# Linear VSS and Distributed Commitments Based on Secret Sharing and Pairwise Checks

Serge Fehr[1,⋆] and Ueli Maurer[2]

[1] BRICS⋆⋆, Department of Computer Science, Aarhus University, Denmark
fehr@brics.dk
[2] Department of Computer Science, ETH Zurich, Switzerland
maurer@inf.ethz.ch

**Abstract.** We present a general treatment of all non-cryptographic (i.e., information-theoretically secure) linear verifiable-secret-sharing (VSS) and distributed-commitment (DC) schemes, based on an underlying secret sharing scheme, pairwise checks between players, complaints, and accusations of the dealer. VSS and DC are main building blocks for unconditional secure multi-party computation protocols. This general approach covers all known linear VSS and DC schemes. The main theorem states that the security of a scheme is equivalent to a pure linear-algebra condition on the linear mappings (e.g. described as matrices and vectors) describing the scheme. The security of all known schemes follows as corollaries whose proofs are pure linear-algebra arguments, in contrast to some hybrid arguments used in the literature. Our approach is demonstrated for the CDM DC scheme, which we generalize to be secure against mixed adversary settings (some curious and some dishonest players), and for the classical BGW VSS scheme, for which we show that some of the checks between players are superfluous, i.e., the scheme is not optimal. More generally, our approach, establishing the minimal conditions for security (and hence the common denominator of the known schemes), can lead to the design of more efficient VSS and DC schemes for general adversary structures.

## 1 Introduction

The concept of *secret sharing* was introduced by Shamir [12] as a means to protect a secret simultaneously from exposure and from being lost. It allows a so called *dealer* to share the secret among a set of entities, usually called *players*, in such a way that only certain specified subsets of the players are able to reconstruct the secret (if needed) while smaller subsets have no information about it. While secret sharing only guarantees security against curious players that try to gather information they are not supposed to obtain but otherwise behave honestly, its stronger version *verifiable secret sharing (VSS)*, introduced

⋆ Most of this research was carried out while the author was employed at ETH Zurich. Supported by the Swiss National Science Foundation (SNF).
⋆⋆ Basic Research in Computer Science (www.brics.dk), funded by the Danish National Research Foundation.

M. Yung (Ed.): CRYPTO 2002, LNCS 2442, pp. 565–580, 2002.

in [4], is secure in the following sense against dishonest players (which are of course also curious) and a dishonest dealer that behave in an arbitrary manner.

*Privacy:* If the dealer is honest, then the curious players learn nothing about the secret $k$.

*Correctness:* After the secret is shared, there exists a unique value $k'$ that can be reconstructed by the players (no matter how the dishonest players behave), and for an honest dealer $k'$ is equal to the shared secret $k$.

Reconstruction must work even if the dealer does not cooperate in the reconstruction. If an *efficient* reconstruction of the secret requires the cooperation of the dealer, then such a scheme is called a *distributed commitment (DC)* scheme. In such a scheme a dishonest dealer can prevent the reconstruction by refusing to cooperate, but he cannot achieve that a different secret is reconstructed, not even with the help of the dishonest players. A DC scheme is almost a VSS, except for the efficiency of the reconstruction, since the players could try all possible behaviors of the dealer in the reconstruction.

*Linear* VSS and DC schemes are a main building block for general secure multi-party protocols. Linearity implies that any linear function on shared values can be computed without interaction by each player (locally) computing the linear function on the corresponding individual shares.

The goal of this paper is a unified treatment of (linear) VSS and DC schemes. We present a very natural and general sharing protocol which converts an arbitrary given linear secret sharing scheme into a DC (or VSS) scheme, provided of course that this is possible at all, by enforcing *pairwise* consistency among the shares of the (honest) players. Namely, by pairwise checking, complaining and accusing, it ensures that pairwise linear dependences among the shares that should hold *do* hold. This seems to be not only a very natural but the only possible approach for the construction of secure DC and VSS schemes in our model (i.e. unconditionally secure and zero error probability), and indeed, all known schemes can be seen as concrete instances of this general approach. Then we state the condition under which such a scheme is a secure DC (or VSS) scheme. This characterization is a predicate in the language of pure linear algebra, depending only on the parameters of the underlying secret sharing scheme and of the sharing protocol.

As a consequence, the security of all known schemes (and possibly even all future ones) follow as corollaries whose proofs are linear-algebra arguments, in contrast to some hybrid arguments used in the literature. This is demonstrated for two schemes, for the CDM DC scheme of [5] and for the classical BGW VSS scheme of [1]. We show how the security of the CDM DC scheme can be proven by a simple linear-algebra argument – even with respect to a mixed adversary which strictly generalizes the results of [5] – and characterize the general-adversary condition under which a secure VSS scheme exists. For the BGW VSS scheme, we show that some of the checks between players are superfluous, i.e., the scheme is not optimal. This also shows that arguing about the security of such schemes becomes conceptually simpler. Finally, our approach, establishing the minimal conditions for security, can lead to the design of linear VSS or DC schemes for

general adversary structures which are more efficient than the schemes resulting from generic constructions as for instance that of [5].

The outline of the paper is as follows. In the next section, we introduce the notation we use throughout the paper, describe the communication and adversary model and define VSS and DC schemes. In Section 3, we consider general, i.e. not necessarily linear, secret sharing schemes and investigate what is needed to achieve a unique reconstruction as required by the above correctness property, while in Section 4 we then show how this is reduced to a linear-algebraic property in case of linear schemes. In Section 5 and 6 we then discuss the already mentioned applications to the existing schemes of [5] and [1], and in Section 7 we draw some final conclusions.

## 2 Preliminaries

### 2.1 Notation

Throughout the paper, $\mathcal{P}$ stands for the *player set* $\mathcal{P} = \{p_1, \ldots, p_n\}$, and for simplicity we set $p_i = i$. We call a subset $\Pi$ of the power set $2^{\mathcal{P}}$ of $\mathcal{P}$ a *(monotone) structure* of $\mathcal{P}$ if it is closed under taking subsets, i.e., if $P \in \Pi$ and $P' \subseteq P$ implies $P' \in \Pi$. We call it a *(monotone) anti-structure* if it is closed under taking supersets, i.e., if the complement $\Pi^c := \{P \in 2^{\mathcal{P}} \mid P \notin \Pi\}$ is a structure. Given two structures $\Pi_1$ and $\Pi_2$, $\Pi_1 \sqcup \Pi_2$ denotes the element-wise union, i.e., the structure

$$\Pi_1 \sqcup \Pi_2 := \{P_1 \cup P_2 \mid P_1 \in \Pi_1, P_2 \in \Pi_2\}.$$

Consider a finite set $\mathcal{K}$ (the set of *secrets*), $n$ finite sets $\mathcal{S}_1, \ldots, \mathcal{S}_n$, where $\mathcal{S}_i$ is the set of possible *shares* for player $p_i$, and let $\mathcal{S}$ be the Cartesian product $\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$. Elements of $\mathcal{S}$ will sometimes be called a *sharing*.

For two sharings $s = (s_1, \ldots, s_n)$ and $\tilde{s} = (\tilde{s}_1, \ldots, \tilde{s}_n)$, the set $\delta(s, \tilde{s}) \subseteq \mathcal{P}$ is defined as

$$\delta(s, \tilde{s}) := \{i \in \mathcal{P} \mid s_i \neq \tilde{s}_i\}.$$

Note that $\delta$ can be treated similar to a metric, as for all $s, s', s'' \in \mathcal{S}$ we have $\delta(s, s) = \emptyset$, $\delta(s, s') = \delta(s', s)$ and $\delta(s, s'') \subseteq \delta(s, s') \cup \delta(s', s'')$.

For a subset $Q = \{i_1, \ldots, i_\ell\} \subseteq \mathcal{P}$, a sharing $s \in \mathcal{S}$ and a subset $U \subseteq \mathcal{S}$ of sharings, $\mathrm{pr}_Q$ denotes the projection $\mathrm{pr}_Q : \mathcal{S} \to \mathcal{S}_{i_1} \times \cdots \times \mathcal{S}_{i_\ell}$, and $s_Q$ and $U_Q$ stand for $s_Q = \mathrm{pr}_Q(s)$ and $U_Q = \{\mathrm{pr}_Q(u) \mid u \in U\}$, respectively. Finally, if $\mathcal{S}_1, \ldots, \mathcal{S}_n$ and hence $\mathcal{S}$ are in fact vector spaces, which will be the case in Section 4, then, for a sharing $s \in \mathcal{S}$, the *support* $\mathrm{supp}(s)$ denotes the smallest set $Q \subseteq \mathcal{P}$ with $\mathrm{pr}_{\mathcal{P} \setminus Q}(s) = (0, \ldots, 0)$, in other words $\mathrm{supp}(s) = \delta(s, 0)$, and, for $Q \subseteq \mathcal{P}$ and $U \subseteq \mathcal{S}$, $U|_Q$ denotes the subset $U|_Q = \{u \in U \mid \mathrm{supp}(u) \subseteq Q\}$.

### 2.2 Model

We consider the *secure-channels model*, as introduced in [1,3], where the set of players (including the dealer) is connected by bilateral synchronous reliable secure channels. Broadcast channels are not assumed to be available, though can be implemented for the cases we consider [2,8] and thus will be treated as given primitives.

Like in previous literature on VSS and secure multi-party computation, we consider a central adversary who can corrupt players, subject to certain constraints, for example an upper bound on the total number of corrupted players. The selection of which player to corrupt can be adaptive, depending on the course of the protocol. The dealer is one of the players that can potentially also be corrupted.

Passive corruption of a player means that the adversary learns the player's entire information, but the player performs the protocol correctly. This models what is often also called "honest but curious" players. Active corruption of a player means that the adversary takes full control and can make the player deviate from the protocol in an arbitrary manner. Such a player is also called dishonest, or simply a cheater. Active corruption is hence strictly stronger than passive corruption. The adversary is characterized by a *privacy structure* $\Delta \subseteq \mathcal{P}$ and an *adversary structure* $\mathcal{A} \subseteq \Delta$ with the intended meaning that the adversary can be tolerated to corrupt any players passively or actively (one variant being the upgrading of a passive corruption to an active corruption), as long as the total set $D$ of corrupted players satisfies $D \in \Delta$ and the subset $A$ of them being actively corrupted satisfies $A \in \mathcal{A}$. In other words, all players in $D \backslash A$ are honest but curious. The complement $\mathcal{H} = \mathcal{A}^c$ is sometimes called the *honest-players structure*.

Finally, we assume that the adversary has unbounded computing power, and we achieve zero error probability.

### 2.3 Definition of VSS and DC

Let $\mathcal{K}$ be a finite set (as described in Section 2.1), let $\Delta$ be a privacy structure, and let $\mathcal{A} \subseteq \Delta$ be an adversary structure (as described in Section 2.2).

**Definition 1.** *A $(\Delta, \mathcal{A})$-secure* verifiable secret sharing *(VSS) scheme is a pair* $(\mathsf{Share}, \mathsf{Rec})$ *of protocols (phases), the* sharing phase*, where the dealer shares a secret $k \in \mathcal{K}$, and the* reconstruction phase*, where the players try to reconstruct $k$, such that the following two properties hold, even if the players of a set $A \in \mathcal{A}$ are dishonest and behave in an arbitrary manner:*

Privacy: *If the dealer remains honest, then the players of any set $D \in \Delta$ with $A \subseteq D$ learn nothing about the secret $k$ as a result of the sharing phase.*

Correctness: *After the secret is shared, there exists a unique value $k'$ that can be reconstructed by the players, and for an honest dealer this value $k'$ is equal to the shared secret $k$.*

*Reconstruction must work even if the dealer does not cooperate in the reconstruction. If an* efficient *reconstruction of the secret requires the cooperation of the dealer, then such a scheme is called a* distributed commitment (DC) *scheme.*

In a DC scheme, a dishonest dealer can prevent the (efficient) reconstruction by refusing to cooperate correctly, but he cannot achieve that a different secret is reconstructed, not even with the help of the dishonest players. Note that if

one would define a default value for the case the dealer refuses to reconstruct, then a cheating dealer would not be committed because he could open a sharing in two different ways: as the real or as the default value.

A VSS or DC scheme is called *linear* if the list of *shares*, i.e., the information given to the players during the sharing phase, is a linear function of the secret and randomly chosen values.

## 3 General Schemes

Even though our goal is a general treatment of *linear* schemes, we first consider arbitrary, not necessarily linear secret sharing schemes and discuss facts that are independent of the linearity of the scheme. More precisely, we present a sufficient condition on the (possibly not correctly) distributed shares in order to have uniqueness of the shared secret as required by the correctness property of VSS and DC schemes. And then, in the next section, we show how this can be achieved using linear schemes.

Most of the arguments of this section have been used – implicitly or explicitly – in the literature, but typically with respect to some restricted model. This unification not only generalizes arguments that have been used before (to non-linear schemes and to a mixed adversary), it also leads to a better understanding of the security of (linear and general) VSS and DC schemes.

Let $\mathcal{K}$ and $\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$ be defined as defined in Section 2.1.

**Definition 2.** *A* secret sharing scheme *is given by a joint conditional probability distribution* $P_{S|K} : \mathcal{S} \times \mathcal{K} \longrightarrow [0,1]$. *The* privacy structure $\Delta$ *is defined as the structure*

$$\Delta = \{D \subseteq \mathcal{P} \mid P_{S_D|K}(\,\cdot\,, k) = P_{S_D|K}(\,\cdot\,, k') \text{ for all } k, k' \in \mathcal{K}\}\ ^{1},$$

*and the* access structure $\Gamma$ *is defined as the anti-structure*[2]

$$\Gamma = \{Q \subseteq \mathcal{P} \mid P_{S|K}(s,k), P_{S|K}(s',k') > 0 \wedge s_Q = s'_Q \implies k = k'\}\,.$$

*A sharing* $s \in \mathcal{S}$ *is called* correct *of a secret* $k$ *if* $P_{S|K}(s,k) > 0$*, and, by defining the relation* $\mathrm{corr} := \{(s,k) \mid P_{S|K}(s,k) > 0\} \subset \mathcal{S} \times \mathcal{K}$*, is denoted by* $(s,k) \in \mathrm{corr}$.

Typically, a secret sharing scheme $P_{S|K}$ is given in terms of an (efficiently computable) function $f : \mathcal{K} \times \mathcal{R} \to \mathcal{S}$, where $\mathcal{R}$ is some finite set, such that $P_{S|K}(\cdot, k)$ is the distribution of $f(k,r)$ for a uniformly random chosen $r \in \mathcal{R}$. This is often directly used as the definition of a secret sharing scheme. Note that we do *not* require, as is usually the case in the literature, that the privacy structure $\Delta$ be the complement $\Gamma^c$ of the access structure $\Gamma$, but for linear schemes this is the case.

By the definition of $\Delta$ and $\Gamma$, the following properties are guaranteed.

[1] $P_{S_D|K}(\,\cdot\,, k)$ is naturally defined by $P_{S_D|K}(s_D, k) = \sum_{s' \in \mathcal{S}: s'_D = s_D} P_{S|K}(s', k)$.

[2] Note that even though $\Gamma$ is an anti-structure, it is called access *structure* (and not access anti-structure).

*Privacy:* For any secret $k$ and for $s = (s_1, \ldots, s_n)$ chosen according to the distribution $P_{S|K}(\cdot, k)$ [3] the shares $s_{i_1}, \ldots, s_{i_k}$ corresponding to a set $D = \{i_1, \ldots, i_k\} \in \Delta$ give no information about the secret $k$.

*Correctness:* For any $(s, k) \in \text{corr}$, the shares $s_{j_1}, \ldots, s_{j_\ell}$ corresponding to a set $Q = \{j_1, \ldots, j_\ell\} \in \Gamma$ uniquely define $k$ (and hence $k$ can – at least in principle – be computed from $s_{j_1}, \ldots, s_{j_\ell}$).

Hence, the correctness property guarantees that the secret is uniquely defined by the set of shares even if some are missing, i.e., in this sense the scheme is robust against lost shares. We now investigate what it means to be robust against *incorrect* shares.

Let $\mathcal{A} \subseteq \Delta$ be an adversary structure.

**Proposition 1.** *The following robustness property is fulfilled if and only if* $\mathcal{P} \notin \Gamma^c \sqcup \mathcal{A} \sqcup \mathcal{A}$.

Robustness: *For any* $(s, k) \in \text{corr}$, *any sharing* $\tilde{s}$ *with* $\delta(s, \tilde{s}) \in \mathcal{A}$ *uniquely defines* $k$, *in the sense that for any* $\tilde{s} \in \mathcal{S}$

$$(s, k), (s', k') \in \text{corr} \wedge \delta(s, \tilde{s}), \delta(s', \tilde{s}) \in \mathcal{A} \implies k = k' \,. \tag{1}$$

Namely, by the definition of $\Gamma$, (1) holds if and only if for every pair $A_1, A_2 \in \mathcal{A}$ the set $Q = \mathcal{P} \setminus (A_1 \cup A_2)$ is in $\Gamma$, which is equivalent to $\mathcal{P} \notin \Gamma^c \sqcup \mathcal{A} \sqcup \mathcal{A}$.

Note that in the literature $\mathcal{A}$ typically coincides with $\Delta$ and, as already mentioned, $\Delta$ with $\Gamma^c$, in which case $\mathcal{P} \notin \Gamma^c \sqcup \mathcal{A} \sqcup \mathcal{A}$ coincides with the $Q^3$ property of [10] which states that no three sets in $\mathcal{A}$ cover $\mathcal{P}$, which itself generalizes the classical bound $t < n/3$. However, we consider this more general case because it gives deeper insight but also because it makes perfect sense to separate the privacy from the adversary structure, i.e., to consider curious as well as dishonest players as argued in Section 2, and in fact will generalize in Section 5 the DC scheme from [5] to such mixed adversaries.

Robustness guarantees that the secret is uniquely defined by the set of shares even if some might be incorrect. If, as usual, the secret $k$ is shared by a so-called *dealer* by choosing $s$ according to $P_{S|K}(\cdot, k)$ and distributing the shares among the players in $\mathcal{P}$, then this allows the correct reconstruction of the secret even if the players of a set $A \in \mathcal{A}$ are dishonest and do not provide correct shares. However, this is only guaranteed to hold if the dealer is honest and indeed distributes a correct sharing $s$ of $k$. Hence, it seems that to achieve security against a possibly dishonest dealer, in the sense that a unique secret is defined, the dealer has to be forced to distribute a *correct* sharing $s$. We will now show in the remainder of this section that this is actually overkill and a weaker condition already suffices.

**Definition 3.** *A function* $\rho : \Gamma \times \mathcal{S} \ni (Q, s) \mapsto \rho^Q(s) \in \mathcal{K}$ *is called a* reconstruction function *for a secret sharing scheme* $P_{S|K}$ *if, for every* $Q \in \Gamma$, $\rho^Q(s)$ *only depends on* $s_Q$, *i.e.,* $\rho^Q : \mathcal{S} \to \mathcal{K}$ *can be seen as a function* $\rho^Q : \mathcal{S}_Q \to \mathcal{K}$,

[3] e.g. computed as $s = f(k, r)$ for a random $r \in \mathcal{R}$

*and* $\rho^Q(s_Q) = k$ *for every correct sharing* $s \in \mathcal{S}$ *of a secret* $k \in K$.
*A (not necessarily correct) sharing* $s \in \mathcal{S}$ *is called a* consistent sharing *of a secret* $k$ *(with respect to* $\rho$*) if* $\rho^Q(s_Q) = k$ *for every* $Q \in \Gamma$*, and is denoted by* $(s,k) \in \mathrm{cons}_\rho$. *And, similarly,* $s_H$ *with* $H \in \Gamma$ *is called a* consistent sharing *of a secret* $k$ for the players in $H$ *(with respect to* $\rho$*) if* $\rho^Q(s_Q) = k$ *for every* $Q \in \Gamma$ *with* $Q \subseteq H$*, and is denoted by* $(s_H,k) \in \mathrm{cons}_\rho^H$ [4].

It is easy to verify that the access structure $\Gamma$ coincides with

$$\Gamma_\rho = \{Q \subseteq \mathcal{P} \mid (s,k),(s',k') \in \mathrm{cons}_\rho \wedge s_Q = s'_Q \implies k = k'\}$$

Indeed, if $Q \in \Gamma_\rho$ and $(s,k),(s',k') \in \mathrm{corr}$ with $s_Q = s'_Q$, then $(s,k),(s',k') \in \mathrm{cons}_\rho$ and hence $k = k'$, and therefore $Q \in \Gamma$. On the other hand, if $Q \in \Gamma$ and $(s,k),(s',k') \in \mathrm{cons}_\rho$ with $s_Q = s'_Q$, then, by the properties of $\rho$, $k = \rho^Q(s_Q) = \rho^Q(s'_Q) = k'$, and therefore $Q \in \Gamma_\rho$.

Hence, arguing as before, we have

**Proposition 2.** *The following strong robustness property is fulfilled for an arbitrary reconstruction function* $\rho$ *if and only if* $\mathcal{P} \notin \Gamma^c \sqcup \mathcal{A} \sqcup \mathcal{A}$.

Strong robustness: *For any* $(s,k) \in \mathrm{cons}_\rho$*, any sharing* $\tilde{s}$ *with* $\delta(s,\tilde{s}) \in \mathcal{A}$ *uniquely defines* $k$*, in the sense that for any* $\tilde{s} \in \mathcal{S}$

$$(s,k),(s',k') \in \mathrm{cons}_\rho \wedge \delta(s,\tilde{s}),\delta(s',\tilde{s}) \in \mathcal{A} \implies k = k'\,. \tag{2}$$

Hence, if indeed $\mathcal{P} \notin \Gamma^c \sqcup \mathcal{A} \sqcup \mathcal{A}$, as long as the dealer is partially honest and hands out a *consistent* (but not necessarily correct) sharing $s$, there is a unique secret $k$ defined, assuming that the shares $s_H$ of an honest-players set $H \in \mathcal{H} = \mathcal{A}^c$ remain unchanged. We finally show that this even holds as long as the dealer hands out a consistent sharing $s_H$ *for the players in* $H$.

**Proposition 3.** *The following very strong robustness property is fulfilled for an arbitrary reconstruction function* $\rho$ *if and only if* $\mathcal{P} \notin \Gamma^c \sqcup \mathcal{A} \sqcup \mathcal{A}$.

Very strong robustness: *For any honest-players set* $H \in \mathcal{H}$ *and* $(s_H,k) \in \mathrm{cons}_\rho^H$*, any sharing* $\tilde{s}$ *with* $s_H = \tilde{s}_H$ *uniquely defines* $k$*, in the sense that for any* $\tilde{s} \in \mathcal{S}$

$$\left.\begin{array}{r} H \in \mathcal{H} \wedge \ (s_H,k) \in \mathrm{cons}_\rho^H \ \wedge \ s_H = \tilde{s}_H \\ \wedge\, H' \in \mathcal{H} \wedge (s'_{H'},k') \in \mathrm{cons}_\rho^{H'} \wedge s'_{H'} = \tilde{s}_{H'} \end{array}\right\} \implies k = k'\,. \tag{3}$$

Indeed, (3) holds if and only if $H \cap H' \in \Gamma$ for all $H, H' \in \mathcal{H}$, which is equivalent to $\mathcal{P} \setminus (A_1 \cup A_2) \in \Gamma$ for all $A_1, A_2 \in \mathcal{A}$, which, as already noticed earlier, is equivalent to $\mathcal{P} \notin \Gamma^c \sqcup \mathcal{A} \sqcup \mathcal{A}$.

[4] Clearly, if $s$ is a consistent sharing then, for any $H \in \Gamma$, $s_H$ is a consistent sharing for the players in $H$; however, if $s_H$ is a consistent sharing for the players in $H$ for some $H$ then, in general, $s_H$ cannot be completed to a consistent sharing $s$.

## 4 Linear Schemes

We have seen in the above Section 3 that the uniqueness of the shared secret (that is required by the correctness property of VSS or DC) is guaranteed if (and only if) $\mathcal{P} \notin \Gamma^c \sqcup \mathcal{A} \sqcup \mathcal{A}$ and if the dealer is at least partially honest and hands out a *consistent* sharing to the honest players, or if he can be forced to behave this way. In this section we now concentrate on *linear* schemes, and we present a very natural sharing protocol which enforces some kind of consistency. Namely, by pairwise checking, complaining and accusing, it ensures *pairwise* consistency among the shares (of the honest players). All known DC and VSS schemes can be seen as concrete instances of this general approach. Finally, we give a characterization in the language of linear algebra of when the sharing protocol results in a secure DC (or VSS) scheme. As a consequence, the security of all known schemes follow as corollaries whose proofs are linear-algebra arguments, and, more generally, it becomes conceptually very simple to argue about the security of such schemes, as it involves only pure linear algebra.

From now on, $\mathcal{K}$ is a field, and $\mathcal{S}_1, \ldots, \mathcal{S}_n$ are vector spaces over $\mathcal{K}$ with inner products $\langle \cdot, \cdot \rangle_{\mathcal{S}_1}, \ldots, \langle \cdot, \cdot \rangle_{\mathcal{S}_n}$, respectively, which naturally induce an inner product $\langle \cdot, \cdot \rangle_{\mathcal{S}}$ for the vector space $\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$ by $\langle s, s' \rangle_{\mathcal{S}} = \sum_i \langle s_i, s'_i \rangle_{\mathcal{S}_i}$.

As usual in linear algebra, for a subset $U \subseteq \mathcal{S}$, $\mathrm{span}(U)$ denotes the subspace consisting of all linear combinations of vectors in $U$ and the *orthogonal complement* $U^{\perp_{\mathcal{S}}}$ is the subspace defined by $U^{\perp_{\mathcal{S}}} := \{s \in \mathcal{S} \mid \langle s, u \rangle_{\mathcal{S}} = 0 \; \forall \, u \in U\}$. We also write $s \perp_{\mathcal{S}} U$ instead of $s \in U^{\perp_{\mathcal{S}}}$.

### 4.1 Secret Sharing

A *linear* secret sharing scheme is given by a pair $(M, \varepsilon)$, consisting of a linear map

$$M : \mathcal{V} \longrightarrow \mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$$

and a vector $\varepsilon \in \mathcal{V}$, where $\mathcal{V}$ is a vector space over the field $\mathcal{K}$ with inner product $\langle \cdot, \cdot \rangle_{\mathcal{V}}$ and $\mathcal{S}$ is as described above. A secret $k \in \mathcal{K}$ is shared by choosing a random $x \in \mathcal{V}$ such that $\langle \varepsilon, x \rangle_{\mathcal{V}} = k$ and computing $s$ as $s = Mx$.

Consider the special case where $\mathcal{V} = \mathcal{K}^e$ for some $e$ and $\mathcal{S}_i = \mathcal{K}^{d_i}$ for some $d_1, \ldots, d_n$, where every inner product is the respective standard inner product, and where $M$ is a matrix multiplication $M : \mathcal{K}^e \to \mathcal{K}^{\Sigma d_i} = \mathcal{K}^{d_1} \times \ldots \times \mathcal{K}^{d_n}$, $x \mapsto M \cdot x$ [5]. In this case, $(M, \varepsilon)$ is called a monotone span program [11]. Clearly, by fixing orthogonal bases of $\mathcal{V}$ and $\mathcal{S}_1, \ldots, \mathcal{S}_n$, respectively, one can always have this simplified and more familiar view. However, as this simplification might (and indeed would in Section 5.1) destroy the naturalness of additional structures in $\mathcal{V}$ or $\mathcal{S}$, we keep this more general view. Nevertheless, because of this reduction, it follows from [11] that the access structure $\Gamma$ and the privacy structure $\Delta$ of a linear secret sharing scheme $(M, \varepsilon)$ are given by

$$\Gamma = \{Q \subseteq \mathcal{P} \mid \exists \, \lambda \in \mathcal{S} : \mathrm{supp}(\lambda) \subseteq Q, M^* \lambda = \varepsilon\}$$

[5] We slightly abuse notation and use the same symbol, $M$, for the matrix $M \in \mathcal{K}^{\Sigma d_i \times e}$ as well as the corresponding linear map $M : \mathcal{K}^e \to \mathcal{K}^{\Sigma d_i} = \mathcal{K}^{d_1} \times \ldots \times \mathcal{K}^{d_n}$.

and $\Delta = \Gamma^c$, respectively, where $M^* : \mathcal{S} \to \mathcal{V}$ is the conjugate of $M$ (i.e. such that $\langle \lambda, Mx \rangle_{\mathcal{S}} = \langle M^*\lambda, x \rangle_{\mathcal{V}}$ for all $\lambda \in \mathcal{S}$ and $x \in \mathcal{V}$, and, in the simplified monotone span program view, $M^* = M^T$, the transposed matrix). Furthermore, any subset $\Lambda$ of

$$\Lambda^{max} = \{\lambda \in \mathcal{S} \mid M^*\lambda = \varepsilon\}$$

which is complete in the sense that for every $Q \in \Gamma$ there exists $\lambda \in \Lambda|_Q$, naturally induces a reconstruction function $\rho : \Gamma \times \mathcal{S} \to \mathcal{K}$ by

$$\rho^Q(s) = \begin{cases} \langle \lambda, s \rangle_{\mathcal{S}} & \text{if } \langle \lambda, s \rangle_{\mathcal{S}} \text{ is the same for every } \lambda \in \Lambda|_Q \\ 0 & \text{otherwise} \end{cases}$$

Note that $\lambda \in \Lambda^{max}$ fulfills $\langle \lambda, s \rangle_{\mathcal{S}} = \langle \lambda, Mx \rangle_{\mathcal{S}} = \langle M^*\lambda, x \rangle_{\mathcal{V}} = \langle \varepsilon, x \rangle_{\mathcal{V}} = k$ for any correct sharing $s$ of a secret $k$.

### 4.2 Verifiable Secret Sharing and Distributed Commitments

Consider a linear secret sharing scheme, given by $M : \mathcal{V} \to \mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$ and $\varepsilon \in \mathcal{V}$, with an access structure $\Gamma$. According to Section 3, in order to turn this scheme into a DC scheme or a VSS, secure against the privacy structure $\Delta = \Gamma^c$ and the adversary structure $\mathcal{A} \subseteq \Delta$, it is necessary that $\mathcal{P} \notin \Delta \sqcup \mathcal{A} \sqcup \mathcal{A}$, and additionally, as part of the sharing procedure, it has to be checked that the dealer behaves partially honest and hands out a *consistent* sharing with respect to some reconstruction function $\rho$ to the honest players. However, it seems to be impossible to *directly* check this kind of consistency, i.e. to verify something like $\langle \lambda, s \rangle = \langle \lambda', s \rangle$ for $\lambda \neq \lambda'$, *without violating privacy*. The only thing that can be checked without violating privacy is *pairwise consistency*, i.e. whether (some) pairwise linear dependences $\langle \gamma, s \rangle = 0$ with $\mathrm{supp}(\gamma) = \{i, j\}$ that should hold indeed *do* hold; namely by comparing in private the respective contributions $\langle \gamma_i, s_i \rangle$ and $\langle \gamma_j, s_j \rangle$ (which, up to the sign, are supposed to be equal) of the two involved players. A player *complains* in case of a pairwise inconsistency, but this may be due to the dealer's *or* another player's misbehavior, and he *accuses* (the dealer) if he knows that the dealer misbehaved. In any case, the dealer has to publicly clarify the situation, such that finally the shares of all honest players *are* pairwise consistent *and* privacy is satisfied. This is described in full detail in the protocol Share below. Finally, a simple linear algebra condition is given that is sufficient (and also necessary) in order for the pairwise consistency to imply consistency with respect to a given reconstruction function, and hence in order for the scheme to result in a secure DC respectively VSS.

Consider the set

$$\mathit{Checks}(M) := \{\gamma \in \ker M^* \mid |\mathrm{supp}(\gamma)| \leq 2\} \subseteq \mathcal{S}$$

of all possible *(pairwise) checking vectors*, where $\ker M^*$ denotes the kernel $\ker M^* = \{\xi \in \mathcal{S} \mid M^*\xi = 0\}$ of $M^*$. Clearly, for any $\gamma \in \mathit{Checks}(M)$ and any *correct* sharing $s = Mx$, we have

$$\langle \gamma, s \rangle_{\mathcal{S}} = \langle \gamma, Mx \rangle_{\mathcal{S}} = \langle M^*\gamma, x \rangle_{\mathcal{V}} = \langle 0, x \rangle_{\mathcal{V}} = 0.$$

For an arbitrary but fixed subset $\mathcal{C} \in \mathit{Checks}(M)$, the following sharing protocol enforces pairwise consistency with respect to the checking vectors $\gamma \in \mathcal{C}$ among the players that remain honest during the execution, without revealing any information about the shared secret. The concrete choice of the protocol is somewhat arbitrary, in that it can be modified in different ways without loosing its functionality and without nullifying the upcoming results. For instance, techniques from [9] can be applied to improve the round complexity (at the cost of an increased communication complexity), and some secret sharing schemes $M$ allow "early stopping".

**Protocol** $\mathsf{Share}_{(M,\varepsilon),\mathcal{C}}(k)$

1. The dealer chooses a random $x \in \mathcal{V}$ such that $\langle \varepsilon, x \rangle = k$, computes $s = Mx$ and sends to every player $p_i \in \mathcal{P}$ the corresponding share $s_i$.
2. For every checking vector $\gamma \in \mathcal{C}$, it is as follows checked whether $\langle \gamma, s \rangle_{\mathcal{S}} = 0$:
   If $\mathrm{supp}(\gamma) = \{p_i\}$, then player $p_i$ verifies whether $\langle \gamma_i, s_i \rangle_{\mathcal{S}_i} = 0$, and he broadcasts an "accusation" against the dealer if it does not hold.
   If $\mathrm{supp}(\gamma) = \{p_i, p_j\}$ with $p_i < p_j$, then then player $p_i$ sends $c_{ij} = \langle \gamma_i, s_i \rangle_{\mathcal{S}_i}$ to $p_j$ who verifies whether $c_{ij} + \langle \gamma_j, s_j \rangle_{\mathcal{S}_j} = 0$ and broadcasts a "complaint" if it does not hold. The dealer answers such a complaint by broadcasting $c_{ij} = \langle \gamma_i, s_i \rangle$, and if this value does not coincide with $p_i$'s $c_{ij}$ respectively if it does not fulfill $c_{ij} + \langle \gamma_j, s_j \rangle_{\mathcal{S}_j} = 0$, then player $p_i$ respectively $p_j$ broadcasts an "accusation" against the dealer.
3. The following is repeated until there is no further "accusation" or the dealer is declared faulty (which requires at most $n$ rounds). For every "accusation" from a player $p_i$, the dealer answers by broadcasting $p_i$'s share $s_i$, and $p_i$ replaces his share by this $s_i$. If this share contradicts the share of some player $p_j$, in the sense that $\langle \gamma_i, s_i \rangle_{\mathcal{S}_i} + \langle \gamma_j, s_j \rangle_{\mathcal{S}_j} \neq 0$ for some $\gamma \in \mathcal{C}$ with $\mathrm{supp}(\gamma) = \{p_i, p_j\}$, then $p_j$ broadcasts an "accusation" (if he has not yet done so in an earlier step). If this share $s_i$ contradicts itself, in the sense that $\langle \gamma_i, s_i \rangle \neq 0$ for some $\gamma \in \mathcal{C}$ with $\mathrm{supp}(\gamma) = \{p_i\}$, or it contradicts a share $s_j$ that has already been broadcast, then the dealer is publicly declared to be faulty.

It is easy to see that if the dealer remains honest, then no matter what the dishonest players do, nobody learns anything beyond his share, and hence the players of any set $D \in \Delta$ learn nothing about the shared secret. Furthermore, independent of the behavior of the dishonest players, if $H$ denotes the set of players that remain honest during the protocol execution (though some might become curious) then the protocol achieves pairwise consistency among the players in $H$, i.e., $\langle \gamma, s \rangle_{\mathcal{S}} = 0$ for every $\gamma \in \mathcal{C}|_H$, or, in other words,

$$s \perp_{\mathcal{S}} \mathcal{C}|_H \,.$$

In order for the protocol to achieve consistency with respect to a reconstruction function $\rho$, it must be guaranteed for a complete subset of reconstruction vectors $\Lambda \subseteq \Lambda^{max}$ that $\langle \lambda, s \rangle = \langle \lambda', s \rangle$ for all $\lambda, \lambda' \in \Lambda|_H$, or, in other words, that

$$s \perp_{\mathcal{S}} \{\lambda - \lambda' \mid \lambda, \lambda' \in \Lambda|_H\} \,.$$

This implies

**Proposition 4.** *Let $\rho : \Gamma \times \mathcal{S} \to \mathcal{K}$ be a reconstruction function induced by a complete subset of reconstruction vectors $\Lambda \subseteq \Lambda^{max}$ (as defined Section 4.1). Then, the sharing protocol $\mathsf{Share}_{(M,\varepsilon),\mathcal{C}}$ is guaranteed to produce a* consistent *sharing for the honest players with respect to $\rho$ if and only if*

$$\{\lambda - \lambda' \mid \lambda, \lambda' \in \Lambda|_H\} \subseteq \mathrm{span}(\mathcal{C}|_H) \quad \textit{for every } H \in \mathcal{H}. \tag{4}$$

Combing this with Proposition 3 leads to

**Theorem 1.** *Let $(M, \varepsilon)$ be a linear secret sharing scheme with privacy structure $\Delta$, $\mathcal{C} \subseteq Checks(M)$ a subset of checking vectors and $\mathcal{A} \subseteq \Delta$ an adversary structure. Then the protocol $\mathsf{Share}_{(M,\varepsilon),\mathcal{C}}$ can be completed to a $(\Delta, \mathcal{A})$-secure DC scheme $(\mathsf{Share}_{(M,\varepsilon),\mathcal{C}}, \mathsf{Rec}_{(M,\varepsilon),\mathcal{C}})$ if (and only if) $\mathcal{P} \notin \Delta \sqcup \mathcal{A} \sqcup \mathcal{A}$ and if (4) holds for some complete subset $\Lambda \subseteq \Lambda^{max}$ of reconstruction vectors.*
*If additionally $\mathcal{C}_{\{i,j\}} \subseteq \mathrm{span}(\mathcal{C}|_{\{i\}\cup Q} \cup \mathcal{C}|_{\{j\}\cup Q})$ for all $i, j$ and every $Q \notin \Delta$, then $\mathsf{Share}_{(M,\varepsilon),\mathcal{C}}$ can be completed to a $(\Delta, \mathcal{A})$-secure VSS scheme.*

*Proof.* With respect to a not necessarily efficient reconstruction procedure, the claim follows from Proposition 4 and 3 (even without the additional requirement for the VSS case). It remains to show the existence of *efficient* reconstruction procedures: In the DC reconstruction, the dealer publishes the vector $x$ used in Step 1 of the sharing protocol and every player $p_i$ publishes his share $s_i$, and then the players take $k = \langle \varepsilon, x \rangle_{\mathcal{V}}$ as the reconstructed secret if $\delta(Mx, s) \in \mathcal{A}$ and reject the reconstruction otherwise (as if the dealer had refused to take part at all). In the VSS reconstruction, every player $p_i$ publishes his share $s_i$, then any share $s_i$ that is pairwise inconsistent (with respect to the checking vectors in $\mathcal{C}$) with the shares of a set $A \notin \mathcal{A}$ is rejected, and the secret is reconstructed from the accepted shares by applying the reconstruction function $\rho$ induced by $\Lambda$. Note that the additional requirement for $\mathcal{C}$ implies that all accepted shares are pairwise consistent and hence consistent with respect to $\rho$. □

To our knowledge, the condition $\mathcal{P} \notin \Delta \sqcup \mathcal{A} \sqcup \mathcal{A}$ for VSS to be possible has not been stated previously in the literature, although the condition for secure multi-party computation has been given in [7]. In the threshold case, this confirms Lemma 1 of [6]: If the total number of (passively) corrupted players is $t$ and if $w$ of them can even be actively corrupted, then VSS is possible if and only if $t + 2w < n$.

The following lemma will be helpful in the next section.

**Lemma 1.** *Predicate (4) is fulfilled if every pair $\lambda, \lambda' \in \Lambda$ fulfills*

$$\lambda - \lambda' \in \mathrm{span}(\mathcal{C}|_{\mathrm{supp}(\lambda)\cup\mathrm{supp}(\lambda')}) \,.$$

*Proof.* Let $H \in \mathcal{H}$ be arbitrary but fixed. Then, for $\lambda, \lambda' \in \Lambda|_H \subseteq \Lambda$, we have by assumption $\lambda - \lambda' \in \mathrm{span}(\mathcal{C}|_{\mathrm{supp}(\lambda)\cup\mathrm{supp}(\lambda')})$, which is of course contained in $\mathrm{span}(\mathcal{C}|_H)$. □

## 5 Application I: Proving the Security of the CDM Scheme

We now demonstrate the power of Theorem 1 and prove the security of the CDM DC scheme [5] by proving a pure linear-algebra statement. We only have to show that $\{\lambda - \lambda' \,|\, \lambda, \lambda' \in \Lambda|_H\} \subseteq \mathrm{span}(\mathcal{C}|_H)$ for every $H \in \mathcal{H}$, or, and that is what we are going to do, that $\lambda - \lambda' \in \mathrm{span}(\mathcal{C}|_{\mathrm{supp}(\lambda)\cup\mathrm{supp}(\lambda')})$ for every pair $\lambda, \lambda' \in \Lambda$. As a by-product, because of our general treatment in Section 3, we generalize the CDM DC scheme to a mixed adversary.

### 5.1 The CDM Scheme

In [5], a generic construction was presented to convert any linear secret sharing scheme, described by a monotone span program, into a linear DC scheme. As mentioned in Section 4, a monotone span program is given by a matrix $M_\circ \in \mathcal{K}^{\Sigma d_i \times e}$ and a vector $\varepsilon_\circ \in \mathcal{K}^e$. The CDM DC scheme works as follows, assuming for simplification that $\varepsilon_\circ = (1, 0, \ldots, 0)^T$ and $d_1 = \ldots = d_n = 1$. To share (or commit to) a secret $k$, the dealer chooses a random *symmetric matrix* $X \in \mathcal{K}^{e\times e}$ with $k$ in the upper left corner and sends the share $s_i = M_{\circ i} \cdot X$ to player $p_i$, where $M_{\circ i}$ denotes the $i$-th row of $M_\circ$. Now, every pair $p_i, p_j$ of players verifies whether $M_{\circ i} \cdot s_j^T = M_{\circ j} \cdot s_i^T$ and, in case it does not hold, start complaining and accusing as in the protocol from the above section.

It is not hard to see that this scheme is a concrete instance of the class of schemes described in the previous section. Indeed, it coincides with $\mathsf{Share}_{(M,\varepsilon),\mathcal{C}}$ for $M$, $\varepsilon$ and $\mathcal{C}$ as described in the following. $M$ is the linear map

$$\begin{aligned} M : \mathcal{V} &\to \mathcal{S} = \mathcal{K}^{n\times e} = \mathcal{K}^e \times \cdots \times \mathcal{K}^e \\ X &\mapsto s = M_\circ \cdot X \end{aligned}$$

where $\mathcal{V}$ is the vector space consisting of all symmetric $e \times e$-matrices over $\mathcal{K}$ and $\langle \cdot, \cdot \rangle_{\mathcal{V}}$ is given by

$$\langle a, b \rangle_{\mathcal{V}} = \sum_{1 \le i,j \le e} a[i,j]b[i,j]$$

for matrices $a$ and $b$ in $\mathcal{V}$ with entries $a[i,j]$ and $b[i,j]$. Furthermore, $\varepsilon \in \mathcal{V}$ is the matrix with a 1 in the upper left corner and zeros otherwise, and the set $\mathcal{C}$ is given by

$$\mathcal{C} = \{\gamma^{ij} = \mu^{ij} - \mu^{ji} \,|\, 1 \le i < j \le n\} \subseteq Checks(M)$$

where $\mu^{ij} \in \mathcal{S}$ has $M_{\circ j}$ as $i$-th row and zero-entries otherwise. In this example the checking vectors $\gamma \in \mathcal{C}$ are in fact matrices.

Note that $\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$ with $\mathcal{S}_i = \mathcal{K}^e$ (and $\langle \cdot, \cdot \rangle_{\mathcal{S}_i}$ the standard inner product) is interpreted as $\mathcal{S} = \mathcal{K}^{n\times e}$. Hence, for any matrix $s \in \mathcal{S}$, $s_i$ is the $i$-th row of $s$, and therefore if $s = M_\circ \cdot X$ then $s_i = M_{\circ i} \cdot X$. Furthermore, $\langle \varepsilon, X \rangle_{\mathcal{V}} = k$ if and only if the upper left corner of $X$ is $k$ and for a check vector $\gamma^{ij} \in \mathcal{C}$ we have $\langle \gamma^{ij}, s \rangle_{\mathcal{S}} = \langle M_{\circ j}, s_i \rangle_{\mathcal{S}_i} - \langle M_{\circ i}, s_j \rangle_{\mathcal{S}_j} = M_{\circ j} \cdot s_i^T - M_{\circ i} \cdot s_j^T$. Hence, $\mathsf{Share}_{(M,\varepsilon),\mathcal{C}}$ indeed coincides with the CDM protocol [5].

Finally, note that (as it is also shown in [5]) the access structure $\Gamma$ of the secret sharing scheme $(M, \varepsilon)$ coincides with the access structure $\Gamma_\circ$ of the original scheme $(M_\circ, \varepsilon_\circ)$.

### 5.2 The Security Proof

If $\lambda_\circ$ is a reconstruction vector for the original secret sharing scheme $(M_\circ, \varepsilon_\circ)$, i.e. $\langle \lambda_\circ, M_\circ x \rangle_{\mathcal{K}^n} = k$ for $x \in \mathcal{K}^e$ with $k$ as first entry (such that $\langle \varepsilon_\circ, x \rangle_{\mathcal{K}^e} = k$), then the matrix $\lambda = [\lambda_\circ |\ 0\ ] \in \mathcal{S}$ with $\lambda_\circ$ as first column and zero-entries otherwise is a reconstruction vector for $M$, i.e. $\langle \lambda, M_\circ X \rangle_{\mathcal{S}} = k$ for $X \in \mathcal{V}$ with $k$ in the upper left corner (such that $\langle \varepsilon, X \rangle_{\mathcal{V}} = k$). Since $\Gamma = \Gamma_\circ$, the subset $\Lambda \subset \Lambda^{max}$ consisting of such reconstruction vectors $\lambda = [\lambda_\circ |\ 0\ ]$ is complete. Furthermore, we will show the following linear-algebraic fact.

**Lemma 2.** *For every pair $\lambda, \lambda' \in \Lambda$,*

$$\lambda - \lambda' \in \operatorname{span}(\mathcal{C}|_{\operatorname{supp}(\lambda) \cup \operatorname{supp}(\lambda')})\,.$$

The following corollary now follows directly from Theorem 1 and Lemma 1, generalizing the results of [5] to a *mixed adversary*.

**Corollary 1.** *The CDM DC scheme based on a linear secret sharing scheme with access structure $\Gamma$ and corresponding privacy structure $\Delta = \Gamma^{\mathrm{c}}$ is secure with respect to an adversary structure $\mathcal{A} \subseteq \Delta$ if and only if $\mathcal{P} \notin \Delta \sqcup \mathcal{A} \sqcup \mathcal{A}$.*

*Proof of Lemma 2:* Let $\lambda = [\lambda_\circ |\ 0\ ]$ and $\lambda' = [\lambda'_\circ |\ 0\ ]$ be reconstruction vectors from $\mathcal{C}$. We have $\sum_i \lambda_\circ[i] M_{\circ i} = {\lambda_\circ}^T \cdot M_\circ = {\varepsilon_\circ}^T = (1, 0, \ldots, 0)$ and hence

$$\sum_i \lambda_\circ[i] \mu^{ji} = \sum_i \lambda_\circ[i] \begin{pmatrix} 0 \\ \boxed{M_{\circ i}} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \boxed{1\,0 \cdots 0} \\ 0 \end{pmatrix}$$

where the non-zero row is at the $j$-th position, and hence $\lambda'$ can be written as

$$\lambda' = [\lambda'_\circ |\ 0\ ] = \sum_j \lambda'_\circ[j] \begin{pmatrix} 0 \\ \boxed{1\,0 \cdots 0} \\ 0 \end{pmatrix} = \sum_j \lambda'_\circ[j] \left( \sum_i \lambda_\circ[i] \mu^{ji} \right) = \sum_{ij} \lambda_\circ[i] \lambda'_\circ[j] \mu^{ji}\,.$$

Similarly $\lambda = \sum_{ij} \lambda_\circ[i] \lambda'_\circ[j] \mu^{ij}$ and therefore

$$\lambda - \lambda' = \sum_{ij} \lambda_\circ[i] \lambda'_\circ[j] \left( \mu^{ij} - \mu^{ji} \right) = \sum_{ij} \lambda_\circ[i] \lambda'_\circ[j] \gamma^{ij} \in \operatorname{span}(\mathcal{C}|_{\operatorname{supp}(\lambda) \cup \operatorname{supp}(\lambda')})\,,$$

which proves the claim. □

## 6 Application II: Reducing the Number of Checks in the BGW Scheme

Theorem 1 tells us that as long as the set $\{\lambda - \lambda' \mid \lambda, \lambda' \in \Lambda|_H\}$ is contained in the subspace $\operatorname{span}(\mathcal{C}|_H) \subseteq \mathcal{S}$, where $H \in \mathcal{H}$ collects the honest players, the

corresponding scheme is secure. By this it is obvious that if the vectors in $\mathcal{C}|_H$ are not linearly independent, then $\mathcal{C}|_H$ contains more vectors than actually needed. We will now use this simple observation to reduce the number of checks in the (symmetric version of the) BGW VSS scheme [1].

The variation of the scheme of [1] where a *symmetric* bivariate polynomial is used instead of an arbitrary one can be seen as a special case of the CDM scheme, where the matrix $M_\circ$ is a Van-der-Monde matrix, i.e., $M_{\circ i} = [1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^t]$ for disjoint $\alpha_1, \ldots, \alpha_n \neq 0$. We have the following fact.

**Lemma 3.** *Let* $Q^* \in \Gamma = \{Q \subseteq \mathcal{P} \mid |Q| \geq t+1\}$ *and* $H \supseteq Q^*$. *Then*

$$\mathrm{span}(\{\gamma^{ij} \in \mathcal{C}|_H \mid i \in Q^* \text{ or } j \in Q^*\}) = \mathrm{span}(\mathcal{C}|_H).$$

As the proof is purely technical and does not give any new insight, it is moved to the appendix. Similarly, it can be shown using linear algebra that $\mathcal{C}_{\{i,j\}} \subseteq \mathrm{span}(\mathcal{C}|_{\{i\}\cup Q} \cup \mathcal{C}|_{\{j\}\cup Q})$ for all $i, j$ and every $Q$ with $|Q| \geq t+1$. The following corollary follows now from Theorem 1, showing that (the symmetric version of) the classical VSS scheme of [1] is not optimal with respect to the number of required pairwise checks.

**Corollary 2.** *The symmetric version of the BGW VSS scheme with threshold privacy structure* $\Delta = \{D \subseteq \mathcal{P} \mid |D| \leq t\}$ *is secure with respect to a threshold adversary structure* $\mathcal{A} = \{A \subseteq \mathcal{P} \mid |A| \leq w\}$ *with* $w \leq t$ *if and only if* $n > t + 2w$, *even if* $\mathcal{C}$ *is replaced by*

$$\bar{\mathcal{C}} = \{\gamma^{ij} \in \mathcal{C} \mid j > w\}.$$

*Proof.* Let $H$ be the set of honest players, hence $|H| \geq n - w > t + w$. Clearly, the set $Q^* = \{i \in H \mid i > w\}$ is in $\Gamma$ and hence $\bar{\mathcal{C}}|_H = \{\gamma^{ij} \in \mathcal{C}|_H \mid i \in Q^* \text{ or } j \in Q^*\}$ fulfills $\mathrm{span}(\bar{\mathcal{C}}|_H) = \mathrm{span}(\mathcal{C}|_H)$. □

Alternatively, this shows that the classical BGW VSS scheme allows "early stopping", as it is also used in the 4-round VSS of [9].

## 7 Conclusions

We presented a general treatment of all linear VSS and DC schemes based on an underlying linear secret sharing scheme, pairwise checks, complaints and accusations (against the dealer), and we analysed the security of this class of schemes. This class covers all currently known linear schemes, and possibly even all future ones. We reduced the security of these schemes to a pure linear-algebra predicate and showed with two concrete examples that this makes arguing about the security of such schemes conceptually very simple, as no cryptographic reasoning is needed anymore but just pure linear algebra. Furthermore, given a fixed adversary structure (e.g. described by a monotone span program) this might allow the construction of secure schemes which are more efficient than the generic construction of [5].

## References


1. M. Ben-Or, S. Goldwasser, and A. Widgerson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *20th Annual ACM Symposium on the Theory of Computing*. ACM Press, 1988.
2. P. Berman, J. A. Garay, and K. J. Perry. Towards optimal distributed consensus (extended abstract). In *30th Annual Symposium on Foundations of Computer Science*. IEEE, 1989.
3. D. Chaum, C. Crepeau, and I. Damgård. Multiparty unconditional secure protocols. In *20th Annual ACM Symposium on the Theory of Computing*. ACM Press, 1988.
4. B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults (extended abstract). In *26th Annual Symposium on Foundations of Computer Science*. IEEE, 1985.
5. R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *Advances in Cryptology - EUROCRYPT 2000*, *Lecture Notes in Computer Science*. Springer, 2000.
6. M. Fitzi, M. Hirt, and U. Maurer. Trading correctness for privacy in unconditional multi-party computation. In *Advances in Cryptology – CRYPTO '98*, *Lecture Notes in Computer Science*. Springer, 1998. Corrected proceedings version.
7. M. Fitzi, M. Hirt, and U. Maurer. General adversaries in unconditional multi-party computation. In *Advances in Cryptology - ASIACRYPT '99*, *Lecture Notes in Computer Science*. Springer, 1999.
8. M. Fitzi and U. Maurer. Efficient byzantine agreement secure against general adversaries. In *International Symposium on Distributed Computing (DISC)*, *Lecture Notes in Computer Science*. Springer, 1998.
9. R. Gennaro, Y. Ishai, E. Kushilevitz, and T. Rabin. The round complexity of verifiable secret sharing and secure multicast. In *33rd Annual ACM Symposium on the Theory of Computing*. ACM Press, 2001.
10. M. Hirt and U. Maurer. Complete characterization of adversaries tolerable in secure multi-party computation (extended abstract). In *16th ACM Symposium on Principles of Distributed Computing*, 1997. Final version appeared in Journal of Cryptology 2000.
11. M. Karchmer and A. Wigderson. On span programs. In *8th Annual Conference on Structure in Complexity Theory (SCTC '93)*. IEEE, 1993.
12. A. Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11), 1979.


## A Proof of Lemma 3

Recall that the checking vectors $\gamma^{ij} \in \mathcal{C}$ (which are actually matrices) are of the following form: The $i$-th row is $M_{\circ j}$, the $j$-th row is $-M_{\circ i}$, and all remaining entries are zero, i.e., $\gamma_i^{ij} = M_{\circ j}$ and $\gamma_j^{ij} = -M_{\circ i}$ and $\gamma_l^{ij} = 0$ for $l \neq i, j$.

*Proof of Lemma 3:* We assume without loss of generality that $Q^* = \{p_{n-t}, \ldots, p_n\}$. Consider an arbitrary but fixed checking vector $\gamma^{i_0 j_0}$ with $i_0, j_0 \in H$ and $i_0 < j_0 < n - t$, i.e. $i_0, j_0 \notin Q^*$ (otherwise, nothing needs to be shown). We have to show that $\gamma^{i_0 j_0}$ is contained in span$(\{\gamma^{ij} \in C|_H \,|\, i \in Q^* \text{ or } j \in Q^*\}$. This will be done by the following claim.

**Claim:** There exists a sequence $\delta^{n-t-1}, \ldots, \delta^n \in \mathrm{span}(\{\gamma^{ij} \in C|_H \,|\, i \in Q^* \text{ or } j \in Q^*\})$ such that for every $n-t-1 \le i \le n$

$$\delta^i_k = \begin{cases} \gamma^{i_0 j_0}_k & \text{if } k \le i \\ \sum_{k \neq l = i+1}^{n} (\lambda^{i_0}_k \lambda^{j_0}_l - \lambda^{i_0}_l \lambda^{j_0}_k) M_{\circ l} & \text{otherwise} \end{cases}$$

where for $1 \le i \le n$ and $n-t \le l \le n$ we let $\lambda^i_l \neq 0$ be such that $\sum_{l=n-t}^{n} \lambda^i_l M_{\circ l} = M_{\circ i}$.

Truly, we can set

$$\delta^{n-t-1} = \sum_{l=n-t}^{n} (\lambda^{j_0}_l \gamma^{i_0 l} - \lambda^{i_0}_l \gamma^{j_0 l}) \in \mathrm{span}(\{\gamma^{ij} \in C|_H \mid i \in Q^* \text{ or } j \in Q^*\})$$

Then for $k \le n-t-1$ we indeed have $\delta^{n-t-1}_k = \gamma^{i_0 j_0}_k$, namely

$$\delta^{n-t-1}_{i_0} = \sum_l \lambda^{j_0}_l M_{\circ l} = M_{\circ j_0} = \gamma^{i_0 j_0}_{i_0}$$

$$\delta^{n-t-1}_{j_0} = -\sum_l \lambda^{i_0}_l M_{\circ l} = -M_{\circ i_0} = \gamma^{i_0 j_0}_{j_0} \quad \text{and}$$

$$\delta^{n-t-1}_k = 0 = \gamma^{i_0 j_0}_k \text{ if } k \neq i_0, j_0$$

while for $k > n-t-1$ we have

$$\delta^{n-t-1}_k = -\lambda^{j_0}_k M_{\circ i_0} + \lambda^{i_0}_k M_{\circ j_0} = -\lambda^{j_0}_k (\sum_{l=n-t}^{n} \lambda^{i_0}_l M_{\circ l}) + \lambda^{i_0}_k (\sum_{l=n-t}^{n} \lambda^{j_0}_l M_{\circ l})$$

$$= \sum_{l=n-t}^{n} (\lambda^{i_0}_k \lambda^{j_0}_l - \lambda^{i_0}_l \lambda^{j_0}_k) M_{\circ l} = \sum_{\substack{l=n-t \\ l \neq k}}^{n} (\lambda^{i_0}_k \lambda^{j_0}_l - \lambda^{i_0}_l \lambda^{j_0}_k) M_{\circ l}$$

And inductively for $i = n-t-1, \ldots, n-1$, given $\delta^i$ as demanded, we can set

$$\delta^{i+1} = \delta^i - \sum_{l=i+2}^{n} (\lambda^{i_0}_{i+1} \lambda^{j_0}_l - \lambda^{i_0}_l \lambda^{j_0}_{i+1}) \gamma^{i+1,l} \in \mathrm{span}(\{\gamma^{ij} \in C|_H \,|\, i \in Q^* \text{ or } j \in Q^*\})$$

Then, clearly, for $k < i+1$ we have $\delta^{i+1}_k = \delta^i_k = \gamma^{i_0 j_0}_k$. Furthermore, we have

$$\delta^{i+1}_{i+1} = \delta^i_{i+1} - \sum_{l=i+2}^{n} (\lambda^{i_0}_{i+1} \lambda^{j_0}_l - \lambda^{i_0}_l \lambda^{j_0}_{i+1}) M_{\circ l} = 0 = \gamma^{i_0 j_0}_{i+1}$$

while for $k > i+1$

$$\delta^{i+1}_k = \delta^i_k + (\lambda^{i_0}_{i+1} \lambda^{j_0}_k - \lambda^{i_0}_k \lambda^{j_0}_{i+1}) M_{\circ i+1} = \sum_{\substack{l=i+2 \\ l \neq k}}^{n} (\lambda^{i_0}_k \lambda^{j_0}_l - \lambda^{i_0}_l \lambda^{j_0}_k) M_{\circ l}$$

as required. □