Gradecast in Synchrony and Reliable Broadcast in Asynchrony with Optimal Resilience, Efficiency, and Unconditional Security

Ittai Abraham* Gilad Asharov†

March 3, 2022

Abstract

We revisit Gradecast (Feldman and Micali, STOC'88) in Synchrony and Reliable Broadcast (Bracha, Information and Computation'87) in Asynchrony. For both tasks ,we provide new protocols that have three desirable properties: (1) *optimal resilience*, tolerating $t < n/3$ malicious parties; (2) are *communication-efficient*, where honest parties send just $O(nL)$ bits for a dealer with a message of $L = \Omega(n)$ bits; (3) and are *unconditionally secure*, (or statistically secure), without needing to rely on any computational or setup assumptions. To the best of our knowledge, no previous work obtains all three properties simultaneously.

1 Introduction

Feldman and Micali's Gradecast [FM88] (in Synchrony), and Bracha's Reliable Broadcast [Bra87] (in Asynchrony) are fundamental protocols from the 1980s. In this paper we provide new protocols for both Gradecast and Reliable Broadcast that obtain three desirable properties:

1. **Communication Efficient**: The total number of bits that honest parties send and receive is just $O(nL)$ bits for a dealer that has a message of size $L = \Omega(n)$ bis. We call this *communication efficient* because this is asymptotically optimal: just sending L bits requires each party to receive L bits for a total of $O(nL)$.

2. **Unconditionally secure**: There are no restrictions on the computational power of the adversary and there are no setup assumptions. The protocol acheives statistical security.

3. **Optimal Resilience**: Tolerating a malicious adversary controlling $t < n/3$ parties. This is the *optimal resilience* for statistical security.

The classic protocol of Bracha [Bra87] is optimally resilient but not communication efficient, broadcasting L bits requires $O(n^2L)$ bits. The protocol of Cachin and Tessaro [CT05] is optimally resilient and nearly (up to polylog factors) communication efficient, but relies on a collision resistant

*VMWare Research. iabraham@vmware.com

†Department of Computer Science, Bar-Ilan University. Gilad.Asharov@biu.ac.il. Sponsored by the Israel Science Foundation (grant No. 2439/20), by JPM Faculty Research Award, by the BIU Center for Research in Applied Cryptography and Cyber Security in conjunction with the Israel National Cyber Bureau in the Prime Minister's Office, and by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 891234

hash function and hence is not unconditionally secure. The recent protocol of Das , Xiang, and Ren [DXR21] is optimally resilient and communication efficient, but still relies on a collision resistant hash function and hence is not unconditionally secure.

Our work shows, perhaps surprisingly, that optimally resilient and communication efficient solutions can be unconditionally secure.

A central contribution of this work is the observation that fundamentally, there is no need to make any *computational assumptions* or setup assumptions (a collision resistant hash function is both a computational assumption and a setup assumption).

1.1 Gradecast in Synchrony

Feldman and Micali's Gradecast protocol [FM88], is a useful building block in synchronous protocols [BDH10b, BDH10a, FGH+02, KK09]. Its formal definition:

Definition 1.1. *In Gradecast a dealer has an input and each party outputs a value and a grade* $\{0, 1, 2\}$ *such that:*

1. *(Validity) If the dealer is honest then all honest parties output the dealer's input and grade 2.*
2. *(Non-equivocation) if two honest parties each output a grade* ≥ 1 *then they output the same value.*
3. *(Agreement) if an honest party outputs grade 2 then all honest parties output the same output and with grade* ≥ 1*.*

In is known that for unconditional security tolerating $t < n/3$ malicious parties is the best one can hope for [FLM85]. Hence such a protocol is said to have optimal resilience. If the number of bits of the dealer's input is L, then the message complexity of the FM's Gradecast protocol is $O(n^2L)$ bits. In this paper we ask the question: Can we reduce the message complexity at the cost of moving from perfect security to unconditional security? We show:

Theorem 1.2. *Let* $\epsilon > 0$ *and* $t \in \mathbb{N}$ *and* $n \geq 3t+1$*. There exists an n-party gradecast protocol that for input of length* $L > n/3 \cdot (\log n^3/\epsilon)$ *bits achieves validity with probability* 1*, and non-equivocation and agreement with probability* $1 - \epsilon$*. The protocol tolerates up to t malicious parties and requires the transmission of* $O(nL)$ *bits.*

1.2 Reliable Broadcast in Asynchrony

Bracha's Reliable Broadcast [Bra87], is a useful building block in asynchronous protocols. The recent paper of Das, Xiang, and Ren [DXR21] has a detailed survey of the usefulness of communication efficient Reliable Broadcast. In particular, it implies Asynchronous Verifiable Secret Sharing and Asynchronous Distributed Key Generation [AJM+21].

Definition 1.3. *In Reliable Broadcast a dealer has an input and each party that terminates outputs a value such that:*

1. *(Validity) If the dealer is honest then all honest parties terminate and output the dealer's input.*
2. *(Non-equivocation) if two honest terminate then their output is the same value.*
3. *(Termination) if an honest party terminates then all honest parties will eventually terminate.*

Here too, it is known that $t < n/3$ is the optimal resilience. If the number of bits of the dealer's input is L, then the message complexity of Bracha's Reliable Broadcast protocol is $O(n^2L)$ bits. In this paper we ask the question: Can we reduce the message complexity at the cost of moving from perfect security to unconditional security?

Theorem 1.4. *Let $\epsilon > 0$ and $t \in \mathbb{N}$ and $n \geq 3t+1$. There exists an n-party reliable broadcast protocol that for input of length $L > n/3 \cdot (\log \frac{n^3}{\epsilon})$ achieves validity with probability 1, and non-equivocation and termination with probability $1-\epsilon$. The protocol tolerates t malicious parties and requires the transmission of $O(nL)$ bits.*

Our result is an improvement of a recent result of Das, Xiang, and Ren [DXR21] in both security and asymptotic efficiently. In that paper a similar result was obtained in the Random Oracle model, under the assumption that the adversary is computationally bounded. Our result is unconditionally secure. Moreover, asymptotically, the use of a hash function requires a domain of size $\log(n/\epsilon^2)$ and hence at least $O(nL\log(n/\epsilon^2)+n^2)$ bits. Our result provides a $\log(1/\epsilon)$ better asymptotic communication complexity.

Prior to the recent result of Das, Xiang, and Ren, the best result was by Cachin and Tassero [CT05], which for optimal resilience, also required the Random Oracle model, computationally bounded adversaries, and $O(nL\log(n/\epsilon^2)\log n+n^2)$ bits.

1.3 Techniques

At a high level our work uses the uni-variant (trivial) Schwartz–Zippel lemma [Sch80, Zip79]. The Schwartz–Zippel lemma is a fundamental tool of unconditional randomized algorithm design and has numerous applications in many domains. In this work we show its applicability to fault tolerant distributed computing by showing how it can provide new trade-offs (better communication efficiency, with less assumptions) for core protocols that have been studied for over 30 years.

Reed solomon codes [Ree60]. Another primitive that we rely on is Reed-Solomon code. Let $\mathbb{F}$ be a finite field such that $|\mathbb{F}| > n$ where n is the number of parties, and let $\alpha_1, \ldots, \alpha_n$ be distinct field elements. To encode a message $m = (m_0, \ldots, m_t)$ where each $m_i \in \mathbb{F}$, the encoding algorithm defines a polynomial $P(x) = m_0 + m_1 x + \ldots + m_t x^t$ and outputs $(P(\alpha_1), \ldots, P(\alpha_n))$. Since two polynomials of degree-t can agree on at most t points, the distance of two messages is at least $n-t$. Thus, we can correct up to $(n-t-1)/2$ errors. When $t < n/3$, this means that we can correct up to t errors. Moreover, the decoding procedure is efficient. That is, given a possibly corrupted codeword $(\delta_1, \ldots, \delta_n) \in \mathbb{F}^n$ that is of distance at most t from a codeword $(\delta'_1, \ldots, \delta'_n)$, the output of the algorithm is a polynomial $P(x)$ such that for every α_i it holds that $\delta'_i = P(\alpha_i)$.

2 Gradecast Protocol for $t < n/3$ (Synchrony)

We prove the following theorem:

Theorem 2.1. *Let $\epsilon > 0$ and $t \in \mathbb{N}$ and $n \geq 3t+1$. Protocol 2.2 is an n-party gradecast protocol such that for input of length $L > n/3 \cdot (\log n^3/\epsilon)$ bits tolerates up to t malicious parties and requires the transmission of $O(nL)$ bits. Security is unconditional, and the probability of error is ϵ.*

Concrete instantiation: for statistical error probability of 2^{-40} we get the sizes as mentioned in Table 1.

The protocol. The dealer encodes its input using a finite field $\mathbb{F}$. We let $||\mathbb{F}|| = L/t$, i.e., $|\mathbb{F}| = 2^{L/t}$. Observe that $L > n/3 \cdot (\log n^3/\epsilon)$ implies that $\frac{n^3}{|\mathbb{F}|} < \epsilon$ and that $|\mathbb{F}| > n$. The dealer first encodes its message using a degree-t polynomial and sends that polynomial to all parties. The parties then exchange random points on the polynomial to check its validity. Once $t+1$ honest parties receive $2t+1$ "good points", the parties can reconstruct the polynomial from the points themselves, and essentially correct the polynomials that other honest parties exist. The protocol is as follows:

n	$L >$
100	0.253 KB
1,000	3.534 KB
10,000	45.34 KB
100,000	0.55 MB
1,000,000	6.53 MB

Table 1: Concrete instantiations. For statistical error probability of 2^{-40}, the table shows the minimum input length $L > n/3 \cdot (\log n^3/\epsilon)$ for which Theorem 2.1 holds.

Protocol 2.2: Gradecast for $t < n/3$ (Synchrony)

- **Input:** The dealer holds $t+1$ field elements, $a_0, \ldots, a_t \in \mathbb{F}$.
- **Public parameters:** n distinct non-zero field elements $\alpha_1, \ldots, \alpha_n$.
- **The protocol:**

  Round 1 – the dealer:
  1. Encode $F(x) = \sum_{i=0}^{t} a_i x^i$ and send $F(x)$ to each party P_i.

  Round 2 – each party P_i (each party sends a random share):
  1. Denote by $F_i(x)$ the polynomial received by party P_i.
  2. Choose $\beta_i \in \mathbb{F}$ uniformly at random.
  3. Send $(\beta_i, F_i(\beta_i))$ to all parties.

  Round 3 – each party P_i (send share if happy):
  1. Let $\{(\beta_j, \gamma_j)\}_{j \in [n]}$ be the message received, where (β_j, γ_j) is the message received from party P_j. If $F_i(\beta_j) = \gamma_j$ for at least $2t+1$ indices $j \in [n]$, then P_i is `happy`.
  2. If P_i is `happy`, then it sends to each other party P_j the message $(\texttt{YourPoint}, F_i(\alpha_j))$.

  Round 4 – each party P_i (reconstruct the polynomial):
  1. If $t+1$ messages $(\texttt{YourPoint}, \gamma_i)$ with the same value γ_i, then send to all parties the message $(\texttt{Reconstruct}, \gamma_i)$ to all parties.
  2. Otherwise, forward $(\texttt{Reconstruct}, \perp)$ to everyone.

- **Output – each party P_i:** Let $(\texttt{Reconstruct}, \delta_k^i)$ be the message P_i receives from party P_k in the previous round (if a value was not received from some party P_k then let $\delta_k^i = \perp$). If received at least $2t+1$ values that are non-$\perp$, use Reed-Solomon decoding procedure to decode $(\delta_1^i, \ldots, \delta_n^i)$ and let $F_i'(x)$ be the reconstructed polynomial obtained from the robust interpolation.
  1. If there is no unique decoding (or did not receive at least $2t+1$ messages), output $\perp$ with grade 0.
  2. Otherwise, if (1) P_i is `happy` in round 3; and (2) $F_i(x) = F_i'(x)$; and (3) in round 4 its value has received $2t+1$ messages $(\texttt{YourPoint}, \gamma_i')$ with $\gamma_i' = F_i'(\alpha_i)$; then output $F_i'(x)$ with grade 2.
  3. Otherwise, output $F_i'(x)$ with grade 1.

Proof of Theorem 2.1: We start with analyzing the efficiency of the protocol: in round 1, the dealer sends $n \cdot (t+1)||\mathbb{F}|| = O(nL)$ bits where recall that $||\mathbb{F}|| = L/t$. In rounds 2, 3 and 4, each party sends at most constant number of points to each other party, i.e., a total of $n^2||\mathbb{F}||$ bits. Thus, we get that the total communication is $O(n^2)$ words, or $O(n^2||\mathbb{F}||) = O(nL)$ bits. We now show that validity, non-equivocation and agreement hold with all but an ϵ error probability. We will show agreement before non-equivocation.

Validity. We first show that if the dealer is honest and holds the message $(a_0, \ldots, a_t)$, then all honest parties output the same message $(a_0, \ldots, a_t)$ with grade 2.

Clearly, the dealer sends the same polynomial $F(x)$ in the first round. Moreover, each honest party evaluates the polynomial on a random point, and sends it to each other party. Since all honest parties hold the same polynomial $F(x)$, they are all happy in round 3. Thus, party P_j receives the point $(\texttt{YourPoint}, F(\alpha_j))$ from at least $2t+1$ parties in round 4 and sends $(\texttt{Reconstruct}, F(\alpha_j))$ to all other parties. That is, at least $2t+1$ parties sends points on the same polynomial of degree-t, $F(x)$. As a result, the robust interpolation succeeds to all parties, and results with $F(x)$. All honest parties interpolate $F(x)$ and output grade 2.

Agreement. We show that except for probability ϵ, if an honest party outputs grade 2 then all honest parties output the same output and with grade ≥ 1. An honest party outputs grade 2 if (see Output, Step 2 in Protocol 2.2):

1. It was happy at round 3, that is, it received from at least $2t+1$ parties random points that agree with $F_i(x)$.
2. There is a unique robust interpolation at the end of round 4 to a polynomial $F'_i(x)$ and $F_i(x) = F'_i(x)$.
3. It received $(\texttt{YourPoint}, \gamma_i)$ with the same γ_i from at least $2t+1$ other parties, and it holds that $\gamma_i = F'_i(\alpha_i)$, where $F'_i(x)$ is the polynomial it has reconstructed;

Since the honest party that outputs grade 2 has received at least $2t+1$ round 3 messages $(\texttt{YourPoint}, \gamma_i)$ with the same γ_i, it means that at least $t+1$ honest parties sent it a point and therefore are happy. We will show below (Lemma 2.3) that except for probability ϵ, all honest parties are happy hold the same polynomial. Thus, all honest parties that are happy in round 3 hold the same polynomial, denoted as $F_i(x)$. Thus, each other honest party P_k in round 3 receives $(\texttt{YourPoint}, F_i(\alpha_k))$ with the same value $F_i(\alpha_k)$ from at least $t+1$ parties. Since all honest parties that are happy hold the same polynomial, and since $|I| \leq t$, each honest party P_k cannot receive any other message that has plurality $t+1$. This implies that P_k must send $(\texttt{Reconstruct}, F_i(\alpha_k))$ to all other parties. Since this holds for any honest party, we get that there all parties receive at least $2t+1$ points on the same polynomial $F_i(x)$, and therefore there is a unique decoding to that polynomial $F_i(x)$. We conclude that all honest parties output the same polynomial $F_i(x)$ with grade at least 1.

To conclude the proof (of agreement), we prove the following lemma:

Lemma 2.3. *All honest parties that are* happy *at round 3 have the same polynomial $F(x)$, except for a probability $\binom{n}{2}\frac{t}{|\mathbb{F}|} < \epsilon$.*

Proof: First, for every two distinct fixed polynomials $f(x), g(x)$ of degree-t it holds that:

$$\Pr_{\beta \leftarrow \mathbb{F}}[f(\beta) = g(\beta)] = \frac{t}{|\mathbb{F}|} \ .$$

To see that, consider the polynomial $p(x) = f(x) - g(x)$. This is a polynomial of degree at most t. If $f(\beta) = g(\beta)$ then $p(\beta) = 0$, i.e., β is a root of the polynomial $p(x)$. Since $p(x)$ is a polynomial of degree at most t, it has at most t roots.

Now, assume that not all honest parties that are happy and hold the same polynomial. This implies that there exists two honest parties P_k, P_j that are happy but hold two distinct polynomials, say $F_k(x), F_j(x)$, respectively. Since each party is happy it must have received $2t+1$ points that agree with its polynomial. Let $\mathsf{Agree}_k \subseteq [n]$ (resp. $\mathsf{Agree}_j \subseteq [n]$) be the set of parties that sent points that were accepted by P_k (resp. P_j). Since $|\mathsf{Agree}_k| \geq 2t+1$ and $|\mathsf{Agree}_k| \geq 2t+1$, and $|\mathsf{Agree}_k \cup \mathsf{Agree}_j| \leq 3t+1$, we get that $|\mathsf{Agree}_k \cap \mathsf{Agree}_j| \geq t+1$. That is, there is at least one honest party in the intersection, i.e., at least one honest party that sent a random point that agreed with both $F_k(x)$ and $F_j(x)$. In any case, either P_k received a correct point from some honest party that does not hold $F_k(x)$, or P_j received a correct point from some honest party that does not hold $F_j(x)$. This occurs with probability at most $t/|\mathbb{F}|$. The claim then holds by a union bound over all pairs of parties P_k, P_j. That is:

$$\binom{n}{2}\frac{t}{|\mathbb{F}|} < \frac{n^3}{|\mathbb{F}|} = \frac{n^3}{2^{L/t}} < \epsilon \ ,$$

where the last step is true since $L > n/3 \cdot (\log \frac{n^3}{\epsilon})$. □

Non-equivocation. We show that if two honest parties output a grade ≥ 1, then they output the same value. A party P_i outputs grade 1 only if:

1. It received at least $2t+1$ round 4 messages $(\texttt{Reconstruct}, \cdot)$;
2. Those $2t+1$ points have a unique interpolation.

Let $F_i(x), F_j(x)$ be the output of honest parties P_i, P_j, respectively, that both have grade ≥ 1. We now show that $F_i(x) = F_j(x)$. To output grade ≥ 1, both must have received $2t+1$ round 4 messages, $(\texttt{Reconstruct}, \cdot)$. Thus, they must have received round 4 messages from at least $t+1$ honest parties. Each such honest party have received at least $t+1$ round 3 messages, $(\texttt{YourPoint}, \gamma)$ with the same value γ, which implies that there is at least one honest party that is happy at round 3. As we saw from Lemma 2.3, except for probability ϵ, all honest parties that are happy hold the same polynomial in round 3. Denote that polynomial as $F'(x)$. We now show that $F_i(x) = F_j(x) = F'(x)$.

In round 3, the happy honest parties send $(\texttt{YourPoint}, F'(\alpha_k))$ to each honest party P_k. Therefore, to reach $t+1$ values that are the same, (except for probability ϵ) the only message that can be sent by an honest P_k in round 4 is the message $(\texttt{Reconstruct}, F'(\alpha_k))$. Since P_i and P_j have a unique interpolation, i.e., there exists a unique polynomial of degree-t that is of distance at most t from the values they have received, then it must be that this decoded codeword is $F'(x)$. The only errors are obtained from the points of the corrupted parties, and those are of distance at most t. We remark that some honest parties might output $\perp$. It might be that some honest parties received $2t+1$ points on $F'(x)$ while others did not (i.e., corrupted parties might contribute correct points to only some subset of honest parties). Recall that non-equivocation requires that all honest parties that output some output with grade ≥ 1 output the same value, and there is no guarantee that all honest parties output the same output. □

3 Reliable Broadcast Protocol for $t < n/3$ (Asynchrony)

We prove the following theorem:

Theorem 3.1. *Let $\epsilon > 0$ and $t \in \mathbb{N}$ and $n \geq 3t+1$. Protocol 3.2 is an n-party reliable broadcast protocol such that for input of length $L > n/3 \cdot (\log \frac{n^3}{\epsilon})$ bits tolerates t malicious parties and requires the transmission of $O(nL)$ bits. The security is unconditional, and the probability of error is ϵ.*

Protocol 3.2 works in the private channel model, i.e., when the adversary cannot see the messages exchanged between honest parties (while it can arbitrarily delay them). In Section 3.1 we add one more round to the protocol and remove this assumption.

We recall that in the asynchronous model, the adversary can arbitrarily delay the transmission of messages between honest parties. Yet, each message from an honest party to another honest party would eventually arrive. The adversary can send arbitrary messages, and therefore there is no guarantee on the messages sent from corrupted parties to honest parties.

Before proceeding to the protocol, we describe some writing conventions for asynchronous protocols, following [CR93]. The protocol is a sequence of instructions. Upon activation, the player scans all instruction in the specified order. Each instruction has one of the three following possible forms:

- ⟨instruction⟩. Here the instruction is carried out at the first activation of the protocol.
- `Wait until` ⟨condition⟩. `Then` ⟨instruction⟩. If the condition is satisfied, and this instruction was not executed in the previous activation, then the instruction is execution. Otherwise, the instruction is ignored.
- `If` ⟨condition⟩ `then` ⟨instruction⟩. Here, if the condition is satisfied, then the instruction is execution, even if it was already executed in a previous activation.

Protocol 3.2: Reliable Broadcast for $t < n/3$ (asynchrony)

- **Input:** The dealer holds $t+1$ field elements $a_0, \ldots, a_t \in \mathbb{F}$.
- **Initialization:** Each P_i sets $F_i = F_i' = \perp$, $\mathsf{Agree_i} = \emptyset$.
- **The protocol:**
  1. **The dealer:** Encode $F(x) = \sum_{i=0}^{t} a_i x^i$ and send $F(x)$ to each party P_i.
  2. **Each party P_i:** Wait until a polynomial is received from the dealer, and set it as F_i. Then, send to each party P_j the point $(\beta_{i,j}, F_i(\beta_{i,j}))$ for a random $\beta_{i,j} \in \mathbb{F}$.
  3. **Each party P_i:**
     (a) Wait until the message $(\beta_{j,i}, \gamma_{j,i})$ is received from party P_j. If $F_i(\beta_{j,i}) = \gamma_{j,i}$ then add j to Agree_i.
     (b) Wait until $|\mathsf{Agree}_i| \geq 2t+1$. Then, P_i is set itself as `happy`. Moreover, it sends `Happy` to each party P_j.
  4. **Each party P_i:**
     (a) Wait until P_i is `happy`, and $2t+1$ messages of `Happy` were received from parties that are in Agree_i, then set $F_i'(x) := F_i(x)$.
     Moreover, send $(\texttt{YourPoint}, F_i(\alpha_j))$, $(\texttt{Reconstruct}, (\alpha_i, F_i(\alpha_i)))$ and the message `Ready` to each party P_j, and move to Output step.
  5. **Each party P_i that did not send `Ready`:**
     (a) Wait until $t+1$ messages $(\texttt{YourPoint}, \gamma_i)$ with the same value γ_i are received. Then, send to each other party $(\texttt{Reconstruct}, (\alpha_i, \gamma_i))$.

(b) If P_i sent already $(\texttt{Reconstruct}, (\alpha_i, \gamma_i))$ but still did not send a `Ready` message, and upon each time a $(\texttt{Reconstruct}, (\cdot, \cdot))$ message arrives, then:
If a total of $2t+1$ messages $(\texttt{Reconstruct}, (\alpha_j, \gamma_j))$ arrived, then use Reed-Solomon decoding procedure to find the unique degree-t polynomial $G_i(x)$ for which $G_i(\alpha_j) = \gamma_j$ for at least $2t+1$ points. If such a polynomial exists, then set $F'_i(x) := G_i(x)$ and send $(\texttt{YourPoint}, F'_i(\alpha_k))$ and `Ready` to each party P_k.
If no such polynomial exists, then wait to receive more $(\texttt{Reconstruct}, (\cdot, \cdot))$ messages.

- **Output – each party P_i:** If $F'_i(x) \neq \perp$ and you have sent `Ready`, and once a total of $2t+1$ `Ready` messages were received (including yourself), output $F'_i(x)$.

Proof of Theorem 3.1:

Validity: We claim that if the dealer is honest then all honest parties output the same polynomial $F(x)$ that the dealer holds as input. We show:

Claim 3.3. *The following holds:*

1. *The first honest party that sends the message* `Ready` *to all parties holds the polynomial $F(x)$ that the dealer holds as input.*
2. *For every $i \in [n]$, the ith honest party that sends the message* `Ready` *to all parties hold the same polynomial $F(x)$ as the first honest party that sent* `Ready`*.*

Proof: There are two options that an honest party would send the `Ready` message:

1. If the party is `happy` and received at least $2t+1$ `Happy` messages, then it holds the same polynomial that it has originally received from the dealer. When $2t+1$ `Ready` messages would arrive, the party would terminate and output that polynomial.
2. If the party has received $2t+1$ messages of the form $(\texttt{Reconstruct}, (\cdot, \cdot))$ and there exists a unique decoding, then the party sets its polynomial to output to the decoded polynomial, and sends the message `Ready` to all other parties.

Clearly, the first honest party that sent `Ready` message must have received $2t+1$ `Happy` messages, since otherwise there are not $2t+1$ messages of the form $(\texttt{Reconstruct}, (\cdot, \cdot))$ sent. This is because a party sends `Reconstruct` only together with a `Ready` message, and no honest party yet sent a `Ready` message. This party holds the same polynomial $F(x)$ that the dealer holds as input.

Now, assume (by induction) that the first i honest parties that sent `Ready` hold the same polynomial $F(x)$ as the dealer holds as input. We claim that the $(i+1)$th party that sends `Ready` holds the same polynomial $F(x)$. If the party sends `Ready` because it receives $2t+1$ `Happy` messages, then it must hold the polynomial $F(x)$ which it has received from the dealer. If the party sends `Ready` because it received $2t+1$ messages $(\texttt{Reconstruct}, (\cdot, \cdot))$ then the honest parties that sent these messages must have send `Ready` messages already (since those are sent together with `Reconstruct`) and by our assumption, those honest parties hold the polynomial $F(x)$. As a result, the only possible polynomial of degree-t that can be decoded is the polynomial $F(x)$. □

The above shows that all honest parties that sends `Ready` message hold the same polynomial $F(x)$ that the dealer holds as input. We also claim that all honest parties would eventually terminate. For that we show that there is a path in which the execution terminates. All honest parties receive the same polynomial from the dealer and send a random point to each other. The adversary might introduce delays, but if a party does not terminate earlier due to unique decoding,

it would eventually receive $2t+1$ "good points" and send a `Happy` message. Moreover, again, if not terminate earlier due to unique decoding, every honest party would (eventually) receive $2t+1$ `Happy` messages. We are guaranteed therefore that all honest parties will send the `Ready` message, eventually, and therefore eventually all honest parties will terminate.

Termination and non-equivocation: Assume that an honest party P_j terminates with output $F'_j(x)$. We will show that all other honest parties must terminate with the same polynomial $F'_j(x)$.

P_j terminates only if it has received $2t+1$ message `Ready`. This implies that there is a set of parties S of honest parties of cardinality at least $t+1$ that sent `Ready` message to P_j. Each honest party sends, together with the `Ready` message, also a message `Reconstruct` and `YourPoint` to each other party. We will show that all honest parties that have sent `Ready` message must hold the same polynomial (except for probability ϵ). Assuming this is true, each party in S sent to each other honest party P_j the message $(\texttt{YourPoint}, \gamma_j)$ with the same value γ_j, i.e., P_j received the same point at least $t+1$ times. Then, it forwards that point as a `Reconstruct` message to each other honest party.

This implies that each honest party eventually sends a `YourPoint` message on the same polynomial, and therefore all honest parties eventually receive $2t+1$ points on the same polynomial $F'_j(x)$. The robust interpolation then succeeds and results with $F'_j(x)$, and each honest party eventually sends also a message `Ready`. As a result, eventually, each honest party will receive $2t+1$ messages `Ready` and terminate.

To conclude, we claim that at any point of time, all honest parties that sent the `Ready` message hold the same polynomial with all but probability ϵ. This is similar to Claim 3.3. All we have to show is that all honest parties that are `happy` hold the same polynomial. This clearly holds for an honest dealer (and with probability 1) whereas for a corrupted dealer this holds with all but probability ϵ. We have:

Claim 3.4. *If the dealer is corrupted, then all honest parties that are* `happy` *in Round 3 hold the same polynomial $F(x)$, except for a probability $\binom{n}{2} \cdot \frac{t}{|\mathbb{F}|}$.*

Proof: As in the proof of Lemma 2.3, for every two distinct and fixed polynomials $f(x), g(x)$ of degree-t it holds that $\Pr_{\beta \leftarrow \mathbb{F}}[f(\beta) = g(\beta)] = \frac{t}{|\mathbb{F}|}$. If there are two honest parties that do not hold the same probability then it must be the some honest party received a point that is "correct" from a party that does not hold the same polynomial, which occurs with probability at most $t/|\mathbb{F}|$. The claim then holds by a union bound over all pairs of parties.

We note that this assumes that the channel between the two honest parties is private. Otherwise, the adversary might choose the polynomial $F_j(x)$ for some party P_j only after it saw the point $\beta_{i,j}$ from P_i. □

This concludes the proof of Theorem 3.1. □

3.1 Reliable Broadcast without Assuming Private Channels

Protocol 3.2 works in the private channels model, where the adversary might choose the polynomials it sends to some honest party P_j based on the the choice of $\beta_{i,j}$ the party P_j receives from some honest P_i. Therefore, we rewrite the first steps of the protocol:

1. **The dealer:** Encode $F(x) = \sum_{i=0}^{t} a_i x^i$ and send $F(x)$ to each party P_i.
2. **Each party P_i:** Wait until a polynomial is received from the dealer, and set it as F_i. Then, send MessageRecieved to each party P_j.

3. **Each party P_i:** If already received a polynomial from the dealer, and upon receiving the message MessageRecieved from P_j, send to P_j the point $(\beta_{i,j}, F_i(\beta_{i,j}))$ for a random $\beta_{i,j} \in \mathbb{F}$.

4. Continue Protocol 3.2 from Step 3.

Note that now for every pair of honest parties, the two parties check that the polynomials agree only after confirming receiving them from the dealer. Thus, the two polynomials are fixed and therefore if they are not the same, they agree on a random point with probability at most $t/|\mathbb{F}|$ as in Claim 3.4.

Acknowledgement

We thank Sourav Das, Xiang Zhuolun and Ling Ren for pointing out the need to address private and non-private channels.

References

[AJM+21] Ittai Abraham, Philipp Jovanovic, Mary Maller, Sarah Meiklejohn, Gilad Stern, and Alin Tomescu. Reaching consensus for asynchronous distributed key generation. In *Proceedings of the 2021 ACM Symposium on Principles of Distributed Computing*, PODC'21, page 363–373, New York, NY, USA, 2021. Association for Computing Machinery.

[BDH10a] Michael Ben-Or, Danny Dolev, and Ezra N. Hoch. Brief announcement: Simple gradecast based algorithms. In *DISC*, volume 6343 of *Lecture Notes in Computer Science*, pages 194–197. Springer, 2010.

[BDH10b] Michael Ben-Or, Danny Dolev, and Ezra N. Hoch. Simple gradecast based algorithms. *CoRR*, abs/1007.1049, 2010.

[Bra87] Gabriel Bracha. Asynchronous byzantine agreement protocols. *Inf. Comput.*, 75(2):130–143, November 1987.

[CR93] Ran Canetti and Tal Rabin. Fast asynchronous byzantine agreement with optimal resilience. In S. Rao Kosaraju, David S. Johnson, and Alok Aggarwal, editors, *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing, May 16-18, 1993, San Diego, CA, USA*, pages 42–51. ACM, 1993.

[CT05] C. Cachin and S. Tessaro. Asynchronous verifiable information dispersal. In *24th IEEE Symposium on Reliable Distributed Systems (SRDS'05)*, pages 191–201, 2005.

[DXR21] Sourav Das, Zhuolun Xiang, and Ling Ren. Asynchronous data dissemination and its applications. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, CCS '21, page 2705–2721, New York, NY, USA, 2021. Association for Computing Machinery.

[FGH+02] Matthias Fitzi, Daniel Gottesman, Martin Hirt, Thomas Holenstein, and Adam Smith. Detectable Byzantine Agreement secure against faulty majorities. In *Proc. 21st ACM Symposium on Principles of Distributed Computing — PODC 2002*, pages 118–126, 7 2002.

[FLM85] Michael J. Fischer, Nancy A. Lynch, and Michael Merritt. Easy impossibility proofs for distributed consensus problems. In *Proceedings of the Fourth Annual ACM Symposium on Principles of Distributed Computing*, PODC '85, page 59–70, New York, NY, USA, 1985. Association for Computing Machinery.

[FM88] Paul Feldman and Silvio Micali. Optimal algorithms for byzantine agreement. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, page 148–161, New York, NY, USA, 1988. Association for Computing Machinery.

[KK09] Jonathan Katz and Chiu-Yuen Koo. On expected constant-round protocols for byzantine agreement. *J. Comput. Syst. Sci.*, 75(2):91–112, February 2009.

[Ree60] Gustave Reed, Irving S.; Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

[Sch80] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In Edward W. Ng, editor, *Symbolic and Algebraic Computation, EUROSAM '79, An International Symposiumon Symbolic and Algebraic Computation, Marseille, France, June 1979, Proceedings*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer, 1979.