The Authentication Complexity of Byzantine Consensus

Kecheng Shi

CISPA Helmholtz Center for Information Security

Abstract

Byzantine broadcast and Byzantine agreement are fundamental problems in distributed computing and building blocks for secure multiparty computation. In complete synchronous networks of n parties with channels identifying the immediate sender, classical results establish how authentication changes resilience to t Byzantine faults. Without initially authenticated public keys, both tasks are possible if and only if $n > 3t$ [PSL80]. With a complete public-key infrastructure (PKI), broadcast tolerates every $t < n$ [DS83], and agreement is possible if and only if $n > 2t$. These thresholds leave a substantial gap: *how much initial authentication is necessary for a given fault bound, and how does its distribution affect feasibility?*

We study this question by allowing each party's designated public verification key to be initially authenticated to any subset of the other parties. We represent this setup by a directed authentication graph G whose vertices are parties, with an edge $x \to y$ exactly when y is a *verifier* of x: that is, x's designated public verification key is initially authenticated to y. We count each edge as one unit and define *authentication complexity* as the *minimum* total bindings over all setups and protocols achieving the required task and fault tolerance. Protocols may establish further authentication during execution without adding initial cost.

We give a tight graph characterization of the initial authentication setups that support agreement, including when each party knows only its own initial key table and is not given the authentication graph. For $2t < n \leq 3t$ and $r = n - 2t$, we show that agreement has authentication complexity $\Theta(\min\{n^2, (n^2/r)\ln(en/r)\})$ and give a protocol with polynomial local computation. At $n = 2t+1$, broadcast requires $\Omega(n \ln^2 n/\ln\ln n)$ initial authentications, and has a construction using $O(n^{3/2}\sqrt{\ln n})$ initial authentications. At this threshold, we also show a complete PKI setup is necessary for agreement. Surprisingly, broadcast has subquadratic authentication complexity even when $t = n/2 + o(n)$. For every fixed fault fraction $\alpha \in (1/2, 1)$, we show its authentication complexity is $\Theta_\alpha(n^2)$. We also determine the exact authentication complexity of broadcast at maximum resilience: $\binom{n}{2} - 1$ initial authentications suffice and are necessary to tolerate $t = n - 1$ faults.

1 Introduction

Byzantine broadcast and Byzantine agreement are fundamental problems in distributed computing and building blocks for secure multiparty computation. They ask how parties can reach a common

decision when some parties behave arbitrarily. In Byzantine broadcast, honest parties must choose the same output, equal to a designated sender's input when that sender is honest. In Byzantine agreement, every party has an input, and honest parties must choose the same output, equal to their common input whenever all honest inputs are the same. It is well known that initial authentication setups change the resilience of Byzantine agreement and broadcast. Over complete synchronous channels, broadcast needs no initially authenticated public keys when $n > 3t$ [PSL80], whereas a complete public-key infrastructure (PKI) can improve the resilience to every $t < n$ [DS83]. A complete PKI lets every party initially authenticate every other party's public key. Between these well-studied cases, a natural question is how much initial authentication is necessary and how the choice of verifiers for each signer affects feasibility of broadcast and agreement. Lenzen, Loss, Shi, and Wagner [LLSW26] show how partial authentication improves resilience beyond $n/3$. With s parties' public keys authenticated to everyone, they construct broadcast from any of these s parties whenever $3t < n + 2s$. We further allow each signer to have any subset of the other parties as its *verifiers* and ask for the minimum number of initial bindings required by each task and fault bound. All verifiers receive the signer's designated key in their initial *key tables*, even when the signer is faulty, and can verify forwarded signed messages under that key.

1.1 Authentication complexity

We consider a set $\mathcal{P}$ of $n \geq 3$ parties and $0 \leq t < n$, with complete reliable synchronous channels identifying the message sender. We focus on *binary* Byzantine broadcast and agreement in this work. We describe the setup using an authentication graph G: an authentication edge $x \to y$ means that y is a verifier of x. Write $V_x = \{y \neq x : x \to y\}$ for the verifiers of x and $\widehat{V}_x = \{x\} \cup V_x$ to include its knowledge of its own key. Let $K_v = \{x : v \in V_x\}$ be the set of other parties whose public keys are initially authenticated to v. The setup has cost $\sum_v |K_v| = |E(G)|$, and a complete PKI setup costs $n(n-1)$. For a task $\mathcal{T}$, we define its *authentication complexity* by

$$A_{\mathcal{T}}(n,t) = \min_{G,\Pi}\{|E(G)| : \Pi \text{ solves } \mathcal{T} \text{ on } G \text{ against at most } t \text{ faults}\}.$$

We minimize over all authentication graphs in our model, with idealized signatures. Protocols may use any finite amount of communication and local computation, subject to a public finite round bound. They may establish further authentication during execution without adding initial cost. Let $A_{\mathsf{BA}}(n,t)$ denote the authentication complexity of Byzantine agreement (BA), and $A_{\mathsf{BB}}(n,t)$ that of broadcast from a designated sender.

1.2 Authentication and resilience

Tight characterization of authentication. We completely characterize which authentication graphs support Byzantine agreement.

Main Theorem 1 (BA characterization)**.** *Let $n \geq 3$ and $0 \leq t < n$. The following are equivalent:*

(i) Byzantine agreement is possible on G.

(ii) $n > 2t$*, and for every three pairwise disjoint sets* $A, B, C \subseteq \mathcal{P}$ *satisfying*

$$n - 2t \le |A|, |B|, |C| \le t, \qquad |A| + |B| + |C| \ge 2n - 3t,$$

there is a signer $x \in C$ *such that*

$$V_x \cap A \neq \varnothing, \qquad V_x \cap B \neq \varnothing.$$

The characterization holds with either a public authentication graph description or only local key tables. For each fixed n, t*, a single deterministic agreement protocol exists on every graph satisfying the condition, using only each party's local key table. The protocol has polynomial local computation and has* $5(t+1)$ *rounds.*

We call the graph requirement in item (ii) the *three-set condition*. The sets A, B, C need not cover all parties. For $n > 3t$, the condition trivially holds since there are no three such sets.

Tight authentication bounds for agreement. We then study necessary authentication costs by minimizing the number of authentication edges among the graphs satisfying the three-set condition. The parameter $r = n - 2t$ measures the minimum difference between the numbers of honest and faulty parties. Our second result determines how the authentication complexity grows as this difference decreases.

Main Theorem 2 (Authentication complexity of Byzantine agreement)**.** *For* $2t < n \le 3t$*, put* $r = n - 2t$*. Then*

$$A_{\mathsf{BA}}(n,t) = \Theta\left(\min\left\{n^2, \frac{n^2}{r}\ln\frac{en}{r}\right\}\right).$$

In particular, at $n = 2t+1$*, every directed authentication edge between distinct parties is necessary. For* $n \le 2t$*, BA is impossible.*

In the nontrivial range, $r = \Theta(n)$ gives $\Theta(n)$ authentication edges; $r = \sqrt{n}$ gives $\Theta(n^{3/2}\ln n)$, and $r = O(\ln n)$ requires $\Theta(n^2)$. Our construction achieves asymptotically optimal total authentication cost while ensuring that each party initially authenticates at most a constant multiple of the average number of keys (Theorem 4.11). In particular, for every fixed fault fraction $\alpha = t/n \in (1/3, 1/2)$, a constant number of authenticated keys per party suffices.

Authentication complexity of Byzantine broadcast. Authenticating the sender's key to everyone does not suffice for broadcast. We give upper and lower bounds on the authentication complexity for broadcast.

Main Theorem 3 (Authentication complexity of Byzantine broadcast)**.** *Let* $n \ge 3$ *and* $1 \le t < n$ *with* $n \le 3t$*.*

If $2t < n \le 3t$*, set* $r = n - 2t$*. Then*

$$\Omega\left(\frac{n\ln^2(n/r)}{\ln\ln(4n/r)}\right) \le A_{\mathsf{BB}}(n,t) \le O\left(\min\left\{\frac{n^2}{r}\ln\frac{n}{r},\ n^{3/2}\sqrt{\ln n}\right\}\right).$$

For every fixed $\alpha \in (1/2, 1)$,

$$A_{\mathsf{BB}}(n, \lfloor \alpha n \rfloor) = \Theta_\alpha(n^2).$$

However, $A_{\mathsf{BB}}(n, t) = o(n^2)$ *whenever* $t = n/2 + o(n)$. *At maximum resilience,* $A_{\mathsf{BB}}(n, n-1) = \binom{n}{2} - 1$.

For a fixed fault fraction $\alpha \in (1/3, 1/2)$, both tasks have linear authentication complexity. Their costs separate at $n = 2t+1$: agreement requires a complete PKI, whereas designated-sender broadcast admits subquadratic cost. Broadcast requires superlinear authentication whenever $n - 2t = o(n)$ in the honest-majority setting. Table 1 summarizes the bounds.

Parameter range	Authentication complexity	Reference
Byzantine agreement		
$2t < n \leq 3t$	$A_{\mathsf{BA}} = \Theta\left(\min\left\{n^2, \frac{n^2}{r} \ln \frac{en}{r}\right\}\right)$	Main Theorem 2
$n = 2t + 1$	$A_{\mathsf{BA}} = n(n-1)$	Theorem 4.11
$n \leq 2t$	$A_{\mathsf{BA}} = +\infty$	Standard
Broadcast from a designated sender		
$\alpha \in (1/3, 1/2)$	$A_{\mathsf{BB}} = \Theta_\alpha(n)$	Main Theorem 3
$t = \lfloor n/2 \rfloor$	$\Omega\left(\frac{n \ln^2 n}{\ln \ln n}\right) \leq A_{\mathsf{BB}} \leq O\left(n^{3/2}\sqrt{\ln n}\right)$	Main Theorem 3
$\alpha \in (1/2, 1)$	$A_{\mathsf{BB}} = \Theta_\alpha(n^2)$	Main Theorem 3
$t = n - 1$	$A_{\mathsf{BB}} = \binom{n}{2} - 1$	Theorem 5.10

Table 1: The main authentication complexity bounds. Here $r = n - 2t$. The rows parameterized by α assume $t/n \to \alpha$ for a fixed α. The constants in the fixed-fraction bounds may depend on α. When $n > 3t$, no signature is needed for achieving broadcast or agreement.

1.3 Related Work

Other definitions of authentication graphs. Beimel and Franklin [BF99] study partially authenticated networks with two separate undirected graphs: communication edges describe available channels, and authentication edges describe pairs sharing secret authentication keys. They characterize reliable transmission between honest endpoints against Byzantine faults. Beimel and Malka [BM05] improve protocol efficiency and study the graph conditions for transmission. Their authentication allows arbitrarily small error against computationally unbounded adversaries. Barak, Canetti, Lindell, Pass, and Rabin [BCL+11] study secure computation without authentication and extend it to directed authentication graphs. Their edge specifies a communication link protected against forgery and replay; the adversary controls delivery.

Incomplete public-key authentication. Borcherding [Bor96] first considers levels of authentication over complete communication networks. His model of partial authentication restricts each public key to being known to all parties or to none. Independently, Lenzen, Loss, Shi, and Wagner [LLSW26] study s *registered* parties whose public keys are authenticated to every party. Their construction establishes feasibility in parameter regimes ruled out by the impossibility claim in [Bor96, Theorem 9][1]. For $n - s \geq 3$, they also show that $3t < n + 2s$ is necessary for broadcast from a registered sender in a model with round-by-round state leakage and a protected ideal signing functionality.

Detectable broadcast. Detectable broadcast allows all honest parties to abort together, but requires broadcast when all parties are honest. Fitzi, Gisin, Maurer, and von Rotz [FGMvR02] achieve this task with information-theoretic security for $t < n/2$ over pairwise secure channels. Fitzi, Gottesman, Hirt, Holenstein, and Smith [FGH+02] achieve it for every $t < n$ using signatures and pairwise authenticated channels, without initially authenticated public keys. Fitzi, Hirt, Holenstein, and Wullschleger [FHHW03] consider two fault bounds $0 \leq t \leq T < n$. With at most t faults, all honest parties must complete broadcast. With more than t but at most T faults, all honest parties must either complete broadcast or abort together. They show that these guarantees are achievable over pairwise secure channels if and only if $t = 0$ or $t + 2T < n$.

Minimal resources. The resources required for secure computation have been studied at several levels. Fitzi, Garay, Maurer, and Ostrovsky [FGMO05] study complete primitives of minimal arity for secure multiparty computation. Beimel and Malkin [BM04] take a quantitative approach to secure reductions, measuring the minimum number of calls to a fixed black-box primitive needed to compute a function securely. For a concrete example of such quantitative requirements, Goyal, Narayanan, and Prabhakaran [GNP22] determine the oblivious-transfer complexity of noisy coin-tossing up to constant factors in the semi-honest, perfectly secure two-party setting. Other setup resources can also enable broadcast beyond the unauthenticated resilience threshold. Narayanan, Prabhakaran, Sangwan, and Watanabe [NPSW23] characterize the three-party correlations from which unconditionally secure broadcast and pseudo-signatures can be realized.

Communication graphs. Fischer, Lynch, and Merritt [FLM85] use graph coverings and overlapping executions to prove consensus impossibility results. Dolev [Dol82] studies Byzantine agreement under communication connectivity constraints. Bansal, Gopal, Gupta, Srinathan, and Vasishta [BGG+11] study undirected communication graphs with a complete public-key infrastructure and revealed private keys of additional parties that follow the protocol. Vaidya and Tseng [VT26] characterize synchronous exact consensus and asynchronous approximate consensus in directed communication networks with globally verifiable signatures.

[1]The proof of that claim unjustifiably claims that nonsigners may remain silent because broadcast from a nonsigning sender is impossible. However, nonsigners can send messages signed by registered parties and assist broadcast from a signing sender, which has been used in the broadcast protocol construction of [LLSW26].

Partial broadcast and non-equivocation. A related line of work studies how local primitives can be combined to achieve global agreement. *Partial broadcast* provides broadcast guarantees within a specified subset of parties. *Non-equivocation* is a weaker primitive that prevents a faulty sender from making honest parties accept conflicting messages under the same message identifier. Fitzi and Maurer [FM00] derive global broadcast from three-party broadcast. Jaffe, Moscibroda, and Sen [JMS12] establish the optimal symmetric three-party channel count $\Theta(n^3/r^2)$ for $2t < n \leq 3t$, where $r = n - 2t$. Loss, Maurer, and Tschudi [LMT18] show that, among three parties with one Byzantine fault, broadcast channels for two parties do not suffice to implement broadcast for the third. Liu-Zhang, Maram, and Maurer [LZMM21] study incomplete minicast networks under general adversaries, and Khan and Vaidya [KV21] characterize consensus feasibility with local multicast channels. Clement, Junqueira, Kate, and Rodrigues [CJKR12] study non-equivocation and transferable authentication in crash-to-Byzantine compilation. Ben-David, Chan, and Shi [BDCS22] give a polynomial-overhead asynchronous compiler preserving security and privacy under a common reference string, PKI, and non-equivocation.

2 Technical Overview

We first prove the graph characterization and then construct agreement.

2.1 Agreement: a graph characterization and tight bounds

2.1.1 Necessary graph condition

The lower bound is straightforward: without agreement on the public keys of enough parties, broadcast or agreement is impossible. In the nontrivial range $2t < n \leq 3t$, suppose the three-set condition fails for A, B, C. Intuitively, no signer in C has a verifier in both A and B. Choose a broadcast sender $S \in C$.

Partition the remaining parties into Z_0, Z_1, Z_2 so that each of the following executions has at least $n - t$ honest parties. In Exec_0, the honest parties are $A \cup C \cup Z_0$, and the sender $S \in C$ has input 0. In Exec_1, the honest parties are $A \cup B \cup Z_1$, and the sender is faulty. In Exec_2, the honest parties are $B \cup C \cup Z_2$, and the sender has input 1.

Give each signer in C distinct keys in Exec_0 and Exec_2, while keeping each party outside C's key fixed. In Exec_1, the key of each signer $x \in C$ matches its Exec_0 key if it has a verifier in A, and its Exec_2 key if it has a verifier in B; choose either of these two keys if it has no verifier in either set.

The simulation in Lemma 4.2 then gives each party in A identical views in $\mathsf{Exec}_0, \mathsf{Exec}_1$ and each party in B identical views in $\mathsf{Exec}_1, \mathsf{Exec}_2$. Validity forces A to output 0 in Exec_0 and B to output 1 in Exec_2. Indistinguishability forces the honest parties in A and B to output different bits in Exec_1, violating consistency. Thus broadcast from S is impossible. Any BA protocol would yield broadcast by having S send its bit directly to every party and then running BA on the received bits, and letting S use its own input. Hence BA is impossible as well.

2.1.2 Construction

We follow the classical approach of constructing BA from weaker agreement protocols [BGP89, FM00]. Our construction first gives Π_{Confirm} with validity and weak consistency, then uses two Π_{Confirm} calls to obtain Π_{GBA} with validity and graded consistency, and finally runs a phase king protocol Π_{BA} with $t+1$ phases and distinct kings to achieve BA. Figure 1 gives the construction and the properties required at each step.

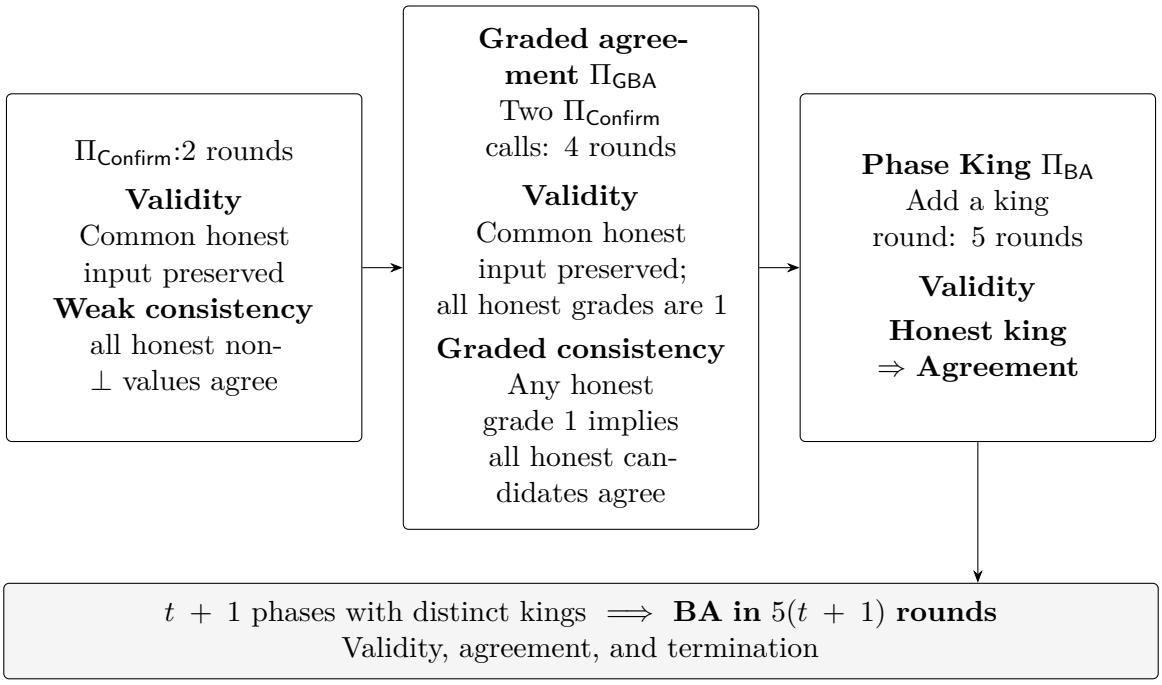

Figure 1: From Π_{Confirm} to Π_{GBA} and Π_{BA}.

Confirm. Validity requires that, if all honest inputs equal b, all honest outputs equal b. Weak consistency requires that any two honest non-$\perp$ outputs are equal; some honest parties may output $\perp$.

The core obstruction is that a faulty signer may send different public keys to different parties, and a forwarded opposite signature under a different key does not show that the signer is faulty, but only initial key tables let parties compare these keys. However, if signer x's direct key is different from the key for x in party j's reported table, at least one of x or j is faulty. Many conflicts may have the same faulty endpoint, so we cannot count a distinct faulty party for every conflict. In our Π_{Confirm} protocol, we resolve these conflicts using matching, where the edges have distinct faulty endpoints, and we take a maximum matching to consider as many disjoint conflicts as possible. A maximum matching of size f requires at least f distinct faulty parties. Each party accepts its bit only if there are at least $n-t$ parties sending the same input b_p to it even after subtracting f.

Specifically, in round one of Π_{Confirm}, each party sends everyone its designated key and signed

input. In round two, each party forwards all direct messages received and its initial key table. A receiver p keeps a signer x in Supp_p if x's valid direct message contains b_p and no forwarded message contains a valid signature for signer x on $1-b_p$ under the key in x's direct message to p. To compare keys, p forms a graph Γ_p on Supp_p: an edge $\{x, j\}$ is added whenever j's reported table contains an entry for x whose key disagrees with the key in x's direct message to the party p (where an honest verifier $j \in V_x$ always reports (x, vk_x)). At the end of round two of Π_{Confirm}, party p outputs

$$\begin{cases} b_p, & |\mathsf{Supp}_p| - \nu(\Gamma_p) \geq n - t, \\ \perp, & \text{otherwise,} \end{cases}$$

where b_p is its input and ν is the maximum matching size, and finding a maximum matching in Γ_p requires polynomial computation. If all honest inputs are equal, all honest signers remain in Supp_p for every honest p. Disjoint matching edges have distinct faulty endpoints, so $|\mathsf{Supp}_p| - \nu(\Gamma_p) \geq n - t$ and every honest party outputs the common input.

To show weak consistency, consider only conflicts between honest and faulty parties. The honest–faulty subgraph is bipartite. Every matching in this subgraph is also a matching in Γ_p, so Kőnig's theorem ([Kőn31], stated in Lemma 4.3) gives a vertex cover of size at most $\nu(\Gamma_p)$. Thus a non-$\perp$ output at p from Π_{Confirm} guarantees a quorum set $Q_p \subseteq \mathsf{Supp}_p$ of size at least $n - t$. This set may contain faulty parties, but if a faulty signer and one of its honest verifiers both remain in Q_p, the signer's direct message must use the designated key. Suppose honest receivers p_0, p_1 accept $0, 1$, and take the corresponding sets Q_{p_0}, Q_{p_1}. Honest signers send the same bit to both receivers, so $C = Q_{p_0} \cap Q_{p_1}$ contains only faulty parties. Write H for the honest set, and put $A = Q_{p_0} \cap H$ and $B = H \cap Q_{p_1}$. These three sets are pairwise disjoint. Since Q_{p_0}, Q_{p_1}, H each have size at least $n - t$, their intersections satisfy

$$n - 2t \leq |A|, |B|, |C| \leq t, \qquad |A| + |B| + |C| \geq 2n - 3t.$$

The three-set condition gives a faulty signer $x \in C$ with an honest verifier in each of A, B. Neither Q_{p_0} nor Q_{p_1} contains an honest–faulty conflict edge, so both direct messages from x must use x's designated key. However, the two direct messages contain opposite bits, and honest receivers p_0 and p_1 forward x's direct messages to one another. The output condition must exclude x from both support sets, a contradiction.

Graded agreement. We then build graded agreement that returns a candidate bit and a grade in $\{0, 1\}$. Validity requires that, if all honest inputs are equal, every honest party keeps this input and outputs with grade 1. Graded consistency requires that, if an honest party has grade 1, all honest candidates agree on the bit, while the other honest parties may have grade 0.

Our graded agreement Π_{GBA} uses two invocations of Π_{Confirm}. Each party starts with its input as candidate and grade 0.

- **First call.** Every party uses its current candidate as input to Π_{Confirm}. If the output is 0, it sets grade 1. Every party then uses the output as its candidate, replacing $\perp$ by 0.
- **Second call.** Every party again uses its current candidate as input to Π_{Confirm}. If the output is 1, it sets grade 1. Every party then uses the output as its candidate, replacing $\perp$ by 1.

Every party executes both calls and keeps grade 1 if it has grade 1 after the first call.

To see graded consistency, suppose an honest party sets grade 1 after the first call. Its output from Π_{Confirm} is then 0, so weak consistency of Π_{Confirm} implies that all honest non-$\perp$ outputs in that call are 0. Replacing $\perp$ by 0 makes all honest candidates equal 0, and the second call preserves this common value. If an honest party sets grade 1 after the second call, its output from Π_{Confirm} is 1. Weak consistency of Π_{Confirm} again implies that all honest non-$\perp$ outputs in that call are 1, so replacing $\perp$ by 1 makes all honest candidates equal 1. For validity, a common honest input is preserved by both calls: if it is 0, every honest party sets grade 1 after the first call; if it is 1, every honest party sets grade 1 after the second call.

Phase King. We then give a BA construction as a phase king protocol with $t+1$ phases and distinct kings, following the phase king approach of Berman, Garay, and Perry [BGP89]. Each phase preserves a common honest value and builds agreement whenever the king is honest. Each phase has four rounds of graded agreement (Lemma 4.5), followed by one round in which the king sends its candidate. In the king's round, parties with grade 1 keep their candidate bit, while the others update with the king's bit. A common honest input gives every honest party an output with the same bit as the common input and grade 1, so the phase preserves their common value even when the king is faulty. If the king is honest and an honest party has grade 1, all honest candidate bits agree, and the king sends this common value. If the king is honest and no honest party has grade 1, all honest parties update with the king's bit.

Since at most t parties are faulty, at least one of the $t+1$ distinct kings is honest. Its phase establishes agreement, and all subsequent phases preserve the common honest value. Running $t+1$ phases therefore gives BA in $5(t+1)$ rounds, with polynomial local computation and $O(n^3(t+1)\kappa)$ honest communication (Theorem 4.6), where κ bounds the size of a signature.

2.1.3 The optimal authentication cost

For $2t < n \leq 3t$, put $r = n - 2t$ and $k = \lceil r/2 \rceil$. The graph characterization gives two cut conditions (Lemma 4.8): a necessary condition for BA is an edge from every r-set to every disjoint r-set; a sufficient condition is an edge from every k-set to every disjoint r-set. We use these conditions to obtain asymptotically matching lower and upper bounds on the authentication cost.

From the necessary condition. Fix an r-set X. At most $r-1$ vertices outside X receive no edge from X: otherwise, choosing r such vertices as Y contradicts the necessary cut condition.

For $r = 1$, this requires all $n(n-1)$ directed edges. For $r \geq 2$, choose X uniformly among all r-sets. For each vertex v, excluding v and its $d^-(v)$ incoming neighbors leaves $\binom{n-d^-(v)-1}{r}$ choices of X. Counting the vertices that receive no edge from X and taking expectations gives

$$\sum_{v \in \mathcal{P}} \frac{\binom{n-d^-(v)-1}{r}}{\binom{n}{r}} \leq r - 1.$$

Using a convex lower bound on each term, applying Jensen's inequality gives a lower bound on the average indegree and hence on the total authentication cost.

From the sufficient condition. Assume the sufficient cut condition holds and suppose the three-set condition fails for A, B, C. Each set has size at least r, and every signer in C has no outgoing edge to at least one of A, B. Hence at least k signers in C have no outgoing edge to the same set. Choosing k of these signers and r vertices from that set contradicts the sufficient cut condition. We construct a graph such that each verifier independently chooses D uniform signers other than itself, with repetitions allowed, and authenticates their keys. For fixed disjoint sets of sizes k, r, the probability of no edge from the first to the second is at most $\exp(-Dkr/(n-1))$. There are $\exp(O(r\ln(en/r)))$ pairs, so a union bound allows $D = O((n/r)\ln(en/r))$. Discarding repeated choices gives at most $\min\{D, n-1\}$ incoming edges per party and $O(\min\{n^2, (n^2/r)\ln(en/r)\})$ edges (Lemma 4.10).

2.2 Byzantine broadcast with an honest majority

We optimize the authentication cost for broadcast with honest majority using our sparse BA construction Π_{BA} instead of fully unauthenticated BA in [LLSW26] and balance the authentication costs. Choose a set K_{reg} of s *registered parties* containing the designated sender S, where $1 \le s \le t$, and authenticate the designated key of every party in K_{reg} to all parties. On the rest of the parties $U_{\text{res}} = \mathcal{P} \setminus K_{\text{reg}}$, replace the unauthenticated BA subprotocol of [LLSW26] by our sparse BA from Section 2.1.3. For BA on U_{res} of $n-s$ parties and fault bound $t-s$, the required inequality improves from $n-s > 3(t-s)$ to $n-s > 2(t-s)$. Our protocol Π_{BB} first runs the gradecast protocol Π_{GC} of [LLSW26], whose outputs $(c_i, g_i) \in \{0,1\}^2$ satisfy:

1. If S is honest with input b, every honest party obtains $(b, 1)$.
2. If an honest party obtains $(c, 1)$, every honest party's value equals c.
3. If K_{reg} contains an honest party, every honest party obtains grade 1.

Every party $i \in U_{\text{res}}$, including those with grade 1, then runs Π_{BA} from Section 2.1.2 on input c_i. Denote party i's output from this BA call by y_i, or set $y_i = 0$ if party i has not output a bit by the public round bound of the BA protocol. The final output is

$$\begin{cases} c_i, & i \in K_{\text{reg}} \text{ or } g_i = 1, \\ y_i, & i \in U_{\text{res}} \text{ and } g_i = 0. \end{cases}$$

Similar to [LLSW26], an honest grade 0 means every party in K_{reg} is faulty. In that case all honest parties lie in U_{res} and the BA fault bound $t-s$ is valid. The common BA output agrees with any honest grade-1 value by BA validity. If no honest party has grade 0, every honest party uses the common gradecast value. Sender validity follows from gradecast validity. The construction gives

$$A_{\mathsf{BB}}(n,t) \le \min_{1 \le s \le t} \{s(n-1) + A_{\mathsf{BA}}(n-s, t-s)\}.$$

For fixed $\alpha \in (1/3, 1/2)$ and $t = \lfloor \alpha n \rfloor$, taking $s = 1$ gives $O_\alpha(n)$ authentication edges. For the lower bound throughout $2t < n \le 3t$, put $r = n - 2t$. With at most t edges, we could choose C as S plus $r-1$ receivers with no outgoing edges, then partition the remaining parties into t-sets A, B with all of S's remaining verifiers in B. No signer in C would have a verifier in A,

contradicting the three-execution argument above. Thus at least $t+1$ edges are necessary, giving $A_{\mathsf{BB}}(n, \lfloor \alpha n \rfloor) = \Theta_\alpha(n)$.

At $n = 2t+1$, BA on U_{res} satisfies $(n-s) - 2(t-s) = s+1$, giving cost $O(ns + (n^2/s)\ln(en/s))$ for broadcast. Balancing the terms at $s = \Theta(\sqrt{n \ln n})$ yields $O(n^{3/2}\sqrt{\ln n})$ authentication edges. This bound holds for every $n > 2t$ and $t \geq 1$ by taking $s = \min\{t, \lceil \sqrt{n \ln n} \rceil\}$.

2.3 The superlinear lower bound near the honest-majority threshold

Even when every receiver is a verifier of the sender, a Byzantine sender can sign both bits, and honest receivers must still agree. However, the argument of Section 2.1.1 no longer applies after simply authenticating the sender's key to all parties. We thus keep the sender's key fixed and consider authentication among receivers.

Write $R = \mathcal{P} \setminus \{S\}$ and $\widehat{V}_z = \{z\} \cup \{v \in \mathcal{P} : z \to v\}$, where $\widehat{V}_z$ includes z's knowledge of its own key. We give a necessary *receiver cut condition* as follows:

For every $W \subseteq \mathcal{P}$ containing S, and every pair of nonempty disjoint sets $A, B \subseteq \mathcal{P} \setminus W$ satisfying

$$n - 2t + |W| \leq |A|, |B| \leq t - |W|, \qquad |A| + |B| < n - |W|,$$

there is a receiver $z \notin W$ whose closed outneighborhood meets both A and B (Lemma 5.5).

Our proof adapts the impossibility argument for weak agreement of Fischer, Lynch, and Merritt [FLM85]. Suppose no such receiver exists, and assume a protocol Π with public round bound T_Π. We construct a ring of $2T_\Pi + 4$ layers, each containing one instance of each party outside W. Each instance remains in its layer in every round (Figure 3).

The receiver instances form overlapping groups, each containing at least $n - t$ instances of distinct parties. Some groups lie within one layer, while others contain instances from two adjacent layers. Set two sender instances, with inputs $0, 1$, at layers 0 and $T_\Pi + 2$, respectively. Each sender is connected only to one of these groups contained in its layer, and both senders use the same designated key. Channels connect instances only in the same or adjacent layers. Each group is fully connected, and each instance is connected to at most one instance of each other party. Since no such receiver exists, we can choose a distinct verification key for each receiver instance so that, within each group, all initial entries for a signer z contain the same key. If the group contains an instance of z, these entries contain the verification key of the instance of z in the group. Thus, when exactly the parties represented in a group are honest, the adversary can simulate all outside receiver instances.

For each group, we construct an execution of Π in which exactly the parties represented in that group are honest. Each honest party p has the same initial state and receives the same messages as the instance of p in that group. Consistency and termination in this execution force all instances in the group to output the same bit by round T_Π. The groups overlap successively in nonempty sets of receiver instances, so their common output bits must also be equal. Thus all receiver outputs must agree.

In the first run, both sender instances follow Π. In the second run, keep the same initial states and key tables, but make the sender in layer $T_\Pi + 2$ silent. The sender in layer 0 and its connected receiver group have the same views as honest parties in an execution. Since this sender has input 0, validity forces every receiver in that group to output 0 by round T_Π. Similarly, in a third run

with the sender in layer 0 silent, validity forces the group connected to the sender in layer $T_\Pi + 2$ to output 1.

We now compare each of these two runs with the first run. The only change is that one sender instance sends no messages. Its cyclic layer distance from the group connected to the other sender is $T_\Pi + 2$. Since messages cross at most one layer per round, induction shows that every receiver in that group has the same state through round T_Π in both runs.

Thus, in the first run, the group connected to the sender in layer 0 must output 0, while the group connected to the sender in layer $T_\Pi + 2$ must output 1. This contradicts the common receiver output in the first run.

Edge counting. For $2t < n \le 3t$, put $r = n - 2t > 0$ and $\Lambda = \ln(n/r)$. For any $W \ni S$ with $4|W| + 3r \le n$, put $R' = \mathcal{P} \setminus W$. Form a bipartite graph on two copies of R' with edge set

$$\bigcup_{z \in R'} (\widehat{V}_z \cap R')_{\mathrm{L}} \times (\widehat{V}_z \cap R')_{\mathrm{R}}.$$

Its diagonal edges force the receiver sets underlying any independent pair to be disjoint. Applying the receiver cut condition to subsets of size $r + |W|$ then excludes every k-by-k independent set with $k \ge r + |W|$.

Write $s_z = |\widehat{V}_z \cap R|$ and $\mu = \sum_{z \in R} s_z$. We adapt Radhakrishnan and Ta-Shma's argument [RTS00, Section 3.3] to this graph condition, counting only receiver edges.

For each suitable integer k, consider the interval $D_k = [n/(k\Lambda^2), n\Lambda^2/k)$. Receivers with s_z above this interval can be included in W: if μ is too small, there are few such receivers, so the receiver cut condition still applies outside W. Receivers below the interval cover at most $s_z^2 \le n s_z/(k\Lambda^2)$ pairs each. A random-deletion argument removes the edges supplied by receivers with $s_z \in D_k$, with the loss of vertices controlled by their total s_z. If this total were too small, the receivers below the interval would supply too few remaining edges: the expected numbers of vertex pairs and edges would contradict the counting consequence of the cut condition proved in Section 5.2.3. Thus each interval contributes $\Omega(n\Lambda)$ to μ.

Increasing k by a factor of at least Λ^4 makes the intervals D_k disjoint. The allowed range of k gives $\Theta(\Lambda/\ln\Lambda)$ such intervals. Since each receiver is counted at most once, summing their contributions and subtracting the $n - 1$ own keys gives $\Omega(n\Lambda^2/\ln\Lambda)$ receiver edges. For bounded Λ, the target bound on total cost is only $\Omega(n)$. The linear lower bound established above gives $A_{\mathsf{BB}}(n,t) \ge t + 1 \ge n/3$ throughout $2t < n \le 3t$, which suffices in this case. At $n = 2t + 1$, we have $\Lambda = \ln n$, giving $\Omega(n \ln^2 n/\ln\ln n)$ and completing the lower bound in Main Theorem 3.

2.4 Byzantine broadcast with a dishonest majority

Fixed dishonest-majority fractions. For every fixed $\alpha \in (1/2, 1)$ and $t = \lfloor \alpha n \rfloor$, we show that broadcast has $\Theta_\alpha(n^2)$ authentication complexity. For the lower bound, we count only edges between receivers. For sufficiently large n, put $d = 2t - n + 1$. Two receivers are *nonadjacent* if neither directed edge between them exists.

The receiver cut condition (Lemma 5.5) implies that every nonadjacent receiver pair a, b has at least d receivers z with $z \to a$ and $z \to b$. Otherwise, choose $W \subseteq \mathcal{P} \setminus \{a, b\}$ of size d containing S

and every receiver z with $z \to a$ and $z \to b$. Apply the receiver cut condition with $A = \{a\}$ and $B = \{b\}$. Since a, b are nonadjacent, the receiver $z \notin W$ given by this condition is neither a nor b. Thus $z \to a$ and $z \to b$, contradicting the choice of W.

We now count receiver edges. If every receiver has at least d incoming edges from other receivers, summing gives at least $d(n-1)$ receiver edges. Otherwise, choose a receiver v with at most $d-1$ such incoming edges. If some receiver u is nonadjacent to v, at least d distinct receivers z satisfy $z \to u$ and $z \to v$, giving v at least d incoming receiver edges, contradicting the choice of v with at most $d-1$ incoming receiver edges. Thus v is adjacent to every other receiver: for every $u \neq v$, at least one of $u \to v$ and $v \to u$ exists. Deleting this receiver removes at least $n-2$ receiver edges. Each remaining nonadjacent pair loses at most one receiver pointing to both parties, so it still has at least $d-1$ receivers pointing to both. Induction on d gives at least

$$d(n-1) - \binom{d+1}{2} = \Omega_\alpha(n^2)$$

authentication edges between receivers (Lemma 5.9). Any protocol with complete PKI gives the matching $O(n^2)$ upper bound. The construction in Section 2.2 still applies when $s > 2t - n$. For $n \leq 2t$, taking $s = \min\{t, 2t - n + \lceil\sqrt{n \ln n}\rceil\}$ gives $O(n(2t-n) + n^{3/2}\sqrt{\ln n})$ edges. This is $o(n^2)$ when $t = n/2 + o(n)$. Section 5.3 gives the formal proofs.

Maximum resilience. At $t = n - 1$, we show that the exact authentication cost is $\binom{n}{2} - 1$. For the upper bound, order the parties as $S = v_0, v_1, \ldots, v_{n-1}$. The initial authentication contains every edge $v_i \to v_j$ with $i < j$, except $v_{n-2} \to v_{n-1}$. This gives $\binom{n}{2} - 1$ authentication edges, Figure 2 gives an example.

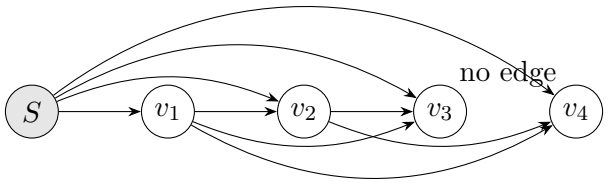

Figure 2: Optimal maximum-resilience setup: all forward edges from an order with S first except the last pair. This five-party graph has only 9 edges; $x \to y$ means that y is a verifier of x.

We induct on n for arbitrary message domains. Two-party broadcast is trivial. For $n \geq 3$, put $U_{\text{tail}} = \{v_2, \ldots, v_{n-1}\}$. Removing v_1 or S leaves the setup required for broadcast on $n-1$ parties, with sender S or v_1, respectively. We use two broadcast calls, each with $n-1$ parties. The input to each broadcast is either $\perp$ or a signed value of S. First, S broadcasts S's input signature on $\{S\} \cup U_{\text{tail}}$. After this call, S sends S's input signature directly to v_1, and parties in U_{tail} send the first call's output to v_1. Then v_1 chooses a valid signature from the first party in the order $S, v_2, \ldots, v_{n-1}$ that sent one, or $\perp$ if none exists, and broadcasts the chosen signature or $\perp$ on $\{v_1\} \cup U_{\text{tail}}$. Parties in U_{tail} use the second call's output if it is a valid signed value of S, and otherwise keep the first call's output; v_1 uses v_1's input to the second call.

Consistency of both calls and the common output rule give all honest parties in U_{tail} the same final output. If v_1 is honest, validity of the second call gives every honest party in U_{tail} v_1's input to the second call. If an honest v_1 chooses $\perp$, forwarding implies that all honest parties in U_{tail} also obtained $\perp$ from the first call. Thus all honest receivers agree. If S is honest, the first call and S's direct message give every honest receiver S's input signature. Every valid signature is on S's input, so the output rule preserves sender validity even when v_1 is faulty.

Lower bound. For the matching lower bound, suppose S is not authenticated to some receiver v. Use the three-execution construction in Lemma 4.2 with $A = \{v\}$, $B = \mathcal{P} \setminus \{S, v\}$, and $C = \{S\}$. The missing sender key at v allows different sender keys on the two sides: the faulty-sender execution preserves v's view from input 0 and the other receivers' views from input 1, forcing disagreement. Thus all $n-1$ sender edges are necessary. For two nonadjacent receivers a, b and each other receiver z, apply Lemma 5.5 with $W = \mathcal{P} \setminus \{a, b, z\}$, $A = \{a\}$, and $B = \{b\}$. Since the only receivers outside W are a, b, z, the receiver cut condition forces $z \to a$ and $z \to b$. Every nonadjacent receiver pair thus has at least $n-3$ receivers pointing to both parties. Applying Lemma 5.9 with $d = n-3$ gives at least

$$(n-3)(n-1) - \binom{n-2}{2} = \binom{n-1}{2} - 1$$

authentication edges between receivers. Adding the $n-1$ sender edges gives

$$(n-1) + \binom{n-1}{2} - 1 = \binom{n}{2} - 1,$$

matching the construction. The full protocol and proof are in Section 5.4.

3 Preliminaries

3.1 The model and tasks

We consider a set $\mathcal{P}$ of $n \geq 3$ parties, a public directed graph $G = (\mathcal{P}, E)$ without self-loops, and a fault bound $0 \leq t < n$. For subprotocols involving fewer than three parties, we use the trivial protocols for broadcast and fault-free agreement, both requiring no initial authentication. For Byzantine broadcast, a designated sender $S \in \mathcal{P}$ has an input bit $b \in \{0, 1\}$. For Byzantine agreement, each party $i \in \mathcal{P}$ has an input bit $b_i \in \{0, 1\}$. Parties communicate over a complete network of reliable channels identifying the immediate sender. In each synchronous round, honest parties send messages determined by their states at its start, and these messages are delivered by its end. The adversary is *rushing*: it may observe all honest messages before choosing corrupted parties' messages for the same round.

Each party i has a distinct designated verification key vk_i and its corresponding signing capability. For distinct parties i, j, we call j a *verifier* of i if vk_i is *initially authenticated* to j. Equivalently, $i \to j$ means that j is a verifier of i. Party j knows its own key for free and receives the initial key table

$$\mathsf{KT}_j = \{(i, \mathsf{vk}_i) : i \in K_j\}, \qquad K_j = \{i \in \mathcal{P} : j \in V_i\}.$$

These are the only initial authentications of parties' public keys. In the *local-key-table* setting, each party receives its own table but does not know G, and the protocol may depend on n, t, S but not on G. Our BA characterization remains valid in this setting (Theorem 4.1 and Corollary 4.7).

Idealized signatures. We use an idealized signature model following the approach of Dolev and Yao [DY81]. In our model, each verification key vk has a non-transferable signing capability $\mathsf{cap}_{\mathsf{vk}}$. Distinct pairs (vk, m) have distinct signatures $\sigma_{\mathsf{vk},m}$, with

$$\mathsf{Sign}(\mathsf{cap}_{\mathsf{vk}}, m) = \sigma_{\mathsf{vk},m}, \qquad \mathsf{Verify}(\mathsf{vk}, m, \sigma) = \mathbf{1}[\sigma = \sigma_{\mathsf{vk},m}].$$

Signing requires $\mathsf{cap}_{\mathsf{vk}}$ and a message m; invalid verification inputs are rejected. A signature can be obtained only by using the corresponding signing capability or by receiving or observing a message containing it. Verification does not show which party a key belongs to unless the signer is initially authenticated to its verifiers. Each protocol call has distinct identifiers. The signed data include the protocol and session identifiers, designated sender, message type, phase, signer, and G if G is public. For communication bounds, let κ bound the size of a signature. Verification keys and all protocol, party, session, call, phase, round, and message identifiers have size $O(\kappa)$. In particular, we set $\ln n = O(\kappa)$.

Adversary and correctness. The adversary is *static*: before the execution, it chooses a set $F \subseteq \mathcal{P}$ with $|F| \leq t$ and gains full control of these parties' states, signing capabilities, and behavior. It knows all designated verification keys and may create fresh keys with their own signing capabilities. Write $H = \mathcal{P} \setminus F$ for the set of honest parties. Protocols are deterministic and must be correct with *zero error* in the idealized signature model. For each fixed G, the same protocol must be correct for every input, every assignment of pairwise distinct designated keys with initially authenticated keys specified by G, every fault set of size at most t, and arbitrary adversarial behavior.

Definition 3.1 (Byzantine broadcast)**.** Write $\mathsf{BB}(G, S, t)$ if there exist a deterministic protocol Π and a public finite round bound T_Π such that every admissible execution with $|F| \leq t$ satisfies:

- **Validity.** If S is honest with input b, every honest output equals b.
- **Consistency.** All honest outputs agree.
- **Termination.** Every honest party outputs a bit by round T_Π.

Definition 3.2 (Byzantine agreement)**.** Each party $i \in \mathcal{P}$ has an input bit b_i. A deterministic protocol Π solves Byzantine agreement if there is a public finite round bound T_Π such that every admissible execution with $|F| \leq t$ satisfies:

- **Validity.** If all honest inputs equal b, every honest output equals b.
- **Agreement.** All honest outputs agree.
- **Termination.** Every honest party outputs a bit by round T_Π.

We write $V_x = \{y : x \to y\}$ for the set of verifiers of x, with outdegree $d^+_G(x) = |V_x|$ and indegree $d^-_G(x) = |K_x|$, omitting the graph subscript on degrees when the graph is clear. We also write $\widehat{V}_x = \{x\} \cup V_x$ for the verifier set together with the signer itself.

3.2 The authentication complexity

Definition 3.3 (Authentication complexity)**.** For a task $\mathcal{T}$ in this model, we define its *authentication complexity* to be the minimum size of authenticated bindings, measured by the total number of initially authenticated public keys given to parties, over all setups and protocols solving that task with fault bound t:

$$A_{\mathcal{T}}(n,t) = \min_{G,\Pi} \sum_{v\in\mathcal{P}} |K_v| = \min_{G,\Pi} |E(G)|.$$

The minimum is $+\infty$ if no such protocol exists. Denote the complexities of broadcast from a designated sender and Byzantine agreement by $A_{\mathsf{BB}}(n,t)$ and $A_{\mathsf{BA}}(n,t)$, respectively.

The cryptographic setup consists only of the designated signing capabilities and initial key tables. Communication and local computation may be arbitrary but finite, and protocols have a public finite round bound.

We also minimize the maximum number of initially authenticated public keys held by any one party. Define

$$A^{\max}_{\mathcal{T}}(n,t) = \min_{G,\Pi} \max_{v\in\mathcal{P}} |K_v|,$$

with the same allowed setups and protocols and the same convention for impossibility.

4 Authentication Complexity of Agreement

We prove Main Theorems 1 and 2, following the necessary condition, construction, and edge bounds of Section 2.1.

4.1 The three-set condition and its necessity

Theorem 4.1 (BA characterization)**.** *Let $n \geq 3$ and $0 \leq t < n$. The following are equivalent:*

(i) Byzantine agreement is possible on G.

(ii) $n > 2t$, and for every three pairwise disjoint sets $A, B, C \subseteq \mathcal{P}$ satisfying

$$n - 2t \leq |A|, |B|, |C| \leq t, \qquad |A| + |B| + |C| \geq 2n - 3t,$$

there is a signer $x \in C$ such that

$$V_x \cap A \neq \varnothing, \qquad V_x \cap B \neq \varnothing.$$

For each fixed n, t, a single deterministic BA protocol works on every graph satisfying the condition, given only each party's own initial key table. For $n = 2t + 1$, BA is possible exactly when G is complete directed. For $n \leq 2t$, BA is impossible.

4.1.1 Necessity: three indistinguishable executions

Lemma 4.2 (Broadcast obstruction)**.** *Let $n \geq 3$ and $0 \leq t < n$. Suppose nonempty, pairwise disjoint sets $A, B, C \subseteq \mathcal{P}$ satisfy*

$$n - 2t \leq |A|, |B|, |C| \leq t, \qquad |A| + |B| + |C| \geq 2n - 3t.$$

If $S \in C$ and

$$\forall x \in C: \quad V_x \cap A = \varnothing \quad \text{or} \quad V_x \cap B = \varnothing, \tag{1}$$

then $\mathsf{BB}(G, S, t)$ is impossible, even if the protocol is required only to terminate eventually.

Proof. Partition the remaining parties into Z_0, Z_1, Z_2. The honest parties in executions $\mathsf{Exec}_0, \mathsf{Exec}_1, \mathsf{Exec}_2$ are respectively,

$$A \cup C \cup Z_0, \qquad A \cup B \cup Z_1, \qquad B \cup C \cup Z_2,$$

each of size at least $n - t$. Set S to be honest in $\mathsf{Exec}_0, \mathsf{Exec}_2$ and faulty in Exec_1. We give A identical local views in $\mathsf{Exec}_0, \mathsf{Exec}_1$ and B identical local views in $\mathsf{Exec}_1, \mathsf{Exec}_2$.

For each $x \in C$, use two instances x^0, x^2 of party x. Both run x's protocol, with separate local states and distinct keys $\mathsf{vk}_x^0, \mathsf{vk}_x^2$, which are x's designated keys in $\mathsf{Exec}_0, \mathsf{Exec}_2$. The two instances of S have inputs $0, 1$. Each party outside C has one key and one instance. In Exec_1, choose x's designated key as vk_x^0 if $V_x \cap A \neq \varnothing$ and vk_x^2 if $V_x \cap B \neq \varnothing$; if $V_x \cap A = V_x \cap B = \varnothing$, choose either vk_x^0 or vk_x^2. By (1), no $x \in C$ has a verifier in both A and B. The instances of parties in A use their Exec_0 key tables, which are correct in Exec_1; those in B use their Exec_2 tables, which are also correct in Exec_1. For $i \in \{0, 1, 2\}$, the instance of each party in Z_i uses its Exec_i key table. For $i \in \{0, 2\}$ and $x \in C$, instance x^i uses x's Exec_i key table.

Connect two instances of different parties whenever they are honest together in some Exec_i. In each round, connected instances exchange the messages prescribed by the protocol, all other channels are silent. Each instance is connected to at most one instance of each other party, so its view is well defined round by round.

To realize Exec_i, each honest party outside C runs its instance; for $i \in \{0, 2\}$, each honest $x \in C$ runs x^i. The adversary simulates all other instances. The signing capability of every simulated instance corresponds either to a corrupted party's designated key or to an additional key generated by the adversary. Every message from an instance run by an honest party in Exec_i to a simulated instance is sent to a party corrupted in Exec_i. Thus the adversary receives any honest signature before the simulation uses it, including signatures contained in other signed messages.

Induction on rounds gives every honest party in Exec_i exactly the view of the instance it runs, with the same keys, signatures, and messages.

Validity forces A to output 0 in Exec_0 and B to output 1 in Exec_2. The identical local views for A in Exec_0 and Exec_1, together with the identical local views for B in Exec_1 and Exec_2 force both outputs in Exec_1, violating agreement. Eventual termination suffices because the two honest-sender executions output at finite times, without a known round bound. □

For necessity in Theorem 4.1, only the $n > 2t$ case is nontrivial. Suppose the three-set condition fails for A, B, C. Choose $S \in C$, from Lemma 4.2 and the BA-to-broadcast reduction, there exists no BA protocol.

4.2 Construction

Lemma 4.3 (Kőnig [Kőn31])**.** *In every bipartite graph, the minimum vertex cover size equals the maximum matching size.*

We then construct a two-round protocol Π_{Confirm} (Protocol 1) using only local key tables. Each party outputs its input bit or $\perp$.

Lemma 4.4. *Let $n \geq 3$ and $n > 2t$, and suppose G satisfies the three-set condition of Theorem 4.1. Then Π_{Confirm} has the following properties.*

(i) ***Validity.*** *If all honest inputs equal b, all honest outputs equal b.*

(ii) ***Weak consistency.*** *Any two honest non-$\perp$ outputs are equal.*

For each receiver p, let Supp_p contain the signers whose valid direct messages agree with p's input and for which no signature under the same public key on opposite bits is forwarded. On this set, an edge $\{x, j\}$ of Γ_p records a disagreement between x's direct key and the key for x in j's reported table.

Protocol 1. Π_{Confirm}

Input. A bit b_p at every party p.

Output. At party p, either its input b_p or $\perp$ after 2 rounds.

Round 1. Direct messages. Each party x sends every party $(x, \mathsf{vk}_x, b_x, \sigma_x)$, where σ_x signs (x, vk_x, b_x). Party p records the message received directly from x as $m_{x,p}$ if it has the prescribed format, its signer field is x, its bit is in $\{0, 1\}$, and its signature is valid; otherwise p records $\perp$. It uses its own message for $m_{p,p}$. For a non-$\perp$ record, write $\widehat{\mathsf{vk}}_{x,p}$ for its contained key.

Round 2. Forwarding. Each party j sends every party the entire vector $(m_{x,j} : x \in \mathcal{P})$ received in the last round and its initial key table KT_j. Party j uses its own vector and table locally.

Local computation. At the end of round two, each party p applies the following rule.

1. **Support and conflicts computation.** Party p puts x in Supp_p if $m_{x,p}$ contains bit b_p and no second-round vector contains a valid message from x on bit $1 - b_p$ under the same key $\widehat{\mathsf{vk}}_{x,p}$. This test uses vectors from all parties. On vertex set Supp_p, party p then locally forms an undirected graph Γ_p: for each table entry $(x, \widehat{\mathsf{vk}})$ received from j, with distinct $x, j \in \mathsf{Supp}_p$, add $\{x, j\}$ if $\widehat{\mathsf{vk}} \neq \widehat{\mathsf{vk}}_{x,p}$.
2. **Output.** Output
$$\begin{cases} b_p, & |\mathsf{Supp}_p| - \nu(\Gamma_p) \geq n - t, \\ \perp, & \text{otherwise}, \end{cases}$$
where ν is the maximum matching size.

Protocol 1. Π_{Confirm} **(continued)**

Message format. Each first-round message has size $O(\kappa)$. Each second-round message has size $O(n\kappa)$, with one vector position per signer and at most one table entry per $x \neq j$. Missing first-round records are $\perp$. Ignore invalid second-round messages and forwarded records; a forwarded record's signer must match its vector position. Reported tables are claims of their senders.

Proof of Lemma 4.4. Let F be the fault set and $H = \mathcal{P} \setminus F$.

Validity. For every honest p, every edge of Γ_p has a faulty endpoint: an honest x sends its designated key, and an honest j reports that same key whenever its table contains an entry for x.

If all honest inputs equal b, then $H \subseteq \mathsf{Supp}_p$ at every honest p. An honest x sends a valid message on b and never signs $1-b$ in this call. Each matching edge uses a distinct faulty endpoint, giving

$$\nu(\Gamma_p) \leq |\mathsf{Supp}_p \cap F|, \qquad |\mathsf{Supp}_p| - \nu(\Gamma_p) \geq |H| \geq n - t.$$

Weak consistency. Suppose honest p_0, p_1 output $0, 1$, respectively. For each i, the honest–faulty edges of Γ_{p_i} form a bipartite graph. By Lemma 4.3, it has a vertex cover of size at most $\nu(\Gamma_{p_i})$. Deleting this cover from Supp_{p_i} gives a set Q_{p_i} with $|Q_{p_i}| \geq n - t$ and no honest–faulty edge inside it. Honest parties send the same bit to both receivers, so $Q_{p_0} \cap Q_{p_1} \subseteq F$. Put $A = Q_{p_0} \cap H$, $B = H \cap Q_{p_1}$, and $C = Q_{p_0} \cap Q_{p_1}$. These sets are pairwise disjoint. Since $|Q_{p_0}|, |H|, |Q_{p_1}| \geq n - t$, each of A, B, C has size at least $n - 2t$. Moreover, $A \subseteq \mathcal{P} \setminus Q_{p_1}$, $B \subseteq \mathcal{P} \setminus Q_{p_0}$, and $C \subseteq \mathcal{P} \setminus H$, so each has size at most t. Moreover,

$$|A| + |B| + |C| = |Q_{p_0}| + |H| + |Q_{p_1}| - |Q_{p_0} \cup H \cup Q_{p_1}| \geq 2n - 3t.$$

The three-set condition gives a faulty signer $x \in C$ and honest verifiers $a_0 \in A \cap V_x$, $a_1 \in B \cap V_x$. Since $x, a_i \in Q_{p_i}$ have no honest–faulty conflict, x's direct key must match vk_x in a_i's reported table. Thus x supports opposite bits at p_0, p_1 under the same designated key. Receivers p_0 and p_1 forward x's direct messages to one another. Each therefore receives a valid signature on the opposite bit under vk_x and excludes x from its support set, contradicting $x \in C$. □

We then give graded agreement Π_{GBA} using two calls to Π_{Confirm}.

Protocol 2. Π_{GBA}

Input. A current bit $x_p \in \{0,1\}$ at each party p. Initialize $c_p = x_p$ and $g_p = 0$.

Output. A candidate bit c_p and a grade $g_p \in \{0,1\}$ at each party p after 4 rounds.

1. **First call (rounds $1,2$).** Perform the following updates in order.
   (a) Set $c_p \leftarrow \Pi_{\mathsf{Confirm}}(c_p)$, with all parties calling Π_{Confirm} jointly on their current candidate bits.
   (b) If $c_p = 0$, set $g_p = 1$.
   (c) If $c_p = \perp$, set $c_p = 0$.
2. **Second call (rounds $3,4$).** Perform the following updates in order.
   (a) Set $c_p \leftarrow \Pi_{\mathsf{Confirm}}(c_p)$, with all parties calling Π_{Confirm} jointly on their current candidate bits.
   (b) If $c_p = 1$, set $g_p = 1$.
   (c) If $c_p = \perp$, set $c_p = 1$.

   Every party executes both calls, even if its grade is already 1; the grade is not reset between them.
3. Output (c_p, g_p).

Lemma 4.5 (Graded agreement)**.** *Let $n \geq 3$ and $n > 2t$, and suppose G satisfies the three-set condition of Theorem 4.1. The 4-round protocol Π_{GBA} in Protocol 2 has the following properties.*

(i) ***Validity.*** *If all honest inputs equal b, all honest outputs are $(b,1)$.*

(ii) ***Graded consistency.*** *If any honest party outputs $(b,1)$, every honest party outputs (b,g) with $g \in \{0,1\}$.*

Proof. If an honest party sets grade 1 in the first call, its output from Π_{Confirm} is 0. Every honest non-$\perp$ output in that call is 0 by Lemma 4.4(ii). Replacing $\perp$ by 0 makes all honest candidate bits equal 0, and the second call preserves this value by Lemma 4.4(i). If an honest party sets grade 1 in the second call, its output from Π_{Confirm} is 1. Every honest non-$\perp$ output in that call is 1, and replacing $\perp$ by 1 makes all honest candidate bits equal 1. If all honest inputs are 0, both calls preserve 0, and the first call sets every honest grade to 1. If all honest inputs are 1, both calls preserve 1, and the second call sets every honest grade to 1. □

We finally construct Π_{BA} using the phase king approach of Berman, Garay, and Perry [BGP89].

Protocol 3. Π_{BA}

Parameters. The $t+1$ distinct parties $\mathsf{king}_1, \ldots, \mathsf{king}_{t+1}$ in a fixed order.

Input. An initial bit b_p at each party p. Party p initializes its current bit to $x_p = b_p$.

Output. A decision bit x_p at each party p.

1. For each $j = 1, \ldots, t+1$, run the following phase.
   (a) **Graded agreement.** Run Π_{GBA} on the current bits, obtaining (c_p, g_p).
   (b) **King round.** Party king_j sends its candidate bit to every party in one round. At the end of the round, if $g_p = 1$, party p sets $x_p = c_p$. Otherwise it sets x_p to the bit received from king_j, using 0 for an invalid message. Party king_j uses its own candidate bit.
2. Output x_p, the final current bit.

Theorem 4.6 (BA from local tables)**.** *Let $n \geq 3$ and $n > 2t$, and suppose G satisfies the three-set condition of Theorem 4.1. There is a deterministic BA protocol Π_{BA} with $5(t+1)$ rounds and polynomial local computation. Its code is independent of G and uses only each party's initial key table. The total communication sent by honest parties is $O(n^3(t+1)\kappa)$.*

Proof. We show two properties of Π_{BA}:

- If all honest current bits equal b, Lemma 4.5 gives candidate bit b and grade 1 to every honest party, so the phase preserves b regardless of its king.
- If the king is honest, its phase ends with agreement. If an honest party outputs $(b, 1)$ from Π_{GBA}, graded consistency (Lemma 4.5(ii)) gives candidate bit b to every honest party, including the king. In the king round, honest parties with grade 1 keep b, while those with grade 0 adopt the honest king's candidate bit, also b. Otherwise, every honest party has grade 0, and all adopt the honest king's candidate bit.

At least one of the $t+1$ distinct kings is honest. Its phase establishes agreement, and all subsequent phases preserve it. Every phase also preserves a common honest input, giving validity. The fixed schedule gives termination in $5(t+1)$ rounds. Each call to Π_{Confirm} sends $O(n^2\kappa)$ bits in its first round. In its second round, each honest party sends $O(n\kappa)$ bits to every party, for $O(n^3\kappa)$ bits in total. There are two calls per phase, followed by one king round using $O(n\kappa)$ bits. This gives $O(n^3(t+1)\kappa)$ honest communication. Checking signatures, constructing Γ_p, and finding a maximum matching require polynomial computation. □

Corollary 4.7. *For fixed n, t, S with $n > 2t$, one deterministic protocol, independent of G, solves $\mathsf{BB}(G, S, t)$ using only local key tables whenever G satisfies the three-set condition of Theorem 4.1, in particular whenever $n > 3t$. It uses $1 + 5(t+1)$ rounds, polynomial local computation, and $O(n^3(t+1)\kappa)$ honest communication.*

Proof. The sender first sends its input directly to every party. Each party uses the received bit as its input to Π_{BA} from Theorem 4.6, using 0 for an invalid message; the sender uses its own input.

BA gives agreement even when the sender is faulty. When the sender is honest, all honest BA inputs equal its input, so BA validity gives broadcast validity. □

4.3 The optimal total and balanced authentication cost

For $2t < n \le 3t$, put $r = n - 2t$. The characterization of Theorem 4.1 reduces authentication complexity to counting edges in graphs satisfying the three-set condition. We use two cut conditions.

Lemma 4.8 (Cut conditions)**.** *Every feasible BA graph has an edge from every r-set to every disjoint r-set. Conversely, an edge from every $\lceil r/2 \rceil$-set to every disjoint r-set suffices for BA.*

Proof. For necessity, fix disjoint r-sets X, Y and choose a disjoint t-set B. Apply the three-set condition with $C = X$ and $A = Y$: the size bounds hold and $|A| + |B| + |C| = 2r + t = 2n - 3t$. Hence there is an edge from X to Y.

For sufficiency, assume that every $\lceil r/2 \rceil$-set has an edge to every disjoint r-set. Suppose, for a contradiction, that the three-set condition fails for some A, B, C. For every signer $x \in C$, either $V_x \cap A = \varnothing$ or $V_x \cap B = \varnothing$. Hence one of A, B receives no outgoing edge from at least $\lceil |C|/2 \rceil \ge \lceil r/2 \rceil$ signers in C. Choosing $\lceil r/2 \rceil$ of these signers and r parties from that same set contradicts the assumed cut condition. □

Lemma 4.9. *Let G be a loopless digraph on n vertices, and let $1 \le r \le n/3$ be an integer. Suppose every ordered pair of disjoint r-sets X, Y has an edge from X to Y, then we have*

$$|E(G)| = \Omega\left(\min\left\{n^2, \frac{n^2}{r}\ln\frac{en}{r}\right\}\right).$$

For $r = 1$, take $X = \{u\}$ and $Y = \{v\}$ for any distinct $u, v \in \mathcal{P}$. The cut condition (Lemma 4.8) requires $u \to v$ and G must be complete and $|E(G)| = n(n-1)$. For $r \ge 2$, the following bound also holds:

$$\frac{|E(G)|}{n} + 1 \ge (n - r + 1)\left[1 - \left(\frac{r-1}{n}\right)^{1/r}\right]. \tag{2}$$

Proof. Assume $r \ge 2$. For an r-set X, let $\mathrm{Miss}(X)$ be the set of parties outside X that receive no authentication edge from X:

$$\mathrm{Miss}(X) = \mathcal{P} \setminus \left(X \cup \bigcup_{x \in X} V_x\right).$$

The cut condition is exactly $|\mathrm{Miss}(X)| \le r - 1$. Choose X uniformly among the r-sets, and write $\bar{d} = |E(G)|/n$, and $(x)_+ = \max\{x, 0\}$. For each v, excluding v and its $d^-(v)$ incoming neighbors leaves $\binom{n-d^-(v)-1}{r}$ choices of X with $v \in \mathrm{Miss}(X)$. Hence

$$r - 1 \ge \mathbb{E}|\mathrm{Miss}(X)| = \sum_v \frac{\binom{n-d^-(v)-1}{r}}{\binom{n}{r}} \ge \sum_v \left(1 - \frac{d^-(v)+1}{n-r+1}\right)_+^r \ge n\left(1 - \frac{\bar{d}+1}{n-r+1}\right)_+^r.$$

The middle inequality uses $n - j \ge n - r + 1$ for $0 \le j < r$. The last inequality is Jensen's inequality for the convex function $d \mapsto (1 - (d+1)/(n-r+1))_+^r$. Rearranging gives (2).

Since $n/r \geq 3$ and $1 - e^{-x} \geq (1 - e^{-1}) \min\{1, x\}$ for $x \geq 0$, that bound implies

$$\bar{d} + 1 = \Omega\left(\min\left\{n, \frac{n}{r} \ln \frac{en}{r}\right\}\right).$$

Also, the cut condition gives $\sum_{x \in X} d^+(x) \geq n - 2r + 1 \geq r$ for every r-set. Taking expectations over X gives

$$\mathbb{E}_X\left[\sum_{x \in X} d^+(x)\right] = \frac{r}{n} \sum_{v \in \mathcal{P}} d^+(v) = r\bar{d} \geq r.$$

Hence $\bar{d} \geq 1$, so $\bar{d} \geq (\bar{d} + 1)/2$. Using the bound on $\bar{d} + 1$ above, we obtain

$$|E(G)| = n\bar{d} \geq \frac{n}{2}(\bar{d} + 1) = \Omega\left(\min\left\{n^2, \frac{n^2}{r} \ln \frac{en}{r}\right\}\right),$$

which proves the claim. □

Lemma 4.10. *Let $2 \leq r \leq N/3$ be an integer and put $k = \lceil r/2 \rceil$. There is an N-vertex loopless digraph with an edge from every k-set to every disjoint r-set, using*

$$O\left(\min\left\{N^2, \frac{N^2}{r} \ln \frac{eN}{r}\right\}\right)$$

edges and maximum indegree $O(\min\{N, (N/r)\ln(eN/r)\})$.

Proof. Each verifier independently chooses $D = \lceil C_0(N/r)\ln(eN/r)\rceil$ uniform signers from the other $N - 1$ parties, with repetitions allowed, and receives their designated keys. For fixed disjoint sets X, Y of sizes k, r, the probability that all Dr choices made by verifiers in Y lie outside X is

$$\left(1 - \frac{k}{N-1}\right)^{Dr} \leq e^{-Dkr/(N-1)}.$$

There are $\binom{N}{k}\binom{N-k}{r} \leq \binom{N}{r}^2 \leq \exp(2r\ln(eN/r))$ pairs. By a union bound, the probability that at least one such pair has no edge from X to Y is at most

$$\binom{N}{k}\binom{N-k}{r} e^{-Dkr/(N-1)} \leq \exp((2 - C_0/2)r\ln(eN/r)) < 1$$

for $C_0 > 4$. Therefore a choice exists that satisfies the cut condition for every pair.

Discarding repeated choices gives maximum indegree at most $\min\{D, N-1\}$ and at most $N\min\{D, N-1\}$ edges. □

Theorem 4.11. *For $2t < n \leq 3t$ and $r = n - 2t$,*

$$A_{\mathsf{BA}}(n,t) = \Theta\left(\min\left\{n^2, \frac{n^2}{r}\ln\frac{en}{r}\right\}\right),$$
$$A^{\max}_{\mathsf{BA}}(n,t) = \Theta\left(\min\left\{n, \frac{n}{r}\ln\frac{en}{r}\right\}\right).$$

For $n = 2t + 1$, the exact values are $A_{\mathsf{BA}} = n(n-1)$ and $A^{\max}_{\mathsf{BA}} = n - 1$; for $n \leq 2t$, both are $+\infty$. These conclusions also hold when parties know only their local key tables.

Proof. By Lemmas 4.8 and 4.9, every feasible graph has the claimed number of edges. Its maximum indegree is at least its average indegree, giving the lower bound on the maximum indegree as well.

For $r \geq 2$, the graph of Lemma 4.10 with $N = n$ satisfies the sufficient cut condition of Lemma 4.8. It therefore supports BA and attains both upper bounds.

For $r = 1$, the necessary cut condition forces the complete directed graph, which gives both exact values. A protocol using only local key tables exists by Theorem 4.1. □

5 Authentication Complexity of Broadcast

We prove Main Theorem 3.

5.1 Broadcast via sparse agreement

We generalize the construction of Lenzen, Loss, Shi, and Wagner [LLSW26] with registered parties (whose keys are authenticated to all parties), replacing its unauthenticated BA with our Π_{BA} from Section 4. Let $K_{\text{reg}} \ni S$, $s = |K_{\text{reg}}|$, and $U_{\text{res}} = \mathcal{P} \setminus K_{\text{reg}}$. Authenticate each party in K_{reg} to everyone else; gradecast uses these keys, and BA uses additional authentication inside U_{res}.

Lemma 5.1. *The protocol Π_{GC} of [LLSW26] is deterministic, runs for $4s$ rounds, and gives each honest party i a pair $(c_i, g_i) \in \{0,1\}^2$, with the following properties for every fault set of size less than n:*

1. *If S is honest with input b, every honest party obtains $(b, 1)$.*
2. *If an honest party obtains $(c, 1)$, every honest party's value equals c.*
3. *If K_{reg} contains an honest party, every honest party's grade equals 1.*

The first two properties and termination follow from [LLSW26, Theorem 3.9], and the third from [LLSW26, Lemma 3.10]. For an execution with at most t faults, the third property gives exactly the guarantee needed by BA on U_{res}:

$$\text{some honest party has grade } 0 \implies K_{\text{reg}} \subseteq F \implies |F \cap U_{\text{res}}| \leq t - s.$$

Lemma 5.2 (Broadcast reduction)**.** *Let $n \geq 3$, $1 \leq t < n$, and $1 \leq s \leq t$ with $n - s > 2(t - s)$. If a graph G_{res} on U_{res} supports BA with fault bound $t - s$, using the $s(n-1)$ authentication edges out of K_{reg} gives a graph G supporting $\mathsf{BB}(G, S, t)$. Consequently,*

$$A_{\mathsf{BB}}(n,t) \leq \min_{\substack{1 \leq s \leq t \\ n-s > 2(t-s)}} \{s(n-1) + A_{\mathsf{BA}}(n-s, t-s)\}. \tag{3}$$

Protocol 4. Π_{BB}

Parameters. A set K_{reg} of s globally authenticated parties containing S, and a BA protocol Π on $U_{\mathrm{res}} = \mathcal{P} \setminus K_{\mathrm{reg}}$ with fault bound $t - s$ and public round bound T_Π.

Input. A bit b at the designated sender S.

Output. A bit at every party after $4s + T_\Pi$ rounds.

1. **Gradecast.** All parties run Π_{GC} from Lemma 5.1, obtaining (c_i, g_i).
2. **BA.** Every party $i \in U_{\mathrm{res}}$, including those with $g_i = 1$, runs Π on input c_i for T_Π rounds. Let y_i be party i's output from Π, and set $y_i = 0$ if party i has not output a bit after these T_Π rounds.
3. **Output.** Party i outputs
$$\begin{cases} c_i, & i \in K_{\mathrm{reg}} \text{ or } g_i = 1, \\ y_i, & i \in U_{\mathrm{res}} \text{ and } g_i = 0. \end{cases}$$

Proof of Lemma 5.2. If all honest parties have grade 1, they output their gradecast values, which agree by the second gradecast property. Otherwise we have $K_{\mathrm{reg}} \subseteq F$: all honest parties are in U_{res}, and BA is within its fault bound. Honest parties with grade 0 use the same BA output. If an honest party has grade 1 with value c, the second gradecast property makes every honest BA input equal c, so BA validity makes outputs from both rules agree.

If S is honest with input b, the first gradecast property gives every honest party $(b, 1)$, proving sender validity. The fixed T_Π-round BA step, with default output 0, guarantees termination even outside its fault bound without changing outputs within it. The authentication edges out of K_{reg} and those inside U_{res} are disjoint, so the setup costs $s(n-1) + |E(G_{\mathrm{res}})|$, proving (3). □

Using our Π_{BA} from Theorem 4.6 as the protocol Π, with $T_\Pi = 5(t - s + 1)$ when $|U_{\mathrm{res}}| \geq 3$, the construction above has at most $4s + 5(t - s + 1)$ rounds without changing its authentication cost.

Put $r_s = (n - s) - 2(t - s) = n - 2t + s$. By Theorem 4.11, the total cost is

$$O\left(ns + \min\left\{ (n-s)^2, \frac{(n-s)^2}{r_s} \ln \frac{e(n-s)}{r_s} \right\} \right). \tag{4}$$

For $n - s > 3(t - s)$, G_{res} is empty. In the honest-majority setting, taking $s = 1$ gives $r_s = n - 2t + 1$ and $O_\alpha(n)$ edges whenever $t/n \to \alpha$ for a fixed $\alpha \in (1/3, 1/2)$.

Corollary 5.3. *For $n \geq 3$ and $1 \leq t < n$,*

$$A_{\mathsf{BB}}(n, t) = O\Big(n(2t - n)_+ + n^{3/2}\sqrt{\ln n} \Big),$$

where $(x)_+ = \max\{x, 0\}$. For $t \leq n/2$, the bound is $O(n^{3/2}\sqrt{\ln n})$. In particular, $A_{\mathsf{BB}}(n, t) = o(n^2)$ whenever $t = n/2 + o(n)$.

Proof. Put $\delta = (2t - n)_+$ and $s = \min\{t, \delta + \lceil \sqrt{n \ln n} \rceil\}$. Choose K_{reg} to contain S and have size s. Authenticating every party in K_{reg} to everyone as in Lemma 5.2 costs at most $n(\delta + \lceil \sqrt{n \ln n} \rceil)$

edges. If $s = t$, the BA fault bound $t - s$ is zero. Otherwise, $r_s = n - 2t + s \geq \sqrt{n \ln n}$ and $\ln(en/r_s) \leq \ln(en) = O(\ln n)$. Thus the additional BA authentication cost is at most

$$O\left(\frac{n^2}{r_s} \ln \frac{en}{r_s}\right) = O(n^{3/2}\sqrt{\ln n}).$$

Adding the authentication cost of the registered parties gives $O(n\delta + n^{3/2}\sqrt{\ln n})$, as claimed. □

5.2 A superlinear lower bound near the honest-majority threshold

Write $R = \mathcal{P} \setminus \{S\}$ and let $E_R := E(G) \cap (R \times R)$ be the authentication edges between receivers. For each receiver $z \in R$, put $s_z = |\widehat{V}_z \cap R|$.

Theorem 5.4 (Broadcast lower bound)**.** *There are constants $c > 0$ and $\Lambda_0 > 1$ with the following property. Let $2t < n \leq 3t$, put $r = n - 2t$, and set $\Lambda = \ln(n/r)$. If $\Lambda \geq \Lambda_0$ and $\mathsf{BB}(G, S, t)$ is feasible, then $|E_R| \geq c\,\frac{n\Lambda^2}{\ln \Lambda}$. In particular, at $n = 2t + 1$, every feasible graph has*

$$|E_R| = \Omega\left(\frac{n \ln^2 n}{\ln \ln n}\right).$$

5.2.1 Step 1: the receiver cut condition

We adapt the ring construction in the proof for weak agreement by Fischer, Lynch, and Merritt [FLM85] to broadcast, keeping the sender's designated key fixed.

Lemma 5.5 (Receiver cut condition)**.** *Let $n \geq 3$ and $1 \leq t < n$, and suppose $\mathsf{BB}(G, S, t)$ is feasible. For every $W \subseteq \mathcal{P}$ containing S, and every pair of nonempty disjoint sets $A, B \subseteq \mathcal{P} \setminus W$ satisfying*

$$n - 2t + |W| \leq |A|, |B| \leq t - |W|, \qquad |A| + |B| < n - |W|,$$

there is a receiver $z \notin W$ such that

$$\widehat{V}_z \cap A \neq \varnothing, \qquad \widehat{V}_z \cap B \neq \varnothing.$$

Proof. Suppose no such receiver exists, and assume a deterministic broadcast protocol Π with public round bound T_Π exists. Set $\ell = 2T_\Pi + 4$ and $j_\star = T_\Pi + 2$. Put $R' = \mathcal{P} \setminus W$. Choose $C \subseteq R' \setminus (A \cup B)$ with

$$|C| = \max\{1, n - t - |A|, n - t - |B|\} \leq \min\{t - |W|, n - |W| - |A| - |B|\}.$$

Set $Z = R' \setminus (A \cup B \cup C)$. Then

$$|A \cup B \cup Z|,\ |B \cup C|,\ |C \cup A| \geq n - t.$$

We build the ring construction (Figure 3) for the proof following the approach of [FLM85].

Protocol instances and initial keys. For each $x \in R'$, create ℓ instances $x^{(j)}$ of Π, with indices taken modulo ℓ. Instance $x^{(j)}$ runs as party x, with its own local state and initial key table. Every instance uses the same public graph G. The instances with index j form layer j; write $X^{(j)} = \{x^{(j)} : x \in X\}$ for $X \subseteq R'$. Each instance remains in its layer in every round.

For each j, connect every $c^{(j)} \in C^{(j)}$ to every $a^{(j+1)} \in A^{(j+1)}$ in both channel directions. For every pair of distinct identities $x, y \in R'$ except pairs with one party in A and the other in C, connect $x^{(j)}$ and $y^{(j)}$ within the same layer, in both directions. No ring instances are created for parties in $W \setminus \{S\}$. Consider the groups

$$\begin{aligned}\widetilde{H}_0^{(j)} &= A^{(j)} \cup B^{(j)} \cup Z^{(j)},\\ \widetilde{H}_1^{(j)} &= B^{(j)} \cup C^{(j)},\\ \widetilde{H}_2^{(j)} &= C^{(j)} \cup A^{(j+1)}.\end{aligned}$$

Each group contains at least $n - t$ instances of distinct parties, and every pair of instances in the group is connected. For every $z \in R'$, choose keys $\mathsf{vk}_{z,j}$, pairwise distinct across all z, j. At each instance of a party in $\widehat{V}_z \cap R'$, use the following key for z. A dash under $A^{(j)}$ means $\widehat{V}_z \cap A = \varnothing$; a dash under $B^{(j)}$ means $\widehat{V}_z \cap B = \varnothing$:

	$A^{(j)}$	$B^{(j)}$	$C^{(j)}$	$Z^{(j)}$
$\widehat{V}_z \cap A \neq \varnothing$	$\mathsf{vk}_{z,j}$	–	$\mathsf{vk}_{z,j+1}$	$\mathsf{vk}_{z,j}$
$\widehat{V}_z \cap A = \varnothing$	–	$\mathsf{vk}_{z,j}$	$\mathsf{vk}_{z,j}$	$\mathsf{vk}_{z,j}$

The first row has no entry in $B^{(j)}$ because $\widehat{V}_z$ cannot intersect both A and B. Since $z \in \widehat{V}_z$, the table also specifies each instance's own key. Instance $z^{(j)}$ uses $\mathsf{vk}_{z,j+1}$ as its own key if $z \in C$ and $\widehat{V}_z \cap A \neq \varnothing$, and $\mathsf{vk}_{z,j}$ otherwise, with indices taken modulo ℓ. For each z, different instances have different own keys. For each $w \in W$, fix a designated key vk_w. Whenever an instance's initial key table contains an entry for w, set that entry to vk_w. Choose these keys to be pairwise distinct and different from every $\mathsf{vk}_{z,j}$ with $z \in R'$. In particular, every initial entry for S contains vk_S.

Consider sender instances $S^{(0)}$ and $S^{(j_\star)}$ with inputs 0 and 1, respectively. Each sender instance follows Π using its own input, initial key table, and received messages. Both use vk_S and the corresponding signing capability. Connect $S^{(0)}$ to every instance in $\widetilde{H}_0^{(0)}$, and $S^{(j_\star)}$ to every instance in $\widetilde{H}_0^{(j_\star)}$, in both directions. For $j \in \{0, j_\star\}$, each entry for a party z in the initial key table of $S^{(j)}$ is $\mathsf{vk}_{z,j}$ if $z \in R'$, and the fixed designated key of z if $z \in W$. For $j \in \{0, j_\star\}$ and $z \in R'$, all existing entries for z in the initial key tables of $\{S^{(j)}\} \cup \widetilde{H}_0^{(j)}$ equal $\mathsf{vk}_{z,j}$. Indeed, the shifted key $\mathsf{vk}_{z,j+1}$ occurs only in the $C^{(j)}$ column, outside $\widetilde{H}_0^{(j)}$. Each instance receives messages only from the instances connected to it. Any message it sends to a party with no connected instance is ignored.

Place $S^{(0)}$ in layer 0 and $S^{(j_\star)}$ in layer $j_\star$. Every channel connects instances in the same layer or in adjacent layers. In each round, each instance sends the messages prescribed by Π using its state at the start of that round, then receives the messages sent to it and updates its state. A message received in a round cannot be forwarded in that round. Thus messages cross at most one layer per round.

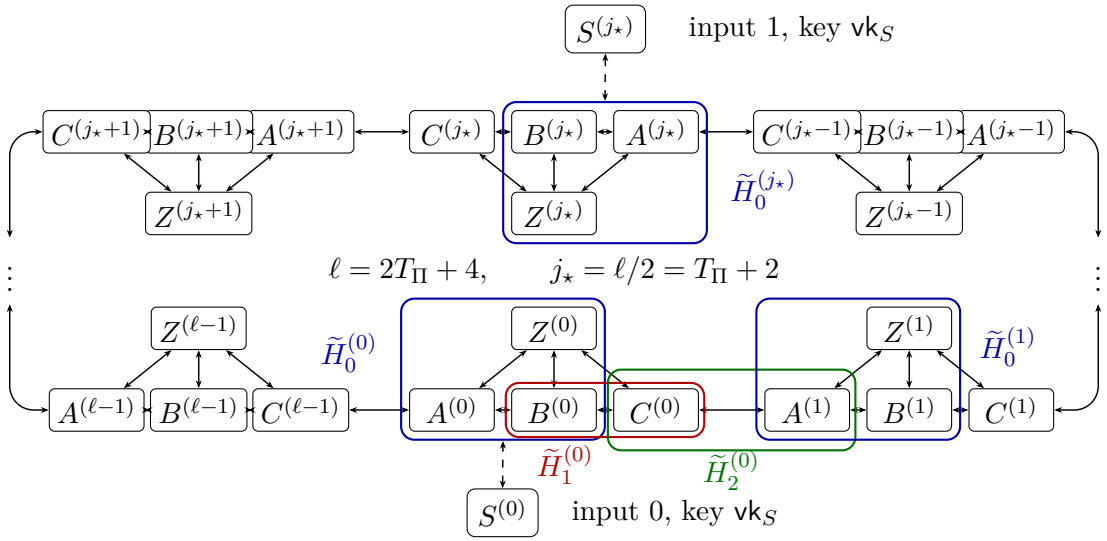

Figure 3: The ring of receiver instances. The index j specifies only the layer of an instance; indices are taken modulo ℓ. A connection between two sets represents all channels in both directions; channels within each set and intermediate layers are omitted. Each outline denotes a group. The groups $\widetilde{H}_0^{(0)}, \widetilde{H}_1^{(0)}, \widetilde{H}_2^{(0)}, \widetilde{H}_0^{(1)}$ overlap successively in $B^{(0)}, C^{(0)}, A^{(1)}$. The cyclic distance between layers 0 and $j_\star$ is $T_\Pi + 2$. Each dashed connection represents direct channels in both directions between the sender instance and every instance in the receiver-instance group. The sender instances use the same key vk_S. Each sender instance is made silent in one of the two runs used to apply sender validity.

Consistency. Fix one group $\widetilde{H}_i^{(j)}$. For each signer z, all initial entries for z in the key tables of instances in $\widetilde{H}_i^{(j)}$ contain the same key. If $\widetilde{H}_i^{(j)}$ contains an instance of z, these entries contain the verification key of the instance of z in $\widetilde{H}_i^{(j)}$. Consider an execution of Π on G in which exactly the parties represented in $\widetilde{H}_i^{(j)}$ are honest. Give each honest party the initial state, key table, and signing capability of its instance in $\widetilde{H}_i^{(j)}$. Choose designated keys to agree with these tables, keeping the keys of parties in W fixed. The adversary simulates every receiver instance in the ring outside the chosen group $\widetilde{H}_i^{(j)}$. It also simulates both sender instances $S^{(0)}$ and $S^{(j_\star)}$, using the corrupted party S's signing capability for its designated key vk_S. The signing capability of each simulated receiver instance corresponds either to a corrupted party's designated key or to an additional receiver key distinct from every honest party's designated key. The adversary generates the additional receiver keys together with the corresponding signing capabilities.

Each instance in $\widetilde{H}_i^{(j)}$ is connected to at most one instance of each other party, and every pair of instances in $\widetilde{H}_i^{(j)}$ is connected. Thus a channel from an instance in $\widetilde{H}_i^{(j)}$ to an instance outside $\widetilde{H}_i^{(j)}$ always has a faulty party's identity at the other end. In each round, the adversary feeds messages sent by honest parties to faulty parties into the corresponding simulated instances. It sends messages from simulated instances to instances in $\widetilde{H}_i^{(j)}$ on the corresponding faulty parties' channels. Every

honest signature used in this simulation has therefore already been received in a message to a faulty party, including signatures contained in other signed messages. Induction on rounds shows that each honest party receives the same messages and has the same state as its instance in $\widetilde{H}_i^{(j)}$. Hence all instances in $\widetilde{H}_i^{(j)}$ output the same bit by round T_Π.

The groups $\widetilde{H}_0^{(j)}, \widetilde{H}_1^{(j)}, \widetilde{H}_2^{(j)}, \widetilde{H}_0^{(j+1)}$ overlap successively in the nonempty sets $B^{(j)}, C^{(j)}, A^{(j+1)}$. Their common output bits must therefore be equal. Every receiver instance belongs to one of these groups, so all receiver instances output the same bit by round T_Π.

Sender validity. Run the ring again from the same initial states and key tables, with $S^{(j_\star)}$ sending no messages in any round. The sender instance $S^{(0)}$ still follows Π with input 0. Consider an execution of Π on G in which exactly S and the parties in $A \cup B \cup Z$ are honest. Give these honest parties the initial states, key tables, and signing capabilities of $S^{(0)}$ and their instances in $\widetilde{H}_0^{(0)}$. Choose designated keys to agree with these tables, keeping the keys of parties in W fixed. The faulty parties are $C \cup (W \setminus \{S\})$, whose size is $|C| + |W| - 1 \leq t - 1$.

The adversary simulates all receiver instances outside $\widetilde{H}_0^{(0)}$ as in the consistency argument. The sender instance $S^{(j_\star)}$ sends nothing, so the simulation requires no signing capability for S. The faulty parties ignore messages that the honest sender sends to them and send nothing to it; their messages to honest receivers are those of the corresponding simulated instances. Induction on rounds gives the honest parties the same states and messages as their instances in this run of the ring. Sender validity therefore forces every receiver in $\widetilde{H}_0^{(0)}$ to output 0 by round T_Π.

Run the ring again from the same initial states and key tables, with $S^{(0)}$ sending no messages and $S^{(j_\star)}$ following Π with input 1. The same argument, using the instances in $\{S^{(j_\star)}\} \cup \widetilde{H}_0^{(j_\star)}$ for the honest parties, forces every receiver in $\widetilde{H}_0^{(j_\star)}$ to output 1 by round T_Π.

Contradiction. Compare the first run, in which both sender instances follow Π, with either run in which one sender instance is made silent. For every $0 \leq r \leq T_\Pi$, each instance at cyclic layer distance greater than r from the sender made silent has the same state through round r in both runs.

For $r = 0$, the initial states and key tables are the same. For the induction step, an instance at distance greater than $r + 1$ and every instance connected to it are at distance greater than r. None is the sender made silent, so all follow Π in both runs. By induction, each has the same state in both runs at the start of round $r + 1$ and therefore sends the same messages in that round. Channels with no connected instance are silent in both runs. The instance at distance greater than $r + 1$ thus receives the same messages and reaches the same state in both runs.

The cyclic distance between layers 0 and $j_\star$ is $T_\Pi + 2$. In the first run, the receivers in $\widetilde{H}_0^{(0)}$ therefore have the same states through round T_Π as when $S^{(j_\star)}$ is silent, and must output 0. The receivers in $\widetilde{H}_0^{(j_\star)}$ also have the same states through round T_Π as when $S^{(0)}$ is silent, and must output 1. This contradicts the common receiver output in the first run. □

5.2.2 Step 2: equal-size receiver sets

Corollary 5.6. *Let $2t < n$, put $r = n - 2t$, and suppose $\mathsf{BB}(G, S, t)$ is feasible. For any $W \subseteq \mathcal{P}$ containing S, put $R' = \mathcal{P} \setminus W$. If $4|W| + 3r \le n$, every pair of disjoint sets $A, B \subseteq R'$ with $|A| = |B| = k \ge r + |W|$ has a receiver $z \in R'$ satisfying*

$$\widehat{V}_z \cap A \neq \varnothing \quad \textit{and} \quad \widehat{V}_z \cap B \neq \varnothing.$$

Proof. Apply Lemma 5.5 to subsets of A, B of size $r + |W|$. □

For fixed R', form a bipartite graph with vertex classes $(R')_{\mathrm{L}}$ and $(R')_{\mathrm{R}}$, both indexed by R', and edges

$$\bigcup_{z \in R'} (\widehat{V}_z \cap R')_{\mathrm{L}} \times (\widehat{V}_z \cap R')_{\mathrm{R}}.$$

A bipartite independent set is a pair of sets with no edges between them. Their corresponding receiver sets must be disjoint: if a receiver belonged to both, its diagonal edge would join the two sets, since $v \in \widehat{V}_v$. Thus Corollary 5.6 excludes k-by-k independent sets for every $k \ge r + |W|$.

5.2.3 Step 3: counting edges

We use the following form of the random-deletion argument of Radhakrishnan and Ta-Shma [RTS00, Section 3.3].

Lemma 5.7. *Let a bipartite graph have $N \ge 1$ vertices on each side and no k-by-k independent set, where $k \ge 1$ is an integer. Suppose its edge set is the union of complete bipartite graphs (bicliques) $L_z \times R_z$ with $|L_z| = |R_z| = a_z$, whose indices are partitioned into I, J. These bicliques may share vertices and edges. Then*

$$\frac{N^2}{4} \le \sum_{z \in I} a_z^2 + k \sum_{z \in J} a_z^2 + 2kN\, 2^{\frac{2}{N} \sum_{z \in I} a_z}. \tag{5}$$

Proof. Fix an induced subgraph H with side sizes x, y and e edges. Assume first that $x \ge k$, and let A consist of the k vertices of smallest degree on the left. Since H has no k-by-k independent set, at most $k - 1$ vertices on the right have no neighbor in A. Hence

$$y - k + 1 \le |N_H(A)| \le \sum_{v \in A} \deg_H(v) \le \frac{ke}{x},$$

giving $xy \le ke + (k-1)x$. For $x < k$, we have $xy \le ky$. Thus every induced subgraph satisfies

$$xy \le k(e + x + y). \tag{6}$$

Put $d = \frac{2}{N} \sum_{z \in I} a_z$ and $p = 2^{-d}$. For each vertex v, let $h(v)$ count the bicliques indexed by I that contain it. On each side, $\sum_v h(v) = Nd/2$. Thus the sets $U_{\mathrm{L}}, U_{\mathrm{R}}$ of vertices with $h(v) \le d$ each have size at least $N/2$. We now restrict the graph to the induced bipartite subgraph on U_{L} and U_{R}. For each $z \in I$, independently choose one side with equal probability and delete its vertices

belonging to that biclique. Then keep each surviving vertex v independently with probability $2^{h(v)-d}$, independently of the previous choices. The final survival probability is $2^{-h(v)}2^{h(v)-d} = p$. A pair $u \in U_{\mathrm{L}}, v \in U_{\mathrm{R}}$ cannot both survive if they belong to a common biclique indexed by I. Otherwise, their deletions depend on disjoint sets of independent choices, so their joint survival probability is p^2.

Let X, Y be the surviving sets and e their number of edges. At most $\sum_{z\in I} a_z^2$ pairs belong to a biclique indexed by I, and every surviving edge belongs to one indexed by J. Therefore

$$\begin{aligned}\mathbb{E}[|X||Y|] &\geq p^2\left(\frac{N^2}{4} - \sum_{z\in I} a_z^2\right),\\ \mathbb{E}e &\leq p^2 \sum_{z\in J} a_z^2,\\ \mathbb{E}(|X|+|Y|) &\leq 2Np.\end{aligned}$$

Apply (6) to each outcome, take expectations, and divide by p^2 to obtain (5). □

Proof of Theorem 5.4. Put

$$\mu = \sum_{z\in R} s_z = |E_R| + n - 1.$$

Take Λ sufficiently large. We may assume $\mu \leq n\Lambda^2/100$, since otherwise subtracting $n-1$ already gives the claimed bound.

Fix an integer k with

$$ne^{-3\Lambda/4} \leq k \leq ne^{-\Lambda/4},$$

and define

$$D_k = \left[\frac{n}{k\Lambda^2}, \frac{n\Lambda^2}{k}\right), \qquad M_k = \{z \in R : s_z \in D_k\}, \qquad \mu_k = \sum_{z\in M_k} s_z.$$

We will show that $\mu_k > n\Lambda/100$ for every such k, and then sum over disjoint intervals D_k.

Remove the sender and the receivers above the interval:

$$W_k = \{S\} \cup \left\{z \in R : s_z \geq \frac{n\Lambda^2}{k}\right\}, \qquad R_k = \mathcal{P} \setminus W_k, \qquad N_k = |R_k|.$$

By the bound on μ,

$$|W_k| \leq 1 + \frac{k\mu}{n\Lambda^2} \leq 1 + \frac{k}{100}.$$

Since $k \geq e^{\Lambda/4}$ and $r/k, k/n \leq e^{-\Lambda/4}$, we have $N_k \geq n/2$ and may apply Corollary 5.6.

Use the bipartite graph from Step 2 on two copies of R_k. For this fixed k, write $a_z = |\widehat{V}_z \cap R_k| \leq s_z$. The biclique indexed by $z \in R_k$ has a_z vertices on each side, and their union has no k-by-k independent set.

Suppose $\mu_k \le n\Lambda/100$. Apply Lemma 5.7 with $N = N_k$, $I = M_k$, and $J = R_k \setminus M_k$. Using $1/k \le e^{-\Lambda/4}$ in the first line, its three terms satisfy

$$\begin{aligned} \sum_{z\in M_k} a_z^2 &\le \frac{n\Lambda^2}{k}\mu_k &&\le \frac{n^2\Lambda^3 e^{-\Lambda/4}}{100}, \\ k\sum_{z\in R_k\setminus M_k} a_z^2 &\le \frac{n}{\Lambda^2}\mu &&\le \frac{n^2}{100}, \\ 2kN_k\, 2^{\frac{2}{N_k}\sum_{z\in M_k} a_z} &\le 2kn\, e^{\Lambda/25} &&\le 2n^2 e^{-21\Lambda/100}. \end{aligned}$$

Since $N_k \ge n/2$, (5) gives

$$\frac{1}{16} \le \frac{1}{100} + \frac{\Lambda^3 e^{-\Lambda/4}}{100} + 2e^{-21\Lambda/100}.$$

This is a contradiction. Thus $\mu_k > n\Lambda/100$.

Finally, put

$$k_0 = \left\lceil ne^{-3\Lambda/4} \right\rceil, \qquad q = \left\lceil \Lambda^4 \right\rceil, \qquad k_j = k_0 q^j \le ne^{-\Lambda/4}.$$

There are $m = \Theta(\Lambda/\ln\Lambda)$ such integers:

$$\ln \frac{ne^{-\Lambda/4}}{k_0} = \frac{\Lambda}{2} + O(1), \qquad \ln q = 4\ln\Lambda + O(1).$$

Moreover,

$$\frac{n\Lambda^2}{k_{j+1}} \le \frac{n}{k_j\Lambda^2},$$

so the intervals D_{k_j} are pairwise disjoint. Each receiver is therefore counted at most once, giving

$$\mu \ge \sum_{j=0}^{m-1} \mu_{k_j} > \frac{mn\Lambda}{100} = \Omega\left(\frac{n\Lambda^2}{\ln\Lambda}\right).$$

Subtracting $n-1$ gives the claimed bound for $|E_R|$. For $n = 2t+1$, we have $r = 1$ and $\Lambda = \ln n$, giving the stated special case. □

5.3 Broadcast with a dishonest majority

Write $R = \mathcal{P} \setminus \{S\}$. We say two receivers are nonadjacent if neither directed edge between them is present.

Lemma 5.8. *If $t \le n-2$ and $n \le 2t$, then for every nonadjacent receiver pair a, b in a feasible graph, at least $d = 2t - n + 1$ receivers z satisfy $z \to a$ and $z \to b$.*

Proof. Suppose nonadjacent receivers a, b have at most $d-1$ receivers z with $z \to a$ and $z \to b$. Choose W of size d, containing S and all such receivers and excluding a, b. Apply Lemma 5.5 with $A = \{a\}$ and $B = \{b\}$. Since a, b are nonadjacent, the receiver given by the cut condition is neither a nor b, contradicting the choice of W. □

Lemma 5.9 (Counting receiver authentication edges)**.** *Let $U \subseteq R$ be a set of $N \geq 1$ receivers, and let $0 \leq d \leq N-1$ be an integer. If, for every nonadjacent pair $a, b \in U$, at least d receivers $z \in U$ satisfy $z \to a$ and $z \to b$, then*

$$\sum_{v \in U} |K_v \cap U| \geq dN - \binom{d+1}{2} = \binom{N}{2} - \binom{N-d}{2}.$$

Proof. We prove the statement by induction on d. The case $d = 0$ is immediate. If every $v \in U$ has $|K_v \cap U| \geq d$, summing gives at least Nd authentication edges with both endpoints in U.

Otherwise, choose $v \in U$ with $|K_v \cap U| < d$. This receiver must be adjacent to every other receiver in U: a nonadjacent pair containing v would give at least d distinct receivers in $K_v \cap U$. Deleting v removes at least $N-1$ authentication edges with both endpoints in U. Each remaining nonadjacent pair loses at most one receiver pointing to both parties, so $U \setminus \{v\}$ satisfies the hypothesis with $d-1$. Applying the induction hypothesis to these $N-1$ receivers gives

$$\sum_{u \in U} |K_u \cap U| \geq N - 1 + (d-1)(N-1) - \binom{d}{2} = dN - \binom{d+1}{2}.$$

□

Fixed dishonest-majority fractions. Fix $\alpha \in (1/2, 1)$. For sufficiently large n, put $t = \lfloor \alpha n \rfloor$ and $d = 2t - n + 1$. By Lemmas 5.8 and 5.9 with $U = R$ and $N = n - 1$,

$$|E_R| = \sum_{v \in R} |K_v \cap R| \geq d(n-1) - \binom{d+1}{2} = \binom{n-1}{2} - \binom{2(n-t)-2}{2} = \Omega_\alpha(n^2).$$

A protocol with complete PKI gives the matching $O(n^2)$ upper bound, so $A_{\mathsf{BB}}(n, \lfloor \alpha n \rfloor) = \Theta_\alpha(n^2)$.

5.4 Maximum resilience with optimal authentication

The protocol below uses two recursive broadcasts. Receivers in both calls keep the output of the first call if the second call yields no valid signature. Messages sent between the calls ensure agreement with the sender of the second call when that party is honest.

Theorem 5.10 (Maximum resilience)**.** *For $n \geq 3$ and a designated sender S,*

$$A_{\mathsf{BB}}(n, n-1) = \binom{n}{2} - 1.$$

An optimal setup consists of all forward edges in an order $S = v_0, v_1, \ldots, v_{n-1}$ except $v_{n-2} \to v_{n-1}$ (Figure 2).

5.4.1 Sufficiency by induction

We construct broadcast by induction on n for every nonempty message domain $\mathcal{M}$ with a fixed default $m_0 \in \mathcal{M}$. For $n = 2$, the sender sends its input directly and outputs it; the receiver outputs the received value if it lies in $\mathcal{M}$, and m_0 otherwise. For $n \geq 3$, put $U_{\text{tail}} = \{v_2, \ldots, v_{n-1}\}$. The sender $S = v_0$ has authentication edges to every receiver. Signatures are sent together with their signed values. Here, a signature is valid if it verifies under S's designated key as an INPUT signature for the n-party broadcast from S.

The input to each recursive broadcast is either $\perp$ or a signed value of S. Both recursive calls use this message domain with default $\perp$. Treat any recursive output without a valid signature as $\perp$.

1. S recursively broadcasts S's input signature on $\{S\} \cup U_{\text{tail}}$.
2. S sends its input signature directly to v_1, and each party in U_{tail} sends its output from the first call to v_1.
3. v_1 chooses a valid signature from the first party in the order $S, v_2, \ldots, v_{n-1}$ that sent one after the first call, or $\perp$ if no party sent one. v_1 broadcasts the chosen signature or $\perp$ on $\{v_1\} \cup U_{\text{tail}}$.

Output. Parties in U_{tail} use the output of the second call if it is a valid signed value of S, and otherwise keep the output of the first call; v_1 uses v_1's input to the second call. Each receiver outputs the message carried by the selected valid signature, or m_0 if the selection is $\perp$; S outputs its input. Only the signature added for the current call is removed; signatures contained in its message are retained. For the outermost binary broadcast, take $\mathcal{M} = \{0, 1\}$ and $m_0 = 0$.

Consistency.

Consistency. By consistency of both broadcast invocations, all honest parties in U_{tail} obtain the same output from each call and therefore select the same final output. If v_1 is honest, validity of the second call ensures that they all receive v_1's input to that call. If this input is a valid signed value of S, they select it. Otherwise, v_1 inputs $\perp$, and forwarding ensures that all honest parties in U_{tail} also obtained $\perp$ from the first call. Keeping the first call's output therefore agrees with v_1's input to the second call. Thus all honest receivers agree.

Validity. If S is honest, the first call provides S's signed input to every honest party in U_{tail}, and every valid signature of S is on that input. Hence selecting a valid signed value from the second call preserves sender validity even if v_1 is faulty. An honest v_1 receives S's signed input directly from S and outputs that input. Thus every honest receiver outputs S's input.

5.4.2 Necessity

Suppose $\mathsf{BB}(G, S, n-1)$ is feasible. First, S must point to every receiver v: otherwise applying Lemma 4.2 with $A = \{v\}$, $B = \mathcal{P} \setminus \{S, v\}$, and $C = \{S\}$ shows there is no broadcast protocol. Thus $n - 1$ sender edges are necessary.

For distinct receivers a, b, z, apply Lemma 5.5 with $W = \mathcal{P} \setminus \{a, b, z\}$, $A = \{a\}$, and $B = \{b\}$. If a, b are nonadjacent, the receiver required by the cut condition must be z, giving

$$a \nrightarrow b,\ b \nrightarrow a \quad \Longrightarrow \quad z \to a,\ z \to b \qquad (z \in R \setminus \{a, b\}). \tag{7}$$

Thus every nonadjacent receiver pair a, b has $n - 3$ receivers z with $z \to a$ and $z \to b$. Applying Lemma 5.9 with $U = R$, $N = n - 1$, and $d = n - 3$ gives

$$|E_R| \geq \binom{n-1}{2} - \binom{2}{2} = \binom{n-1}{2} - 1.$$

Adding the sender's $n - 1$ edges gives exactly $\binom{n}{2} - 1$.

Proof of Main Theorem 3. **Honest-majority lower bound.** Let $2t < n \leq 3t$, put $r = n - 2t$, and write $\Lambda = \ln(n/r)$. Theorem 5.4 gives the lower bound when Λ is sufficiently large. When Λ is bounded, it suffices to prove $A_{\mathsf{BB}}(n, t) \geq t + 1 \geq n/3$. Suppose a feasible graph has at most t authentication edges. There are at least $n - t - 1 \geq r - 1$ receivers with no outgoing edges. Let C consist of S and $r - 1$ such receivers. Since S has at most t outneighbors, partition the remaining $2t$ parties into t-sets A, B with $V_S \setminus C \subseteq B$. Then $V_x \cap A = \varnothing$ for every $x \in C$. Since $S \in C$, Lemma 4.2 contradicts feasibility.

Honest-majority upper bounds. Taking $s = 1$ in Lemma 5.2 gives $(n - s) - 2(t - s) = r + 1$ and hence $O((n^2/r)\ln(n/r))$ edges. Corollary 5.3 gives the other bound, $O(n^{3/2}\sqrt{\ln n})$.

Dishonest-majority fractions. The fixed-fraction bounds follow from Lemmas 5.8 and 5.9 and a complete PKI. The bound $A_{\mathsf{BB}}(n, t) = o(n^2)$ for $t = n/2 + o(n)$ follows from Corollary 5.3, and the exact cost at maximum resilience is given by Theorem 5.10. □

6 Open problems

For broadcast, there is a gap near the honest-majority threshold. In particular, at $n = 2t + 1$,

$$\Omega\left(\frac{n \ln^2 n}{\ln \ln n}\right) \leq A_{\mathsf{BB}}(n, t) \leq O\left(n^{3/2}\sqrt{\ln n}\right).$$

Closing this gap remains open.

Broadcast on a given authentication graph. A necessary and sufficient condition for designated-sender broadcast on an arbitrary authentication graph remains open for general fault bounds. For fixed n, t, S, it remains open whether a single protocol using only local key tables can solve broadcast on every authentication graph G for which $\mathsf{BB}(G, S, t)$ is feasible when G is public.

Authentication cost per party. For BA, one construction achieves optimal total authentication cost and maximum indegree simultaneously up to constant factors (Theorem 4.11). For broadcast with $t = \lfloor \alpha n \rfloor$, our results imply $A^{\max}_{\mathsf{BB}} = \Theta_\alpha(1)$ for fixed $\alpha \in (1/3, 1/2)$ and $A^{\max}_{\mathsf{BB}} = \Theta_\alpha(n)$ for fixed

$\alpha \in (1/2, 1)$. In each regime, one construction simultaneously achieves optimal total authentication cost and maximum indegree up to constant factors. At $n = 2t + 1$, however, we only know

$$\Omega\left(\frac{\ln^2 n}{\ln \ln n}\right) \leq A^{\max}_{\mathsf{BB}}(n, t) \leq O\left(\sqrt{n \ln n}\right).$$

The lower bound follows by averaging. The upper bound applies the reduction of Lemma 5.2 with $s = \Theta(\sqrt{n \ln n})$ globally authenticated parties and the BA graph from Theorem 4.11. It remains open whether each party's initial key table can have $\operatorname{polylog} n$ entries, and whether one setup and protocol can simultaneously achieve $A_{\mathsf{BB}}(n, t)$ and $A^{\max}_{\mathsf{BB}}(n, t)$ up to constant factors.

References

[BCL+11] Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. Secure computation without authentication. *Journal of Cryptology*, 24(4):720–760, October 2011. doi:10.1007/s00145-010-9075-9.

[BDCS22] Naama Ben-David, Benjamin Y. Chan, and Elaine Shi. Revisiting the power of non-equivocation in distributed protocols. In Alessia Milani and Philipp Woelfel, editors, *41st ACM Symposium Annual on Principles of Distributed Computing*, pages 450–459, Salerno, Italy, July 25–29, 2022. Association for Computing Machinery. doi:10.1145/3519270.3538427.

[BF99] Amos Beimel and Matthew K. Franklin. Reliable communication over partially authenticated networks. *Theoretical Computer Science*, 220(1):185–210, 1999.

[BGG+11] Piyush Bansal, Prasant Gopal, Anuj Gupta, Kannan Srinathan, and Pranav Kumar Vasishta. Byzantine agreement using partial authentication. In *Distributed Computing (DISC 2011)*, volume 6950 of *Lecture Notes in Computer Science*, pages 389–403. Springer, 2011. doi:10.1007/978-3-642-24100-0_38.

[BGP89] Piotr Berman, Juan A. Garay, and Kenneth J. Perry. Towards optimal distributed consensus (extended abstract). In *30th Annual Symposium on Foundations of Computer Science*, pages 410–415, Research Triangle Park, NC, USA, October 30 – November 1, 1989. IEEE Computer Society Press. doi:10.1109/SFCS.1989.63511.

[BM04] Amos Beimel and Tal Malkin. A quantitative approach to reductions in secure computation. In Moni Naor, editor, *TCC 2004: 1st Theory of Cryptography Conference*, volume 2951 of *Lecture Notes in Computer Science*, pages 238–257, Cambridge, MA, USA, February 19–21, 2004. Springer Berlin Heidelberg, Germany. doi:10.1007/978-3-540-24638-1_14.

[BM05] Amos Beimel and Lior Malka. Efficient reliable communication over partially authenticated networks. *Distributed Computing*, 18(1):1–19, 2005. doi:10.1007/s00446-004-0119-y.

[Bor96] Malte Borcherding. Levels of authentication in distributed agreement. In *Distributed Algorithms (WDAG 1996)*, volume 1151 of *Lecture Notes in Computer Science*, pages 40–55. Springer, 1996. URL: https://publikationen.bibliothek.kit.edu/44698.

[CJKR12] Allen Clement, Flavio Junqueira, Aniket Kate, and Rodrigo Rodrigues. On the (limited) power of non-equivocation. In Darek Kowalski and Alessandro Panconesi, editors, *31st ACM Symposium Annual on Principles of Distributed Computing*, pages 301–308, Funchal, Madeira, Portugal, July 16–18, 2012. Association for Computing Machinery. doi:10.1145/2332432.2332490.

[Dol82] Danny Dolev. The Byzantine generals strike again. *Journal of Algorithms*, 3(1):14–30, 1982. doi:10.1016/0196-6774(82)90004-9.

[DS83] Danny Dolev and H. Raymond Strong. Authenticated algorithms for Byzantine agreement. *SIAM Journal on Computing*, 12(4):656–666, 1983. doi:10.1137/0212045.

[DY81] Danny Dolev and Andrew Chi-Chih Yao. On the security of public key protocols (extended abstract). In *22nd Annual Symposium on Foundations of Computer Science*, pages 350–357, Nashville, TN, USA, October 28–30, 1981. IEEE Computer Society Press. doi:10.1109/SFCS.1981.32.

[FGH+02] Matthias Fitzi, Daniel Gottesman, Martin Hirt, Thomas Holenstein, and Adam Smith. Detectable byzantine agreement secure against faulty majorities. In Aleta Ricciardi, editor, *21st ACM Symposium Annual on Principles of Distributed Computing*, pages 118–126, Monterey, CA, USA, July 21–24, 2002. Association for Computing Machinery. doi:10.1145/571825.571841.

[FGMO05] Matthias Fitzi, Juan A. Garay, Ueli M. Maurer, and Rafail Ostrovsky. Minimal complete primitives for secure multi-party computation. *Journal of Cryptology*, 18(1):37–61, January 2005. doi:10.1007/s00145-004-0150-y.

[FGMvR02] Matthias Fitzi, Nicolas Gisin, Ueli M. Maurer, and Oliver von Rotz. Unconditional byzantine agreement and multi-party computation secure against dishonest minorities from scratch. In Lars R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 482–501, Amsterdam, The Netherlands, April 28 – May 2, 2002. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-46035-7_32.

[FHHW03] Matthias Fitzi, Martin Hirt, Thomas Holenstein, and Jürg Wullschleger. Two-threshold broadcast and detectable multi-party computation. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 51–67, Warsaw, Poland, May 4–8, 2003. Springer Berlin Heidelberg, Germany. doi:10.1007/3-540-39200-9_4.

[FLM85] Michael J. Fischer, Nancy A. Lynch, and Michael Merritt. Easy impossibility proofs for distributed consensus problems. In Michael A. Malcolm and H. Raymond Strong, editors, *4th ACM Symposium Annual on Principles of Distributed Computing*, pages 59–70, Minaki, Ontario, Canada, August 5–7, 1985. Association for Computing Machinery. doi:10.1145/323596.323602.

[FM00] Matthias Fitzi and Ueli M. Maurer. From partial consistency to global broadcast. In *32nd Annual ACM Symposium on Theory of Computing*, pages 494–503, Portland, OR, USA, May 21–23, 2000. ACM Press. doi:10.1145/335305.335363.

[GNP22] Saumya Goyal, Varun Narayanan, and Manoj Prabhakaran. Oblivious-transfer complexity of noisy coin-toss via secure zero communication reductions. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022: 20th Theory of Cryptography Conference, Part III*, volume 13749 of *Lecture Notes in Computer Science*, pages 89–118, Chicago, IL, USA, November 7–10, 2022. Springer, Cham, Switzerland. doi:10.1007/978-3-031-22368-6_4.

[JMS12] Alexander Jaffe, Thomas Moscibroda, and Siddhartha Sen. On the price of equivocation in byzantine agreement. In Darek Kowalski and Alessandro Panconesi, editors, *31st ACM Symposium Annual on Principles of Distributed Computing*, pages 309–318, Funchal, Madeira, Portugal, July 16–18, 2012. Association for Computing Machinery. doi:10.1145/2332432.2332491.

[Kőn31] Dénes Kőnig. Graphok és matrixok. *Matematikai és Fizikai Lapok*, 38:116–119, 1931. English translation by Gábor Szárnyas. URL: https://arxiv.org/abs/2009.03780.

[KV21] Muhammad Samir Khan and Nitin H. Vaidya. Byzantine consensus with local multicast channels. In *DISC 2021*, volume 209 of *LIPIcs*, pages 26:1–26:16, 2021. Directed-hypergraph version. URL: https://arxiv.org/abs/2109.01205, doi:10.4230/LIPIcs.DISC.2021.26.

[LLSW26] Christoph Lenzen, Julian Loss, Kecheng Shi, and Benedikt Wagner. Byzantine consensus in the partially authenticated setting. In *PODC 2026*, 2026. Full version: Cryptology ePrint Archive, Paper 2026/470. URL: https://eprint.iacr.org/2026/470.

[LMT18] Julian Loss, Ueli Maurer, and Daniel Tschudi. Strong separations between broadcast and authenticated channels. In *DISC 2018*, volume 121 of *LIPIcs*, pages 36:1–36:17, 2018. doi:10.4230/LIPIcs.DISC.2018.36.

[LZMM21] Chen-Da Liu-Zhang, Varun Maram, and Ueli Maurer. On broadcast in generalized network and adversarial models. In *OPODIS 2020*, volume 184 of *LIPIcs*, pages 25:1–25:16, 2021. doi:10.4230/LIPIcs.OPODIS.2020.25.

[NPSW23] Varun Narayanan, Vinod M. Prabhakaran, Neha Sangwan, and Shun Watanabe. Complete characterization of broadcast and pseudo-signatures from correlations. In

Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part II*, volume 14005 of *Lecture Notes in Computer Science*, pages 563–593, Lyon, France, April 23–27, 2023. Springer, Cham, Switzerland. doi:10.1007/978-3-031-30617-4_19.

[PSL80] Marshall Pease, Robert Shostak, and Leslie Lamport. Reaching agreement in the presence of faults. *Journal of the ACM*, 27(2):228–234, 1980. doi:10.1145/322186.322188.

[RTS00] Jaikumar Radhakrishnan and Amnon Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM Journal on Discrete Mathematics*, 13(1):2–24, 2000. Author version. URL: https://www.cs.tau.ac.il/~amnon/Papers/RT.siam00.pdf, doi:10.1137/S0895480197329508.

[VT26] Nitin H. Vaidya and Lewis Tseng. Byzantine consensus in directed graphs with message authentication, 2026. arXiv:2605.11309v2. URL: https://arxiv.org/abs/2605.11309v2.

AI methodology. We used ChatGPT (Codex) Astra 6 to assist with writing, verifying, finding reference [RTS00, Kőn31] and helping with probability and combinatoric computation. We also taken several presentation suggestions from Google Deep Review. The author verified the correctness and originality of all content, including references.