Round-Optimal and Efficient Verifiable Secret Sharing

Matthias Fitzi[1⋆], Juan Garay[2⋆⋆], Shyamnath Gollakota[3⋆⋆⋆], C. Pandu Rangan[3†], and Kannan Srinathan[4]

[1] Department of Computer Science, Aarhus University, Denmark.
fitzi@daimi.au.dk
[2] Bell Labs – Lucent Technologies, 600 Mountain Ave., Murray Hill, NJ 07974.
garay@research.bell-labs.com
[3] Department of Computer Science and Engineering, IIT Madras, India.
{shyam@cse.iitm, rangan@iitm}.ernet.in
[4] International Institute of Information Technology, Hyderabad, India.
srinathan@iiit.ac.in

Abstract. We consider perfect verifiable secret sharing (VSS) in a synchronous network of n processors (players) where a designated player called the *dealer* wishes to distribute a secret s among the players in a way that no t of them obtain any information, but any $t+1$ players obtain full information about the secret. The round complexity of a VSS protocol is defined as the number of rounds performed in the sharing phase. Gennaro, Ishai, Kushilevitz and Rabin showed that three rounds are necessary and sufficient when $n > 3t$. Sufficiency, however, was only demonstrated by means of an inefficient (i.e., exponential-time) protocol, and the construction of an efficient three-round protocol was left as an open problem.

In this paper, we present an efficient three-round protocol for VSS. The solution is based on a three-round solution of so-called *weak verifiable secret sharing* (WSS), for which we also prove that three rounds is a lower bound. Furthermore, we also demonstrate that one round is sufficient for WSS when $n > 4t$, and that VSS can be achieved in $1 + \varepsilon$ amortized rounds (for any $\varepsilon > 0$) when $n > 3t$.

1 Introduction

Secret sharing [2, 9] is one of the most important primitives used for the construction of secure multi-party protocols. In secret sharing, a "dealer" wants to share a secret s among a set of n players such that no set of t players will be

⋆ Supported by SECOQC, Secure Communication based on Quantum Cryptography, under the Information Societies Technology Programme of the European Commission, IST-2003-506813.
⋆⋆ Work partly done while visiting the Centre de Recerca Matemàtica, Barcelona.
⋆⋆⋆ Work partly done at Bell Labs India, Bangalore
† Work partly done while visiting Bell Labs, Murray Hill, supported by DIMACS.

able to reconstruct the secret while any set of $t+1$ or more players will be able to reconstruct the secret by combining their shares.

Verifiable secret sharing [4] (VSS) extends ordinary secret sharing for the use in presence of active corruption where an adversary may corrupt up to t players in an arbitrary way. In VSS, it is required that no t players get any information about the secret whereas the n players together can reliably reconstruct the secret even if t of them deliver wrong information.

Prior work. Secret sharing was introduced in [2, 9] together with a perfectly secure solution for any number $n > t$ of players in the presence of passive corruption, i.e., where no t players get any Shannon information about secret s and any $t+1$ players get full information about s.

On the other hand, perfectly secure VSS is (efficiently) achievable if and only if $n > 3t$ [1]. When additionally given a broadcast channel among the players, unconditionally secure VSS (with negligible error) can be achieved if $n > 2t$ [8]. As a building block for the VSS protocol in [8], a "degraded" variant of VSS is introduced called *weak* verifiable secret sharing (WSS), where the reconstructed value may also be some default value, in case the dealer is corrupted.

VSS has been extensively studied. Of relevance to our work is the study of the problem's *round complexity* by Gennaro, Ishai, Kushilevitz and Rabin [5], who give tight bounds for perfectly secure VSS. Specifically, it is shown that for $n > 4t$ one round is sufficient when $t = 1$ and that two rounds is a tight bound for general t. For the optimal $n > 3t$, it is shown that three rounds is sufficient as well as necessary; the protocol achieving it, however, requires exponential time. The existence of efficient three-round protocols was left as an open problem.

Our contributions. In this paper, we solve this open problem by presenting an efficient three-round protocol for VSS perfectly secure for $n > 3t$. The solution is based on a three-round protocol for WSS which we demonstrate to be round optimal itself, by first showing three-round optimality of a problem that we call *weak secure multicast* (WSM), and then showing a reduction to WSS. Furthermore, we show that perfectly secure WSS is efficiently achievable in one round when $n > 4t$ (and $t > 1$). Finally, we present a simple protocol for perfectly secure VSS with amortized $1+\varepsilon$ rounds for any $\varepsilon > 0$ when $n > 3t$ — which is of special interest for secure multi-party computation [1, 3], where a large number of VSS protocols are run sequentially.

Organization of the paper. We start in Section 2 by presenting the model and definitions of the secret sharing problems we are considering. Section 3 is dedicated to WSS, where we present round-optimal protocols for the cases $n > 3t$ and $n > 4t$. We derive the efficient round-optimal and player-optimal protocol for VSS in Section 4. The amortized $(1+\varepsilon)$-round protocol is described in Section 5. We conclude with some final remarks in Section 6. For ease of readability, the round optimality proof for player-optimal WSS based on WSM is presented in the appendix.

2 Model and Definitions

We assume a set $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ of n players including dealer D, say, $D = P_1$, and assume the standard model of a fully connected network of pairwise secure channels, plus a common broadcast channel, which can be used to force a player to send the same message to all the other players. Furthermore, we assume the presence of an active adversary who may corrupt up to t of the players in an arbitrarily malicious way. Such a corrupted player is called *dishonest* whereas an uncorrupted player is called *honest*. The adversary is modeled to be *rushing* (i.e., it can base the dishonest players' messages for round r on the honest players' messages of the same round), *adaptive* (the adversary can adaptively corrupt players as the protocol proceeds), but *non-mobile* (over the whole period, the adversary corrupts at most t different players). We call such an adversary a "t-adversary." We demand perfect security, i.e., that the resulting protocol has zero error and that no Shannon information is leaked to the adversary.

We consider several forms of secret sharings with different security properties. As in [5], the protocols for all of them have the same following two-phase structure: In a primary phase, the dealer D distributes a secret s, while in a second, later phase, the players cooperate in order to retrieve it. More specifically, the structure is as follows:

Sharing phase: The dealer initially holds secret $s \in \mathcal{K}$ where $\mathcal{K}$ is a finite field of sufficient size; and each player P_i finally holds some private information v_i (possibly consisting of several field elements).

Reconstruction phase: In this phase, each player P_i reveals (some of) his private information v_i. Then, on the revealed information v_i' (a dishonest player may reveal $v_i' \neq v_i$), a reconstruction function is applied in order to compute the secret, $s = \mathrm{Rec}(v_1', \cdots, v_n')$.

The sharing phase as well as the reconstruction phase may consist of several communication rounds. We model communication along the lines of [5] where, in each round, a player can privately send messages to other players and/or broadcast a message to all players. With respect to this model, the round complexity of a secret-sharing protocol is defined as the number of such communication rounds that the protocol requires *in the sharing phase*.

Common requirements. The following requirements have to be satisfied by all secret-sharing protocols we discuss in this paper.

Privacy: If D is honest, then the adversary's view during the sharing phase reveals no information about s. More formally, the adversary's view is identically distributed under all different values of s.

Correctness: If D is honest, then the reconstructed value is equal to the secret s.

Depending on the particular "strength" of the secret-sharing protocol, different commitment properties are required.

Verifiable secret sharing (VSS). An n-player protocol is called a (perfect) (n, t)-VSS protocol if, for any t-adversary, the following condition holds in addition to the privacy and correctness conditions:

COMMITMENT: After the sharing phase, a unique value s^* is determined which will be reconstructed in the reconstruction phase; i.e., $s^* = \mathrm{Rec}(v'_1, \cdots, v'_n)$ regardless of the views provided by the dishonest players.

Weak verifiable secret sharing (WSS). An n-player protocol is called a (perfect) (n, t)-WSS protocol if, for any t-adversary, the following condition holds in addition to the privacy and correctness conditions:

WEAK COMMITMENT: After the sharing phase there is a unique value $s^* \in \mathcal{K}$ such that either s^* or default value $\perp \notin \mathcal{K}$ will be reconstructed in the reconstruction phase; i.e., $\mathrm{Rec}(v'_1, \cdots, v'_n) \in \{\perp, s^*\}$ regardless of the views provided by the dishonest players.

Round complexity and efficiency. As in [5], we define the round complexity of a secret-sharing protocol as the number of communication rounds in its *sharing phase* — reconstruction can always be done in a single round by having each player reveal all the information he has. A VSS protocol is *efficient* if the total computation and communication performed by all honest players is polynomial in n and the size of the secret.

3 Round-Optimal WSS

We begin by giving a three-round (n, t)-WSS protocol for $n > 3t$, which is optimal, followed by a one-round (n, t)-WSS protocol for $n > 4t$.

3.1 Round-optimal WSS for $\mathbf{n > 3t}$

The protocol is based on the four-round (n, t)-VSS protocol for $n > 3t$ given in [5]; essentially, it consists of that protocol's first three rounds, with a modified reconstruction phase. Unlike the protocol in [5], where inconsistencies between the shares of honest players are eliminated by using error correcting codes, we use a different technique to detect the dishonest players who deliver false information in the reconstruction phase.

We now present the protocol. The secret s is assumed to be taken from a finite field $\mathcal{K}$, $|\mathcal{K}| > n$; additionally, $1, 2, ..., n$ are interpreted as (arbitrary) distinct non-zero field elements. We call this protocol $(\frac{n}{3})$-`WSS`.[1]

[1] For simplicity; strictly speaking, it should be "$\lfloor \frac{n-1}{3} \rfloor$-`WSS`."

Sharing phase: The sharing phase consists of the following three rounds:

1. – D chooses a random bivariate polynomial $F \in \mathcal{K}[x, y]$ of degree at most t in each variable, satisfying $F(0, 0) = s$. D sends to each player P_i the (univariate) polynomials $f_i(x) = F(x, i)$ and $g_i(y) = F(i, y)$.
   – Player P_i sends to each player P_j an independent random "pad" r_{ij} picked uniformly from $\mathcal{K}$.
2. Player P_i broadcasts:
   – $a_{ij} = f_i(j) + r_{ij}$ $\quad$ (r_{ij} is the pad P_i sent to P_j)
   – $b_{ij} = g_i(j) + r_{ji}$ $\quad$ (r_{ji} is the pad P_i received from P_j)
3. For each pair $a_{ij} \neq b_{ji}$, the following happens:
   – P_i broadcasts $\alpha_{ij} = f_i(j)$
   – P_j broadcasts $\beta_{ji} = g_j(i)$
   – D broadcasts $\gamma_{ij} = F(j, i)$

   A player is said to be *unhappy* if the value which he broadcast does not match the dealer's value. If there are more than t unhappy players, disqualify the dealer and stop.[2] $\diamond$

Reconstruction phase: Every happy player P_i broadcasts his polynomials $f_i(x) = F(x, i)$ and $g_i(y) = F(i, y)$.

Each player P_i now constructs a *consistency graph* G over the set of happy players such that there exists an edge between P_j and P_k in G if and only if $f_j(k) = g_k(j)$ and $g_j(k) = f_k(j)$. Since these polynomials are broadcast, every player P_i constructs the same graph G.

Now each player P_i constructs a set $CORE$ of players as follows. Initially, all the players in G whose node degree is at least $n - t$ are inserted into the set. Next, players in $CORE$ consistent with less than $n - t$ other players in $CORE$ are removed. This process continues until no more players can be removed from the set. If the resulting $CORE$ set contains less than $n - t$ elements then P_i outputs $\perp$ — otherwise, P_i reconstructs the polynomial $F^*(x, y)$ defined by any $t + 1$ players in $CORE$, and the secret $s^* = F^*(0, 0)$ is reconstructed. $\diamond$

That finishes the description of protocol $(\frac{n}{3})$-`WSS`. We now show that it is a (n, t)-WSS protocol for $n > 3t$.

As suggested by the construction of graph G above, we say that (the polynomials of) two players P_i and P_j are consistent if the corresponding values of their polynomials (as opened in the reconstruction phase) match, i.e., if $f_i(j) = g_j(i)$ and $g_i(j) = f_j(i)$. Similarly, we say a player P_i is consistent with bivariate polynomial $F(x, y)$ if $f_i(x)$ and $g_i(y)$ lie on $F(x, y)$, i.e., $f_i(x) = F(x, i)$ and $g_i(y) = F(i, y)$. We first prove the following about players in $CORE$.

Lemma 1. *If $|CORE| \geq n - t$, then all the players in CORE are consistent with a polynomial fixed at the end of the sharing phase.*

---
[2] If necessary, the secret can be assigned a public default value when the dealer gets disqualified.

Proof. At the end of the sharing phase, all the honest happy players are consistent with each other and their shares define a unique bivariate polynomial $F^H(x,y)$ with degree at most t in both variables. To be in $CORE$, every player P_i must be consistent with (at least) $n-t$ players in $CORE$. Moreover, every player in $CORE$ is happy. So there are at least $n-2t \geq t+1$ honest players in $CORE$ with whom P_i is consistent. These $t+1$ players define a unique polynomial $f_i(x)$ of degree at most t for P_i, which is in turn consistent with $F^H(x,y)$. Thus, the polynomial provided by P_i must be $f_i(x)$. Therefore, every player in $CORE$ is consistent with $F^H(x,y)$. □

Theorem 1. *Protocol* $(\frac{n}{3})$-`WSS` *is an efficient, three-round* (n,t)*-WSS protocol for* $n > 3t$.

Proof. Number of rounds and efficiency are evident. We prove the WSS properties in turn.

- Privacy: We only need to consider the case when D is honest. Since D distributes consistent information, any pair P_i and P_j of honest players publishes the same mutual padded values. Thus, due to the randomness of the pads, the adversary's view is indistinguishable under different secrets.
- Correctness: If D is honest then all (at least $n-t$) honest players will be happy, and D will not be disqualified in the sharing phase. Since all honest players are mutually consistent, they all end up in set $CORE$ whereas a dishonest player can only be in $CORE$ by revealing his correct polynomials. Thus the information revealed by the players in $CORE$ is consistent with polynomial F and $s^* = F^*(0,0) = F(0,0) = s$ is reconstructed.
- Weak commitment: We need only consider the case when D is dishonest. If $|CORE| < n-t$ then all the players compute $s^* = \perp$ and weak commitment is satisfied. On the other hand, consider $|CORE| \geq n-t$. In this case, it directly follows from Lemma 1 that the secret constructed is the free term of $F^H(x,y)$.

□

We now state a property of the above protocol which will be used in the correctness proof for our VSS protocol in the next section.

Lemma 2. *If the dealer is not disqualified in the reconstruction phase of* $(\frac{n}{3})$-`WSS`, *then the polynomial* $F^*(x,y)$ *reconstructed in that phase is consistent with all the honest happy players.*

Proof. As proved in Lemma 1, the polynomial reconstructed at the end of the reconstruction phase is $F^H(x,y)$. This $F^H(x,y)$ is defined as the polynomial constructed by any $t+1$ honest happy players. Thus the polynomial constructed is consistent with all the honest happy players. □

Round optimality. The proof of the following theorem is given in Appendix A.

Theorem 2. *For* $n \leq 4t$ $(t > 1)$*, there is no perfect* (n,t)*-WSS protocol requiring less than three rounds.*

3.2 Round-optimal WSS for n > 4t

When $n > 4t$, perfectly secure WSS can be efficiently achieved in one round as follows.

Sharing phase: D chooses a random bivariate polynomial $F \in \mathcal{K}[x, y]$ of degree at most t in each variable satisfying $F(0, 0) = s$ and sends to each player P_i the polynomials $f_i(x) = F(x, i)$ and $g_i(y) = F(i, y)$. □

Reconstruction phase: Player P_i broadcasts the polynomials $F(x, i)$ and $F(i, y)$ he received in the sharing phase. Player P_i constructs a consistency graph G and a set $CORE$ as in protocol $(\frac{n}{3})$-`WSS`. Finally, if $|CORE| < n - t$, P_i computes $\perp$; otherwise, $s^* = F^*(0, 0)$, where $F^*(0, 0)$ is the unique bivariate polynomial of degree at most t in both variables defined by any $t + 1$ players in $CORE$. □

Theorem 3. *Perfectly secure WSS is efficiently achievable in one round when* $n > 4t$.

Proof. We prove that the above protocol achieves the three conditions of WSS.

- Privacy: Privacy is obvious since the adversary only gets information about at most t players' shares.
- Correctness: If the dealer D is honest then he sends correct shares to all the players. Thus, at the end of the reconstruction phase, set $CORE$ contains (at least) $n - t$ honest players, D is not disqualified, and the secret s is reconstructed since any other secret s^* can be consistent with at most $2t < n - t$ players.
- Weak commitment: We need only consider the case when D is dishonest. If $|CORE| < n - t$, then all the players compute $\perp$ and weak commitment is satisfied. On the other hand, assume that $|CORE| \geq n - t$. This implies that there is a set $\mathcal{C}$ of at least $n - 2t$ consistent honest players defining a unique secret s^*. Out of set $\mathcal{C}$ at most t players can be consistent with a polynomial defining a different secret $s' \neq s^*$. Thus at most $|\mathcal{P} \setminus \mathcal{C}| + t \leq n - (n - 2t) + t = 3t < n - t$ players overall can be consistent with secret s' — implying weak commitment on s^*.

□

4 Round-Optimal VSS for n > 3t

We now present an efficient three-round (n, t)-VSS protocol for $n > 3t$. Its round optimality follows from the lower bound in [5].

We first give some of the intuition behind our protocol. Overall, we follow the approach in [5] (and in the previous section), where the dealer first hides the secret in a bivariate polynomial $F(x, y)$, and each player P_i gets the respective univariate polynomials $F(x, i)$ and $F(i, y)$ as his secret information. Then, every pair of players compare their common shares by "blinding" them with a random pad and then broadcasting them. In the reconstruction phase the random pads are revealed, allowing the players to compute the shares and finally reconstruct the secret. However, our twist is as follows. In order to guarantee that each player P_i's random pads get revealed consistently, P_i shares a random field element using a round-optimal, player-optimal (n, t)-WSS protocol — namely, protocol $(\frac{n}{3})$-`WSS` from the previous section, and chooses his pads as *points on the respective polynomial*, as opposed to independently at random as in [5] and in the previous section for WSS. Players whose $(\frac{n}{3})$-`WSS` protocol instance fails, also get disqualified from the main protocol; on the other hand, players whose protocol instance succeeds enable the reconstruction of all the pads, and in turn the computation of the main shares. Using these multiple instances of an (n, t)-WSS protocol also replaces the need for explicit error correcting codes, as required by some of the VSS protocols (the efficient ones) in [5].

We now present our VSS protocol in detail. We will use superscript "W" to denote the quantities corresponding to the $(\frac{n}{3})$-`WSS` protocols that are run in order to WSS the players' random pads. We call the resulting VSS protocol $(\frac{n}{3})$-`VSS`.

Sharing phase: The sharing phase consists of the following three rounds:

1. – Dealer D chooses a random bivariate polynomial $F \in \mathcal{K}[x, y]$ of degree at most t in each variable satisfying $F(0, 0) = s$. D sends to P_i the polynomials $f_i(x) = F(x, i)$ and $g_i(y) = F(i, y)$.
   – Player P_i, $i = 1, \ldots, n$, selects a random value r_i and starts an instance of $(\frac{n}{3})$-`WSS` acting as a dealer in order to share r_i by means of bivariate polynomial $F_i^W(x, y)$ $(F_i^W(0, 0) = r_i)$. We call this instance $(\frac{n}{3})$-`WSS`$_i$. Round 1 of $(\frac{n}{3})$-`WSS`$_i$ is run.
2. Player P_i broadcasts the following:
   – $a_{ij} = f_i(j) + F_i^W(0, j)$
   – $b_{ij} = g_i(j) + F_j^W(0, i)$

   Concurrently, round 2 of $(\frac{n}{3})$-`WSS`$_i$, $i = 1, \ldots, n$, also takes place.
3. For each pair $a_{ij} \neq b_{ji}$ the following happens:
   – P_i broadcasts $\alpha_{ij} = f_i(j)$
   – P_j broadcasts $\beta_{ji} = g_j(i)$
   – D broadcasts $\gamma_{ij} = F(j, i)$

   Concurrently, round 3 of $(\frac{n}{3})$-`WSS`$_i$, $i = 1, \ldots, n$, also takes place.

   A player is said to be *unhappy* if the value that he broadcast does not match the dealer's value. If there are more than t unhappy players, disqualify D and stop.

Local computation:
– Let $\mathcal{H}$ denote the set of happy players. Remove from $\mathcal{H}$ each player P_i who gets disqualified as the dealer in protocol instance $(\frac{n}{3})$-`WSS`$_i$. Now, if $|\mathcal{H}| < n - t$ then disqualify D and stop.

- For the remaining players, let $\mathcal{H}_i^W$ denote the set of happy players in instance $(\frac{n}{3})$-$\mathtt{WSS}_i$. For each player $P_i \in \mathcal{H}$, check that there exist at least $n-t$ players in $\mathcal{H}$ who are also in $\mathcal{H}_i^W$; if not, remove P_i from $\mathcal{H}$. Let us call this final set $CORE_{Sh} := \mathcal{H}$. If $|CORE_{Sh}| < n-t$ then disqualify D and stop. $\diamond$

Reconstruction phase: For each $P_i \in CORE_{Sh}$, run the reconstruction phase of $(\frac{n}{3})$-$\mathtt{WSS}_i$, concurrently.

Local computation: Now each player P_i constructs a set $CORE_{Rec}$ as follows. Initially, $CORE_{Rec} := CORE_{Sh}$.

- Remove from $CORE_{Rec}$ every player P_i such that the outcome of $(\frac{n}{3})$-$\mathtt{WSS}_i$ equals $\perp$.
- For every $P_i \in CORE_{Rec}$, use the values a_{ij} he broadcast in round two of the sharing phase to compute

$$f_i(j) = a_{ij} - F_i^W(0, j), \quad 1 \le j \le n. \tag{1}$$

- Interpolate these points. Check that the resulting polynomial $f_i(x)$ is a polynomial of degree at most t. If not, remove P_i from $CORE_{Rec}$.
- Reconstruct the secret by taking any $t+1$ polynomials $f_i(x)$, $P_i \in CORE_{Rec}$, to obtain $F^*(x, y)$, and compute $s^* = F^*(0, 0)$. $\diamond$

Lemma 3. *If D is honest, then $CORE_{Sh}$ contains all the honest players.*

Proof. First, since D is honest, all honest players are happy with respect to $F(x, y)$. Thus, initially, $\mathcal{H}$ contains all the honest players. Similarly, the set of happy players corresponding to $(\frac{n}{3})$-$\mathtt{WSS}_i$ started by a honest player P_i will contain all the honest players. Thus $|\mathcal{H}_i^W| \ge n-t$ and all the honest players will be in $\mathcal{H}$. Also, since all honest players are mutually consistent, an honest player P_i is consistent with $n-t$ players in $\mathcal{H}$ and thus $P_i \in CORE_{Sh}$. $\square$

Lemma 4. *If D does not get disqualified in the sharing phase then all the honest players in $CORE_{Sh}$ are consistent with each other and, when $|CORE_{Sh}| \ge n-t$, consistently define a unique polynomial $F^H(x, y)$ of degree at most t in each variable. Furthermore, when D is honest, $F^H(x, y) = F(x, y)$.*

Proof. Since the honest players use their pads faithfully there are no inconsistencies between honest players in $CORE_{Sh}$. Furthermore, if $|CORE_{Sh}| \ge n-t$, then there are at least $t+1$ honest players in $CORE_{Sh}$ defining a unique polynomial $F^H(x, y)$. Finally, in case the dealer is honest, it holds that $F^H(x, y) = F(x, y)$. $\square$

Lemma 5. *If D does not get disqualified in the sharing phase then, at the end of the reconstruction phase, there are at least $t+1$ honest players in $CORE_{Rec}$.*

Proof. In the reconstruction phase a player P_i gets removed from $CORE_{Rec}$ in only two cases: 1) the reconstruction phase of $(\frac{n}{3})$-$\mathtt{WSS}_i$ results in $\perp$, or 2) the reconstruction phase of $(\frac{n}{3})$-$\mathtt{WSS}_i$ succeeds but the resulting polynomial $f_i(x)$ is of degree larger than t. By the properties of WSS, both cannot happen with respect to a honest player, and thus at least $n-2t > t$ honest players in $CORE_{Sh}$ remain in $CORE_{Rec}$. $\square$

Lemma 6. *If D does not get disqualified in the sharing phase, then any $t+1$ players in $CORE_{Rec}$ define the same bivariate polynomial.*

Proof. If a dishonest player P_i remains in $CORE_{Rec}$, then the reconstruction phase of $(\frac{n}{3})$-$\mathtt{WSS}_i$ has succeeded. By Lemma 2 this implies that the reconstructed polynomial $F_i^W(x,y)$ is consistent with all the happy honest players with respect to $(\frac{n}{3})$-$\mathtt{WSS}_i$. By Lemma 5 there are at least $t+1$ honest players in $CORE_{Rec}$ who, by Lemma 4, define a unique polynomial $F^H(x,y)$ of degree at most t in both variables. Thus, every player remaining in $CORE_{Rec}$ is consistent with $F^H(x,y)$, and the lemma follows. □

Theorem 4. *Protocol* $(\frac{n}{3})$-$\mathtt{VSS}$ *is an efficient, perfectly secure three-round (n,t)-VSS protocol for $n > 3t$.*

Proof (sketch). We only have to consider the case when D is honest. The number of rounds and polynomial-time computation are immediate. We prove the three VSS properties in turn.

Privacy: Assume that, at the end of the reconstruction phase, the players in $\mathcal{A} \subset \mathcal{P}$, $|\mathcal{A}| \leq t$, are corrupted. Let $\mathrm{View}_{\mathcal{A}}^k$, $1 \leq k \leq 3$, denote the adversary's view after step k of the sharing phase. Note that, for all $P_a \in \mathcal{A}$, the polynomials $F_a^W(x,y)$ are exclusively used in order to blind values already known to the adversary, and therefore we can ignore these polynomials.
After step 2 of the sharing phase, the adversary holds (at most) the following polynomials: $F(x,a)$, $F(a,y)$, $F_i^W(x,a)$, and $F_i^W(a,y)$, and it holds that, for all $P_i, P_j \notin \mathcal{A}$, $H\left(F(x,i)|\,\mathrm{View}_{\mathcal{A}}^2\right) = \log|\mathcal{K}|$, $H\left(F_i^W(j,x)|\,\mathrm{View}_{\mathcal{A}}^2\right) = H\left(F_i^W(0,x)|\,\mathrm{View}_{\mathcal{A}}^2\right) = \log|\mathcal{K}|$. Furthermore, for $P_i, P_j \notin \mathcal{A}$, $i \neq j$, the polynomials $F_i^W(x,y)$ and $F_j^W(x,y)$ are independent.
In step 3, in addition, the polynomials $S_i(x) = F(x,i) + F_i^W(0,x)$ get revealed. That is, each $F(x,i)$ is blinded with an independent polynomial $F_i^W(0,x)$ where $H\left(F_i^W(0,x)|\,\mathrm{View}_{\mathcal{A}}^2\right) = \log|\mathcal{K}|$. Thus, it is still the case that for any $P_i \notin \mathcal{A}$, $H\left(F(x,i)|\,\mathrm{View}_{\mathcal{A}}^3\right) = \log|\mathcal{K}|$, and therefore, $H\left(F(0,0)|\,\mathrm{View}_{\mathcal{A}}^3\right) = \log|\mathcal{K}|$; hence, privacy follows.

Correctness: We only consider the case when D is honest. By Lemma 3, all the honest players will be in $CORE_{Sh}$, thus $|CORE_{Sh}| \geq n-t$, and the dealer is not disqualified in the sharing phase. By Lemma 4, the shares of the honest players in $CORE_{Sh}$ define the dealer's original polynomial $F^H(x,y) = F(x,y)$. Obviously, all honest players remain in $CORE_{Rec}$, and by Lemma 6, $s = F(0,0)$ gets reconstructed from the shares of any $t+1$ players in $CORE_{Rec}$.

Commitment: If D is dishonest and does not get disqualified in the sharing phase, then $|CORE_{Sh}| \geq n-t$ and, by Lemma 5, at least $t+1$ honest players from $CORE_{Sh}$ remain in $CORE_{Rec}$. By Lemma 4, all honest players in $CORE_{Sh}$ consistently define the same polynomial $F^H(x,y)$ after the sharing phase. Thus, the $t+1$ honest players in $CORE_{Sh} \cap CORE_{Rec}$ still uniquely define $F^H(x,y)$ and, by Lemma 6, $s^* = F^H(0,0)$ gets reconstructed from the shares of any $t+1$ players in $CORE_{Rec}$.

□

5 VSS in $(1+\varepsilon)$ Rounds

Depending on the particular application, minimizing the round complexity of a stand-alone protocol might not always be the best way to optimize. In multi-party computation, for example, where a large number of VSS protocols are executed sequentially, it is useful to minimize the overall *amortized* round complexity of the VSS instances.

A number m of sequential (n,t)-VSS executions can be easily achieved in $1+O(\frac{1}{m})$ amortized rounds by "deferring" the commitment as follows. Suppose we have a $k-$round (n,t)-VSS protocol, and we need to execute m instances of it. In an initial phase, dealer D (or all future dealers in the application, respectively) shares (in parallel) a set of random elements $r_1,\ldots,r_m$ using the given (n,t)-VSS protocol. The sharing phase of the j-th execution of the (n,t)-VSS protocol, $j=1,\ldots,m$ then simply consists of the dealer broadcasting a correction term $c_j = s_j - r_j$, where s_j is the secret to be shared in this instance. The correction term c_j can be handled in two different ways:

1. c_j is incorporated in the reconstruction phase. That is, after the reconstruction of random element r_j, each player locally computes $s_j = r_j + c_j$; or
2. the sharing is immediately "corrected" at the end of the sharing phase, by having every player P_i compute $F'_k(x,i) = F_k(x,i) + c_k$ and $F'_k(i,y) = F_k(i,y) + c_k$.

Theorem 5. *Any number m of sequential VSS protocols for $n > 3t$ is efficiently achievable in $m+2$ rounds, thus implying $1+\varepsilon$ amortized rounds per instance for any $\varepsilon > 0$ when m is sufficiently large.*

Proof. Using any k-round (n,t)-VSS protocol the above approach results in $m+k-1$ rounds overall, or $1+\frac{k-1}{m}$ rounds per VSS. In particular, using the round-optimal protocol from Section 4 results in $1+\frac{2}{m}$ rounds per VSS instance. Thus, in order to achieve $1+\varepsilon$ amortized rounds, it is sufficient to choose $m \geq \frac{2}{\varepsilon}$. $\square$

6 Summary

In this paper we gave efficient three-round protocols for perfectly secure WSS and VSS when $n > 3t$, and showed that there is no (n,t)-WSS protocol involving less than three rounds when $n \leq 4t$. Furthermore, we gave an efficient one-round protocol for perfectly secure WSS when $n > 4t$, and demonstrated that perfectly secure VSS can be achieved in $(1+\varepsilon)$ rounds when $n > 3t$.

The following table summarizes the tight bounds on the round complexity of perfectly secure WSS and VSS as given in [5] and in this paper — where round optimality is always achieved efficiently. ("—" stands for impossibility.)

Protocol	Threshold	Number of rounds
WSS	$n \leq 3t$	—
	$3t < n \leq 4t$	3
	$4t < n$	1
VSS	$n \leq 3t$	—
	$3t < n \leq 4t$	3
	$4t < n$ $(t > 1)$	2
	$4t < n$ $(t = 1)$	1

Note that, same as some (but not all) of the protocols in [5], although our solution for VSS fulfills the standard VSS definition, it is not powerful enough to allow for general multi-party computation. In particular, multiplication of shared secrets is not directly possible since the sharing phase of two different VSS invocations may end up in different $CORE_{Sh}$ sets.

Furthermore, note that, also as the protocols in [5], our VSS protocol satisfies the stronger VSS definition in [7] (Definition 3.3.13) requiring that any set of $t+1$ honest players be able to reconstruct the shared secret. This condition is satisfied because any set of $t+1$ honest players can reconstruct the WSS-shared secrets of all players in $CORE_{Sh}$.

Finally, it can be easily seen that our protocols also work with respect to a (possibly corrupted) external dealer while still tolerating t corrupted players among the "share holders."

Acknowledgements

We thank the anonymous reviewers for *TCC '06* for their many helpful comments.

References

1. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 1–10, 1988.
2. G. R. Blakley. Safeguarding cryptographic keys. In *1979 National Computer Conference*, volume 48 of *AFIPS Conference proceedings*, pages 313–317. AFIPS Press, 1979.
3. D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 11–19. ACM Press, 1988.
4. B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science (FOCS '85)*, pages 383–395, 1985.
5. R. Gennaro, Y. Ishai, E. Kushilevitz, and T. Rabin. The round complexity of verifiable secret sharing and secure multicast. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (STOC '01)*, pages 580–589, 2001.

6. R. Gennaro, M. O. Rabin, and T. Rabin. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In *Proceedings of the 17th ACM Symposium on Principles of Distributed Computing (PODC '98)*, pages 101–111, 1998.
7. O. Goldreich. Secure multi-party computation, final (incomplete) draft, version 1.4, Oct. 2002.
8. T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC '89)*, pages 73–85, 1989.
9. A. Shamir. How to share a secret. *Commun. ACM*, 22:612–613, 1979.

A Proof of Theorem 2

We show that for $n \leq 4t$, perfect WSS is not possible in less than three rounds. We do this along the lines of the impossibility proof for two-round VSS in [5]. We first introduce the problem of *weak secure multicast* (WSM) and show that perfectly secure WSM is impossible in less than three rounds when $n \leq 4t$. Finally, we show that r-round WSS implies r-round WSM, thus proving the theorem.

Weak secure multicast (WSM). Consider an n-player protocol among player set $\mathcal{P} = \{P_1, \ldots, P_n\}$ wherein *sender* $D \in \mathcal{P}$ holds an input m and each player in *multicast set* $M \subseteq \mathcal{P}$ $(D \in M)$ finally computes an output. Such a protocol is called a (perfect) *WSM protocol* if, for any t-adversary, the following conditions hold:

Privacy: If all players in M are honest then the adversary learns no information about D's input m.

Correctness: If D is honest then all honest players in M output m.

Weak Agreement: Even if D is dishonest, all dishonest players in M output a value in $\{m^*, \perp\}$, where m^* is an unique element in $\mathcal{K}$ and a distinguished value $\perp \notin \mathcal{K}$.

Similarly to VSS, WSM is the "weak" variant of the *secure multicast* (SM) problem formalized in [5], where the Agreement condition, demanding that all the honest players output the same value even if the sender is dishonest, is replaced by Weak Agreement above.

The proof of Theorem 2 follows by proving the impossibility of the following problem and subsequently reducing it to related problems, the last one being the existence of a two-round WSS protocol.

Lemma 7. *There is no deterministic* 3*-player protocol satisfying the following requirements:*

1. *The protocol is a* $(3, 1)$*-WSM protocol with* M *being the set of all players.*
2. *The protocol has three communication rounds, where only* D *speaks in the first round.*

3. *If all players are honest then the broadcast messages are independent of D's message m.*

The proof of this lemma is identical to the proof of Lemma 7 in [5] for the non-existence of a $(3, 1)$-SM protocol satisfying similar requirements.

Lemma 8. *There is no two-round perfect* $(4, 1)$*-WSM protocol with* $M = \{P_1, P_2, P_3\}$ *(and* $D = P_1$*).*

Proof (sketch). The existence of such a protocol would imply the existence of the protocol specified in Lemma 7. The proof is almost identical to that of Lemma 6 for the impossibility of a two-round $(4, 1)$-SM protocol in [5]. The minor modification is that it is based on our Lemma 7 (instead of their Lemma 7), which accounts for the alternative output $\perp$ of WSM; even though this outcome avoids violation of weak agreement, it still violates correctness. □

Lemma 9. *There is no two-round perfect* $(4, 1)$*-WSS protocol.*

Proof (sketch). Again, the proof of similar Lemma 3 (and thus of Lemma 5) of [5], which reduces the impossibility of a two-round (n, t)-VSS protocol to the impossibility of a two-round (n, t)-SM protocol, can be based on our Lemma 8, directly implying this stronger lemma. □

Finally, the proof of Theorem 2 follows from Lemma 9 by a standard player partitioning and simulation argument.