Bingo: Adaptivity and Asynchrony in Verifiable Secret Sharing and Distributed Key Generation

Ittai Abraham[1], Philipp Jovanovic[2], Mary Maller[3], Sarah Meiklejohn[2,4], and Gilad Stern[5](✉)

[1] Intel Labs, Petach Tikva, Israel
[2] University College London, London, UK
[3] Ethereum Foundation and PQShield, Bern, Switzerland
mary.maller@ethereum.org
[4] Google, Mountain View, USA
[5] The Hebrew University of Jerusalem, Jerusalem, Israel
gilad.stern@mail.huji.ac.il

Abstract. We present Bingo, an adaptively secure and optimally resilient packed asynchronous verifiable secret sharing (PAVSS) protocol that allows a dealer to share $f + 1$ secrets with a total communication complexity of $O(\lambda n^2)$ words, where λ is the security parameter and n is the number of parties. Using Bingo, we obtain an adaptively secure validated asynchronous Byzantine agreement (VABA) protocol that uses $O(\lambda n^3)$ expected words and constant expected time, which we in turn use to construct an adaptively secure high-threshold asynchronous distributed key generation (ADKG) protocol that uses $O(\lambda n^3)$ expected words and constant expected time. To the best of our knowledge, our ADKG is the first to allow for an adaptive adversary while matching the asymptotic complexity of the best known static ADKGs.

1 Introduction

The ability of a party to distribute a secret among a set of other parties (i.e., *secret sharing*) is a fundamental cryptographic primitive, with applications such as Byzantine agreement, threshold cryptography, and secure multiparty computation [1–5]. At its most basic level, secret sharing involves one honest dealer, sharing one secret among a set of n parties, so that if at least t parties coordinate they can reconstruct the secret (where notably an adversary is assumed to control strictly fewer than t parties).

There are many functional enhancements of secret sharing, including *verifiable* secret sharing (VSS) [6], where parties can verify the validity of their shares even in the face of a malicious dealer, and *packed* secret sharing [7], where a dealer can deal m secrets in a way that is more efficient than just running m iterations of the protocol. In terms of enhancements to the network model, *asynchronous* secret sharing [8,9] requires no assumptions about the delay on

H. Handschuh and A. Lysyanskaya (Eds.): CRYPTO 2023, LNCS 14081, pp. 39–70, 2023.
https://doi.org/10.1007/978-3-031-38557-5_2

messages between parties or the order in which they are received. Finally, and crucially for systems that are expected to run for long periods of time, *adaptively secure* secret sharing protocols [10] allow the adversary to corrupt parties over time rather than starting with a static set of parties that it controls.

Verifiable secret sharing has traditionally seen many applications in multiparty computation [4,11,12]. In recent years, people have also noticed the potential of VSS for preventing malicious MEV (*maximal extractable value*) in blockchains [13,14]. Indeed, frontrunning-as-a-service companies such as Flashbots are able to extract millions of dollars of value by reordering transactions on the Ethereum blockchain,[1] and in doing so increase overall costs for users. Using VSS, parties could share their transactions among a set of validators rather than sending them in the clear. It is crucial in this and many other real-world settings for the VSS to be not only efficient but also adaptively secure even when operated over an asynchronous network such as the internet.

Our main construction, Bingo, fills exactly this gap: it is an adaptively secure packed asynchronous verifiable secret sharing (PAVSS) protocol that allows a dealer to share $f + 1$ secrets with a total communication complexity of just $O(\lambda n^2)$ words, where n is the total number of parties and f is the number of malicious parties. Additionally, Bingo is *optimally resilient* in assuming that $n = 3f + 1$, and supports three different types of reconstruction:

- Reconstruction of a single secret, which does not reveal any information about any non-reconstructed secrets.
- Given an index k, reconstruction of the sum of the k-th secrets shared by several different dealers, which does not reveal any information about any non-reconstructed secrets.
- Reconstruction of all secrets at once, which can be viewed as reconstructing a degree-$2f$ sharing.

Each of these has a word complexity of $O(\lambda n^2)$ and requires a constant number of rounds. In terms of assumptions, Bingo requires a PKI and a univariate powers-of-tau setup [15] (of size $O(\lambda n)$ words) and is proved secure against algebraic adversaries [16].

Using Bingo, we construct two more advanced primitives: *validated asynchronous Byzantine agreement* (VABA) and *distributed key generation* (DKG). These are both essential protocols in constructing secure distributed systems, with DKG in particular emerging as an important tool for supporting a variety of distributed applications [3,5,17]. Again, for both of these protocols to be run in realistic distributed environments like the internet, it is essential that they be asynchronous and adaptively secure.

We first use Bingo to construct an adaptively secure VABA protocol that reaches agreement on messages of size $O(n)$ and requires just $O(\lambda n^3)$ words. Second, we use Bingo and our VABA protocol to construct an adaptively secure high-threshold *asynchronous* distributed key generation (ADKG) protocol. Our ADKG protocol requires just $O(1)$ expected rounds and $O(\lambda n^3)$ expected words,

1 https://explore.flashbots.net/.

and has a secret key that is a field element (which in particular makes it compatible with standard threshold signature schemes like BLS [18]). We rely on the one-more discrete log assumption and prove security with respect to algebraic adversaries [16]; recent work by Bacho and Loss suggests that these relatively strong assumptions may be needed to support adaptively secure DKG for BLS [19]. To the best of our knowledge, ours is the first asynchronous protocol to be proven adaptively secure, and even previous synchronous adaptively secure protocols required $\Omega(n^4)$ sent words [19,20].

1.1 Technical Overview

The conceptual decomposition of distributed protocols to a distributed computing part against a weaker adversary and a cryptographic commitment and zero-knowledge part goes back to the foundational result of Goldreich, Micali, and Wigderson [21]. Here we present a high-level overview of Bingo by decomposing it into two parts: an efficient distributed protocol that is resilient to *omission failures* (i.e., failures that are non-malicious) and an efficient polynomial commitment scheme that essentially forces the malicious adversary to behave as an omission adversary. We start in Sect. 3 with our polynomial commitment scheme, then show in Sect. 4 how to use it to get an AVSS, Bingo, that tolerates adaptive malicious adversaries. Our construction builds on the KZG polynomial commitment scheme [22], which means relying on a powers-of-tau setup [15]. Our public parameters are backwards compatible with prior universal setups [23].

Step One: Bingo for Omission Failures. In this setting, the goal is to share a degree-$2f$ polynomial among $3f+1$ parties, f of which may suffer omission failures. Due to asynchrony, the dealer can interact with only $2f+1$ parties, and since f of them may have omission failures, the remaining $f+1$ honest parties need to enable all honest parties to eventually receive their share of the secret. Here we use the known technique [4,24–26] of having the dealer share a bivariate polynomial $\phi(X,Y)$ of degree at most $2f$ in X and degree f in Y. Visually, we think of a matrix of size $n \times n$ of the evaluations of $\phi(X,Y)$ at roots of unity $\{\omega_1,\ldots,\omega_n\}$, as shown in Fig. 1. As such, we think of the polynomial $\phi(X,\omega_i)$ as the i-th *row* of the polynomial, which we denote by α_i, and the polynomial $\phi(\omega_i,Y)$ as the i-th *column* of the polynomial, which we denote by β_i. The dealer then sends each party i the i-th row. Each party can then wait for $2f+1$ parties to acknowledge receiving their rows before knowing that they will be able to complete the protocol. This works because once $f+1$ honest parties have their row we are guaranteed that all honest parties will eventually be able to recover their share in the following way: First, each honest party i that received a row from the dealer sends each party j the value $\phi(\omega_j,\omega_i)$. Hence each honest party j receives at least $f+1$ points on its j-th column and is able to reconstruct it. Second, once party j reconstructs its column, it sends each party i the value $\phi(\omega_j,\omega_i)$. In this way, all honest parties eventually reconstruct their columns, so each honest party i hears at least $2f+1$ values for row i and can reconstruct it.

As described, each party needs to send just $O(n)$ words and the protocol takes a constant number of rounds.

$$
\begin{array}{c|ccccccc}
 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 & \beta_6 & \beta_7 \\
\hline
\alpha_1 & v_{11} & v_{12} & v_{13} & v_{14} & v_{15} & v_{16} & v_{17} \\
\alpha_2 & v_{21} & v_{22} & v_{23} & v_{24} & v_{25} & v_{26} & v_{27} \\
\alpha_3 & v_{31} & v_{32} & v_{33} & v_{34} & v_{35} & v_{36} & v_{37} \\
\alpha_4 & v_{41} & v_{42} & v_{43} & v_{44} & v_{45} & v_{46} & v_{47} \\
\alpha_5 & v_{51} & v_{52} & v_{53} & v_{54} & v_{55} & v_{56} & v_{57} \\
\alpha_6 & v_{61} & v_{62} & v_{63} & v_{64} & v_{65} & v_{66} & v_{67} \\
\alpha_7 & v_{71} & v_{72} & v_{73} & v_{74} & v_{75} & v_{76} & v_{77}
\end{array}
\qquad
\begin{array}{c|ccccccc}
 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 & \beta_6 & \beta_7 \\
\hline
\alpha_1 & v_{11} & v_{12} & v_{13} & v_{14} & v_{15} & v_{16} & v_{17} \\
\alpha_2 & \boxed{v_{21}} & v_{22} & \boxed{v_{23}} & v_{24} & \boxed{v_{25}} & \boxed{v_{26}} & \boxed{v_{27}} \\
\alpha_3 & v_{31} & v_{32} & v_{33} & v_{34} & v_{35} & v_{36} & v_{37} \\
\alpha_4 & v_{41} & v_{42} & v_{43} & v_{44} & v_{45} & v_{46} & v_{47} \\
\alpha_5 & v_{51} & v_{52} & v_{53} & v_{54} & v_{55} & v_{56} & v_{57} \\
\alpha_6 & v_{61} & v_{62} & v_{63} & v_{64} & v_{65} & v_{66} & v_{67} \\
\alpha_7 & v_{71} & v_{72} & v_{73} & v_{74} & v_{75} & v_{76} & v_{77}
\end{array}
$$

Fig. 1. A graphical representation of Bingo's sharing process showing the two ways in which party i can obtain their secret polynomial. The row polynomials are denoted by $\alpha_i = \phi(X, \omega_i)$ whereas the column polynomials are denoted by $\beta_i = \phi(\omega_i, Y)$. On the left-hand side, party 2 receives α_2 directly from the (honest) dealer. On the right-hand side, party 2 did not receive their polynomial from the dealer. Instead i receives evaluations of the column polynomials β_j from at least $2f+1$ other parties. Because $\beta_j(\omega_2) = \alpha_2(\omega_j)$, this is equivalent to obtaining $2f+1$ evaluations of α_2, meaning party 2 can obtain α_2 by interpolation.

Step Two: Bingo for Malicious Failures. In order to move from omission failures to malicious failures with adaptive security, we use a perfectly hiding bivariate *polynomial commitment scheme* (PCS) that essentially forces the malicious parties to act as if they can only have omission failures.

Our bivariate PCS has five desirable properties: (1) it requires a standard $O(\lambda n)$ univariate powers-of-tau setup; (2) a commitment has size $O(\lambda n)$; (3) given a commitment to $\phi, \hat{\phi}$, one can generate commitments to all rows; (4) given $f+1$ evaluations on column j, one can generate evaluation proofs for all points of column j; and (5) given $2f+1$ evaluations on row i, one can generate evaluation proofs for all points in row i. Perhaps surprisingly, our PCS commits to a bivariate polynomial $\phi(X, Y)$ of degree f in each column and degree $2f$ in each row by simply committing to $f+1$ specific rows, where a commitment to row i is just a KZG univariate polynomial commitment for $\phi(X, \omega_i)$ of degree $2f$. It is easy to see that this fulfills the first two properties. For the third property, we prove that interpolation in the exponent of any $f+1$ row commitments generates commitments to all rows. In order to reduce computation costs, it is also possible to compute the interpolated coefficients and send them instead of sending the commitments. Every party can then evaluate commitments in the exponent instead of interpolating $f+1$ commitments and evaluating the rest.

From Bingo to VABA and ADKG. We detail how to use Bingo to obtain a VABA protocol and an ADKG protocol in Sect. 5. Using Bingo's $O(n^2)$ word complexity for packing $O(n)$ secrets allows us to associate with each party a random value based on secrets from $f+1$ parties at a total cost of just $O(n^3)$ words. This random value, when used as a party's rank, allows us to construct adaptively secure *leader election* and *proposal election* protocols, which in turn allow us to build a VABA protocol with $O(n^3)$ expected word complexity for

Table 1. A comparison of AVSS schemes, in terms of: (1) the best amortized word complexity and (2) the batch size needed to obtain that complexity; (3) the need to rely on a CRS setup (where ● means there is no trusted setup and ○ means there is); (4) the maximum degree of the shared polynomial (where the schemes with maximum degree $2f$ can be used for sharing any degree between f and $2f$); and (5) the cryptographic assumptions needed to prove security. None of the prior schemes have been proved secure against an adaptive adversary, and all schemes have a constant round complexity.

Scheme	Word complexity	Batch size	CRS setup	Max degree	Assumptions
Cachin et al. [1]	$O(\lambda n^3)$	$O(1)$	●	$2f$	DL
Backes et al. [27]	$O(\lambda n^2)$	$O(1)$	○	f	q-SDH, q-polyDH
Haven [28]	$O(\lambda n)$	$O(n \log n)$	●	$2f$	DL, ROM*
hbACSS [29]	$O(\lambda n)$	$O(n^2)$	○	f	q-SDH
Bingo (this work)	$O(\lambda n)$	$O(n)$	○	$2f$	q-SDH, AGM

* Haven requires the secret to be distributed uniformly at random.

$O(n)$ sized inputs. This construction uses the ability to individually reconstruct sums of secrets shared by different dealers.

To obtain an ADKG, each party uses Bingo's $O(n^2)$ word complexity for a *high threshold* secret; i.e., with a threshold of $2f + 1$ (or more generally any threshold between $f+1$ and $2f+1$). Using the VABA protocol above on inputs formed from $f + 1$ completed high-threshold sharings allows us to reach agreement on a common BLS secret key formed from the sum of $f+1$ high-threshold secret sharings. Once agreement is reached, we reveal the BLS public key by using the standard "recovering in the exponent" technique. We prove that the resulting BLS signature scheme is adaptively secure using the framework of Bacho and Loss [19], relying on the $2f + 1$-one-more discrete log assumption and the algebraic group model.

1.2 Related Work

Tables 1 and 2 provides a comparison with the most relevant prior AVSS and ADKG schemes. Cachin et al. [1] study asynchronous verifiable secret sharing (AVSS) in the computational setting. The earlier works of Feldman and Micali [35] and Canetti and Rabin [9] study AVSS in the private channel setting. Backes, Datta, and Kate [27] provide the first construction with asymptotically optimal $\mathcal{O}(\lambda n^2)$ word complexity for AVSS. They use the seminal pairing-based polynomial commitment scheme due to Kate, Zaverucha, and Goldberg (KZG) [22]. Compared to Backes et al., we provide the same asymptotically optimal $O(\lambda n^2)$ word complexity with an $O(n)$ improvement in the size of the secret and a scheme that is proven to be adaptively secure.

AlHaddad, Varia, and Zhang [28] obtain a high-threshold AVSS, Haven, for uniformly random secrets with $O(n^2)$ word complexity. Moreover, their scheme can be instantiated with a setup-free polynomial commitment scheme [36–39] at

Table 2. A comparison of ADKG schemes, in terms of: (1) the best word complexity; (2) the expected number of rounds; (3) the need to rely on a CRS setup (where ● means there is no trusted setup and ○ means there is); (4) the maximum reconstruction threshold; and (5) the cryptographic assumptions needed to prove security. None of the prior schemes have been proved secure against an adaptive adversary.

Scheme	Word complexity	Rounds	CRS setup	Max threshold	Assumptions
Kate et al. [30]	$O(\lambda n^4)$	$O(n)$	●	f	DL, ROM
Kokoris-Kogias et al. [17]	$O(\lambda n^4)$	$O(n)$	●	$2f$	DL
Abraham et al. [31]	$O(\lambda n^3)$	$O(1)$	●	f	SXDH, BDH, ROM†
Das et al. [32]	$O(\lambda n^3)$	$O(\log n)$	●	$2f$	DDH, ROM
Groth and Shoup [33]	$O(\lambda n^3)$	$O(1)$	●	f	DL, ROM
This work	$O(\lambda n^3)$	$O(1)$	○	$2f$	q-SDH$^\diamond$

† Abraham et al. require the secret key to be a group element.

$^\diamond$ We prove that our protocol satisfies oracle-aided simulatability [19], as opposed to the more general notions of secrecy [34] or key expressability [3]. To some extent, this can be thought of as introducing a reliance on the one-more discrete logarithm (OMDL) assumption.

a $O(n^2 \log n)$ word complexity. Because our construction enables packed secret sharing and allows for arbitrary secrets, we can share n arbitrary secrets with the same word complexity ($O(n^2)$) that it takes AlHaddad et al. to share one random secret.

Yurek et al. [29] provide three variant protocols called hbACSS, which are proved secure against a static adversary. These protocols achieve batching rather than packing (because they use an f-by-f polynomial), but for each shared secret they are (quasi)linear in both computation and communication overhead in an amortized sense. While AVSS protocols with efficient batching allow for sharing many secrets more efficiently than sharing them separately, packed secret sharing protocols [7] do so by sharing them on the same high-degree polynomial. These sharings can then be used where high-degree polynomials are needed (e.g. in high-degree DKGs), whereas simple batching does not suffice for these purposes. Because Bingo is packed (due to its use of a $2f$-by-f polynomial) it achieves linear overheads after sharing $O(n)$ secrets (which we rely on in our leader election protocol), whereas the hbACSS protocols achieve the same overheads after sharing $O(n^2)$ secrets. A construction using a $2f$-by-f bivariate polynomial has previously been suggested in [40].

There has been considerable recent interest in practical ADKG and the building blocks needed to support it. Kokoris-Kogias, Malkhi, and Spiegelman [17] obtain a high threshold ADKG with $O(n^4)$ communication complexity and $O(n)$ rounds. Gurkan et al. suggest an aggregatable publicly verifiable secret sharing (PVSS) scheme [3] that builds upon the SCRAPE PVSS of Cascudo and David [41]. When combined with the consensus protocol of Abraham et al. [31], the result of Gurkan et al. yields a high-threshold ADKG with $O(n^3 \log n)$ communication complexity and $O(1)$ expected time that is secure against static adversaries. Their secret key is a group element, however, which makes it incompatible with commonly used threshold cryptography schemes, such as BLS, that require field elements as secrets. Cascudo and David [42] introduce Albatross, which uses packed secret sharing to build a randomness beacon that shares $O(n^2)$ random values. Albatross also uses the SCRAPE PVSS as a backend and thus cannot be used to share a field element (and has a static security proof).

Das, Xiang, and Ren [43] provide a reliable broadcast protocol that, among other improvements, removes the logarithmic factor from the consensus protocol of Abraham et al. [31] to get $O(n^3)$ communication complexity and $O(1)$ expected time. Das et al. [32] provide a high-threshold DKG that has a field element as a secret key, $O(n^3)$ word complexity, and is secure against a static adversary. In the optimistic case it runs in $O(1)$ rounds, but in the face of a Byzantine attacker it requires an expected $O(\log(n))$ rounds.

Groth and Shoup [33] provide a DKG that has $O(n^3)$ word complexity and avoids a trusted setup. There is a rigorous security analysis only for static corruptions, however, and their scheme doesn't support high-threshold reconstruction. In terms of their underlying AVSS, it has an amortized linear cost with a batch size of $n \log n$. We get the same amortized cost for a batch size of n, which we need in our weak leader election protocol (in the full version of the paper [44]).

2 Definitions

In this section we start by defining basic notation, and then defining polynomial commitment schemes and reliable broadcast as basic building blocks to be used in our constructions. Following that, we discuss the way we model interactive protocols in order to finally define packed asynchronous verifiable secret sharing.

2.1 Preliminaries

For a finite set S, we denote by $|S|$ its size and by $x \xleftarrow{\$} S$ the process of sampling a member uniformly from S and assigning it to x. Further, $\lambda \in \mathbb{N}$ denotes the security parameter and 1^λ denotes its unary representation. For two integers $i \leq j$, we define $[i, j] = \{i, \ldots, j\}$, and for every $n \in \mathbb{N}$ we define $[n] = \{1, \ldots, n\}$. We define $\omega_1, \ldots, \omega_n$ to be n different roots of unity of order $n + f$. In a slight abuse of notation, we define ω_0 to be 0 and $\omega_{-f}, \ldots, \omega_{-1}$ to be the remaining f roots of unity of order $n + f$. PPT stands for probabilistic polynomial time. By $y \leftarrow A(x_1, \ldots, x_n)$ we denote running algorithm A on inputs $x_1, \ldots, x_n$ and assigning its output to y, and by $y \xleftarrow{\$} A(x_1, \ldots, x_n)$ we denote running $A(x_1, \ldots, x_n; R)$ for a uniformly random tape R. Adversaries are modeled as randomized algorithms. We use code-based games in our security definitions [45]. A game $\mathsf{G}^{\mathsf{sec}}_{\mathcal{A}}(\lambda)$, played with respect to a security notion sec and adversary $\mathcal{A}$, has a MAIN procedure whose output is the output of the game. $\Pr[\mathsf{G}^{\mathsf{sec}}_{\mathcal{A}}(\lambda)]$ denotes the probability that this output is equal to 1.

Our constructions rely on the discrete logarithm assumption (dlog) which says that it is hard to output x given g^x, where g is a generator of a group $\mathbb{G}$ of prime order p and $x \xleftarrow{\$} \mathbb{F}_p$. We also rely on the *q-strong Diffie-Hellman* assumption ($\mathsf{q\text{-}sdh}$) [46], which says that it is hard to output a pair $(c, g^{1/(x+c)})$ given $(g, g^x, g^{x^2}, \ldots, g^{x^q}, \hat{g}, \hat{g}^x) \in \mathbb{G}_1^{q+1} \times \mathbb{G}_2^2$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are groups of prime order p, generated by g and $\hat{g}$, and form a bilinear group, q is an integer, and $x \xleftarrow{\$} \mathbb{F}_p$. Finally, our DKG application relies on the k-one-more discrete logarithm (omdl) assumption [47], which says that it is hard to output $(x_1, \ldots, x_k) \in \mathbb{F}_p^k$ given $(g, g^{x_1}, \ldots, g^{x_k}) \in \mathbb{G}^{k+1}$, where g is a generator of a group $\mathbb{G}$ of prime order p and $x_1, \ldots, x_k \xleftarrow{\$} \mathbb{F}_p$, and at most $k-1$ queries to a discrete log oracle DL that on input X outputs $\log_g(X)$. We use bp to denote the parameters defining a bilinear group with extra generators; i.e., $\mathsf{bp} = (g, \hat{g} \in \mathbb{G}_1, h \in \mathbb{G}_2, \mathbb{G}_T, e)$.

Some properties of our constructions are proved secure in the algebraic group model (AGM) [16]. In the AGM, whenever an adversary outputs a group element it must output the algebraic representation of that element relative to all the group elements it has seen thus far; i.e., if it has seen $X_1, \ldots, X_m$ then upon outputting a new element Y it must output $a_1, \ldots, a_m$ such that $Y = \prod_i X_i^{a_i}$.

2.2 Polynomial Commitments

We define a *polynomial commitment scheme* (PCS) as consisting of the following algorithms:

- $\mathsf{srs} \xleftarrow{\$} \mathsf{Setup}(1^\lambda)$ takes as input a security parameter and outputs a commitment key srs.
- $\boldsymbol{C} \xleftarrow{\$} \mathsf{Commit}(\mathsf{srs}, \phi)$ takes as input the commitment key and a polynomial ϕ and outputs a commitment $\boldsymbol{C}$. We often specify the randomness $\hat{\phi}$ explicitly using the notation $\boldsymbol{C} \leftarrow \mathsf{Commit}(\mathsf{srs}, \phi, \hat{\phi})$.
- $m, \hat{m}, \pi \leftarrow \mathsf{Eval}(\mathsf{srs}, \phi, \hat{\phi}, \omega)$ takes as input a commitment key, a pair of polynomials, and a point on which to evaluate. It returns $m = \phi(\omega)$, $\hat{m} = \hat{\phi}(\omega)$ and a proof π that $m, \hat{m}$ are consistent with ω.
- $0/1 \leftarrow \mathsf{Verify}(\mathsf{srs}, \boldsymbol{C}, \omega, m, \hat{m}, \pi)$ takes as input a commitment key, a commitment, an opening point, a pair of openings, and a proof π. It returns 1 if it is convinced that $(m, \hat{m})$ is a valid opening of $\boldsymbol{C}$ at ω and 0 otherwise.

In what follows, we often omit the commitment key srs as an explicit input to the other algorithms. Following Kate et al. [22], we require that a PCS satisfies *correctness*, meaning that $\mathsf{Verify}(\mathsf{Commit}(\phi, \hat{\phi}), \omega, \mathsf{Eval}(\phi, \hat{\phi}, \omega)) = 1$ and both *polynomial binding* and *evaluation binding*. These say, respectively, that an adversary cannot open a single commitment to two different values and that an adversary cannot output two valid but incompatible evaluations of the same pair of polynomials, as represented by a single commitment.

Definition 1 (Polynomial binding). [22] *Consider a game* $\mathsf{G}_{\mathcal{A}}^{poly\text{-}binding}(\lambda)$ *in which an adversary* $\mathcal{A}$ *takes* 1^λ *as input and outputs the tuple* $(\phi_1, \hat{\phi}_1, \phi_2, \hat{\phi}_2)$, *and wins if (1)* $\mathsf{Commit}(\phi_1, \hat{\phi}_1) = \mathsf{Commit}(\phi_2, \hat{\phi}_2)$ *and (2)* $(\phi_1, \hat{\phi}_1) \neq (\phi_2, \hat{\phi}_2)$. *We say the PCS satisfies* polynomial binding *if for all PPT adversaries* $\mathcal{A}$ *there exists a negligible function* $\nu(\cdot)$ *such that* $\Pr[\mathsf{G}_{\mathcal{A}}^{poly\text{-}binding}(\lambda)] < \nu(\lambda)$.

Definition 2 (Evaluation binding). [22] *Consider a game* $\mathsf{G}_{\mathcal{A}}^{\textit{eval-binding}}(\lambda)$ *in which an adversary* $\mathcal{A}$ *takes* 1^λ *as input and outputs* $(\boldsymbol{C}, \omega, m_1, \hat{m}_1, \pi_1, m_2, \hat{m}_2, \pi_2)$*, and wins if (1)* $\mathsf{Verify}(\boldsymbol{C}, \omega, m_i, \hat{m}_i, \pi_i) = 1$ *for* $i \in \{1, 2\}$ *and (2)* $(m_1, \hat{m}_1) \neq (m_2, \hat{m}_2)$*. We say the PCS satisfies* evaluation binding *if for all PPT adversaries* $\mathcal{A}$ *there exists a negligible function* $\nu(\cdot)$ *such that* $\mathsf{Pr}[\mathsf{G}_{\mathcal{A}}^{\textit{eval-binding}}(\lambda)] < \nu(\lambda)$.

We define another important property for a PCS, *interpolation binding*, which says that given enough evaluations of a committed pair of polynomials, the interpolated polynomials obtained from these evaluations must be the ones contained inside the commitment. For this we use the notation $p \leftarrow \mathsf{Interpolate}(\{\omega_i, y_i\}_i)$ to denote using Lagrange interpolation to obtain a degree-d polynomial given $d+1$ evaluation points and their corresponding evaluations.

Definition 3 (Interpolation binding). *Consider the game* $\mathsf{G}_{\mathcal{A}}^{\textit{int-binding}}(1^\lambda)$ *defined as follows*

$$
\begin{array}{l}
\underline{\textsc{main}(1^\lambda, d)} \\
\mathsf{srs} \xleftarrow{\$} \mathsf{Setup}(1^\lambda, d) \\
(\boldsymbol{C}, \{(\omega_i, m_i, \hat{m}_i, \pi_i)\}_{i \in [d+1]}) \xleftarrow{\$} \mathcal{A}(\mathsf{srs}) \\
p(X) \leftarrow \mathsf{Interpolate}(\{(\omega_i\, m_i)\}_{i \in [d+1]}) \\
\hat{p}(X) \leftarrow \mathsf{Interpolate}(\{(\omega_i, \hat{m}_i)\}_{i \in [d+1]}) \\
\textit{check } \omega_i \neq \omega_j \textit{ for all } i \neq j \\
\textit{check } \mathsf{Verify}(\mathsf{srs}, \boldsymbol{C}, \omega_i, m_i, \hat{m}_i, \pi_i) = 1 \textit{ for all } i \in [d+1] \\
\textit{check } \boldsymbol{C} \neq \mathsf{Commit}(\mathsf{srs}, p(X); \hat{p}(X)) \\
\textit{if all checks pass return } 1\textit{, else return } 0
\end{array}
$$

We say the PCS satisfies interpolation binding *if for all PPT adversaries* $\mathcal{A}$ *there exists a negligible function* $\nu(\cdot)$ *such that* $\Pr[\mathsf{G}_{\mathcal{A}}^{\textit{int-binding}}(1^\lambda)] < \nu(\lambda)$.

In our construction of Bingo, we do not use the hiding property defined by Kate et al. as it did not fit our use case. We instead provide a new hiding definition, capturing the ability of a simulator to both open commitments and provide evaluations without knowledge of the underlying polynomials. As this definition is somewhat specific to our usage of KZG within Bingo, and in particular to the way in which it is embedded in a bivariate polynomial commitment (as described below), it can be found in the full version of the paper [44].

In a *bivariate* PCS, ϕ is a polynomial in indeterminates X and Y. This means we consider an additional algorithm:

- $\boldsymbol{A} \leftarrow \mathsf{PartialEval}(\mathsf{srs}, \boldsymbol{C}, V_n)$ takes as input the commitment key, the bivariate commitment, and a set of partial evaluation points V_n of size n. It outputs n partial evaluations, consisting of commitments to univariate polynomials $\alpha(X) \leftarrow \phi(X, v)$ and $\hat{\alpha}(X) \leftarrow \hat{\phi}(X, v)$ for each $v \in V_n$.

To prove evaluations of ϕ and $\hat{\phi}$, we can use these univariate polynomials as input to Eval, and their commitments as input to Verify (which must now take in two evaluation points ω and ω_v rather than a single one). In terms of correctness, we define an algorithm $\boldsymbol{A} \leftarrow \mathsf{CPE}(\phi, \hat{\phi}, V_n)$ that first runs Commit on ϕ and $\hat{\phi}$ and then runs $\mathsf{PartialEval}$ on its output $\boldsymbol{C}$ and V_n. We then require that $\mathsf{Verify}(\mathsf{CPE}(\phi, \hat{\phi}, V_n), (\omega, v), \mathsf{Eval}(\phi(X, v), \hat{\phi}(X, v), \omega)) = 1$ for all $v \in V_n$.

2.3 Reliable Broadcast

A *reliable broadcast* is an asynchronous protocol with a designated *sender*. The sender has some input value m from a known domain $\mathcal{M}$ and each party may output a value in $\mathcal{M}$. A reliable broadcast has the following properties assuming all *nonfaulty* (i.e., uncorrupted) parties participate in the protocol:

- **Validity.** If the sender is nonfaulty, then every nonfaulty party that completes the protocol outputs the sender's input value m.
- **Agreement.** The values output by any two nonfaulty parties are the same.
- **Termination.** If the dealer is nonfaulty, then all nonfaulty parties complete the protocol and output a value. Furthermore, if some nonfaulty party completes the protocol, every nonfaulty party completes the protocol.

2.4 Packed Asynchronous Verifiable Secret Sharing (PAVSS)

We define a packed AVSS using two interactive protocols that take place between n parties: Share and $\mathsf{Reconstruct}$. In Share, the designated dealer receives as input a set of secrets $s_0, \ldots, s_m$ from a finite field $\mathbb{F}$ and all other parties receive no input. None of the parties have any output at the end of Share, but they do update their local state. Because the AVSS is packed, there are $m + 1$ possible invocations of $\mathsf{Reconstruct}$, one for each index k. Each party thus provides k as input to the protocol, and has as output a field element $v_k \in \mathbb{F}$, which represents their local view of the k-th secret shared by the dealer.

We formally define the environment for a PAVSS in the full version of the paper, in terms of capturing the ways in which the adversary can control the network (i.e., when honest parties receive messages) and the other actions the adversary can take. We then formally define three security properties for a PAVSS, which we informally summarize here.

Our first definition, *termination*, sets the conditions under which nonfaulty parties can be guaranteed to complete Share and $\mathsf{Reconstruct}$. Briefly, it says that (1) if the dealer is nonfaulty then all nonfaulty parties will complete Share; (2) if one nonfaulty party completes Share then all nonfaulty parties will; and (3) if all nonfaulty parties complete Share and invoke $\mathsf{Reconstruct}(k)$ then they all will complete $\mathsf{Reconstruct}(k)$. Our next definition, *correctness*, captures the requirement that all nonfaulty parties who complete $\mathsf{Reconstruct}(k)$ should agree on the same secret, which in turn should be the same as the one used by the dealer (if it was also nonfaulty). Our final definition, *secrecy*, captures the requirement that an adversary should not be able to learn anything about the k-th secret until the point at which some nonfaulty party invokes $\mathsf{Reconstruct}(k)$.

Our specific PAVSS scheme, Bingo, is also *complete* in the sense that every party has a share of each of the secrets (this can be seen in the proof of Theorem

$\underline{\mathsf{KZG.Setup}(\mathsf{bp}, d_1)}$ $\tau, x \xleftarrow{\$} \mathbb{F}$ $\hat{g} \leftarrow g^x$ $\mathsf{srs} \leftarrow (\mathsf{bp}, h, h^\tau, \{g^{\tau^i}, \hat{g}^{\tau^i}\}_{i=0}^{d_1})$ return srs	$\underline{\mathsf{KZG.Eval}(\mathsf{srs}, \alpha(X), \hat{\alpha}(X), \omega_i)}$ $m \leftarrow \alpha(\omega_i)$ $\hat{m} \leftarrow \hat{\alpha}(\omega_i)$ $q(X) \leftarrow (\alpha(X) - m)/(X - \omega_i)$ $\hat{q}(X) \leftarrow (\hat{\alpha}(X) - \hat{m})/(X - \omega_i)$ $\pi \leftarrow g^{q(\tau)}\hat{g}^{\hat{q}(\tau)}$ return $(m, \hat{m}, \pi)$
$\underline{\mathsf{KZG.Commit}(\mathsf{srs}, \alpha(X); \hat{\alpha}(X))}$ $\boldsymbol{C} \leftarrow g^{\alpha(\tau)}\hat{g}^{\alpha(\tau)}$ return $\boldsymbol{C}$	$\underline{\mathsf{KZG.Verify}(\mathsf{srs}, \boldsymbol{C}, \omega_i, m, \hat{m}, \pi)}$ if $e(\boldsymbol{C}g^{-m}\hat{g}^{-\hat{m}}, h) = e(\pi, h^{\tau - \omega_i})$ return 1 else return 0

Fig. 2. The hiding univariate KZG polynomial commitment scheme.

3, in which every party guarantees it has a share before terminating). Beyond the above three properties, this thus makes Bingo a packed asynchronous complete secret sharing (ACSS) scheme [4].

3 A Bivariate Polynomial Commitment Scheme

3.1 Construction

Our construction for a bivariate polynomial commitment scheme, given in Fig. 3, builds heavily on top of the univariate PCS due to Kate et al. [22]. As such, we first present this construction in Fig. 2.

In both commitment schemes, the setup outputs universal powers-of-tau parameters [15], meaning they are backwards compatible with prior trusted setups [23]. Let $\phi(X, Y)$ be a bivariate polynomial with degree d_1 in X and degree d_2 in Y. A commitment to $\phi(X, Y)$ first decomposes $\phi(X, Y)$ into $d_2 + 1$ univariate polynomials $\phi_i(X)$ such that $\phi(X, Y) = \sum_{i=0}^{d_2} \phi_i(X)Y^i$. The randomness $\hat{\phi}(X, Y)$ is decomposed in the same manner. Then each of the $\phi_i(X)$ are committed to using $\mathsf{KZG.Commit}$ with randomness $\hat{\phi}_i(X)$. A commitment $\boldsymbol{C}$ such that $|\boldsymbol{C}| = d_2$ has maximum degree d_2 in Y and d_1 in X.

The partial evaluation algorithm takes as input a commitment $\boldsymbol{C}$ and a set of distinct points V_n of size n. It then runs a discrete Fourier transform (DFT) that maps a polynomial to a set of evaluations. Because the DFT/iDFT algorithm is a linear transformation, it can be applied to (homomorphic) group exponents in the exact same way as it is run for field elements, without having to know the discrete logarithms. To avoid confusion, we nevertheless denote the algorithms acting on field elements as DFT and iDFT and the algorithms acting on group elements as DFTExp and iDFTExp. PartialEval thus runs and outputs

$\underline{\mathsf{Setup}(\mathsf{bp}, d_1)}$
return $\mathsf{KZG.Setup}(\mathsf{bp}, d_1)$

$\underline{\mathsf{PartialEval}(\mathsf{srs}, \boldsymbol{C}, V_n)}$
$\boldsymbol{A} \leftarrow \mathsf{DFTExp}(\boldsymbol{C}, V_n)$
return $\boldsymbol{A}$

$\underline{\mathsf{Eval}(\mathsf{srs}, \alpha(X), \hat{\alpha}(X), \omega_i)}$
return $\mathsf{KZG.Eval}(\mathsf{srs}, \alpha(X), \hat{\alpha}(X), \omega_i)$

$\underline{\mathsf{Commit}(\mathsf{srs}, \phi(X,Y); \hat{\phi}(X,Y))}$
$\sum_{i=0}^{d_2} \phi_i(X)Y^i \leftarrow \mathsf{parse}(\phi(X,Y))$
$\sum_{i=0}^{d_2} \hat{\phi}_i(X)Y^i \leftarrow \mathsf{parse}(\hat{\phi}(X,Y))$
$\boldsymbol{C} \leftarrow \{g^{\phi_i(\tau)}\hat{g}^{\hat{\phi}_i(\tau)}\}_{i=0}^{d_2}$
return $\boldsymbol{C}$

$\underline{\mathsf{Verify}(\mathsf{srs}, \boldsymbol{A}, (i,j), m, \hat{m}, \pi)}$
return $\mathsf{KZG.Verify}(\mathsf{srs}, \boldsymbol{A}_j, \omega_i, m, \hat{m}, \pi)$

$\underline{\mathsf{GetProofs}(\{(w_i, y_i, \hat{y}_i, \pi_i)\}_{i\in[f+1]}, V_n)}$
$\beta(X) \leftarrow \mathsf{Interpolate}\left(\{(w_i, y_i)\}_{i\in[d_1+1]}\right)$
$\hat{\beta}(X) \leftarrow \mathsf{Interpolate}\left(\{(w_i, \hat{y}_i)\}_{i\in[d_1+1]}\right)$
$\boldsymbol{P} \leftarrow \mathsf{InterpolateExp}\left(\{(w_i, \pi_i)\}_{i\in[d_1+1]}\right)$
$z_1, \ldots, z_n \leftarrow \mathsf{DFT}(\beta(X), V_n)$
$\hat{z}_1, \ldots, \hat{z}_n \leftarrow \mathsf{DFT}(\hat{\beta}(X), V_n)$
$\bar{\pi}_1, \ldots, \bar{\pi}_n \leftarrow \mathsf{DFTExp}\,(\boldsymbol{P}, V_n)$
return $\{(z_i, \hat{z}_i, \bar{\pi}_n)\}_{i\in[n]}$

Fig. 3. Our bivariate PCS, built on top of the KZG univariate PCS. The set V_n consists of n roots of unity, i.e., values ω_i such that $\omega_i^n = 1$.

$$\mathsf{DFTExp} : ((g^{a_0}, \ldots, g^{a_{d_1}}), \mathbb{F}^n) \mapsto \{g^{\sum_{j=0}^{d_1} a_j \omega_i^j}\}_{i=0}^{n-1}.$$

If V_n is a multiplicative subgroup of $\mathbb{F}$ containing roots of unity, then DFT and DFTExp run in time $n\log(n)$. Note that it is possible to replace the DFTs with simple Lagrange interpolation in any field without using roots of unity, but DFTs are used to improve efficiency. If $W \subset V_n$ is a subset of roots of unity, then interpolation over W runs in time $n\log^2(n)$ [48]. In addition to the interpolation algorithm $p \leftarrow \mathsf{Interpolate}(\{(\omega_i, y_i)\})$, we denote by $P \leftarrow \mathsf{InterpolateExp}(\{(\omega_i, Y_i)\})$ the algorithm that performs these operations in the exponent (i.e., by acting on group elements). We also denote by $Y \leftarrow \mathsf{EvalExp}(\omega, P)$ the algorithm that performs polynomial evaluation in the exponent.

To verify that a commitment opens at (ω_i, ω_j) to $(m, \hat{m})$, we take as input the partial evaluation $\boldsymbol{A}$ over the set V_n where $\omega_j \in V_n$. Then $\boldsymbol{A}_j = g^{\phi(\tau,\omega_j)}\hat{g}^{\hat{\phi}(\tau,\omega_j)}$ is a KZG commitment to $\phi(X, \omega_j)$ under randomness $\hat{\phi}(X, \omega_j)$. The prover can thus provide a KZG opening proof that $\boldsymbol{A}_j$ opens at ω_i to m under randomness $\hat{m}$ (i.e., the output of $\mathsf{KZG.Eval}$), which the verifier can check using $\mathsf{KZG.Verify}$.

The security of our bivariate PCS follows directly from the security of the KZG univariate PCS, in terms of polynomial binding, evaluation binding, and hiding, which follow in turn from the $\mathsf{q\text{-}sdh}$ assumption. We next prove, in the algebraic group model [16], that the underlying univariate PCS also satisfies interpolation binding. A proof of this lemma can be found in the full version of the paper [44].

Lemma 1. *If the* dlog *and* $\mathsf{q\text{-}sdh}$ *assumptions hold, then interpolation binding (Definition 3) holds for the KZG PCS.*

3.2 Commitment and Proof Interpolation

For any bivariate polynomial $\phi(X, Y)$ of degree d_1 in X we have that the points $\phi(\omega_{v_1}, \omega_j), \ldots, \phi(\omega_{v_{d_1+1}}, \omega_j)$ suffice to interpolate the partial evaluation $\phi(X, \omega_j)$. A special property about our bivariate PCS is that, given a commitment $\boldsymbol{C}$ and $d_1 + 1$ openings (with respect to the same ω_j), parties can also compute the opening proofs for $\boldsymbol{C}$ at (x, ω_j) for any $x \in \mathbb{F}$. This will be useful in Bingo when the dealer is dishonest.

In Fig. 3 we describe an additional algorithm $\{(z_i, \hat{z}_i, \bar{\pi}_i)\} \leftarrow \mathsf{GetProofs}(\{(v_i, y_i, \hat{y}_i, \pi_i)\}, V_n)$ that takes as input $d_1 + 1$ opening points, their evaluations and associated proofs, and a set V_n, and outputs n evaluations and their associated proofs over the bigger set V_n. In Lemma 2 we prove the correctness of this algorithm, namely that if every opening $(y_i, \hat{y}_i, \pi_i)$ verifies with respect to the commitment $\boldsymbol{C}$ and the indices (j, w_i), then every output $(z_k, \hat{z}_k, \bar{\pi}_k)$ also verifies with respect to $(\boldsymbol{C}, k, j)$. A proof of this lemma can be found in the full version of the paper [44].

Lemma 2. *Let* $\boldsymbol{C}$ *be a bivariate polynomial commitment, let* $\boldsymbol{A}$ *be such that* $\boldsymbol{A} \leftarrow \mathsf{PartialEval}(\boldsymbol{C}, V_n)$*, let* v_i *be indices such that* $w_i = \omega_{v_i}$ *for every* $i \in [d_1 + 1]$*, and let* $\{(v_i, y_i, \hat{y}_i, \pi_i)\}_{i \in [d_1+1]}$ *be values such that* $\mathsf{VerifyEval}(\boldsymbol{A}, (j, v_i), y_i, \hat{y}_i, \pi_i) = 1$ *for all* $i \in [d_1 + 1]$*. If*

$$\{(z_i, \hat{z}_i, \bar{\pi}_i)\}_{i \in [n]} \leftarrow \mathsf{GetProofs}(\{(w_i, y_i, \hat{y}_i, \pi_i)\}_{i \in [d_1+1]}, V_n)$$

then $\forall k \in [n],\ \mathsf{VerifyEval}(\boldsymbol{A}, (j, k), \beta_j(\omega_k), \hat{\beta}_j(\omega_k), \bar{\pi}_k) = 1.$

Below we prove an additional useful property of our bivariate PCS, namely that by performing interpolation in the exponent on the partial (univariate) commitments we can recover the bivariate commitment.

Lemma 3. *Let* $v_1, ..., v_{d_2+1} \in [n]$ *be distinct values, and let* $\alpha_{v_1}(X), \ldots, \alpha_{v_{f+1}}(X)$ *and* $\hat{\alpha}_{v_1}(X), \ldots, \hat{\alpha}_{v_{f+1}}(X)$ *be polynomials of degree no greater than* d_1*. Define* $\phi(X, Y), \hat{\phi}(X, Y)$ *to be the unique bivariate polynomials of degree* d_1 *in* X *and* d_2 *in* Y *such that* $\forall i \in [d_1 + 1]\ \alpha_{v_i}(X) = \phi(X, \omega_{v_i}), \hat{\alpha}_{v_i}(X) = \hat{\phi}(X, \omega_{v_i})$*. If* $\forall i \in [d_2 + 1]\ D_i = \mathsf{Commit}(\alpha_{v_i}(X);\ \hat{\alpha}_{v_i}(X))$ *and* $\boldsymbol{C} = \mathsf{InterpolateExp}(\{(\omega_{v_i}, D_i)\}_{i \in [f+1]})$*, then* $\boldsymbol{C} = \mathsf{Commit}(\mathsf{srs}, \phi(X, Y);\ \hat{\phi}(X, Y))$*.*

Proof. First note that $\phi(\tau, Y) = \mathsf{Interpolate}(\{(\omega_{v_i}, \phi(\tau, \omega_{v_i})\}_{i \in [f+1]})$. By construction $D_i = \mathsf{Commit}(\mathsf{srs}, \alpha_{v_i}; \hat{\alpha}_{v_i}) = g^{\alpha_{v_i}(\tau)} \hat{g}^{\hat{\alpha}_{v_i}(\tau)} = g^{\phi(\tau, \omega_{v_i}) + x\hat{\phi}(\tau, \omega_{v_i})}$, where $\hat{g} = g^x$. Thus

$$(g^{\phi_0(\tau) + x\hat{\phi}_0(\tau)}, \ldots, g^{\phi_f(\tau) + x\hat{\phi}_f(\tau)}) = \mathsf{InterpolateExp}\left(\{(\omega_{v_i}, D_i)\}_{i \in [f+1]}\right).$$

This shows the lemma because

$$(g^{\phi_0(\tau) + x\hat{\phi}_0(\tau)}, \ldots, g^{\phi_f(\tau) + x\hat{\phi}_f(\tau)}) = \mathsf{Commit}(\mathsf{srs}, \phi(X, Y);\ \hat{\phi}(X, Y)).$$

4 Bingo: Packed Asynchronous Verifiable Secret Sharing

In this section we present Bingo, our packed AVSS scheme. We discuss its design in Sect. 4.1 and its security in Sect. 4.2.

4.1 Design

Bingo consists of a sharing protocol BingoShare (Algorithm 2), and a reconstruction protocol BingoReconstruct (Algorithm 3). Additional reconstruction protocols for reconstructing sums of secrets and batch reconstructing are presented in Algorithm 4 and Algorithm 5, respectively. Moreover, BingoShare uses a subprotocol BingoDeal (Algorithm 1), that describes the steps performed by the dealer. In more detail:

BingoDeal. The dealer receives secrets $s_k \in \mathbb{F}$ for $k \in [0, m]$ as inputs. It then uniformly samples two bivariate polynomials $\phi, \hat{\phi}$ over $\mathbb{F}$ of degrees $2f$ in X and f in Y such that $\phi(\omega_{-k}, \omega_0) = s_k$ for $k \in [0, m]$. This can be done by uniformly sampling values for $\phi(\omega_i, \omega_0)$ for $i \in [f]$ and interpolating the resulting $\phi(X, \omega_0)$. Following that, the dealer simply uniformly samples $\phi(X, \omega_i)$ for $i \in [f]$ by directly sampling their coefficients, and interpolating the resulting $f + 1$ polynomials into a bivariate polynomial ϕ. The dealer then computes the *row projections* $\alpha_i(X) = \phi(X, \omega_i)$ and $\hat{\alpha}_i(X) = \hat{\phi}(X, \omega_i)$, and the *column projections* $\beta_i(Y) = \phi(\omega_i, Y)$, and $\hat{\beta}_i(Y) = \hat{\phi}(\omega_i, Y)$ for all $i \in [n]$. Looking ahead, the asymmetric degrees of the polynomials (α of degree $2f$ and β of degree f) help parties know that if they complete the BingoShare protocol, every other party will eventually do so as well. By definition, $\alpha_i(\omega_j) = \beta_j(\omega_i)$ and $\hat{\alpha}_i(\omega_j) = \hat{\beta}_j(\omega_i)$ for any $i, j \in [n]$. The dealer then broadcasts a commitment to this polynomial (formed using our bivariate PCS), using reliable broadcast, and privately sends every party $i \in [n]$ its pair of row polynomials α_i and $\hat{\alpha}_i$.

Algorithm 1. $\mathsf{BingoDeal}(s_0, \ldots, s_m)$

uniformly sample $\phi(X, Y)$ with degree $2f$ in X and f in Y s.t. $\phi(\omega_{-k}, \omega_0) = s_k \ \forall k \in [0, m]$
uniformly sample $\hat{\phi}(X, Y)$ with degree $2f$ in X and f in Y
$\mathsf{CM} \leftarrow \mathsf{Commit}(\phi; \hat{\phi})$
for all $i \in [n]$ **do**
    $\alpha_i(X) \leftarrow \phi(X, \omega_i), \hat{\alpha}_i(X) \leftarrow \hat{\phi}(X, \omega_i)$
(reliably) broadcast $\langle$"commits", $\mathsf{CM}\rangle$
send $\langle$"polynomials", $\alpha_i, \hat{\alpha}_i\rangle$ to every $i \in [n]$

BingoShare. The goal of BingoShare (Algorithm 2) is for each party i to learn their row polynomials α_i and $\hat{\alpha}_i$. As depicted in Fig. 1, there are two ways this can happen. First, if the dealer is honest, they send the polynomials in BingoDeal and party i learns them directly (lines 7-10).

If the dealer is corrupt, however, party i may never receive a "polynomials" message. In this case other nonfaulty parties can help i as follows. First, they use their α polynomials to help other parties learn their β column polynomials (lines 15-23), taking advantage of the fact that $\alpha_j(\omega_\ell) = \beta_\ell(\omega_j)$ (we omit the $\hat{\alpha}$ and $\hat{\beta}$ polynomials in this description, but the process for them is identical). In other words, if party ℓ is given $\alpha_j(\omega_\ell)$ by enough other parties j then it can use GetProofs to compute evaluations and proofs for all other parties, as shown in line 21. Importantly, while party ℓ could interpolate β_ℓ and compute the evaluations directly, it would be unable to form the proofs using Eval as the proof for each party j needs to verify against cm_j (i.e., a commitment to α_j and not β_ℓ).

In the previous step, each party ℓ thus sends evaluations $\beta_\ell(\omega_i)$ to each party i. After receiving enough of these polynomials, party i can then interpolate α_i (in line 31). Before completing the protocol, parties make sure that enough parties have received their row and column polynomials and are helping everybody reach the end of the protocol. This is done by parties sending "done" messages after having received their row and column polynomial, and terminating only after $n - f$ such messages have been received, guaranteeing that at least $f + 1$ nonfaulty parties shared their information. Note that if one party receives its row and column polynomials, it does not know that all parties will eventually receive enough information to interpolate their polynomials as well. Therefore, parties have to wait to actually receive $n - f$ "done" messages before terminating, even if they received enough information to send their own "done" message.

BingoReconstruct. Once parties have finished the sharing phase, they can start recovering the shared secrets for all $k \in [0, m]$. The execution of BingoReconstruct may not be required in all cases, however, as it depends on the concrete application in which Bingo is used. To start recovery of the secret at index k, each party i evaluates its polynomials α_i and $\hat{\alpha}_i$ at position ω_{-k} and creates a proof $\pi_{\alpha,i,-k}$ showing that the evaluations are correct with respect to the commitment cm_i. Afterwards, party i sends a "rec" message with the evaluations $\alpha_i(\omega_{-k})$, $\hat{\alpha}_i(\omega_{-k})$ and the proof $\pi_{\alpha,i,-k}$ to all other parties j. Once party i receives its first "rec" message from party j, it verifies that the included shares are correct and, if so, stores the tuple $(j, \alpha_j(\omega_{-k}))$ in a set $\mathsf{shares}_{i,k}$. Finally, once party i has received $f + 1$ different correct shares for the shared secret at index k, it interpolates $\mathsf{shares}_{i,k}$ to a polynomial β_{-k}, outputs $\beta_{-k}(\omega_0)$ as the secret, and terminates. Note that the points $\alpha_j(\omega_{-k})$ should equal $\phi(\omega_{-k}, \omega_j)$. Interpolating $f + 1$ such points (with different values for j) yields the polynomial $\beta_{-k}(Y) = \phi(\omega_{-k}, Y)$, so $\beta_{-k}(\omega_0) = \phi(\omega_{-k}, \omega_0) = s_k$ as required.

Algorithm 2. $\mathsf{BingoShare}_i()$

if i is the dealer with input $s_0, \ldots, s_m$ **then**
  $\mathsf{BingoDeal}(s_0, \ldots, s_m)$
$\alpha_i \leftarrow \perp, \hat{\alpha}_i \leftarrow \perp, \mathsf{cm} \leftarrow \emptyset$
$\mathsf{points}_{\alpha,i} \leftarrow \emptyset, \mathsf{points}_{\hat{\alpha},i} \leftarrow \emptyset, \mathsf{proofs}_{\beta,i} \leftarrow \emptyset$
upon receiving a $\langle$"commits", $\mathsf{CM}\rangle$ broadcast from the dealer, **do**
  $\mathsf{cm} \leftarrow \mathsf{PartialEval}(\mathsf{CM}, \{\omega_1, \ldots, \omega_n\})$ ▷ $\mathsf{cm} = (\mathsf{cm}_1, \ldots, \mathsf{cm}_n)$
upon receiving the first $\langle$"polynomials", $\alpha'_i, \hat{\alpha}'_i\rangle$ message from the dealer, **do**
  upon $\mathsf{cm} \neq \emptyset$, **do**
    if $\alpha_i = \perp$ and $\mathsf{KZG.Commit}(\alpha'_i, \hat{\alpha}'_i) = \mathsf{cm}_i$ **then**
      $\alpha_i \leftarrow \alpha'_i, \hat{\alpha}_i \leftarrow \hat{\alpha}'_i$ ▷ save $\alpha_i, \hat{\alpha}_i$ if consistent with cm
upon $\alpha_i \neq \perp$ and $\mathsf{cm}_i \neq \perp$, **do** ▷ upon having row, help others with columns
  for all $j \in [n]$ **do**
    $\alpha_i(\omega_j), \hat{\alpha}_i(\omega_j), \pi_{\alpha,i,j} \leftarrow \mathsf{Eval}(\alpha_i, \hat{\alpha}_i, \omega_j)$
    send $\langle$"row", $\alpha_i(\omega_j), \hat{\alpha}_i(\omega_j), \pi_{\alpha,i,j}\rangle$ to party j
upon receiving the first $\langle$"row", $\alpha_j(\omega_i), \hat{\alpha}_j(\omega_i), \pi_{\alpha,j,i}\rangle$ message from j, **do**
  upon $\mathsf{cm}_j \neq \perp$, **do** ▷ collect points and interpolate column
    if $|\mathsf{proofs}_{\beta,i}| < f + 1$ **then** ▷ no need to collect points if interpolated
      if $\mathsf{Verify}(\mathsf{cm}, (i, j), \alpha_j(\omega_i), \hat{\alpha}_j(\omega_i), \pi_{\alpha,j,i}) = 1$ **then**
        $\mathsf{proofs}_{\beta,i} \leftarrow \mathsf{proofs}_{\beta,i} \cup \{(\omega_j, \alpha_j(\omega_i), \hat{\alpha}_j(\omega_i), \pi_{\alpha,j,i})\}$
        if $|\mathsf{proofs}_{\beta,i}| = f + 1$ **then** ▷ enough to interpolate column proofs
          $(y_1, \hat{y}_1, \pi_1), \ldots, (y_n, \hat{y}_n, \pi_n) \leftarrow \mathsf{GetProofs}(\mathsf{proofs}_{\beta,i}, \{\omega_1, \ldots, \omega_n\})$
          for all $j \in [n]$ **do**
            send $\langle$"column", $y_j, \hat{y}_j, \pi_n\rangle$ to party j ▷ help others with rows
upon receiving the first $\langle$"column", $\beta_j(\omega_i), \hat{\beta}_j(\omega_i), \pi_{\beta,j,i}\rangle$ message from j, **do**
  upon $\mathsf{cm} \neq \emptyset$, **do** ▷ collect points and interpolate row
    if $\alpha_i = \perp$ **then** ▷ no need to collect points if already have α_i
      if $\mathsf{Verify}(\mathsf{cm}, (j, i), \beta_j(\omega_i), \hat{\beta}_j(\omega_i), \pi_{\beta,j,i}) = 1$ **then**
        $\mathsf{points}_{\alpha,i} \leftarrow \mathsf{points}_{\alpha,i} \cup \{(\omega_j, \beta_j(\omega_i))\}$
        $\mathsf{points}_{\hat{\alpha},i} \leftarrow \mathsf{points}_{\hat{\alpha},i} \cup \{(\omega_j, \hat{\beta}_j(\omega_i))\}$
        if $|\mathsf{points}_{\alpha,i}| = 2f + 1$ **then** ▷ enough to interpolate row
          $\alpha_i \leftarrow \mathsf{Interpolate}(\mathsf{points}_{\alpha,i}), \hat{\alpha}_i \leftarrow \mathsf{Interpolate}(\mathsf{points}_{\hat{\alpha},i})$
upon $\alpha_i \neq \perp, \hat{\alpha} \neq \perp$ and $|\mathsf{proofs}_{\beta,i}| = f + 1$, **do**
  send $\langle$"done"$\rangle$ to all parties
upon receiving $\langle$"done"$\rangle$ messages from $n - f$ parties, **do**
  upon $\alpha_i \neq \perp, \hat{\alpha}_i \neq \perp$, and $|\mathsf{proofs}_{\beta,i}| = f + 1$, **do**
    terminate

Algorithm 3. $\mathsf{BingoReconstruct}_i(k)$ for $k \in [0, m]$

1: $\mathsf{shares}_{i,k} = \emptyset$
2: $\alpha_i(\omega_{-k}), \hat{\alpha}_i(\omega_{-k}), \pi_{\alpha,i,-k} \leftarrow \mathsf{Eval}(\alpha_i, \hat{\alpha}_i, \omega_{-k})$
3: send $\langle$"rec"$, k, \alpha_i(\omega_{-k}), \hat{\alpha}_i(\omega_{-k}), \pi_{\alpha,i,-k}\rangle$ to all parties
4: **upon** receiving the first $\langle$"rec"$, k, \alpha_j(\omega_{-k}), \hat{\alpha}_j(\omega_{-k}), \pi_{\alpha,j,-k}\rangle$ message from j, **do**
5:     **if** $\mathsf{Verify}(\mathsf{cm}, (-k, j), \alpha_j(\omega_{-k}), \hat{\alpha}_j(\omega_{-k}), \pi_{\alpha,j,-k}) = 1$ **then**
6:         $\mathsf{shares}_{i,k} \leftarrow \mathsf{shares}_{i,k} \cup \{(\omega_j, \alpha_j(\omega_{-k}))\}$ ▷ $\alpha_i(\omega_{-k}) = \phi(\omega_{-k}, \omega_i) = \beta_{-k}(\omega_i)$
7:         **if** $|\mathsf{shares}_{i,k}| = f + 1$ **then** ▷ enough to interpolate $-k$'th column
8:             $\beta_{-k} \leftarrow \mathsf{Interpolate}(\mathsf{shares}_{i,k})$
9:             **output** $\beta_{-k}(\omega_0)$ and **terminate**

4.2 Security

The security of Bingo scheme is captured in the following main theorem.

Theorem 1. *If the underlying commitment scheme is secure, then the pair* (BingoShare, BingoReconstruct)*, as specified in Algorithms 2 and 3, is an f-resilient packed AVSS for $m+1$ secrets, for any $m \leq f < \frac{n}{3}$.*

To prove this, we argue for correctness, termination, and secrecy in turn. To prove correctness and termination, we first prove a series of lemmas that consider the relationship between the committed polynomials represented by CM and the polynomials $\alpha_i, \hat{\alpha}_i, \beta_i, \hat{\beta}_i$ held by a nonfaulty party i at the point at which they complete Share. In all of the following lemmas we consider many instances of the BingoShare and BingoReconstruct protocols running simultaneously with both faulty and nonfaulty dealers. Each of the lemmas focuses on one of those instances and argues that certain values are consistent within that one instance. We first show that the existence of an extractor that can, for both faulty and nonfaulty dealers, output polynomials ϕ and $\hat{\phi}$ such that $\mathsf{CM} = \mathsf{Commit}(\phi;\ \hat{\phi})$.

The following lemma demonstrates the existence of an extractor that outputs polynomials consistent with the dealers broadcast commitment CM whenever a single nonfaulty party completes BingoShare. Where the polynomial commitment scheme is binding, this ensures that the output of BingoReconstruct is fully determined once an honest party completes. A proof of this lemma can be found in the full version of the paper [44].

Lemma 4. *Assume some nonfaulty party completed the* BingoShare *protocol with respect to the commitment* CM *broadcast from the dealer. Suppose the (univariate) polynomial commitment scheme satisfies interpolation binding. There exists an efficient extractor* Ext *that receives the views of the nonfaulty parties and outputs a pair of bivariate polynomials $\phi(X, Y)$ and $\hat{\phi}(X, Y)$ of degree $2f$ in X and f in Y such that $\mathsf{CM} = \mathsf{Commit}(\phi(X, Y);\ \hat{\phi}(X, Y))$. Furthermore, if the dealer is nonfaulty, then $\forall k \in [0, m]$ $s_k = \phi(\omega_{-k}, \omega_0)$.*

Corollary 1. *Assume some nonfaulty party completed the* BingoShare *protocol, that the extractor from Lemma 4 returns $\phi(X,Y), \hat{\phi}(X,Y)$, and the PCS satisfies polynomial binding. If some nonfaulty party i updates $\alpha_i(X), \hat{\alpha}_i(X)$ to values other than $\perp$, then $\alpha_i(X) = \phi(X,\omega_i)$ and $\hat{\alpha}_i(X) = \hat{\phi}(X,\omega_i)$.*

Proof. Suppose a nonfaulty party updates $\alpha_i(X), \hat{\alpha}_i(X)$ and an extractor outputs $\phi(X,Y)$ and $\hat{\phi}(X,Y)$ such that $\mathsf{CM} = \mathsf{Commit}(\phi(X,Y);\ \hat{\phi}(X,Y))$. By the correctness of PartialEval we have that $\mathsf{cm}_i = \mathsf{Commit}(\phi(X,\omega_i);\ \hat{\phi}(X,\omega_i))$. If $(\alpha_i(X), \hat{\alpha}_i(X)) \neq (\phi(X,\omega_i), \hat{\phi}(X,\omega_i))$, then the adversary could simulate all nonfaulty parties, find two openings of cm_i and thus break polynomial binding.

Now assume that some nonfaulty party completes the protocol and define $\phi(X,Y)$, $\hat{\phi}(X,Y)$ to be extracted polynomials. The next lemma demonstrates that any point accepted by any nonfaulty party is consistent with $\phi(X,Y)$, $\hat{\phi}(X,Y)$. A proof of this lemma can be found in the full version of the paper [44].

Lemma 5. *If (1) the dealer broadcasts a $\langle$"commits", $\mathsf{CM}\rangle$ message and it gets received by a nonfaulty party, and (2) the underlying PCS satisfies evaluation binding and interpolation binding, and (3) some nonfaulty party completes the* BingoShare *protocol at time t, then define $\phi(X,Y), \hat{\phi}(X,Y) \leftarrow \mathsf{Ext}(\mathsf{view}_t)$ for* Ext *as in Lemma 4. Then the following properties hold:*

- *if a nonfaulty party i adds (j, y_j) and $(j, \hat{y}_j)$ to $\mathsf{points}_{\alpha,i}$ and $\mathsf{points}_{\hat{\alpha},i}$ respectively in lines 28 and 29, then $y_j = \phi(\omega_j, \omega_i)$ and $\hat{y}_j = \hat{\phi}(\omega_j, \omega_i)$, and*
- *if a nonfaulty party i adds $(j, y_j, \hat{y}_j, \pi_j)$ to $\mathsf{proofs}_{\beta,i}$ in line 19, then $y_j = \phi(\omega_i, \omega_j)$ and $\hat{y}_j = \hat{\phi}(\omega_i, \omega_j)$.*

Proofs of the following theorems can all be found in the full version of the paper. For the correctness property, we start by extracting $\phi, \hat{\phi}$ at the time the first nonfaulty party completes BingoShare and define $r_k = \phi(\omega_{-k}, \omega_0)$ for every $k \in [0, m]$. Parties reconstruct by sending the values $\phi(\omega_{-k}, \omega_i)$, interpolating the polynomial $\phi(\omega_{-k}, Y)$ and evaluating it at ω_0. Therefore, as long as Lemma 5 holds, reconstruction is successful.

Theorem 2. *If* q-sdh *and interpolation binding (Definition 3) hold, then Bingo satisfies correctness.*

For the termination property, showing that if the dealer is nonfaulty then all nonfaulty parties complete the BingoShare protocol and that all nonfaulty parties complete the BingoReconstruct protocol is straightforward and is done by following the messages the dealer and nonfaulty parties are guaranteed to send. Proving that all nonfaulty parties complete the BingoShare protocol if one does, on the other hand, is more subtle and requires leveraging the asymmetric degrees of $\phi, \hat{\phi}$. We start by noting that if some nonfaulty party completed the protocol, at least $f+1$ nonfaulty parties updated their row polynomials $\alpha_i, \hat{\alpha}_i$. These parties send "row" messages to all parties, allowing all nonfaulty parties to receive at least $f+1$ evaluation on their columns $\beta_i, \hat{\beta}_i$. Since those polynomials are of degree f, this is enough to interpolate the polynomials and proofs and send "column" messages. After receiving such a message from all $n - f \geq 2f + 1$ nonfaulty parties, every party will be able to interpolate their rows, which are of degree no greater than $2f$, and complete the $\mathsf{BingoShare}$ protocol.

Theorem 3. *If* $\mathsf{q\text{-}sdh}$ *and interpolation binding (Definition 3) hold, then Bingo satisfies termination.*

To argue for secrecy, we need to rely on one additional property of the polynomial commitment scheme: that there exist algorithms $\mathsf{SimCommit}$, $\mathsf{SimPartialEval}$ and $\mathsf{SimOpen}$ that allow for the simulation of bivariate commitments, partial evaluations, and openings of commitments respectively. We note that $\mathsf{SimOpen}$ works as follows: $\psi, \hat{\psi} \xleftarrow{\$} \mathsf{SimOpen}(\tau_s, \mathsf{cm}_\psi, \{y_i, \hat{y}_i\}_i)$ takes in a trapdoor τ_s, a commitment cm_ψ, and a set of evaluations of $y_i, \hat{y}_i$, and outputs a pair of polynomials ψ and $\hat{\psi}$ such that $\mathsf{cm}_\psi = \mathsf{Commit}(\psi, \hat{\psi})$, $\psi(v_i) = y_i, \hat{\psi}(v_i) = \hat{y}_i$ for all i, and the distribution over $(\psi, \hat{\psi})$ is uniform, given the above restriction. Importantly, this must hold even for adversarially chosen evaluation points v_i and evaluations y_i, (representing the adversary's ability to see points from this party before corrupting it). For completeness, we provide a formal definition of this property in the full version of the paper.

Theorem 4. *If* $\mathsf{q\text{-}sdh}$ *holds then Bingo satisfies secrecy.*

Finally, we prove the message, word, and round complexity of our protocol. We define asynchronous rounds following Canetti and Rabin [9], and define words as the basic objects (counters, indices, etc.) that make up a message, with cryptographic objects requiring $O(\lambda)$ words.

Theorem 5. *The* $\mathsf{BingoShare}$ *protocol requires* $O(\lambda n^2)$ *words and messages to be sent overall by all nonfaulty parties. Furthermore, if the bivariate and univariate PCSs satisfy correctness, interpolation binding, partial evaluation binding and evaluation binding, then every nonfaulty party completes the protocol in* $O(1)$ *rounds after the first nonfaulty party does so, and if the dealer is nonfaulty, all parties complete the protocol in* $O(1)$ *rounds. In addition, for every* k*, the* $\mathsf{BingoReconstruct}(k)$ *protocol requires* $O(\lambda n^2)$ *words and* $O(n^2)$ *messages to be sent overall by all nonfaulty parties, and takes* $O(1)$ *asynchronous rounds to complete.*

Corollary 2. *For any* $m = \Omega(n)$*, there exists a packed AVSS protocol sharing* m *secrets requiring* $O(\lambda n^2 \cdot \frac{m}{n})$ *words to be sent by nonfaulty parties in the sharing algorithm and* $O(\lambda n^2)$ *words to be sent while reconstructing any secret.*

Proof. Assume without loss of generality that $f = \frac{n-1}{3}$. The dealer can take the m secrets and partition them into $\left\lceil \frac{m}{f+1} \right\rceil = \Theta(\frac{m}{n})$ batches of no more than $f + 1$ secrets. The i-th secret s_i can be identified as the $(i \mod f+1)$-th secret in the $\lfloor \frac{m}{f+1} \rfloor$-th batch. The dealer then shares each batch using $\mathsf{BingoShare}$, yielding a communication complexity of $\Theta(\lambda n^2 \cdot \frac{m}{n})$. Reconstructing the secret entails calling $\mathsf{BingoReconstruct}$ once, yielding a word complexity of $O(\lambda n^2)$.

Remark 1. It is possible to share $m+1$ secrets with a polynomial of degree $f+m$ in X and f in Y, without changing the proofs. This yields rows of degree $f+m$ instead of degree $2f$.

Algorithm 4. $\mathsf{BingoReconstructSum}_i(\mathsf{dealers}, k)$ for $k \in [0, m]$

$\mathsf{shares}_{i,k} \leftarrow \emptyset$
$\forall i \in [n]$ $\mathsf{cm}'_i \leftarrow \prod_{j \in \mathsf{dealers}} \mathsf{cm}_{i,j}$
$\mathsf{cm}' \leftarrow (\mathsf{cm}'_1, \ldots, \mathsf{cm}'_n)$
$v_{i,k}, \hat{v}_{i,k}, \pi_{i,k} \leftarrow \mathsf{Eval}(\sum_{j \in \mathsf{dealers}} \alpha_{i,j}, \sum_{j \in \mathsf{dealers}} \hat{\alpha}_{i,j}, \omega_{-k})$
send $\langle$"rec"$, k, v_{i,k}, \hat{v}_{i,k}, \pi_{i,k}\rangle$ to all parties
upon receiving the first $\langle$"rec"$, k, v_{j,k}, \hat{v}_{j,k}, \pi_{j,k}\rangle$ message from j, **do**
  if $\mathsf{Verify}(\mathsf{cm}', (-k, j), v_{j,k}, \hat{v}_{j,k}, \pi_{j,k}) = 1$ **then**
    $\mathsf{shares}_{i,k} \leftarrow \mathsf{shares}_{i,k} \cup \{(\omega_j, v_{j,k})\}$
    if $|\mathsf{shares}_{i,k}| = f+1$ **then**
      $\beta_{-k} \leftarrow \mathsf{Interpolate}(\mathsf{shares}_{i,k})$
      output $\beta_{-k}(\omega_0)$ and **terminate**

4.3 Efficient Reconstruction

In this section, we highlight two ways to efficiently reconstruct secrets shared using BingoShare, namely how to reconstruct sums of secrets and how to batch-reconstruct multiple secrets.

First, we observe that sharing $O(n)$ secrets requires sending $O(\lambda n^2)$ words and reconstructing each secret requires $O(\lambda n^2)$ words. One way to leverage the efficient sharing protocol is by reconstructing significantly fewer secrets than the number of secrets shared. This can be done by using the fact that the KZG PCS is additively homomorphic, meaning if $\mathsf{cm}_1, \ldots, \mathsf{cm}_\ell$ are commitments to $(\phi_1, \hat{\phi}_1), \ldots, (\phi_\ell, \hat{\phi}_\ell)$ respectively, then $\prod_{i=1}^{\ell} \mathsf{cm}_i$ is a commitment to the polynomials $(\sum_{i=1}^{\ell} \phi_i, \sum_{i=1}^{\ell} \hat{\phi}_i)$. Therefore, let dealers be a set of dealers for which party i completed BingoShare, and set some $k \in [0, m]$. Then, if we define $r_{k,j}$ to be the k-th secret in the BingoShare invocation with j as dealer, parties can reconstruct $\sum_{j \in \mathsf{dealers}} r_{k,j}$. We provide the code for reconstructing the sum of several shared secrets in Algorithm 4 and highlight that $\alpha_{i,j}, \hat{\alpha}_{i,j}$ are the polynomials $\alpha_i, \hat{\alpha}_i$ set by party i when running BingoShare with j as dealer. Similarly, $\mathsf{cm}_{i,j}$ is the commitment cm_i in the BingoShare invocation with j as dealer.

It is also possible to batch-reconstruct all m secrets at once while sending only $O(\lambda n^2)$ words, as demonstrated in Algorithm 5. Observe that all secrets are values of the form $\phi(\omega_{-k}, \omega_0)$ for $k \in [0, m]$. This means that instead of reconstructing each secret by interpolating the polynomials $\phi(\omega_{-k}, Y)$ and evaluating them at ω_0, it is possible to interpolate the degree-$2f$ polynomial $\phi(X, \omega_0)$ in order to reconstruct all m secrets. This requires parties to send points on their β polynomials, and to provide adequate proofs. Seeing as those proofs need to be

Algorithm 5. $\mathsf{BingoReconstructBatch}_i()$

$\mathsf{shares}_i \leftarrow \emptyset$
$\mathsf{cm}_0 \leftarrow \mathsf{PartialEval}(\mathsf{CM}, \{\omega_0\})$ ▷ only compute partial for ω_0
$(y_0, \hat{y}_0, \pi_0) \leftarrow \mathsf{GetProofs}(\mathsf{proofs}_{\beta,i}, \{\omega_0\})$ ▷ only compute proof for ω_0
send $\langle$"rec"$, y_0, \hat{y}_0, \pi_0\rangle$ to all parties
upon receiving the first $\langle$"rec"$, y_j, \hat{y}_j, \pi_j\rangle$ message from j, **do**
  if $\mathsf{Verify}((\mathsf{cm}_0), (0, j), y_j, \hat{y}_j, \pi_j) = 1$ **then**
    $\mathsf{shares}_i \leftarrow \mathsf{shares}_i \cup \{(\omega_j, y_j)\}$
    if $|\mathsf{shares}_i| = n - f$ **then** ▷ reconstruct along 0'th row, use $\geq 2f + 1$ shares
      $\alpha_0 \leftarrow \mathsf{Interpolate}(\mathsf{shares}_i)$
      output $(\alpha_0(\omega_0), \alpha_0(\omega_{-1}), \ldots, \alpha_0(\omega_{-m}))$ and **terminate**

interpolated and verified with respect to a commitment to $\phi(X, \omega_0), \hat{\phi}(X, \omega_0)$, we use PartialEval and GetProofs to compute those commitments and proofs.

In both BingoReconstructSum and BingoReconstructBatch, parties send a single message of the exact same size as the one sent in BingoReconstruct, resulting in identical complexity. The proofs that the BingoReconstructSum protocol and the BingoReconstructBatch protocol satisfy the required properties is identical to the proof of BingoReconstruct, using the commitments cm' and cm_0 respectively instead of cm, and is thus omitted. See the proofs of correctness and termination of BingoReconstruct for details.

5 From Bingo to ADKG

In this section we show how to use Bingo to achieve an adaptively secure asynchronous distributed key generation (ADKG) protocol that has $O(\lambda n^3)$ communication complexity of and produces a field element as a secret key. Our protocol can be used as a DKG for a low threshold of $f+1$, a high threshold of $2f+1$, or any threshold in between. This versatility enables setting up threshold signature schemes for different uses. For example, using a threshold of $f+1$ proves that at least one nonfaulty party signed a message, whereas using a threshold of $2f+1$ proves that a Byzantine quorum signed a message (which has an honest party in common with any other Byzantine quorum). The below description is consistent with an ADKG protocol with a threshold of $2f+1$, but the protocol can be adjusted to a general threshold of $f+m+1$ for $0 \leq m \leq f$ by having each dealer share only $m+1$ secrets.

In order to get to a DKG we use Bingo at two layers:

1. We use Bingo to get an adaptively secure *validated asynchronous Byzantine agreement* (VABA) protocol. The protocol, presented in the full version of the paper, allows proposals (inputs) of size $O(n)$ and requires $O(n^3)$ expected words.
2. Each party then uses Bingo to share a potential contribution to the DKG. Once the VABA protocol reaches agreement on a proposal, we use the ability of Bingo to reconstruct the sum of secrets. This sum is the secret key, however,

whereas the goal of the DKG is to generate the public key. We thus perform this reconstruction only in the exponent.

In more detail, we start by defining CM_j, $\mathsf{proofs}_{\beta,i,j}$ as the values CM, $\mathsf{proofs}_{\beta,i}$ in the invocation of $\mathsf{BingoShare}$ with j as dealer. Intuitively, our DKG protocol works as follows. First, each party j acts as the dealer for $f+1$ secrets, which we can think of as their 0-th row polynomial $\alpha_{0,j}$. Parties must then agree on a set of dealers whose secrets will contribute to the threshold public key g^s, where the corresponding secret key s is the polynomial $\alpha_{\sum} = \sum_{j \in \mathsf{dealers}} \alpha_{0,j}$ evaluated at ω_0. This agreement requires the use of a VABA protocol. Informally, a VABA protocol allows each party to input a value and output some agreed-upon value in a way that is *correct*, meaning all nonfaulty parties that complete the protocol output the same value, and *valid*, meaning that values output by nonfaulty parties satisfy some external validity function. For a formal definition of a VABA protocol, see the full version of the paper [44].

Once this set is agreed upon using the VABA protocol, parties act to reconstruct the g^s term, as well as their own secret share. For the set of agreed dealers $\mathsf{dealers}$, this latter value for party i is the sum of the column polynomials $\beta_{i,j}$ evaluated at ω_0, where $\beta_{i,j}$ is i's column polynomial in the $\mathsf{BingoShare}$ invocation with j as the dealer. Because $\beta_{i,j}(\omega_0) = \alpha_{0,j}(\omega_i)$, this is equivalent to evaluating α_{Σ} at ω_i. If enough parties share these evaluation points, they can thus interpolate α_{Σ} and evaluate it at ω_0 to reconstruct the secret key. Note that parties do not directly store their $\beta_{i,j}$ polynomials, so they must interpolate evaluations and proofs from their $\mathsf{proofs}_{\beta,i,j}$ sets. Similarly, parties do not compute a commitment to the 0-th row of the polynomial during $\mathsf{BingoShare}$, so they must compute it using CM_j for each dealer j.

We describe how to construct our VABA protocol in the full version of the paper, following closely the path of Abraham et al. [31], whose protocol structure is similar to ours but uses an aggregated PVSS transcript instead of $\mathsf{BingoShare}$. This means we use their Gather protocol and Bingo to build a *weak leader election* protocol, relying particularly on the ability in Bingo to reconstruct sums of secrets, as described in the previous section. From this weak leader election protocol, in which parties are guaranteed to elect the same nonfaulty party with only constant probability p, we build a *proposal election* protocol, and from that we build an adaptively secure VABA protocol. Our protocol has $O(\lambda n^3)$ word complexity and assumes the existence of a PKI and the setup required for the KZG polynomial commitment scheme [22].

Before describing our DKG based on this VABA protocol, we must first extend the $\mathsf{BingoReconstructSum}_i$ algorithm (Algorithm 4). Essentially, whereas $\mathsf{BingoReconstructSum}_i$ reconstructs the sum s of the k-th secrets across a given set of dealers, we need to be able to compute the public key g^s, which involves computing the sum in the exponent. The algorithm for party i, given in Algorithm 6, is similar to $\mathsf{BingoReconstructSum}_i$ but instead of sending y_i and $\hat{y}_i$ to other parties (the evaluations of $\sum_{j \in \mathsf{dealers}} \alpha_{i,j}$ and $\sum_{j \in \mathsf{dealers}} \hat{\alpha}_{i,j}$ at point 0 respectively) it sends $Y_i \leftarrow g^{y_i}$ and $\hat{Y}_i \leftarrow g^{\hat{y}_i}$ as well as proofs of knowledge of y_i and $\hat{y}_i$. We denote by $\pi \xleftarrow{\$} \mathsf{PoK.Prove}(Y, y)$ and $0/1 \leftarrow \mathsf{PoK.Verify}(Y, \pi)$ the respective algorithms for proving and verifying knowledge of y, and by Verify' the PCS algorithm that takes in $Y, \hat{Y}$ rather than $y, \hat{y}$, which is defined as follows.

– $0/1 \leftarrow \mathsf{Verify}'(\mathsf{cm}, \omega, Y, \hat{Y}, \pi)$ Output 1 if $e(\mathsf{cm} \cdot (Y \cdot \hat{Y})^{-1}, h) = e(\pi, h^{\tau-\omega})$, and otherwise output 0.

Finally, we denote by $Y_j \leftarrow \mathsf{IntEvalExp}(\{v_i, Y_i\}_{i=0}^{2f}, \omega_j)$ the algorithm that performs $\mathsf{EvalExp}(\omega_j, \mathsf{InterpolateExp}(\{v_i, Y_i\}_i))$; i.e., that interpolates the degree-$2f$ polynomial given $2f+1$ evaluations and then evaluates it at ω_j (all in the exponent).

With this subprotocol and our VABA in place, we construct our full DKG as shown in Algorithm 7. Once a party has completed $\mathsf{BingoShare}$ for at least $f+1$ dealers, it asks at least $f+1$ other parties to verify that those $\mathsf{BingoShare}$ sessions were indeed completed by sending the set of those dealers in a "proposal" message. After completing the $\mathsf{BingoShare}$ calls for all of these dealers, those parties reply with a signature on the set of $f+1$ dealers. All parties then agree on a set of $f+1$ dealers, $\mathsf{dealers}$, and $f+1$ signatures, sigs, using the VABA protocol with an external validity function defined as follows:

$$\begin{aligned}\mathsf{checkValidity}(\mathsf{dealers}, \mathsf{sigs}) = (&|\mathsf{dealers}| \geq f+1 \ \wedge \ |\mathsf{sigs}| \geq f+1 \ \wedge \\ &\mathsf{Verify}(\mathsf{pk}_j, \sigma_j, \mathsf{dealers}) \ \forall (j, \sigma_j) \in \mathsf{sigs}).\end{aligned} \tag{1}$$

If this holds, meaning at least $f+1$ parties provided a signature for the set of dealers, then at least one nonfaulty party provided a signature. This nonfaulty party thus completed $\mathsf{BingoShare}$, and by termination every nonfaulty party will eventually do so as well. Parties then wait to complete the $f+1$ $\mathsf{BingoShare}$ calls for the agreed set of dealers. Party i can then invoke $\mathsf{BingoSumExpAndRec}_i$ to output pk and sk_i.

Algorithm 6. $\mathsf{BingoSumExpAndRec}_i(\mathsf{dealers})$

$\mathsf{shares}_i \leftarrow \emptyset$
$\forall j \in \mathsf{dealers}$ $\mathsf{cm}_{0,j} \leftarrow \mathsf{PartialEval}(\mathsf{CM}_j, \{\omega_0\})$
$\mathsf{cm}_0 \leftarrow \prod_{j \in \mathsf{dealers}} \mathsf{cm}_{0,j}$
$\forall j \in \mathsf{dealers}$ $y_{i,j}, \hat{y}_{i,j}, \pi_{i,j} \leftarrow \mathsf{GetProofs}(\mathsf{proofs}_{\beta,i,j}, \{\omega_0\})$
$\mathsf{sk}_i \leftarrow \sum_{j \in \mathsf{dealers}} y_{i,j}, \hat{y}_i \leftarrow \sum_{j \in \mathsf{dealers}} \hat{y}_{i,j}, \pi_i \leftarrow \prod_{j \in \mathsf{dealers}} \pi_{i,j}$
$Y_i \leftarrow g^{\mathsf{sk}_i}, \pi \xleftarrow{\$} \mathsf{PoK.Prove}(Y_i, \mathsf{sk}_i)$
$\hat{Y}_i \leftarrow g^{\hat{y}_i}, \hat{\pi} \xleftarrow{\$} \mathsf{PoK.Prove}(Y_i, \hat{y}_i)$
send $\langle$"key share"$, Y_i, \hat{Y}_i, \pi_i, \pi, \hat{\pi}\rangle$ to all parties
upon receiving the first $\langle$"key share"$, Y_j, \hat{Y}_j, \pi_j, \pi, \hat{\pi}\rangle$ message from party j, **do**
  if $\mathsf{Verify}'(\mathsf{cm}_0, \omega_j, Y_j, \hat{Y}_j, \pi_j) = \mathsf{PoK.Verify}(Y_j, \pi) = \mathsf{PoK.Verify}(\hat{Y}_j, \hat{\pi}) = 1$ **then**
    $\mathsf{shares}_i \leftarrow \mathsf{shares}_i \cup \{(\omega_j, Y_j)\}$
    if $|\mathsf{shares}_i| = 2f+1$ **then**
      $\mathsf{pk} \leftarrow \mathsf{IntEvalExp}(\mathsf{shares}_i, \omega_0)$
      output $(\mathsf{pk}, \mathsf{sk}_i)$ and **terminate**

Algorithm 7. $\mathsf{ADKG}_i()$

$\mathsf{prop}_i \leftarrow \emptyset, \mathsf{dealers}_i \leftarrow \emptyset, \mathsf{sigs}_i \leftarrow \emptyset$
$s_0, \ldots, s_f \xleftarrow{\$} \mathbb{F}$
call BingoShare as dealer sharing $s_0, \ldots, s_f$
participate in BingoShare with j as dealer for every $j \in [n]$
upon completing BingoShare with j as dealer, **do**
  $\mathsf{dealers}_i \leftarrow \mathsf{dealers}_i \cup \{j\}$
  if $|\mathsf{dealers}_i| = f + 1$ **then** ▷ choose $f + 1$ dealers to propose
    $\mathsf{prop}_i \leftarrow \mathsf{dealers}_i$
    send $\langle$"proposal"$, \mathsf{prop}_i\rangle$ to every $j \in [n]$
upon receiving the first $\langle$"proposal"$, \mathsf{prop}_j\rangle$ message from party j, **do**
  upon completing BingoShare with k as leader for every $k \in \mathsf{prop}_j$, **do**
    send $\langle$"signature"$, \mathsf{Sign}(\mathsf{sk}_i, \mathsf{prop}_j)\rangle$ to party j ▷ confirm share completion
upon receiving $\langle$"signature"$, \sigma_j\rangle$ from j, **do**
  if $\mathsf{prop}_i \neq \emptyset$ and $\mathsf{Verify}(\mathsf{pk}_j, \mathsf{prop}_i, \sigma_j) = 1$ **then**
    $\mathsf{sigs}_i \leftarrow \mathsf{sigs}_i \cup \{(j, \sigma_j)\}$
    if $|\mathsf{sigs}_i| = f + 1$ **then**
      invoke VABA with input $(\mathsf{prop}_i, \mathsf{sigs}_i)$ and external validity function checkValidity ▷ agree on a set of dealers, at least one honest signature on proposal
upon VABA terminating with output $(\mathsf{prop}, \mathsf{sigs})$, **do**
  upon completing the BingoShare call with j as dealer for every $j \in \mathsf{prop}$, **do**
    invoke $\mathsf{BingoSumExpAndRec}_i$ with input prop ▷ reconstruct from agreed dealers
upon $\mathsf{BingoSumExpAndRec}_i$ terminating with output $(\mathsf{pk}, \mathsf{sk}_i)$, **do**
  output pk and **terminate**

In terms of the security of our DKG, we follow Gennaro et al. [34] in showing that it satisfies *robustness*, meaning that all honest parties agree on the same public key and that there exists an algorithm to allow parties to reconstruct the corresponding secret key.

Theorem 6. *If* Bingo *and the VABA protocol both satisfy correctness and termination, and the VABA protocol satisfies validity, then the ADKG in Algorithm 7 satisfies robustness against an adaptive adversary that can control f parties, where the total number of parties is $n > 3f$.*

We prove this formally in the full version of the paper. Intuitively, we already showed in the Bingo correctness proof that each iteration of BingoShare defines a polynomial and that when running BingoReconstruct each party can use only their share of this polynomial. In Bingo, reconstruction is done on the field element directly, but in the DKG we just need to show that it also holds when done in the exponent. This follows in a relatively straightforward way given that parties are also required to provide proofs of knowledge in their "key share" messages.

For secrecy, it is not clear how to satisfy the definition of Gennaro et al., as the Bingo secrecy definition guarantees the ability to simulate interactions in the BingoShare protocol but for a DKG we need to be able to continue simulating throughout reconstruction (albeit in the exponent) despite not knowing the underlying secret or polynomial. We instead prove that our protocol satisfies the notion of *oracle-aided algebraic simulatability*, as recently defined by Bacho and Loss [19, Definition 3.1]. This means that, following their results, our DKG can be used securely only in the context of threshold BLS signatures.

Definition 4 (Oracle-aided algebraic simulatability). [19] *A DKG protocol has* $(t, k, T_{\mathcal{A}}, T_{\mathsf{Sim}})$-oracle-aided algebraic simulatability *if for every adversary* $\mathcal{A}$ *that runs in time at most* $T_{\mathcal{A}}$ *and corrupts at most* t *parties, there exists an algebraic simulator* Sim *that runs in time at most* T_{Sim}*, makes* $k-1$ *queries to a discrete log oracle* $\mathsf{DL}(\cdot)$*, and satisfies the following properties:*

- *On input* $\xi \leftarrow (g^{z_1}, \ldots, g^{z_k})$*,* Sim *simulates the role of the honest parties in an execution of the DKG. At the end of the simulation, Sim outputs the public key* $\mathsf{pk} = g^x$*.*
- *On input* $\xi \leftarrow (g^{z_1}, \ldots, g^{z_k})$ *and for* $i \in [k-1]$*, let* g_i *denote the* i*-th query to* DL*. Let* $(\hat{a}_i, a_{i,1}, \ldots, a_{i,k})$ *denote the corresponding algebraic coefficients, i.e. the values such that* $g_i = g^{\hat{a}_i} \cdot \prod_{j=1}^{k} (g^{z_j})^{a_{i,j}}$ *and denote by* $(\hat{a}, a_{0,1}, \ldots, a_{0,k})$ *the algebraic coefficients corresponding to* pk*. Then the following matrix is invertible:*
$$L := \begin{pmatrix} a_{0,1} & a_{0,2} & \cdots & a_{0,k} \\ a_{1,1} & a_{1,2} & \cdots & a_{1,k} \\ \vdots & \vdots & & \vdots \\ a_{k-1,1} & a_{k-1,2} & \cdots & a_{k-1,k} \end{pmatrix}.$$
Whenever Sim *completes a simulation of an execution of the DKG, we call* L *the* simulatability matrix *of* Sim *(for this particular simulation).*
- *Denote by* $\mathsf{view}_{\mathcal{A},y,\mathsf{DKG}}$ *the view of* $\mathcal{A}$ *in an execution of the DKG conditioned on all honest parties outputting* $\mathsf{pk} = y$*. Similarly, denote by* $\mathsf{view}_{\mathcal{A},\xi,y,\mathsf{Sim}}$ *the view of* $\mathcal{A}$ *when interacting with* Sim *on input* ξ*, conditioned on Sim outputting* $\mathsf{pk} = y$*. (For convenience,* Sim*'s final output* pk *is omitted from* $\mathsf{view}_{\mathcal{A},\xi,y,\mathsf{Sim}}$*). Then, for all* y *and all* ξ*,* $\mathsf{view}_{\mathcal{A},\xi,y,\mathsf{Sim}}$ *and* $\mathsf{view}_{\mathcal{A},y,\mathsf{DKG}}$ *are computationally indistinguishable.*

Intuitively, our DKG simulator follows the Bingo secrecy simulator during the BingoShare interactions and otherwise behaves honestly up until the point at which it has to send a "key share" message. It then uses the omdl challenges to define points on a polynomial and sends "key share" messages that are consistent with these points. Crucially, this polynomial is also consistent with the public key that the simulator needs to output, which it also chooses from its omdl challenge. If a party is corrupted after sending a "key share" message, the simulator can then create the appropriate state by calling its DL oracle. Access to the DL oracle is essential in doing this precisely because we need adaptive security and thus the simulator does not know in advance which parties will be corrupted.

Theorem 7. *If* Bingo *satisfies correctness and secrecy and the VABA satisfies correctness and external validity, then the ADKG in Algorithm 7 has* $(f, 2f+1)$*-oracle-aided algebraic security against an adaptive adversary that can control* f *parties, where the total number of parties is* $n > 3f$*.*

Proof. We begin by describing the simulator $\mathsf{Sim}_{\mathcal{A}}^{\mathsf{DL}(\cdot)}$, which takes in a generator g and $2f+1$ group elements $Z_0, Z_1, \ldots, Z_f, \hat{Z}_1, \ldots, \hat{Z}_f$. To simulate nonfaulty parties in the DKG protocol, Sim acts as the Bingo simulator during $\mathsf{BingoShare}$ interactions (this simulator is guaranteed to exist by secrecy, and is described in the proof of Theorem 4.) During all other parts of the DKG before line 20, the simulator behaves honestly; i.e. it honestly computes and sends "proposal" messages, responds with "signature" messages when it receives "proposal" messages, and invokes the VABA protocol once it has enough signatures.

When the first nonfaulty party completes the VABA protocol with output $(\mathsf{dealers}, \mathsf{sigs})$, Sim sets C to be the set of currently corrupted parties. From the correctness of the VABA protocol, all nonfaulty parties also output $(\mathsf{dealers}, \mathsf{sigs})$. In addition, from the external validity property, sigs contains at least $f+1$ signatures on the set $\mathsf{dealers}$, which means that it includes at least one signature from a nonfaulty party. Nonfaulty parties only sign $\mathsf{dealers}$ if they have completed the $\mathsf{BingoShare}$ invocations with j as dealer for every $j \in \mathsf{dealers}$, and thus at least one nonfaulty party completed the protocol for each such dealer. As shown in Lemma 4, for every faulty dealer $j \in \mathsf{dealers}$, it is possible to extract polynomials $\phi_j, \hat{\phi}_j$ from the combined views of the nonfaulty parties, which Sim can do as it has these views and behaves completely honestly when the dealer is faulty. On the other hand, in the proof of Theorem 4, the simulator defines polynomials $\alpha_{i,j}, \hat{\alpha}_{i,j}, \beta_{i,j}, \hat{\beta}_{i,j}$ for every faulty i in the simulated $\mathsf{BingoShare}$ invocation with a nonfaulty j as dealer. Putting this together, Sim thus knows the polynomials $\alpha_{i,j}, \hat{\alpha}_{i,j}, \beta_{i,j}, \hat{\beta}_{i,j}$ for faulty dealers $j \in \mathsf{dealers}$ and all parties i and the polynomials $\alpha_{i,j}, \hat{\alpha}_{i,j}, \beta_{i,j}, \hat{\beta}_{i,j}$ for nonfaulty dealers $j \in \mathsf{dealers}$ and faulty parties i.

Let ℓ be the number of parties corrupted at the time the first nonfaulty party completes the VABA protocol, and let $C = \{i_1, \ldots, i_\ell\}$. Sim chooses $I = \{i_{\ell+1}, \ldots, i_f\} \subset [n]$ to be some subset of $[n]$ of size $f-k$ such that $C \cap I = \emptyset$ (for example, the $f-k$ minimal indices that aren't in C). Sim chooses an additional set $I' = \{i_{f+1}, \ldots, i_{2f}\}$[2] such that $I' \cap C = \emptyset$ and $I' \cap I = \emptyset$. Finally, let $i_{2f+1}, \ldots, i_n$ be the indices of the remaining parties, i.e. $\{i_{2f+1}, \ldots, i_n\} = [n] \setminus (C \cup I \cup I')$. Sim then defines $Z'_0 \leftarrow Z_0$ and $i_0 = 0$, as well as the following:

- For every $k \in [\ell]$, $Z'_{i_k} \leftarrow g^{\sum_{j \in \mathsf{dealers}} \beta_{i_k,j}(0)}$ and $\hat{Z}'_{i_k} \leftarrow \hat{g}^{\sum_{j \in \mathsf{dealers}} \hat{\beta}_{i_k,j}(0)}$.
- For every $k \in \{\ell+1, \ldots, f\}$, $Z'_{i_k} \leftarrow Z_k$ and $\hat{Z}'_{i_k} \leftarrow \hat{Z}_k$.
- For every $k \in \{f+1, \ldots, 2f\}$, Sim samples $z_{i_k}, \hat{z}_{i_k} \xleftarrow{\$} \mathbb{F}$ and sets $Z'_{i_k} \leftarrow g^{z_{i_k}}$ and $\hat{Z}_{i_k} \leftarrow \hat{g}^{\hat{z}_{i_k}}$.
- For every $k \in \{2f+1, \ldots, n\}$, $Z'_{i_k} \leftarrow \mathsf{IntEvalExp}(\{(\omega_{i_m}, Z'_{i_m})\}_{m=0}^{2f}, \omega_{i_k})$.

[2] For a threshold of $f+m+1$, define $I' = \{i_{f+1}, \ldots, i_{f+m}\}$ instead.

The simulator then computes $Z'_\tau \leftarrow \mathsf{IntEvalExp}(\{(\omega_{i_m}, Z'_{i_m})\}_{m=0}^{2f}, \tau)$, as well as $\mathsf{cm}_0 \leftarrow \prod_{j\in\mathsf{dealers}} \mathsf{cm}_{0,j}$ (as computed in $\mathsf{BingoSumExpAndRec}$), and $\hat{Z}'_\tau \leftarrow (\mathsf{cm}_0(Z'_\tau)^{-1})^{\frac{1}{x}}$. It computes $\hat{Z}'_{i_k} \leftarrow \mathsf{IntEvalExp}(\{(\omega_{i_m}, \hat{Z}'_{i_m})\}_{m\in[2f]} \cup \{(\tau, \hat{Z}'_\tau)\}, \omega_{i_k})$ for every $k \in \{2f+1, \dots, n\}$. Finally, Sim calls its discrete log oracle 2ℓ times on $Z_{i_1}, \dots, Z_{i_\ell}, \hat{Z}_{i_1}, \dots, \hat{Z}_{i_\ell}$.

After computing these values, Sim is now ready to simulate nonfaulty parties in Algorithm 6. Whenever a nonfaulty party i should send a "key share" message, Sim computes $\pi_i \leftarrow (\mathsf{cm}_0 \cdot (Z'_i\hat{Z}'_i)^{-1})^{\frac{1}{\tau-\omega_i}}$ as well as simulated proofs of knowledge $\pi, \hat{\pi}$ for Z'_i and $\hat{Z}'_i$ respectively. Sim then adds messages to the buffer as if i sent the message $\langle$"key share"$Z'_i, \hat{Z}'_i, \pi_i, \pi, \hat{\pi}\rangle$ to all parties. If the adversary corrupts party i after this point and $i \notin \{i_{f+1}, \dots, i_{2f}\}$, Sim calls its discrete log oracle twice to get $z_i = \mathsf{DL}(Z'_i), \hat{z}_i = \mathsf{DL}(\hat{Z}'_i)$. On the other hand, if the adversary corrupts party i and $i \in \{i_{f+1}, \dots, i_{2f}\}$, it uses the previously sampled z_i and $\hat{z}_i$ instead and does not call its DL oracle. It then generates i's view following the Bingo simulator (described in the proof of secrecy) in all invocations of Bingo with honest dealers except for one nonfaulty dealer $j \in \mathsf{dealers}$, including generating appropriate α and β polynomials for i. For this dealer j, it uniformly samples a degree-f polynomial $\beta_{i,j}(Y)$ such that $\beta_{i,j}(0) = z_i - \sum_{k\in\mathsf{dealers}\setminus\{j\}} \beta_{i,k}(0)$ and $\alpha_{k,j}(\omega_i) = \beta_{i,j}(\omega_k)$ for all corrupted k. Similarly, it samples a degree-f polynomial $\hat{\beta}_{i,j}(Y)$ such that $\hat{\beta}_{i,j}(0) = \hat{z}_i - \sum_{k\in\mathsf{dealers}\setminus\{j\}} \hat{\beta}_{i,k}(0)$ and $\hat{\alpha}_{k,j}(\omega_i) = \hat{\beta}_{i,j}(\omega_k)$ for every corrupted k. Again following the Bingo simulator, Sim calls $\mathsf{SimOpen}$ to define $\alpha_{i,j}, \hat{\alpha}_{i,j}$ given the sampled $\beta_{i,j}, \hat{\beta}_{i,j}$, i.e. it computes $\alpha_{i,j}, \hat{\alpha}_{i,j} \xleftarrow{\$} \mathsf{SimOpen}(\tau_s, \mathsf{cm}_{i,j}, c_{i,j}, \{\omega_k, \beta_{k,j}(\omega_i), \hat{\beta}_{k,j}(\omega_i)\}_{k\in C})$, where C is the set of currently corrupted parties and $c_{i,j}$ is the auxiliary information computed by the Bingo simulator when running $\mathsf{BingoShare}$ with i as the dealer. Finally, in order to generate i's view as a dealer, Sim runs the Bingo simulator to generate the polynomials $\phi_i$and $\hat{\phi}_i$ and associated view. Sim then adds i to the set of corrupted parties and continues in the simulation. At the point at which some nonfaulty party completes the DKG protocol, let $j_{\ell+1}, \dots, j_{\ell+m}$ be the indices of the parties corrupted after the first nonfaulty party completed the VABA protocol such that for every $k \in \{\ell+1, \dots, \ell+m\}$, $j_k \notin I'$. Sim chooses indices $j_{\ell+m+1}, \dots, j_f \notin I'$ of parties that weren't corrupted by the adversary and calls $\mathsf{DL}(Z'_{j_k})$ and $\mathsf{DL}(\hat{Z}'_{j_k})$ for every $k \in \{\ell+m+1, \dots, f\}$. Finally, Sim outputs Z_0 as pk and terminates.

We must now argue that the simulator satisfies the requirements of oracle-aided algebraic security, namely that it correctly simulates interactions with honest parties and that the matrix containing its algebraic coefficients is invertible. For the first requirement, Theorem 4 tells us that the simulated runs of the $\mathsf{BingoShare}$ protocol are computationally indistinguishable from normal runs of the protocol. The simulator then runs the DKG protocol honestly up to line 20. In the non-simulated invocation of $\mathsf{BingoSumExpAndRec}$, each nonfaulty party i sends a "key share" message with $Y_i = g^{\sum_{j\in\mathsf{dealers}} \beta_{i,j}(0)}$, $\hat{Y}_i = \hat{g}^{\sum_{j\in\mathsf{dealers}} \hat{\beta}_{i,j}(0)}$, π_i being the unique proof for which Verify' verifies (once the other values have been fixed), and two proofs of knowledge. Importantly, the pair of polynomials $\phi_\Sigma = \sum_{j\in\mathsf{dealers}} \phi_j$ and $\hat{\phi}_\Sigma = \sum_{j\in\mathsf{dealers}} \phi_j$ satisfy $\mathsf{cm}_0 = \mathsf{Commit}(\phi_\Sigma; \hat{\phi}_\Sigma)$. Note that $\sum_{j\in\mathsf{dealers}} \beta_{i,j}(0) = \sum_{j\in\mathsf{dealers}} \phi_j(\omega_i, 0)$ and similarly $\sum_{j\in\mathsf{dealers}} \hat{\beta}_{i,j}(0) = \sum_{j\in\mathsf{dealers}} \hat{\phi}_j(\omega_i, 0)$. From Theorem 4, before some nonfaulty party calls $\mathsf{BingoReconstruct}(0)$ on a value shared by a nonfaulty dealer, the value is entirely independent of the adversary's view. This is because the simulator could complete the run to correctly reconstruct any possible secret from that point on. Therefore, since the one nonfaulty dealer in $\mathsf{dealers}$ uniformly sampled its secrets, the sum is uniform and independent of the adversary's view. In the simulation, the nonfaulty parties also send messages with $Z'_i, \hat{Z}'_i$ such that their discrete logs lie on uniformly sampled polynomials of the same degree that are consistent with cm_0 and the points $\sum_{j\in\mathsf{dealers}} \phi_j(\omega_k, 0)$ and $\sum_{j\in\mathsf{dealers}} \hat{\phi}_j(\omega_k, 0)$ of faulty parties. In addition, the proof π is the unique proof for which Verify' verifies, and the proofs of knowledge are perfectly simulated. Finally, whenever a party i is corrupted during $\mathsf{BingoSumExpAndRec}$, its view is made consistent with $Z'_i, \hat{Z}'_i$ and the rest of the $\mathsf{BingoShare}$ simulation is identical to the simulation described in Theorem 4. Its view is thus sampled identically as well.

We now consider the matrix defined by the algebraic coefficients given by Sim when querying its DL oracle, with the goal of proving that it is invertible. For each $i \in [\ell]$, the algebraic representation for the oracle call $\mathsf{DL}(Z_i)$ is simply the indicator vector that equals 1 in the coordinate corresponding to the input element Z_i and 0 elsewhere. Similarly, for each $i \in [\ell]$, the algebraic representation for $DL(\hat{Z}_i)$ is the indicator vector for $\hat{Z}_i$, and the algebraic representation of $\mathsf{pk} = Z_0$ is the indicator vector for Z_0. We can thus rearrange the rows and columns of the matrix—which does not affect its invertibility—so that the first 2ℓ rows and columns are the indicator vectors corresponding to the elements $Z_1, \ldots, Z_\ell, \hat{Z}_1, \ldots, \hat{Z}_\ell$. The remaining algebraic expressions for each $\mathsf{DL}(Z'_i)$ call result from interpolating $Z'_0, Z'_1, \ldots Z'_f$ and then evaluating at ω_i, both of which are linear functions. The algebraic expressions for $\hat{Z}'_i$ are computed in a similar fashion. The first set of elements were not used in forming any of the $Z'_i, \hat{Z}'_i$ group elements, and thus the rearranged matrix is a block matrix of the form $L = \begin{pmatrix} I & 0 \\ 0 & A \end{pmatrix}$, where I is the identity matrix of size $2\ell \times 2\ell$ and A is a matrix with the algebraic representation of the $\mathsf{DL}(Z'_i)$ and $\mathsf{DL}(\hat{Z}'_i)$ calls, as well as the algebraic representation of Z_0.

In order to show that L is invertible, it is enough to show that A is invertible, since I is trivially invertible. We do that by showing that the linear transformation defined by A is invertible. Let $j_{\ell+1}, \ldots, j_f$ be defined as above. Then A represents some linear transformation from $Z_0, Z_{\ell+1}, \ldots, Z_f, \hat{Z}_{\ell+1}, \ldots, \hat{Z}_f$ to $\mathsf{pk}, Z'_{j_{\ell+1}}, \ldots, Z'_{j_f}, \hat{Z}'_{j_{\ell+1}}, \ldots, \hat{Z}'_{j_f}$. This function has the same size domain and range (since the number of elements is the same), so to prove that it is invertible it suffices to show that it is one-to-one. Assume that two sets of inputs $Z_0, Z_{\ell+1}, \ldots, Z_f, \hat{Z}_{\ell+1}, \ldots, \hat{Z}_f$ and $X_0, X_{\ell+1}, \ldots, X_f, \hat{X}_{\ell+1}, \ldots, \hat{X}_f$ yield the same output $\mathsf{pk}, Z'_{j_{\ell+1}}, \ldots, Z'_{j_f}, \hat{Z}'_{j_{\ell+1}}, \ldots, \hat{Z}'_{j_f}$. The discrete logs of

$Z'_0, Z'_1, \ldots, Z'_n$ and Z'_τ all lie on the same f-degree polynomial, and thus any $f+1$ such elements define the polynomial fully and the rest of the points. Therefore, the elements $Z'_0, Z'_{i_1}, \ldots, Z'_{i_\ell}, Z'_{j_{\ell+1}}, \ldots, Z'_{j_f}$ fully define the entire set $Z'_0, Z'_1, \ldots, Z'_n$. In this case, $Z'_0, Z'_{j_{\ell+1}}, \ldots, Z'_{j_f}$ are all parts of the output of the function, and $Z'_{i_1}, \ldots, Z'_{i_\ell}$ are constants computed directly by Sim. Therefore, the function's output uniquely defines $Z'_0, Z'_1, \ldots, Z'_n, Z'_\tau$. Note that by construction $Z'_0 = Z_0 = X_0$ and also $Z'_{i_k} = Z_k = X_k$ for every $k \in \{\ell+1, \ldots, f\}$, and thus the first half of the inputs is equal. In addition, $\hat{Z}'_\tau$ is uniquely defined given the previous values, and thus $\hat{Z}'_\tau, \hat{Z}'_{i_1}, \ldots, \hat{Z}'_{i_\ell}, \hat{Z}'_{j_{\ell+1}}, \ldots, \hat{Z}'_{j_f}$ define the group elements $\hat{Z}'_1, \ldots, \hat{Z}'_n$. Therefore, for similar reasons, $\hat{Z}'_{i_k} = \hat{Z}_k = \hat{X}_k$ for every $k \in \{\ell+1, \ldots, f\}$. In other words, all elements of the input must be equal, and thus the function is one-to-one. □

Acknowledgements. We would like to thank Alin Tomescu, Kobi Gurkan, Julian Loss, and Renas Bacho for many insightful discussions. Gilad Stern was supported by the HUJI Federmann Cyber Security Research Center in conjunction with the Israel National Cyber Directorate (INCD) in the Prime Minister's Office.

References

1. Cachin, C., Kursawe, K., Lysyanskaya, A., Strobl, R.: Asynchronous verifiable secret sharing and proactive cryptosystems. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, pp. 88–97 (2002)
2. Cachin, C., Kursawe, K., Shoup, V.: Random Oracles in Constantinople: practical asynchronous byzantine agreement using cryptography. J. Cryptol. **18**, 219–246 (2005)
3. Gurkan, K., Jovanovic, P., Maller, M., Meiklejohn, S., Stern, G., Tomescu, A.: Aggregatable distributed key generation. In: Canteaut, A., Standaert, F.-X. (eds.) EUROCRYPT 2021. LNCS, vol. 12696, pp. 147–176. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77870-5_6
4. Patra, A., Choudhury, A., Rangan, C.P.: Efficient Asynchronous verifiable secret sharing and multiparty computation. J. Cryptol. **28**(1), 49–109 (2015). https://doi.org/10.1007/s00145-013-9172-7
5. Syta, E., et al.: Scalable Bias-Resistant Distributed Randomness. In: 38th IEEE Symposium on Security and Privacy, San Jose, CA, May 2017
6. Chor, B., Goldwasser, S., Micali, S., Awerbuch, B.: Verifiable secret sharing and achieving simultaneity in the presence of faults (extended abstract). In: 26th Annual Symposium on Foundations of Computer Science, pp. 383–395 (1985)
7. Franklin, M.K., Yung, M.: Communication complexity of secure computation (extended abstract). In: Proceedings of the 24th Annual ACM Symposium on Theory of Computing, pp. 699–710. ACM (1992)
8. Ben-Or, M., Canetti, R., Goldreich, O.: Asynchronous secure computation. In: Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing, pp. 52–61 (1993)
9. Canetti, R., Rabin, T.: Fast asynchronous Byzantine agreement with optimal resilience. In: Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing, pp. 42–51 (1993)

10. Cramer, R., Damgård, I., Dziembowski, S., Hirt, M., Rabin, T.: Efficient multi-party computations secure against an adaptive adversary. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 311–326. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_22
11. Chopard, A., Hirt, M., Liu-Zhang, C.-D.: On communication-efficient asynchronous MPC with adaptive security. In: Nissim, K., Waters, B. (eds.) TCC 2021. LNCS, vol. 13043, pp. 35–65. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-90453-1_2
12. Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In: Proceedings of the 21st Annual ACM Symposium on Theory of Computing, pp. 73–85. ACM (1989)
13. Daian, P., et al.: Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. In: IEEE Symposium on Security and Privacy (2020)
14. Qin, K., Zhou, L., Gervais, A.: Quantifying blockchain extractable value: how dark is the forest? In: IEEE Symposium on Security and Privacy (2022)
15. Bowe, S., Gabizon, A., Miers, I.: Scalable Multi-party Computation for ZK-SNARK Parameters in the Random Beacon Model. Cryptology ePrint Archive, Paper 2017/1050 (2017)
16. Fuchsbauer, G., Kiltz, E., Loss, J.: The algebraic group model and its applications. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10992, pp. 33–62. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96881-0_2
17. Kokoris Kogias, E., Malkhi, D., Spiegelman, A.: Asynchronous distributed key generation for computationally-secure randomness, consensus, and threshold signatures. In: CCS 2020: 2020 ACM SIGSAC Conference on Computer and Communications Security (2020)
18. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. J. Cryptol. **17**(4), 297–319 (2004)
19. Bacho, R., Loss, J.: On the adaptive security of the threshold BLS signature scheme. In: Proceedings of ACM CCS 2022 (2022)
20. Canetti, R., Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Adaptive security for threshold cryptosystems. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 98–116. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_7
21. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA, pp. 218–229. ACM (1987)
22. Kate, A., Zaverucha, G.M., Goldberg. I.: Constant-size commitments to polynomials and their applications. In: Advances in Cryptology - ASIACRYPT 2010, pp. 177–194 (2010)
23. Kohlweiss, M., Maller, M., Siim, J., Volkhov, M.: Snarky ceremonies. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021. LNCS, vol. 13092, pp. 98–127. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-92078-4_4
24. Abraham, I., Asharov, G., Patil, S., Patra, A.: Asymptotically Free Broadcast in Constant Expected Time via Packed VSS. In: IACR Cryptol. ePrint Arch. (2022). https://eprint.iacr.org/2022/1266
25. Abraham, I., Asharov, G., Yanai, A.: Efficient perfectly secure computation with optimal resilience. J. Cryptol. **35**(4), 27 (2022)
26. Kate, A., Miller, A., Yurek, T.: Brief Note: Asynchronous Verifiable Secret Sharing with Optimal Resilience and Linear Amortized Overhead (2019). arXiv: 1902.06095 [cs.CR]

27. Backes, M., Datta, A., Kate, A.: Asynchronous computational VSS with reduced communication complexity. In: Topics in Cryptology – CT-RSA 2013, pp. 259–276 (2013)
28. AlHaddad, N., Varia, M., Zhang., H.: High-threshold AVSS with optimal communication complexity. In: Financial Cryptography and Data Security, pp. 479–498 (2021)
29. Yurek, T., Luo, L., Fairoze, J., Kate, A., Miller, A.K.: hbACSS: how to robustly share many secrets. In: Proceedings of the Network and Distributed System Security Symposium (NDSS) 2022 (2022)
30. Kate, A., Huang, Y., Goldberg, I.: Distributed key generation in the wild. In: Proceedings of ICDCS (2009)
31. Abraham, I., Jovanovic, P., Maller, M., Meiklejohn, S., Stern, G., Tomescu, A.: Reaching consensus for asynchronous distributed key generation. In: PODC 2021: ACM Symposium on Principles of Distributed Computing 2021, pp. 363–373 (2021)
32. Das, S., Yurek, T., Xiang, Z., Miller, A., Kokoris-Kogias, L., Ren, L.: Practical asynchronous distributed key generation. In: 2022 IEEE Symposium on Security and Privacy (SP), pp. 2518–2534 (2022)
33. Groth, J., Shoup, V.: Design and analysis of a distributed ECDSA signing service. In: Cryptology ePrint Archive (2022). https://eprint.iacr.org/2022/506
34. Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Secure distributed key generation for discrete-log based cryptosystems. J. Cryptol. **20**(1), 51–83 (2007)
35. Feldman, P., Micali, S.: Optimal algorithms for byzantine agreement. In: Proceedings of the 20th Annual ACM Symposium on Theory of Computing, pp. 148–161. ACM (1988)
36. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: Fast reed-solomon interactive oracle proofs of proximity. In: 45th International Colloquium on Automata, Languages, and Programming (ICALP 2018), pp. 14:1–14:17 (2018)
37. Ben-Sasson, E., Goldberg, L., Kopparty, S., Saraf, S.: DEEP-FRI: sampling outside the box improves soundness. In: 11th Innovations in Theoretical Computer Science Conference, ITCS, pp. 5:1–5:32 (2020)
38. Bootle, J., Cerulli, A., Chaidos, P., Groth, J., Petit, C.: Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 327–357. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_12
39. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., Maxwell, G.: Bulletproofs: short proofs for confidential transactions and more. In: 2018 IEEE Symposium on Security and Privacy, pp. 315–334 (2018)
40. Choudhury, A., Patra, A.: An efficient framework for unconditionally secure multiparty computation. IEEE Trans. Inf. Theory. **63**(1), 428–468 (2017). https://doi.org/10.1109/TIT.2016.2614685
41. Cascudo, I., David, B.: Scrape: scalable randomness attested by public entities. In: Gollmann, D., Miyaji, A., Kikuchi, H. (eds.) ACNS 2017. LNCS, vol. 10355, pp. 537–556. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-61204-1_27
42. Cascudo, I., David, B.: ALBATROSS: publicly AttestabLe BATched randomness based on secret sharing. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020. LNCS, vol. 12493, pp. 311–341. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64840-4_11
43. Das, S., Xiang, Z., Ren, L.: Asynchronous data dissemination and its applications. In: CCS 2021: 2021 ACM SIGSAC Conference on Computer and Communications Security, pp. 2705–2721 (2021)

44. Abraham, I., Jovanovic, P., Maller, M., Meiklejohn, S., Stern, G.: Bingo: Adaptivity and Asynchrony in Verifiable Secret Sharing and Distributed Key Generation (2022). https://eprint.iacr.org/2022/1759
45. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_25
46. Boneh, D., Boyen, X.: Short signatures without random oracles and the SDH assumption in bilinear groups. J. Cryptol. **21**(2), 149–177 (2008)
47. Bellare, M., Namprempre, C., Pointcheval, D., Semanko, M.: The one- more-RSA-inversion problems and the security of Chaum's blind signature scheme. J. Cryptol. **16**3 (2003)
48. von zur Gathen, J., Gerhard, J.: Modern Computer Algebra (3rd edn.) Cambridge University Press (2013). ISBN: 978-1-107-03903-2