structures that a secret-sharing scheme can handle and those that a reconstructing party might regard as reasonable. Once that distinction is drawn, one can consider it an important but out-of-model step that the recovering party discards any share asserting an access structure it deems unreasonable. A simple special is when the receiver knows what the right access structure is. It can provide this side information to Recover.

A well-known variant of secret sharing [41] envisages that a shareholder who trusts her own share \(S\) is
performing recovery. In such a case, explanations from Recover that do not include this share should be regarded as implausible. More generally, we have enriched Recover so that any subset of shares can be designated as trusted. Only explanations that include all trusted shares are considered valid. Note that marking any share as trusted establishes a known access-structure, too. Both make it harder for an adversary to obstruct message recovery.

One way for the receiving party to obtain assurance that a given share is trusted is for the share to be digitally signed by the dealer and for the reconstructing party to know the dealer’s public key. Such a model for secret sharing meaningful disadvantages the adversary, but takes us outside our basic model.

Coin recovery. Our enriched syntax demands that Recover, when presented the set of shares $S$, return not only $M$ and $V$ but also the coins $R$ that were used in the sharing of $M$ and gave rise to $V \subseteq S$. Why?

The returned coins serve as a certificate that the valid shares really could arise from a legal sharing of the message $M$. Beyond this, a unique explanation $(M, R, V)$ for the set of shares $S$ becomes a demonstration that, for an honest dealer, it was a single sharing of $M$ that gave rise to shares $V$. In effect, returning $R$ and absorbing it into the Errx definition makes the definition stronger, ensuring that it was one sharing from which we are seeing shares. It eliminates degeneracies about what Recover should do when, for example, two shares of a 2-out-of-4 secret-sharing are combined with two shares from a different 2-out-of-4 secret-sharing for the same message. Such possibilities returning $\perp$ (as we think they should) would thwart claims that Errx security imply robustness; they would make it untrue. We find that to be undesirable: error-correction intuitively should imply robustness (once side conditions are added so that robustness becomes achievable), but with other definitional choices we explored that do not surface $R$, such a claim is untrue.

7 Constructions

This section provides schemes and transformations for achieving ADSS. We start with a version of Shamir’s secret-sharing scheme, $S_1$. It achieves classical privacy, Priv$, and works for threshold access structures. We then provide the main construction of this paper: the transformation AX. It turns an ADSS scheme $S$ achieving only Priv$ security into an ADSS scheme $SS = AX[S]$ that achieves Priv and Auth security. Finally, transformation EX adds in Errx security. Proofs for our constructions are in Appendix C.

Transformations AX and EX leave unchanged the access structure of the scheme they are applied to, so $SS_1 = EX \circ AX \circ S_1$ is the concrete ADSS scheme we put forward for threshold access structures. To handle arbitrary access structures all that is needed is to start with a base-level scheme that works for arbitrary access structures. We give such a scheme, $S_2$, in Appendix B. The access structures are presented as a circuit of threshold gates. Scheme $SS_2 = EX \circ AX \circ S_2$ is our suggestion for an ADSS scheme on arbitrary access structures.

We discuss the efficiency of our schemes at the end of this section.

Base-level scheme $S_1$. We begin by describing Shamir secret-sharing [40], but with a few minor twists: scheme $S_1$ operates over the field $\mathbb{F}$ with $2^d$ points and is extended blockwise; the polynomial coefficients are determined by a pseudorandom generator (PRG) based on a pseudorandom function (PRF); and, in keeping
with our syntax, a description of the (threshold) access structure is an input to Share. Concretely, Fig. 7 defines secret-sharing scheme $S_1 = S_1[\beta, f]$ where

1. $\beta \geq 2$ is the blocklength. In practice, one would likely select $\beta = 8$, corresponding to the partitioning of a plaintext into bytes; and
2. $f: \{0,1\}^\times \times \mathbb{N} \times \{0,1\}^\ast \to \{0,1\}^\ast$ formalizes how the entropy source $R \in \{0,1\}^\ast$ is used to create the internal randomness. We require $|f_R^i(x)| = \ell$ (the first two arguments of $f$ written as a subscript then superscript).

The set $S_1.Acc$ contains all $(k,n)$ (a string that encodes $k$ and $n$) where $1 \leq k \leq n < 2^\beta$. The access-structure naming function $S_1.Acc$ maps each $(k,n) \in S_1.Acc$ to the set $A_{k,n} = \{U \in [1..n] : |U| \geq k\}$. The message space of $S_1$ is $\text{Msg} = B^\ast$ where $B = \{0,1\}^\beta$. The randomness space is $\text{Rand} = \{0,1\}^\kappa$. The scheme uses the finite field $F$ having $2^\beta$ points, which must be more than the maximum number of parties. We fix some canonical representation of field points as $\beta$-bit strings. We interchangeably regard $\beta$-bit strings, numbers in $[0..2^\beta - 1]$, and points in $F$. For lines 106 and 111 recall that the fourth and fifth components of a share $S_i$ represent the public portion $S_i.pub$ and the tag $S_i.tag$. Both are $\varepsilon$ since scheme $S_1$ doesn’t support tags and doesn’t mark any portion of a share as public.

The security of $S_1$ relies on the PRF security of $f$, which is defined in Appendix C.1. We give the following proposition, which states that if $f$ is a secure PRF, then $S_1[\beta, f]$ is Priv$\$$ secure. Recall the latter is Priv restricted to input-selectors in the class $I^{\text{priv}S\$$}, namely those who pick the coins in their Deal queries uniformly and independently of anything else.

**Proposition 1.** Let $S_1 = S_1[\beta, f]$ with $\beta \geq 2$ and $f: \{0,1\}^\kappa \times \mathbb{N} \times \{0,1\}^\ast \to \{0,1\}^\ast$. Then $S_1$ satisfies Priv$\$$. Concretely, given input-selector $I \in I^{\text{priv}S\$$}$ and given Priv-adversary $A$ we build a PRF-adversary $B$ such that $\text{Adv}^{\text{priv}S\$$}_{S_1,I}(A) \leq \text{Adv}_{f}^{\text{priv}B}(B)$.

**Main construction AX.** The AX transformation turns a Priv$\$$-secure secret-sharing scheme $S$ into a secret-sharing scheme $SS$ that augments this with Priv- and Auth-security. $SS$ uses the enriched ADSS syntax but does not yet target error correction; that will come next. The AX transformation also expands the message space—scheme $SS$ can share messages of any length, while $S$ might only be able to share short ones. AX also handles associated-data, which scheme Shares is not required to support. The access structures that can be handled by $SS$ are exactly those that can be handled by $S$. Besides the secret-sharing scheme $S$ the transformation will use PRF and a random-oracle-modeled hash-function. The former can be built from the latter, but we leave them separate because we anticipate, for example, an AES-based construction for the PRF and a SHA256-based construction for the hash.

The AX transformation is given in Fig. 8. It specifies $SS$.Share and $SS$.Recover for $SS = AX[S, f]$. Access-structure naming function $SS$.Acc is $S$.Acc.

**Theorem 1.** Let $SS = AX[S, f]$ where $S$ is an ADSS scheme with message space $\text{Msg} \supseteq \{0,1\}^\kappa$, tag space $\text{Tag} = \{\varepsilon\}$, and entropy space $\text{SS}.\text{Rand} = \{0,1\}^\kappa$, and where $f: \{0,1\}^\kappa \times \mathbb{N} \times \{0,1\}^\ast \to \{0,1\}^\ast$. Then:

1. If $S$ is Priv$\$$-secure then $SS$ is Priv-secure. Given an input-selector $I$ making $q_0$ calls to Deal and adversary $AA$ (attacking the Priv security of $SS$) making $q$ queries to Hash, we build input-selector $I \in I^{\text{priv}S\$$}$ and adversaries $A$ and $B$ s.t.

\[
\text{Adv}^{\text{priv}SS}_{SS,I}(AA) \leq 2(q_0 + q)\text{pred}(I) + \epsilon
\]

2. $SS$ is Auth-secure. For any $A$ making $q_0$ queries to Hash, we have $\text{Adv}^{\text{auth}SS}_{SS}(A) \leq (q_0 + 1)(q_0 + 2) - 2^{-2\varepsilon+1}$. A more explicit theorem statement would quantify the resources of the constructed adversaries. In this case, adversary $A$ makes $q_0$ queries to Deal and $q$ queries to Hash, while $B$ makes $q_0$ queries to New and $2q$ queries per instance to $Fn$. The running times of $A$ and $B$ are about the same as that of $AA$. For brevity we omit such details in this and other result statements. They can be gleaned from the proofs.

**Error correction with EX.** Fig. 9 defines a transformation EX that turns an enriched ADSS scheme $S$ into an error-correcting scheme $SS$. EX avoids making any changes to Share, putting all the work in Recover.

For line 80, a set of shares $S'$ is said to be $K$-plausible if all the shares in $S'$ name the same access-structure encoding $A$, and $A = K$ if $K$ names an access structure; the shares name distinct identities in $[1..n(\text{Acc}(A))]$; these parties are authorized according to Acc($\text{Acc}(A)$); the shares all have the same tag $T$; and the shares include all those in $K$ if $K$ is a set of shares. Further scheme-dependent criteria can be added without harming the.
correctness of EX as long as one omits no element of \( \mathcal{P}(S) \) that could arise in a valid sharing that respects the known information \( K \). As an example, if Share happens to place the same word \( J \) in each share of a deal then the definition of \( K \)-plausible sets can further include the constraint that all shares have the same \( J \)-value. Lines 82–83 look for a first explanation \( S_i \) for \( S \) such that the identified set of valid shares \( \mathcal{V} \) is equal to \( S_i \). If we fail to find one, we fail at line 84. Otherwise we seek at lines 86–88 a second explanation for \( S \). If we find one, we again fail, but now because there are two explanations for \( S \). At line 85 we prune the plausible second explanations to only include those that are not a subset of the first.

**Theorem 2.** Let \( S \) be any enriched ADSS scheme with full correctness, and let \( SS = EX[S] \). Then:
procedure SS.Recover(κ, S)
80 let S₁,...,Sₜ ∈ ℙ(S) include all κ-plausible sets
81 of shares, arranged so that Sᵢ ∪ Sⱼ ⇒ i ≤ j
82 for i ← 1 to w do
83 if (M, R, V) ← S.Recover(κ, Sᵢ) and V = Sᵢ then goto 85
84 return ⊥
85 (Sᵢ,…,Sₜ) ← \{Sᵢ₊₁,…,Sₜ\} \ ℙ(V)
86 for i ← 1 to w do
87 if (M’, R’, V’) ← S.Recover(κ, S’ᵢ) and V’ ⊆ V then
88 return ⊥
89 return (M, R, V)

Fig. 9. The EX construction. The method turns an enriched ADSS scheme S into an enriched ADSS scheme SS = EX[S] with Errx security. We let SS.Acc = S.Acc and SS.Share = S.Share. For a set of shares Sᵢ ⊆ S to be “plausibly valid” all the shares of Sᵢ must have the same access structure and tag, and they must have distinct identities in from that access structures.

1. If S is Auth-secure then so is SS. Concretely, given adversary AA (for attacking the Auth security of S), we construct adversary A with complexity similar to AA (for attacking the Auth security of S) such that \( \text{Adv}^\text{auth}_{SS}(AA) \leq \text{Adv}^\text{auth}(A) \).
2. SS is perfectly Errx-secure. Concretely, for any adversary A, \( \text{Adv}^\text{errx}_{SS}(A) = 0 \).

Efficiency of the constructions. We apply AX and then EX to S₁ to obtain a threshold scheme SSS₁, or AX and then EX to S₂ to obtain a scheme SSS₂ for any access structure. These schemes are highly efficient: sharing an m-byte message M will take \( O(m) \) time and, more concretely, about the amount of time to symmetrically encrypt and hash M. This assumes a fixed number of shareholders n, a fixed access-structure encoding A, a fixed tag T, and fixed scheme parameters. Concretely, to share M one will need to apply a hash function like SHA-256 to a string that’s \(|A| + |T| + κ\) bits longer than M (likely κ ∈ \{128, 256\}); run a blockcipher like AES in counter mode to generate a pad κ bits longer than |M|; and run a sharing under S₁/S₂. That last part is fast because the message being shared is just the κ-bit string K. For S₂ one needs time linear in the number of threshold gates in the circuit described by A. Practical access structures will have no more than a few gates.

Message recovery for AX o S₁ or AX o S₂ takes about the same time as sharing, but once EX is added the recovery process can be slow: exponential in the number of shares n presented to Recover. In the worst case, the recovery algorithm, given \( S = \{S₁,...,Sₙ\} \), might inspect as many as \( 2^ₙ \) subsets of \( S \). Still, in practical contexts the number n is likely to be so small that \( 2^ₙ \) is still small. Beyond this, we have designed EX so that exponential-time recovery can only arise when there are adversarial edits to shares, not just omissions. In the setting where shares are either valid or absent, Recover will run in essentially the same time as Share.

8 Conclusions & Open Problems

Classical secret-sharing envisages an adversary that does no more than erase some users’ shares. Its only aim is to learn what it shouldn’t know. Real adversaries aren’t so restrained. In response, one can reduce expectations or increase guarantees. We’ve done the latter.

An unresolved technical problem is how to achieve Errx security with efficient worst-case message-recovery time. Many constructions are plausible. For example, one could add n hash values to each of the n shares, a check-value for each share on each share, using these to partition shares into plausible subsets. Or one could add to each share a dealer-generated digital signature. We suspect that techniques like these can work, and can also make for a simpler Recover than that of EX.

We have not implemented our ADSS schemes. We hope to soon see implementations by others, both as a callable library and as an end-user tool. Ultimately, ADSS implementations should conform to a standards document, such as an RFC. In this way, techniques for adept secret-sharing may become as fixed as those for, say, authenticated encryption.

Our formulation of ADSS has shares leak metadata such as the share number and the operative access structure. Definitions and schemes for metadata-concealing ADSS should be possible.

Underlying our work has been a belief that secret sharing has been underutilized. Secret sharing is not just a tool for doing other things; it is also an aim directly tied to a human aspiration. Shamir wrote in 1979 [40] that “Threshold schemes are ideally suited to applications in which a group of mutually suspicious individuals with conflicting interests must cooperate.” Such cooperation is needed now more than ever.

Acknowledgments

A meeting with J. Alex Halderman and Laurent Richard led to this project. A later meeting with staff at the Free-
dom of the Press Foundation helped clarify our goals, especially authenticity.

Thanks to John Chan, Jake Craige, Fred Jacobson, Romain Ruetschi, and Conor Schaefer for useful feedback. Thanks to the PoPETs referees for their excellent comments and suggestions.

Bellare and Dai were supported by NSF CNS 1717640, Rogaway by NSF CNS 1717542.

References


[27] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage.
A Relations

Our Auth security goal for ADSS may seem similar to the verifiable secret-sharing (VSS) goal to the first formulated by Chor, Goldwasser, Micali, and Awerbuch (CGMA85) [18]. In this section we contrast these goals. Then we contrast Auth with robustness [15, 31] and, finally, with repairability [25, 32].

A.1 Comparison with VSS

VSS arose in the context of multiparty computation (MPC), where each party would, in a first phase, share out its secret, and later, in a second phase, compute on these shares. For the second phase to work, it was important that, at the end of the first phase, honest parties could be sure that, for each dealer, there existed a single value such that, if, at some later stage, an authorized subset of honest parties attempted recovery, they would recover this unique value.

The original VSS method of CGMA85 [18] involved interaction among the shareholders. Feldman was the first to describe a non-interactive scheme for VSS [21]. Each shareholder performs a local verification step, applying a verification algorithm specified by the scheme to its own share and some public quantity broadcast by the dealer. The result informs a party if its share is valid. This local validity was required to ensure the global unique recoverability property.

Thus two points of difference with ADSS that emerge from the above are: (1) the presence, in a VSS setting, of the verification algorithm; and (2) the presence, in the model for VSS, of a broadcast channel. ADSS does not have a verification algorithm and does not anticipate a broadcast model. Formally, for different definitions D of ours like Auth or Errx, questions like “does VSS imply D, or does D imply VSS” do not make formal sense, as the goals involve different syntax and models.

Rather than end the comparison on this unsatisfactory note, we treat VSS in the ADSS context. We extend the syntax and model to include a verification algorithm and a broadcast channel. With a formal definition of VSS in place, we show that a VSS-secure scheme is Auth-secure. That is, VSS is effectively a stronger definition than Auth.

However, achieving VSS instead of Auth seems to involve more work: known VSS schemes are substantially less efficient than the Auth-secure schemes we
Game $G_{\text{VSS}}^{\text{auth}}(A)$

80 $H ← \Omega; (A', S', S') ← A^H$
81 if $(∃ S, S' ∈ S ∪ S' : S, \text{pub} ≠ S', \text{pub})$ then return false
82 if $(∃ S ∈ S ∪ S' : \text{VSS.Verify}(S) = 0)$ then return false
83 if $(S, \text{id} ∉ \text{VSS.Acc}(A)$ or $S', \text{id} ∉ \text{VSS.Acc}(A'))$ then return false
84 return $(M ≠ M')$

Fig. 10. Game defining VSS security of a broadcast-model VSS scheme $\text{VSS} = (\text{Acc}, \text{Share}, \text{Recover}, \text{Verify})$

propose. Worse, VSS needs what is, in our context, the untenable assumption of a broadcast channel: for our motivating use cases, this isn’t present.

FORMALIZING VSS. To enable a formal comparison of Auth and VSS we formalize VSS using ADSS-like syntax. We say that a scheme for verifiable-ADSS is a four-tuple of deterministic algorithms $\text{VSS} = (\text{Acc}, \text{Share}, \text{Recover}, \text{Verify})$. We require that $S = (\text{Acc}, \text{Share}, \text{Recover})$ is an ADSS scheme, called the ADSS scheme induced by $\text{VSS}$. The new algorithm

Verify: Share $→ \{0, 1\}$

will tell a shareholder whether or not its share $S$ is valid. Basic correctness for $\text{VSS}$ is that of its induced ADSS scheme together with the requirement that $S = \text{Share}^H(A, M, R, T)$ implies that $\text{Verify}^H(S[i]) = 1$ for all $i$. We may speak of Priv, Auth security of $\text{VSS}$, by which we simply mean those of its induced ADSS scheme.

The new requirement is VSS-security. Consider the $G_{\text{VSS}}^{\text{auth}}(A)$ game on the left of Fig. 10. The VSS advantage of $A$ is defined by

$$\text{Adv}_{\text{VSS}}^{\text{VSS}}(A) = \text{Pr}[G_{\text{VSS}}^{\text{auth}}(A)] .$$

In the game, the adversary at line 81 returns an access structure description $A$ and two sets $S, S'$ of shares. Line 82 enforces the broadcast constraint that the public portions of all shares are the same. Line 83 says that all shares have passed verification. Line 84 says that the parties underlying both sets of shares are authorized. With these constraints, security (the adversary does not win) requires that the two sets of shares recover to a common, non-$\perp$ value.

VSS IMPLIES AUTH. Let $\text{VSS} = (\text{Acc}, \text{Share}, \text{Recover}, \text{Verify})$ be a verifiable-ADSS scheme. Define

$$\text{procedure Recover}'(S)$$

if $(∃ S ∈ S : \text{Verify}(S) = 0)$ then return $⊥$

$Y ← \text{Recover}'(S);$ return $Y$

The following says that ADSS scheme $S' = (\text{Acc}, \text{Share}, \text{Recover})'$ satisfies Auth.

Proposition 2. Let $\text{VSS} = (\text{Acc}, \text{Share}, \text{Recover}, \text{Verify})$ be a verifiable-ADSS scheme and let ADSS scheme $S' = (\text{Acc}, \text{Share}, \text{Recover})'$ be defined as above. Given adversary $A_{\text{auth}}$, we build adversary $A_{\text{vss}}$, about as efficient as $A_{\text{auth}}$, such that $\text{Adv}_{\text{VSS}}^{\text{auth}}(A_{\text{auth}}) ≤ \text{Adv}_{\text{VSS}}^{\text{VSS}}(A_{\text{vss}})$.

Proof. We define $A_{\text{vss}}$ as follows:

$$\text{Adversary } A_{\text{vss}}^H(S, S') ← A_{\text{auth}}^H Y ← \text{Recover}'(S); Y' ← \text{Recover}'(S')$$

if $(Y = ⊥$ or $Y' = ⊥)$ then return $⊥$

$A ← \text{S.as}; A' ← S', \text{as}; (M, V) ← Y; (M', V') ← Y'$

return $(A, A', S, S')$

Our syntax demands Recover$(S)$ return $⊥$ unless the public parts of all $S ∈ S$ are the same and likewise for $S'$. If $A_{\text{auth}}$ wins in game $G_{\text{VSS}}^{\text{auth}}(A_{\text{auth}})$ then $S ≠ ⊥$ and $S' ≠ ⊥$. Since additionally $S ∩ S' ≠ \emptyset$, we get that all shares in $S$ and $S'$ have the same public part, ensuring that line 82 of game $G_{\text{VSS}}^{\text{auth}}(A_{\text{vss}})$ does not return false. The definition of Recover' tells us that line 83 also does not return false. Our syntax demands that if Recover$(S)$ returns the non-$\perp$ value $(M, V)$ then access structures $S$, as, $A$ of all $S ∈ S$ are the same and additionally $S, \text{id} ∈ \text{Acc}(A)$, and likewise for $S'$. So line 84 also does not return false. Now if $A_{\text{auth}}$ wins we have $Y, Y' ≠ ⊥$ and $M ≠ M'$, so $A_{\text{vss}}$ wins.

A.2 Comparison with robustness

Robustness was introduced in [31] and formalized in [15]. We start by adapting the notion of the latter to ADSS. We consider the game of Fig. 11 and let $\text{Adv}_{\text{rob}}^{\text{rob}}(A) = \text{Pr}[G_{\text{rob}}^{\text{rob}}(A)]$ be the advantage of an adversary $A$ in this game. The game picks $R$ at random. The adversary runs in two phases. In the first, it returns $A, M, T$ and state information $S$. The game then creates $S ← S, \text{Share}^H(A, M, R, T)$. In its second stage, given $S$, the adversary can adaptively corrupt parties, one by one, obtaining their shares, as long as the set $G$ of uncorrupted parties remains authorized and the set $B$ of bad (corrupted) parties remains unauthorized. Finally the adversary outputs a set $B$ of shares for the cor-
and define adversary \( \text{Adv} \).

**Proposition 3.** Define adversary \( \text{Recover} \) as follows:

\[
\text{Recover}(S) = \begin{cases} 
\text{Acc}, & \text{if } (G \setminus \{i\} \not\in \text{Acc}(A)) \text{ then return } \bot \\
\text{B Base-Level Scheme } S', & \text{if } (B \cup \{i\} \in \text{Acc}(A)) \text{ then return } \bot 
\end{cases}
\]

This adversary runs \( \text{Adv}_{\text{rob}} \), simulating the latter's \( \text{Corrupt} \) oracle. It returns the set of shares that game \( G_{\text{rob}}^{\text{Grb}}(A_{\text{rob}}) \) would pass to Recover, with the known information set to \( \emptyset \). Let \( Y' \leftarrow \text{Recover}'(S) \) and if \( Y' \not= \bot \) then parse it as \((M',R',V') \leftarrow Y'\). Suppose \( \text{Adv}_{\text{rob}} \) wins in game \( G_{\text{rob}}^{\text{Grb}}(A_{\text{rob}}) \). This means either \( Y' = \bot = M' \not= M \). We want to show \( \text{Adv}_{\text{errx}} \) wins in game \( G_{\text{errx}}^{\text{Grb}}(A_{\text{errx}}) \). This means we must show that \( Y' \not= \text{UniqueExplanation}(\emptyset,S) \). This is true because all members of Explanations \( H(A,S) \) have the form \((A,M,R,V)\) for some \( V \).

**Robustness of an ADSS scheme does not imply that it has our Auth property.** For example, in a robust 2-of-3 threshold scheme, if a share \( S[1] \) for \( M \) is combined with shares \( S[2] \) and \( S[3] \) for another secret \( M' \), then all parties, including the first, must recover \( M' \), and party 1 is provided no indication that \( M' \) is not the secret that was used to create \( S[1] \). In the same situation, an auth scheme would return \( \bot \), so that party 1 is not given a secret inconsistent with her share. In fact, Auth implies non-robustness, and robustness permits that a party can recover anything that an adversary chooses if it controls the remaining shares.

**A.3 Comparison with repairability**

Repairable threshold schemes [25, 32] allow a party to reconstruct a missing share by interacting with fellow shareholders. In our applications, we do not anticipate that shareholders have any desire or ability to interact with one another prior to recovery. They might not even know who other shareholders are, or how to reach them. We anticipate that if a party has lost her share, or thinks it may no longer be accurate, she can ask the dealer to regenerate it. If reproducibility was targeted, the dealer can give the party the same share as before. Without reproducibility, the dealer would need to re-share the secret, which means it must contact all other shareholders and get them to replace their shares.

**B Base-Level Scheme S2**

We describe an alternative to \( S1 \) that supports arbitrary access structures instead of just threshold ones. The ac-
Fig. 12. Secret-sharing scheme \( S_2 \) for achieving classical privacy and accommodating any access structure. On reconstruction, shares are either unchanged or absent. \( S_2 = S_2[\beta, f, \lambda] \) depends on \( \beta, \lambda, \mu \in \mathbb{N} \) and \( f : \{0, 1\}^\mu \times \mathbb{N} \times \{0, 1\}^\nu \rightarrow \{0, 1\}^\nu \) satisfying \( |f_\mu^e| = \ell \). Hash function \( H^\nu(x) \) returns \( \ell \) uniform bits. The access structure is described by a circuit \( c = (n, q, in, th) \) of threshold gates each having fewer than \( 2^h \) inputs. Sharing depends on random bits \( R \in \{0, 1\}^\kappa \). No tag \( T \) is supported. Top: Illustration of sharing with an access structure having AND gates 4 and 5, and OR gate 6. Each wire \( i \) is associated with a \( \lambda \)-bit token \( X_i \). The boxed text describes how the dealer computes randomizer \( U \), tokens \( X_i \), ciphertext \( C \), and the \( L_{i,j} \) labels. The share for party \( i \) has a \( X_i \) for its secret part and a public part that includes \( C, U \), and all the \( L_{i,j} \) labels. Bottom: Definition of the scheme. Arithmetic at line 213 is in the finite field with \( 2^9 \) points. Procedure Interpolate is as before. Procedures share and recover use arguments and local variables \( M \) and \( S_i \) distinct from the caller’s variables by those names.
cess structure is represented by a circuit of threshold gates, a compact way to describe any access structure. That threshold gates are rich enough to represent any access structure follows from the fact that AND and OR gates are threshold gates, these two gates are already enough to represent any monotone Boolean function, and access structures must be monotone.

We name our scheme S2. It combines the folklore idea of Yao’s secret-sharing scheme [3, 28, 42] with Benaloh-and-Leichter’s scheme for monotone formulas [16]. The reason we call Yao’s scheme “folklore” is because there is no written description of it by him. Rather, he sketched the idea in one or more talks, including one in 1989 [2, p. 228].

The reason for attending to non-threshold access structures is that natural ones do arise. They tend to be simple—things like “2 and (1 or 3)”, meaning that one requires the participation of shareholder 1 or 3. Function shows connectivity that could be described by a simple—things like “2 and (1 or 3)”, meaning that one requires the participation of shareholder 1 or 3.

**Threshold Circuits.** The top of Fig. 12 depicts a threshold circuit \( C = (n, q, in, th) \) with \( n = 3 \) inputs and \( q = 3 \) gates. The input wires are numbered 1, 2, 3. The gates, and the wires coming out of them, are numbered 4, 5, 6. Wire 6 is the output wire. The drawing shows connectivity that could be described by a function \( in \) from gates to sets of wires where \( in(4) = \{1, 2\}, \) \( in(5) = \{2, 3\}, \) and \( in(6) = \{4, 5\}. \) The threshold value for gates 4 and 5 (written near its apex) is 2, \( th(4) = th(5) = 2, \) so these are 2-out-of-2 gates, meaning two-input AND gates. The threshold value of gate 6 is 1, \( th(6) = 1, \) so this is a two-input OR gate. The circuit computes the boolean function \( x_1x_2 \lor x_2x_3 = x_2(x_1 + x_3) \) over bits \( x_1, x_2, x_3 \) and thereby encodes the access structure \( A = \{(1, 2), \{2, 3\}, \{1, 2, 3\}\}. \)

Proceeding more formally, we follow a minimalistic formalization for garbled circuits [9], saying that a threshold circuit (that is, a circuit of threshold gates) is a 4-tuple \( C = (n, q, in, th) \). The values \( n \geq 2 \) and \( q \geq 1 \) represent the number of input wires and the number of gates, respectively. We number input wires \( Inp = \{1..n\} \), gates \( Gates = \{n+1..n+q\} \), and all wires \( Wires = \{1..n+q\} \). We identify a gate with the wire coming out of it. The output wire for the entire circuit is wire \( n+q \). Function \( in: Gates \to \mathcal{P}(Wires) \) identifies the inputs to each gate, \( |in(g)| \geq 2 \). We will alternatively regard \( in(g) \) as a numerically ordered list (e.g., \( in(4) = (1, 2) \) rather than \( in(4) = \{1, 2\} \)). Function \( th: Gates \to \mathbb{N} \) is the threshold value of each gate (how many of the inputs must be 1 for the output to be). We require that for all \( g \in Gates, 0 \neq in(g) \subseteq \{1..g-1\} \) (so no cycles) and \( 1 \leq th(g) \leq |in(g)| \).

For \( k \in \{1..n\} \) and \( X \in \{0, 1\}^n \) let \( TH_k(X) \) be 1 if \( X \) has \( k \) or more 1-bits, and 0 otherwise. For \( X \in \{0, 1\}^n \) and \( I \subseteq \{1..n\} \), let \( X[I] \) be the \( |I| \)-bit substring of \( X \) that includes only the bits at positions in \( I \) (indexing starting at 1). For a threshold circuit \( C = (n, q, in, th) \) and \( X \in \{0, 1\}^n \), define \( C(X) = Eval(C, X) \) by

\[
\text{procedure} \quad Eval(C, X) \\
\quad (n, q, in, th) \leftarrow C \\
\quad \text{for } g \leftarrow n + 1 \text{ to } n + q \text{ do} \\
\quad \quad X[g] \leftarrow TH_{th(g)}(X[\text{in}(g)]) \\
\quad \text{return} \quad X[n+q]
\]

For compactness, the code above extends the \( n \)-bit string \( X \) to \( n + q \) bits, using the additional \( q \) bits to record the values flowing on non-input wires.

A threshold circuit \( C = (n, q, in, th) \) names an \( n \)-party access structure \( A = Acc(C) \) that contains \( G \subseteq \{1..n\} \) exactly when \( C(G) = 1 \), where \( G \) is the \( n \)-bit string with \( G[i] = 1 \) when \( i \in G \) and \( G[i] = 0 \) when \( i \notin G \).

**Base-Level Scheme S2.** We begin with an informal description, using the example at the top of Fig. 12. Consider the task you face in reconstructing a secret \( M \). You obtain from shares the circuit shown in the figure—everything drawn in black—and the gate labels \( L_{i,j} \) written in blue. You also extract from each share the strings we call \( C \) and \( U \). All these things are public. The secret part of the share \( S_i \) from party \( i \) is the \( \lambda \)-bit token we denote \( X_i \). For input wires, you either have the token (if party \( i \) provided a share) or you do not, whence one can regard \( X_i = \bot \). You now propagate tokens up the circuit, getting tokens or \( \bot \)-values for each gate, in numerical order. For each gate, if you have the threshold number of tokens for incoming wires then you will be able to propagate your tokens across the gate, getting a token for the output wire of the gate. If you don’t have a threshold number of tokens for the gate, then the outgoing token is \( \bot \). At line 226, we take the convention that if \( X_{th} = \bot \) for some \( i \), then \( X_{th} = \bot \). Continuing in this way, you obtain a token for the output wire exactly when you held input tokens for an authorized set of users. If you obtain an output token, you use it to decrypt the ciphertext \( C \) that accompanies the circuit. The result is the recovered secret.

How do you propagate a threshold number of tokens from the input wires of a gate to its output wire? The gate label for each gate functions as a ciphertext which gets decrypted using a corresponding token...
as the key. The decryption also depends on $U$ and the gate number. The plaintext that results is a share of the token for the wire coming out of the gate. The recovered shares are combined using polynomial interpolation (Shamir’s method) to recover the needed token. That’s all there is to it. The top-right of Fig. 12 shows the sharing process, while what we just described the recovery process.

More formally now, scheme $\mathcal{S}2 = \mathcal{S}2[\beta, f, \lambda]$ is parameterized by a block length $\beta$ (likely 8), a PRF $f : \{0,1\}^* \times \mathbb{N} \times \{0,1\}^* \rightarrow \{0,1\}^*$ satisfying $|f_{\mathcal{H}}^{\ell}(x)| = \ell$ for all $x$, and integer $\lambda$ (the length of gate-labels). The scheme depends on a hash function $H : \{0,1\}^N \times \{0,1\}^* \rightarrow \{0,1\}^*$, given as an oracle and satisfying $|H(\ell, x)| = \ell$. We write $H^\ell(x)$ for $H(\ell, x)$. The message space for $\mathcal{S}2$ is $\mathcal{S}2.\text{Msg} = \{0,1\}^*$ and the coins are $\text{Rand} = \{0,1\}^\kappa$.

Strings in $\mathcal{S}2.\text{Access}$ encode threshold circuits $(n, q, m, \text{th})$ where $|in(j)| < 2^3$ for $j \in \{n+1, \ldots,n+q\}$. Each circuit $\mathcal{C}$ encoded by a string in $\mathcal{S}2.\text{Access}$ represents the access structure $\mathcal{S}2.\text{Acc}(\mathcal{C})$ as described above. The sharing and recovery algorithms of $\mathcal{S}2$ are given in Fig. 12. It is not hard to check the basic correctness of $\mathcal{S}2[\beta, f, \lambda]$, which we do in Appendix C.3.

We move on to show that $\mathcal{S}2[\beta, f, \lambda]$ satisfies Priv$\$ security if $f$ is a secure PRF. In particular, we give the following theorem, which relates the Priv$\$ advantage of a given adversary $\mathcal{A}$ to the PRF advantage of a related PRF adversary plus “small terms” given that $\lambda$ are sufficiently large. The proof of the following is in Appendix C.5.

**Theorem 3.** Let $\mathcal{S}2 = \mathcal{S}2[\beta, f, \lambda]$ for valid parameters $\beta, f, \lambda$. Then $\mathcal{S}2$ satisfies Priv$\$. Concretely, given input-selector $I \in \mathcal{I}^{\text{Priv}\$}$ making $q_0$ DEAL queries, whose access structures has overall gate count of at most $g$, and given Priv-adversary $\mathcal{A}$ making $q_\text{hl}$ queries to $H$, we construct a PRF adversary $\mathcal{B}$ such that

$$\text{Adv}^{\text{Priv}\$}_{\mathcal{S}2, I}(\mathcal{A}) \leq \text{Adv}^{\text{PRF}}_f(\mathcal{B}) + \frac{g(g - 1) + 2q_\text{hl}}{2^\lambda + 1}.$$  \hspace{1cm} (2)

Adversary $\mathcal{B}$ is efficient when $I$ and $\mathcal{A}$ are.

Use of a random-oracle-modeled hash function in $\mathcal{S}2$ is only for convenience: the encryption at lines 205 and 207 could also have been done with a standard-model tool, like the same PRF $f$.

---

**C Proofs**

**C.1 PRF security definition**

Before providing any proofs we define PRF-advantage, adapting a multiuser variant from Bellare, Canetti, and Krawczyk [6], which lets the adversary simultaneously attack any number of independently keyed instances, the adaption being that their formalization was for fixed-output-length (FOL) PRFs, while we are using variable-output-length (VOL) PRFs. When that number of instances is at most $q$, the advantage degrades by a multiplicative factor of $q$ relative to the usual, single instance case. That result is in the reference above for the FOL case, but it is easy to check that it also holds in the VOL case.

Let $f : K \times N \times X \rightarrow \{0,1\}^\ell$ be a function. Consider the game $G^{\text{PRF}}_f$ given in Fig. 13. We define the (multi-user) PRF-advantage of adversary $\mathcal{A}$ attacking $f$ as

$$\text{Adv}^{\text{PRF}}_f(\mathcal{A}) = 2 \Pr[G^{\text{PRF}}_f(\mathcal{A}) = 1].$$

**C.2 Equivalence of Errx notions**

We claim that the two definitions of Errx given in Section 6 are equivalent. To see this, we fix a hash function $H \in \Omega$, as well as some $K \in \text{Known}$ and $S \in \text{Shares}$. Let $E_1 = \text{Explanations}^H(K, S)$ be the set returned by the algorithm given in lines 78–7A. Let $E_2 = \text{Explanations}^H(K, S)$ be the set returned by the alternate algorithm. First, suppose $K \in \text{Access}$. Let $(K, M, R, V) \in E_2$, which means that there exists some $T \in \text{Tag}$, $G \in \text{Acc}(K)$, such that for $S \leftarrow \text{Share}^H(K, M, R, T)$, we have that $V = S[G]$ and $S \subseteq S$ (viewing $S$ as a set). Consider $	ext{Recover}^H(K, V)$, by full correctness, we will get back $(M, R, V)$. Furthermore,
\(\forall \text{as} = K\) since honestly dealt shares should have the same access structure. This means that \((K, M, R, V) \in E_1\). On the other hand, let \((\forall \text{as}, M, R, V) \in E_1\), which means that \((M, R, V) = \text{Recover}^H(K, S')\) for some \(S' \subseteq S\). By the validity condition, \(\forall\) is authorized, meaning \(\forall = S[G]\) for \(S = \text{Share}^H(\forall \text{as}, M, R, V, \text{tag})\), and some \(G \in \text{Acc}(K)\). This means that \((\forall \text{as}, M, R, V) \in E_1\). Second, suppose \(K \in \text{Shares}\). Let \((A, M, R, V) \in E_2\), which means that for some \(T \in \text{Tag}\) and \(G \in \text{Acc}(A)\), \(S \subseteq S = \text{Share}^H(A, M, R, T)\) and \(K \subseteq \forall = S[G]\). By full correctness, \(\text{Recover}^H(K, \forall)\) must return \((M, R, V)\). Furthermore, \(\forall \text{as} = A\). Hence \((A, M, R, V) \in E_2\). On the other hand, let \((\forall \text{as}, M, R, V) \in E_1\), which means that \((M, R, V) = \text{Recover}^H(K, S')\) for some \(S' \subseteq S\). By the validity condition, \(\forall\) must be an authorized subset of \(S = \text{Share}^H(\forall \text{as}, M, R, V, \text{tag})\), meaning \(\forall = S[G]\) for some \(G \in \text{Acc}(\forall \text{as})\). By requirements of Recover, we know that \(K \subseteq \forall \subseteq S'\). Hence \((\forall \text{as}, M, R, V) \in E_2\). We conclude that \(E_1 = E_2\).

### C.3 Correctness of the constructions

**Basic correctness of S1[\(\beta, f\)].** We show S1 satisfies basic correctness. Let \((k, n) \in S1.\text{Access}, M \in \text{Msg}, R \in \{0, 1\}^n\), and \(S \leftarrow S1.\text{Share}(k, n), M, R, \epsilon\). Let \(G \subseteq \mathcal{P}([1..n])\). If \(G \in \text{Acc}(k, n)\) then \(|G| \geq k\), which means that line 113 will not return \(\bot\) in S1.Recover\((S[G])\) and the recovery will succeed (since 113 is the only place in S1.Recover that can fail for a properly formatted set of shares). On the other hand, if \(G \notin \text{Acc}(k, n)\) then \(|G| < k\), which means that line 113 will return \(\bot\) in S1.Recover\((S[G])\).

**Basic correctness of S2[\(\beta, f, \lambda\)].** We check that S1 satisfies basic correctness. Let \(\xi = (n, q, \text{in}, \text{th}) \in S2.\text{Access}, M \in S2.\text{Message}, R \in \{0, 1\}^n, H \in \Omega\), and \(S \leftarrow S2.\text{Share}(\xi, M, R, \epsilon)\). Let \(G \subseteq \mathcal{P}([1..n])\). We claim that if the check of line 21D holds for a gate \(g \in [n + 1..n + q]\) then the \(X_g\) recovered is the same as the \(X_g\) sampled in the original sharing; furthermore, if the check of line 21D does not hold for gate \(g\), then \(X_g = \bot\). This can be checked by induction on \(g \in [n + 1..n + q]\) and we omit the details. Let \(s_G\) be a string of length \(n\) such that \(s_G[i] = 1\) if \(i \in G\) and 0 otherwise. If \(G \in \text{Acc}(\xi)\) then \(\xi(s_G) = 1\) by definition. Note that this means line 21D will succeed for \(g = n + q\) when we run S2.Recover\(^H(S[G])\), which means that \(X_{n+q} = \bot\) and in turn \(M\) will be recovered correctly. On the other hand, suppose \(G \notin \text{Acc}(\xi)\), then \(\xi(s_G) = 0\). Note that this means line 21D will fail for \(g = n + q\) in S2.Recover\(^H(S[G])\), resulting in \(X_{n+q} = \bot\). Hence S2.Recover\(^H(S[G])\) will return \(\bot\) at line 21J.

**Full correctness of S3 = AX[\(S, f\)].** We first check that S3 satisfies basic correctness if S does. Let \(A \in S3.\text{Access}, M \in S3.\text{Message}, R \in \{0, 1\}^n, H \in \Omega\), and \(S \leftarrow S2.\text{Share}(\xi, M, R, \epsilon)\). Let \(G \subseteq \mathcal{P}([1..n(\text{Acc}(A))])\).

Consider S3.Recover\(^H(S[G])\). If \(G \in \text{Acc}(A)\), we note that by the basic correctness of S3, the correct \((K, S)\) can be recovered at line 316 and in turn the correct \(M\) and \(R\). This means that the check at 319 will also succeed and the \((A, M)\) returned by S3.Recover\(^H(S[G])\) is correct. On the other hand, suppose \(G \notin \text{Acc}(A)\). Then by the basic correctness of S3, S3.Recover\(^H(S[G])\) will return \(\bot\) at line 313. We move on to check the validity condition. Fix some \(H \in \Omega, K\), and \(S \in \text{Shares}\). Suppose \((M, R, V) \leftarrow S3.\text{Recover}(\xi, S)\). Then by construction (specifically line 31B), we know that \(V = S\) indeed came from an honest sharing of \(M\) and \(R\).

**Full correctness of S3 = EX[S].** Fix some scheme \(S\), \(H \in \Omega, A \in \text{Access}, M \in S3.\text{Message}, R \in \text{Rand}, T \in \text{Tag}\). Let \(S = S3.\text{Share}(\xi, M, R, T)\) and \(K \in \{A\} \cup \text{P}(S)\).

If \(G \in \text{Acc}(A)\) then full correctness of S implies that S3.Recover\(^H(K, S[G])\) = \((M, \text{R}, S[G])\), this also means that S3.Recover\(^H(K, S[G])\) = \((M, \text{R}, S[G])\) (line 83 terminates with \(i = 1\)). If \(G \notin \text{Acc}(A)\) then by monotonicity, we know that for any \(S' \subseteq S[G]\), S3.Recover\(^H(K, S')\) = \(\bot\). This means that S3.Recover\(^H(K, S[G])\) = \(\bot\) (must be returned at line 84). Validity condition is inherited because both scheme share the same sharing algorithm and that S3.Recover\(^H(K, S[G])\) only returns S3.Recover\((K, S')\) for some \(S' \subseteq S\).

### C.4 Proof of Proposition 1

Besides the use of the PRF \(f\), scheme S1 is essentially Shamir’s scheme [40]. The shares of Shamir’s scheme can be perfectly simulated as long as no more shares than the threshold is given out. Implementing this intuition, let us consider games \(G_0\) and \(G_1\) given in Fig. 14. Note that \(G_0\) is the same as \(G_{\text{priv}}^{\text{rev1}}\). Thus,

\[
\text{Adv}_{S,1}^{\text{priv}}(\xi) = 2 \cdot \text{Pr}[G_0] - 1 .
\]  

Since S1 does not use on any random-oracle-modeled hash function, we omit writing \(H\) and giving it to the adversary \(A\). We emphasize that since \(\xi \in \text{Priv}^{\text{rev}}, R\) is sampled uniformly at random for each DEAL query regardless of the \(R\) value in the input. Coefficients \(R_{i,j}\) are derived using \(f\) (with a uniformly random and independent seeds, \(R\)) in \(G_0\) but are randomly sampled in

\[
\text{Adv}_{S,1}^{\text{priv}}(\xi) = 2 \cdot \text{Pr}[G_0] - 1 .
\]
Game $G_0$, $G_1$, and $G_2$

$c \leftarrow \{0,1\}; \quad \alpha \leftarrow 0$
$(S_t, B) \leftarrow \Box^\text{Deal}$

if ( $\exists j : B[j] \in \text{Acc}(A[j])$ ) then return false
\[ c' \leftarrow \mathcal{A}(S_t, S_1, B[1], \ldots, S_n, B[n], P) \]
return (c = c')

procedure $\mathcal{A}(A, M_0, M_1, R, T)$

$M \leftarrow M_\alpha; \quad \alpha \leftarrow \alpha + 1; \quad (k, n) \leftarrow A; \quad R \leftarrow \{0,1\}^k$
$M_1 \cdots M_n \leftarrow \langle 0 \cdots 0 \rangle$

for (i,j) $\in [1,k-1] \times [1,m]$ do

$R_{i,j} \leftarrow \mathcal{R}_i(j, i); \quad G_1, G_2; \quad R_{i,j} \leftarrow \langle 0,1 \rangle^2$

for $i \in [1..n]$ do

for $j \in [1..m]$ do

$B_{i,j} \leftarrow M_j + R_{j,1} \cdot i + \ldots + R_{j,k-1} \cdot i^k$

$G_2; \quad \beta_{i,j} \leftarrow \langle 0 \cdots 0 \rangle$

$S_i \leftarrow (i, (k, n), B_{1, \ldots, B_{i-1}}, \cdot, \cdot, \cdot)$

$S_0 \leftarrow (S_1, \ldots, S_n); \quad P[\alpha] \leftarrow S_0; \quad \text{return} \quad \text{end procedure}$

Fig. 14. Game $G_0$, $G_1$, $G_2$ used in the proof of Proposition 1.

$\Box^\text{New,Fu}$

$c \leftarrow \{0,1\}; \quad \alpha \leftarrow 0$
$(S_t, B) \leftarrow \Box^\text{Deal}$

if ( $\exists j : B[j] \in \text{Acc}(A[j])$ ) then return false
\[ c' \leftarrow \mathcal{A}(S_t, S_1, B[1], \ldots, S_n, B[n], P) \]
return (c = c')

procedure $\mathcal{A}(A, M_0, M_1, R, T)$

$M \leftarrow M_\alpha; \quad \alpha \leftarrow \alpha + 1; \quad \text{New}(); \quad (k, n) \leftarrow A$
$M_1 \cdots M_n \leftarrow \langle 0 \cdots 0 \rangle$

for (i,j) $\in [1,k-1] \times [1,m]$ do

$R_{i,j} \leftarrow \mathcal{A}i(\alpha, \beta, (i, j))$

for $i \in [1..n]$ do

for $j \in [1..m]$ do

$B_{i,j} \leftarrow M_j + R_{j,1} \cdot i + \ldots + R_{j,k-1} \cdot i^k$

$S_i \leftarrow (i, (k, n), B_{1, \ldots, B_{i-1}}, \cdot, \cdot, \cdot)$

$S_0 \leftarrow (S_1, \ldots, S_n); \quad P[\alpha] \leftarrow S_0; \quad \text{return} \quad \text{end procedure}$

Fig. 15. PRF-adversary $\Box$ used in the proof of Proposition 1.

$G_1$. It is standard to check that

$\Pr[G_0] = \Pr[G_1] + \text{Adv}^\text{PRF}[\Box]$,

(4)

where $\Box$ is the PRF-adversary given in Fig. 15. Consider the game $G_2$ given in Fig. 14. The values of $B_{1,j}$ are randomly sampled in $G_2$. We claim that

$\Pr[G_1] = \Pr[G_2]$.

(5)

This is because for any random degree $k$ polynomial over $F$, any $k - 1$ distinct points are uniformly distributed.

Game $G_0$, $G_1$, and $G_2$

$c \leftarrow \{0,1\}; \quad \alpha \leftarrow 0$
$(S_t, B) \leftarrow \Box^\text{Deal}$

if ( $\exists j : B[j] \in \text{Acc}(A[j])$ ) then return false
\[ c' \leftarrow \langle 0 \cdots 0 \rangle \]
return (c' = c)

procedure $\mathcal{A}(A, M_0, M_1, R, T)$

$\alpha \leftarrow \alpha + 1; \quad A[\alpha] \leftarrow A; \quad M_0 = M_0$ \leftarrow $M_1$
$R_0 \leftarrow R \leftarrow \{0,1\}^k; \quad (n_a, q_a, m_a, t_a) \leftarrow A$

for $i \in [1..n + q]$ do

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

if $X_i \in X'$ then

bad $\leftarrow$ true

$G_0; \quad X_i \leftarrow f_{\text{PRF}}(i)$

$X \leftarrow X \cup \{X_i\}$

for $g \in [n + 1..n + q]$ do

$(\epsilon_1, \ldots, \epsilon_q) \leftarrow (g, n, g)\leftarrow \text{th}(g)$

$(X_1, \ldots, X_n, g) \leftarrow \text{share}^R_{\beta, g, \lambda}(X_g)$

For $i \in [1..n]$ do $L_{i,g} \leftarrow X_i \oplus H^\lambda(i, g, X_i)$

$L \leftarrow \langle L_{1,g}, g \in [n+1..n+q]; i \in \text{in}(g)\rangle$

$C \leftarrow H^{\lambda(n+q)}(X_{n+q}) \oplus M_i; \quad \ell \leftarrow \langle C, L\rangle$

for $i \in [1..n]$ do $S_i \leftarrow (i, A, X_i, \ell, \cdot, \cdot, \cdot)$

$S^{(\alpha)} \leftarrow (S_1, \ldots, S_n); \quad P[\alpha] \leftarrow S^{(\alpha)}; \quad \text{return} \quad \text{end procedure}$

procedure $\text{Hash}^\lambda(x)$

if not $T[x, \ell]$ then $T[x, \ell] \leftarrow \{0,1\}^\ell$

return $T[x, \ell]$

Fig. 16. Games $G_0$, $G_1$, $G_2$ used in the proof of Theorem 3. Algorithm score is defined in Fig. 12.

Note the two games return false if the adversary attempts to maintain more coins (points) than the threshold $k$. Finally, since the information given to $\mathcal{A}$ does not depend on the bit $c$ in game $G_2$, we have that

$\Pr[G_2] = \frac{1}{2}$.

(6)

Putting (3), (4), (5) and (6) together concludes the proof.

C.5 Proof of Theorem 3

Equation (2) holds trivially if $g \geq 2^k$, so we restrict to the case where $g < 2^k$. Let $\mathcal{A}$ be an adversary and consider the game $G_2^\text{PRF}(\mathcal{A})$, where $I \in \text{Priv}^\text{PRF}_R$. Recall that this is the class of input-selectors that select coins $R$ independently and uniformly at random for each $\text{Deal}$ query. Consider the games $G_0$, $G_1$ and $G_2$ given in Fig. 16. In contrast to $G_2^\text{PRF}(\mathcal{A}, M_0, M_1, \ell)$, we lazily sample $H$ for each query via the procedure $\text{HASH}$ given in game $G_0$ (which is the same one used for $G_1$ and $G_2$). Game

\[ \Box^\text{Dea} \]
Game $H_0$, $H_1$ and $H_2$

c ← \{0, 1\}; α ← 0; (S, B) ← T_{\text{Deal}}

for $i$ ← 1, . . . , α do

for $i$ ← 1, . . . , $n$ do $s_i[j] ← (i ∈ B[j])$

for $g$ ← $n_1 + 1$ to $n_1 + α$ do

$s_j[g] ← \text{TH}_{\text{std}(j)}(g; \text{in}(j)(g); s_j[\text{in}(j)[g]])$

$(i_1, . . . , i_θ) ← \text{in}(j)(g); α ← \text{th}(j)(g)$

$(X_{i_1}, . . . , X_{i_θ}) ← \text{share}_{k,n,g}(X_j)$

For $i$ ← 1, . . . , $n$

\[H_2: \text{if } s_j[g] = 0 \text{ then } X_i^{(α)} = \{0, 1\}^λ \]

$L_{i,g} ← X_i^{(α)} ⊕ H^λ(i,g,X_i)$

\[H_2': \text{if } (∃α : s_n[i^{(α)} + q^{(α)}] = 1) \text{ then return false} \]

$c' ← A^{H2}(S[1], . . . , S[n]; [B[1]], . . . , [B[n]]), P^{(1)}, . . . , P^{(α)})$

return $(c' = c)$

procedure Deal($A$, $M_0$, $M_1$, $R$)

α ← α + 1; $A[n] ← A; RL^{(α)} ← R = \{0, 1\}^κ$

$M_0^{(α)} ← M_0; M_1^{(α)} ← M_1$

$(n^{(α)}, q^{(α)}, \text{in}(g), \text{th}(g)) ← A$

for $i$ ← 1, . . . , $n^{(α)} + q^{(α)}$

\[X_i^{(α)} ← \{0, 1\}^λ \times X; V[X_i^{(α)}] ← α; X ← X \cup \{X\} \]

$L_i^{(α)} = L_i^{(0)} + 1; g ∈ [n^{(α)} + 1, n^{(α)} + g^{(α)}], i ∈ \text{in}(g)(g)$

$C^{(α)} ← \{0, 1\}^{|M|}; C ← (L^{(α)}, C^{(α)})$

for $i$ ← 1, . . . , $n$

\[$S_i^{(α)} ← (S_0, . . . , S_{nα}) ; P^{(α)} ← S^{(α)}_{\text{pub}} \]$

return $(c' = c)$

procedure Hash$^α(x)$

\[j ← \perp; \text{if } X[j] = 0 \text{ then } X[j] = \{0, 1\}^f \]

\[(i, g, X) ← X[V[X] \text{ and } i \neq j; Z ← X_i^{(j)} ⊕ z_j^{(j)}; (i_1, . . . , i_θ) ← \text{in}(j)(g); α ← i_θ \]

\[X ← X_i^{(j)} ⊕ z_j^{(j)}; X ← X \cup \{X\} \]

\[L_i^{(α)} = L_i^{(0)} + 1; g ∈ [n^{(α)} + 1, n^{(α)} + g^{(α)}], i ∈ \text{in}(g)(g) \]

$C^{(α)} ← \{0, 1\}^{|M|}; C ← (L^{(α)}, C^{(α)})$

for $i$ ← 1, . . . , $n$

\[$S_i^{(α)} ← (S_0, . . . , S_{nα}) ; P^{(α)} ← S^{(α)}_{\text{pub}} \]$

return $(c' = c)$

procedure $H_{\text{deal}}(x)$

\[j ← \perp; \text{if } (X[j] = 0 \text{ then } X[j] = \{0, 1\}^f \]

\[(i, g, X) ← X[V[X] \text{ and } i \neq j; Z ← X_i^{(j)} ⊕ z_j^{(j)}; (i_1, . . . , i_θ) ← \text{in}(j)(g); α ← i_θ \]

\[X ← X_i^{(j)} ⊕ z_j^{(j)}; X ← X \cup \{X\} \]

\[L_i^{(α)} = L_i^{(0)} + 1; g ∈ [n^{(α)} + 1, n^{(α)} + g^{(α)}], i ∈ \text{in}(g)(g) \]

$C^{(α)} ← \{0, 1\}^{|M|}; C ← (L^{(α)}, C^{(α)})$

for $i$ ← 1, . . . , $n$

\[$S_i^{(α)} ← (S_0, . . . , S_{nα}) ; P^{(α)} ← S^{(α)}_{\text{pub}} \]$

return $(c' = c)$

Fig. 18. PRF-adversary $B$ used in the proof of Theorem 3. Algorithm $Share$ is defined in Fig. 12.

whose PRF advantage bounds the closeness of these two games. We note that $G_1$ and $G_2$ are identical-until-bad. By the Fundamental Lemma of Game Playing [14] and the standard birthday argument,

\[
\Pr[G_1] - \Pr[G_2] \leq \Pr[G_1 \text{ sets bad}] = \frac{g(g-1)}{2^{λ+1}}. \tag{9}
\]

Next, we shall rewrite the code of Deal so that the labels $L$ do not contain information about bit $c$. Concretely, consider $H_0$ given in Fig. 17. The label $L_{i,j}^{(α)}$ are randomly sampled in $H_0$. Note that game $H_0$ “programs” the hash function given to $A$ to behave consistently with the $L_{i,j}^{(α)}$. Furthermore, in game $H_0$, we compute whether each wire is known to the adversary and store this information inside variable $s$. Specifically, $s_{n}[g] = 1$ if and only if the adversary can compute the label for wire $g$ in the $α$-th sharing from the set of corrupt shares. Game $H_0$ is constructed to behave identically to $G_2$, and

\[
\Pr[G_2] = \Pr[H_0]. \tag{10}
\]

Next, let us consider games $H_1$ given in Fig. 17. Game $H_1$ no longer programs Hash to return the correct value when the corresponding gate is not corrupt (unknown to the adversary via corrupt shares). Since $H_0$ and $H_1$ are identical-until-bad,

\[
\Pr[H_0] - \Pr[H_1] \leq \Pr[H_1 \text{ sets bad}]. \tag{11}
\]
We shall bound $\Pr[H_1]$ and $\Pr[H_1 \text{ sets bad.}]$. First, bit $c$ is only used when computing the value $Z$ for the output gates in HASH, and in $H_1$, HASH is not programmed to output $Z$ when the gate is not corrupt (which must be true for all output gates). Hence $H_1$ does not leak any information about bit $c$, and

$$\Pr[H_2] = \frac{1}{2}. \quad (12)$$

Next, consider $H_2$, which differ from $H_1$ only in the value of $X_{i,g}^{(a)}$ for $g \in \left\{ (n^{(a)} + 1) \ldots (n^{(a)} + q^{(a)}) \right\}$ such that $s_n[g] = 0$ (gate $g$ is not corrupt). Similar to the proof of Proposition 1, we can substitute the values of $s_n$ and the definition of $bad$. Hence for each value of $X_{i,g}^{(a)}$ we can substitute the values of $X_{i,g}^{(a)}$ to uniform random ones. So,

$$\Pr[H_1 \text{ sets bad.}] = \Pr[H_2 \text{ sets bad.}]. \quad (13)$$

Also, no information about $X_{i,g}^{(a)}$ is given if $s_n[g] = 0$. Hence for each Hash query there is at most $2^{-\lambda}$ probability of setting $bad$. Using a union bound over $q_n$ queries to Hash, we have

$$\Pr[H_2 \text{ sets bad.}] \leq \frac{q_n}{2^{\lambda}}. \quad (14)$$

Finally, Equation (2) is derived by combining Equations (7–14) and the definition of $\text{Adv}_{\text{priv}^S}$:

$$\text{Adv}_{\text{priv}^S}(S, [f, \lambda], \ell(A)) = 2 \Pr[\text{Adv}_{\text{priv}^S}(S, [f, \lambda], \ell(A))] - 1. \quad (15)$$

### C.6 Proof of Theorem 1

For part 1, consider the games $G_0$ and $G_1$ given in Fig. 19. For simplicity, we will consider oracles $h$ and $H$ separately. Our game sequence will modify the code for $H$ while keeping the code for $h$ unchanged. In addition, we will give adversary access to both $H$ and $h$, instead of Hash. Game $G_0$ is $G_{\text{priv}^S}(AA)$ with a lazily sampled $H$ (via procedure Hash) and the sharing algorithm of $SS$.Share. Queries to Hash in $G_0$ are programmed to be consistent with queries to $\text{Deal}$ (note that Hash queries happen after all $\text{Deal}$ queries are made). The only difference between game $G_1$ and game $G_0$ is that Hash is not programmed to be consistent with $\text{Deal}$ by omitting the boxed code. By construction, $G_0$ and $G_1$ are identical-until-bad. Hence

$$\frac{1}{2} + \frac{1}{2} \text{Adv}_{\text{priv}^S}(AA) = \Pr[G_0]$$

$$= \Pr[G_1] + (\Pr[G_0] - \Pr[G_1])$$

$$\leq \Pr[G_1] + \Pr[G_1 \text{ sets bad.}], \quad (15)$$

where the inequality is by the Fundamental Lemma of Game Playing [14]. We move on to bound $\Pr[G_1]$ and $\Pr[G_1 \text{ sets bad.}]$. Consider game $G_2$ and game $G_3$ given in Fig. 19. Game $G_2$ differs from $G_1$ only by the value of $Z$ given to $SS$.Share. Game $G_3$ differs from $G_2$ only in uniform sampling of ciphertext $C$ and $D$. We build input selector $I$ (which is in class $\text{I}_{\text{priv}^S}$) as well as PrivS adversaries $A_0$ and $A_1$ (all given in Fig. 20) such that

$$\Pr[G_1] = \Pr[G_2] + \text{Adv}_{\text{priv}^S}(A_0)$$

and

$$\Pr[G_1 \text{ sets bad.}] = \Pr[G_2 \text{ sets bad.}] + \text{Adv}_{\text{priv}^S}(A_1). \quad (17)$$

To check the above, notice that the only difference between $G_1$ and $G_2$ is the input message to $\text{Deal}$. Hence, we can utilize the PrivS game for the underlying scheme $S$ to bridge the different between $G_1$ and $G_2$. Furthermore, adversary $A_0$ is built to simulate and return the

![Fig. 19. Games $G_0$, $G_1$, $G_2$, and $G_3$ for proof of part 1 of Theorem 1. The boxed code are only executed by the game(s) indicated.](image-url)
Fig. 20. Left: input-selector \( \mathbb{I} \). Right: Adversaries \( A_0, A_1 \) and \( A \) for proof of part 1 of Theorem 1.

---

Fig. 21. Adversaries for part 1 of Theorem 1. Left: adversaries \( \mathcal{B}_0, \mathcal{B}_1, \) and \( \mathcal{B} \). Right: Predictor \( P \).
return value of either game $G_1$ or game $G_2$, while $A$ is built to simulate and return the flag $\text{bad}$. This justifies (16) and (17). Since $A$ behaves as $A_d$ based on a randomly chosen bit $d$,

$$
2 \cdot \text{Adv}^{\text{privs}}_{S,\bar{S}}(A) = \text{Adv}^{\text{privs}}_{S,\bar{S}}(A_0) + \text{Adv}^{\text{privs}}_{S,\bar{S}}(A_1) .
$$

(18)

We proceed to bound $\Pr[G_2]$ and $\Pr[G_2 \text{ sets bad}]$. We build PRF adversaries $\mathbb{B}_0$ and $\mathbb{B}_1$ (given in the left panel of Fig. 21) such that

$$
\Pr[G_2] = \Pr[G_3] + \text{Adv}^\text{prf}(\mathbb{B}_0) (19)
$$

and

$$
\Pr[G_2 \text{ sets bad}] = \Pr[G_3 \text{ sets bad}] + \text{Adv}^\text{prf}(\mathbb{B}_1) . (20)
$$

The above is true because the only different between game $G_2$ and game $G_3$ is how values of $C$ and $D$ are derived (game $G_2$ uses $f$ while game $G_3$ samples them uniformly at random). Since $B$ behaves as $\mathbb{B}_d$ based on a randomly chosen bit $d$,

$$
2 \cdot \text{Adv}^\text{prf}(\mathbb{B}) = \text{Adv}^\text{prf}(\mathbb{B}_0) + \text{Adv}^\text{prf}(\mathbb{B}_1) . (21)
$$

Finally, we claim that

$$
\Pr[G_3] = \frac{1}{2} 
$$

(22)

and

$$
\Pr[G_3 \text{ sets bad}] \leq (q_d + q) \cdot \text{pred}(\Pi) .
$$

(23)

Equation (22) is by the fact that no information about bit $c$ is leaked to either the input selector nor the adversary. Equation (23) is justified as follows. Consider a given in the right panel of Fig. 21, which makes at most $q_d + q$ queries to Hash. Predictor $P$ randomly selects and $(M, R)$ from one of the Hash queries to return as the its guess. If $G_3$ sets $\text{bad}$, then it must be that some query $X$ to Hash matches some $X_j$ during the execution of $AA$. We lastly need to check that the inputs and oracle for $AA$ is simulated correctly for $AA$ by $P$—this is possible because in $G_3$, variables $C, D$ and $Z$ are all uniformly random and can be simulated by $P$. This justifies Equation (23). Finally, Equation (1) is obtained by combining Equations (15–23).

For part 2, consider the game $G^\text{auth}_{SS}(A)$, modified as per our Section 6 discussion on adjusting Auth, to allow for Recover also returning coins. Let $(M, R, V)$ and $(M', R', V')$ be the variables defined on line 52' and 53'. If $V \cap V' \neq \perp$ and $(M, R) \neq (M', R')$ it must be that there is a collision among the $J$-values in the two different sharings—that is, a collision on the first $2\kappa$-bits in the output of $H$. This is because line 31B ensures that the $J_i$ values are the same across all shares. Overall, there are at most $q_3 + 2$ queries to $H$ (since Recover calls $H$ exactly once). Hence the game outputs true with probability at most $(q_3 + 1)(q_3 + 2)^{-2\kappa}$.

### C.7 Proof of Theorem 2

For part 1, consider the adversary $A$ (constructed from $AA$) and games $G_0, G_1$ given in Fig. 22. Adversary $A$ runs $AA$ to obtain inputs that it forwards to $SS\text{Recover}$, and returns only the valid sets of shares $\mathcal{V}_{SS}^\text{SS}, \mathcal{V}'_{SS}$ returned by $SS\text{Recover}$. By construction $G_0 = G^\text{auth}_{SS}(AA)$ and $G_1 = G^\text{auth}_{SS}(A)$. By construction of EX (in particular line 83 in Fig. 9) and the full correctness of $SS$, we know that if neither of the two runs of $SS\text{Recover}$ returns $\perp$ then it must be that $\mathcal{V}_{SS} = \mathcal{V}_{SS}^\text{SS}, \mathcal{V}'_{SS} = \mathcal{V}'_{SS}, M_{SS} = M_{SS}^\text{SS}$, and $M_{SS}' = M_{SS}'^\text{SS}$. Hence

$$
\text{Adv}^\text{auth}_{SS}(AA) = \Pr[G_0] \leq \Pr[G_1] = \text{Adv}^\text{auth}_{SS}(A) . (24)
$$

which concludes the proof for part 1.

For part 2, fix some $H \in \Omega$. We claim that for any $(K, S)$,

$$
SS\text{Recover}^H(K, S) = \text{UniqueExplanation}^H(K, S) .
$$

Before we show this we first point out some useful facts about $SS\text{Recover}$ and $\text{SRecover}$. First, if $\text{SRecover}^H(K, S) = (M, R, S)$ then $SS\text{Recover}^H(K, S) = (M, R, S)$ (take $S_1 = S$ at the for loop at line 82). Second, if $SS\text{Recover}^H(K, S) \neq \perp$ then it must be that $SS\text{Recover}^H(K', S') \neq \perp$ for some $S' \subseteq S$. Now to show (25), consider the set $E = \text{Explanations}^H(K, S)$ and consider the following cases.

Case 1: $E = \emptyset$. First, we necessarily have

$$
\text{UniqueExplanation}^\text{Hash}(K, S) = \perp
$$

by the definition of UniqueExplanation. Second, $SS\text{Recover}^H(K, S)$ is also $\perp$ since there does not exists $S_i \subseteq S$ that makes $S\text{Recover}^H(K, S_i)$ return non-$\perp$.

Case 2a: $E \neq \emptyset$, $\text{UniqueExplanation}^H(K, S) = \perp$. We will show that $SS\text{Recover}^H(K, S) = \perp$. Let $S_1, \ldots, S_w$ be the $K$-plausible shares defined on line 80 of $SS\text{Recover}^H(K, S)$. Let $S_i$ be the first share (smallest $i$) for which $(M, R, V) \leftarrow S\text{Recover}^H(K, S_i)$ and $S_i = \perp$ is true. Note that $SS\text{Recover}(K, S_i)$ must also return $(M, R, V)$. Hence $S_i \in \text{Explanations}^H(K, S)$. We claim that there must exist some $j > i$ such that $S_j \in \text{Explanations}^H(K, S)$ and $S_j \not\subseteq S_i$. This is the by
the fact that UniqueExplanation$^H(K, S)$ returns ⊥. To see this, suppose for contradiction that for all $j > i$ such that $S_j \in \text{Explanations}^H(K, S)$, $S_j \subsetneq S_i$. Then since the list of $K$-plausible shares were exhaustive, $S_i$ must have made the if statement at line 73–75 true, which contradicts the assumption for case 2a. The existence of such $S_j$ means that for $(M_j, R_j, V_j) \leftarrow \text{SS.} \text{Recover}^H(K, S_j)$, $V_j \subseteq V_i$. Lastly, there exists some $k \geq j$ such that $S_k = V_j$. Furthermore, we have that for $(M_k, R_k, V_k) \leftarrow \text{SS.} \text{Recover}^H(K, S_k)$, $V_k \subseteq V_i$. This means that $\text{SS.} \text{Recover}^H(K, S)$ returns ⊥ at line 88.

Case 2b: $E \neq \emptyset$, UniqueExplanation$^H(K, S) \neq \bot$. We will show that $\text{SS.} \text{Recover}^H(K, S) \neq \bot$. Let $S_0 \subseteq S$ be a set of shares whose recovery $(M, R, V) \leftarrow \text{SS.} \text{Recover}^H(K, S)$ makes the if-statement true at line 73 of UniqueExplanation$^H(K, S)$. Let $S_1, \ldots, S_w$ be the $K$-plausible shares defined on line 80 of $\text{SS.} \text{Recover}^H(K, S)$. Now consider the sequence of $K$-plausible shares resulting from $S_0 \subseteq S$ (this is a subsequence of $S_1, \ldots, S_w)$, say $S'_1, \ldots, S'_v$. Suppose $S'_v = S_j$ for some $j \geq 1$ (there is a unique $j$ that satisfy this). We claim that for any $0 < i < j$ either $\text{SS.} \text{Recover}^H(K, S_i) = \bot$ or $(\cdot, V_i) \leftarrow S_i$, $V_i \neq S_i$. This means that during the run of $\text{SS.} \text{Recover}^H(K, S)$, the for-loop at line 83 ends with $i = j$. Seeking a contradiction, suppose $\text{SS.} \text{Recover}^H(K, S_i) \neq \bot$ and for $(\cdot, V_i) \leftarrow S_i$, $V_i = S_i$. We know that $S_i \in \text{Explanations}^H(K, S)$. Hence $S_i = V_i \subseteq V_j$. This means that $j \leq i$, which contradicts the assumption that $i < j$. Lastly, note that $\text{SS.} \text{Recover}^H(K, S)$ only returns ⊥ if there exists $S' \in \{S_1, \ldots, S_w\} - \mathcal{P}(S_j)$ such that $\text{SS.} \text{Recover}^H(K, S') = (\cdot, S')$ and $S' \not\subseteq S_j$ (note that $\text{SS.} \text{Recover}^H(K, S') = \text{S.} \text{Recover}^H(K, S')$ here). But this cannot be true since this would mean that $S' \in \text{Explanations}^H(K, S)$ and it would have made UniqueExplanation$^H(K, S)$ return ⊥.