Security of Fixed-Weight Repetitions of Special-Sound Multi-Round Proofs

Michele Battagliola[1], Riccardo Longo[2], Federico Pintore[3], Edoardo Signorini[4,5], and Giovanni Tognolini[3]

[1] Università Politecnica delle Marche, Ancona, Italy
[2] Fondazione Bruno Kessler, Center for Cybersecurity, Trento, Italy
[3] Università di Trento, Trento, Italy
[4] Telsy, Turin, Italy
[5] Politecnico di Torino, Turin, Italy

Abstract. Interactive proofs are a cornerstone of modern cryptography and as such used in many areas, from digital signatures to multy-party computation. Often the knowledge error κ of an interactive proof is not small enough, and thus needs to be reduced. This is usually achieved by repeating the interactive proof in parallel t times. Recently, it was shown that parallel repetition of any $(k_1, \ldots, k_\mu)$-special-sound multi-round public-coin interactive proof reduces the knowledge error from κ to κ^t, which is optimal. However, in many cases parallel repetitions lead to a significant increase in transcript size. A common technique to mitigate this drawback, which is often used in digital signatures obtained by using the Fiat-Shamir transform, is to use fixed-weight challenges, i.e. vectors of challenges having a constant number of entries equal to a fixed value. While widely used, this method has not been fully assessed from a security standpoint. In particular, the effect of the technique on the knowledge error of the special-sound repeated interactive proof has remained unstudied. In this work, we fill the gap and prove that a fixed-weight repetition of a $(k_1, \ldots, k_\mu)$-special-sound multi-round public-coin interactive proof is still knowledge sound. We provide an explicit bound for the knowledge error of the protocol, proving that it matches with the cheating probability of a dishonest prover. Our results apply to some recently-proposed digital signatures which are supposed to be quantum resistant, for example CROSS.

1 Introduction

Interactive Proofs. An interactive proof for a binary relation $R \subseteq \{0,1\}^* \times \{0,1\}^*$ allows a prover $\mathcal{P}$ to convince a verifier $\mathcal{V}$ that a statement x admits a witness w, i.e. $(x, w) \in R$, or even that they know a witness. It is standard to require an interactive proof to be complete and sound[6]. When an interactive

[6] A verifier $\mathcal{V}$ accepts the proof produced by a honest prover $\mathcal{P}$ – having in input $(x, w) \in R$ – with high probability, and a verifier $\mathcal{V}$ rejects proofs for a statement x which does not admit any witness with high probability, respectively.

proof is meant to allow a prover to convince a verifier they know a witness, it is further required to be knowledge sound. Informally, this means that any dishonest prover who does not know a witness can only convince a verifier with some small probability κ, which is called the knowledge error. This property is formalised by requiring that there exists an efficient algorithm - the extractor - that, given oracle access to a dishonest prover who succeeds with probability $\epsilon > \kappa$, outputs a witness with probability at least $\epsilon - \kappa$ up to a multiplicative polynomial loss in the security parameter. In practice, it is usually easier to verify that the interactive proof is special-sound, since this implies knowledge soundness. A 3-round public-coin interactive proof is special-sound if there exists an efficient algorithm that, given two valid transcripts (a, c, z) and (a, c', z') relative to the same statement x and with distinct second messages (challenges) $c \neq c'$, outputs a witness w for x. This property can be generalised to $(2\mu + 1)$-round public-coin interactive proofs, leading to the notion of $(k_1, \ldots, k_\mu)$-special soundness, which coincides with the standard special-soundness notion when $\mu = 1$ and $k_1 = 2$.

Often the knowledge error κ of an interactive proof is not small enough security-wise, and thus needs to be reduced. This is usually achieved by repeating the interactive proof in parallel t times. Recently, Attema and Fehr [AF22] proved that t parallel repetitions of a $(k_1, \ldots, k_\mu)$-special-sound multi-round public-coin interactive proof reduces the knowledge error from κ to κ^t, which is optimal.

Digital signatures. With the threat of quantum computers looming ever closer, the cryptographic community has reacted by developing alternative cryptographic solutions supposed to be resistant even to quantum algorithms. This collective effort has been further invigorated by the NIST call for standardisation [NIS17]. While the first standards covering key encapsulation and signatures are about to be drafted, the situation with the latter is not considered fully satisfactory, so NIST has launched an “on-ramp” process to standardise new signature schemes [NIS23]. Looking at the numerous signatures submitted to the NIST calls, two main generic design techniques stand out: the hash-and-sign construction and the Fiat-Shamir one. Introduced by Fiat and Shamir in [FS87], the Fiat-Shamir transform allows to turn any public-coin interactive proof into a non-interactive proof and, consequently, into a digital signature. Informally, the Fiat-Shamir transform replaces random challenges sent by the verifier with outputs of a hash function. Many post-quantum digital signatures have been designed exploiting this paradigm [Bar+21; Bal+23; Cho+23; BKV19; De +20; Duc+18], which for some post-quantum areas has proven to be the only viable option (e.g. isogeny-based cryptography). Fiat-Shamir digital signatures *inherit* the main security properties of the starting interactive proof, which almost always enjoys special soundness. In particular, the security of the resulting signature relates to the knowledge error determined by the special soundness. However, many interactive proofs, with notable exceptions like SQISign [De +20], only have very small (often binary) challenge spaces, which result in a big knowledge error. This is therefore one of those cases where the knowledge error is decreased by performing t parallel repetitions of the base interactive proof.

The fixed-weight optimisation. Parallel repetition of the base interactive proof significantly impacts the efficiency of the resulting scheme. A few generic techniques have been proposed to mitigate this issue. Some of them aim at limiting the number t of repetitions (e.g. the multiple-public-key optimisation like in [BKV19; DG19]), obtaining an improvement in both execution time and transcript size at the cost, for example, of bigger public keys. Other techniques, on the other hand, aim at reducing the transcript size at the cost of a slight increase in execution time. This is particularly desired when storage or transmission latency are the main concern. Among the latter techniques, one of the most common optimisations is using *fixed-weight challenge vectors*[7]. The challenges are the random coins sent by the verifier to the prover and here, by fixed-weight challenge vectors, we mean vectors of challenges having a constant number of entries equal to a fixed value. This optimisation is particularly helpful when different challenges have drastically different response sizes, like in [Bal+23; GPV24; Bar+21; Cho+23; RST23; Beu+23; BKP20].

The security of this solution is well understood in the case of a 3-round, public-coin, special-sound interactive proof, i.e. $\mu = 1$ and $k_1 = 2$. In fact, in this case the special soundness of the base interactive proof is preserved by the fixed-weight repeated interactive proof. However, the picture becomes fuzzy when $\mu = 1$ and $k_1 > 2$, and even more when $\mu > 1$. In particular, in the case of $(k_1, \ldots, k_\mu)$-special-sound multi-round public-coin interactive proofs with $k_1 > 2$ it is not clear whether the fixed-weight t-fold parallel repetition satisfies any useful notion of special soundness. In light of this and the implications it would have on the provable security of existing protocols like CROSS [Bal+23] or [GPV24] and future signatures, the following research question naturally arises:

> *Does a fixed-weight repetition of a $(k_1, \ldots, k_\mu)$-special-sound multi-round public-coin interactive proof enjoy knowledge soundness?*

Our Contribution. Building on the results from [AF22] we positively answer the question above by explicitly building a knowledge extractor and precisely bounding the knowledge error.

More precisely, we prove that the t-fold repetition with fixed weight w of a $(k_1, \ldots, k_\mu)$-special-sound multi-round proof is knowledge sound. We also provide an explicit expression for the knowledge error of the repeated interactive proof, which coincides with the cheating probability of a dishonest prover, showing that our result is optimal. In addition, it allows to formally prove the security of the interactive proofs underlying some recent post-quantum signatures, such as CROSS [Bal+23] and the recent SIDH-based signature of [GPV24].

[7] This optimisation is sometimes also referred as the one with *unbalanced* challenge vectors.

One of the main results of [AF22] is a knowledge extractor $\mathcal{E}$ for k-special-sound interactive proofs, whose success probability when applied to a dishonest prover $\mathcal{P}^*$ can be expressed in terms of a novel characterization of the power of $\mathcal{P}^*$. Specifically, the ability of $\mathcal{P}^*$ to correctly answer to a random challenge is measured by $\delta_k(\mathcal{P}^*)$, its worst-case success probability when $k-1$ challenges are removed from the challenge space. This new framework is particularly convenient when moving to the parallel-repetition of the interactive proof. In fact, starting from a dishonest prover $\mathcal{P}^*$ against the t-parallel repetition of a k-special-sound proof, it is possible to build t provers $\mathcal{P}_1^*, \dots, \mathcal{P}_t^*$ against the single instance of the interactive proof. By applying the previous extractor in parallel to the provers of the single instance, the probability of witness extraction can be expressed via $\delta_k(\mathcal{P}_1^*) + \dots + \delta_k(\mathcal{P}_t^*)$. From this, an optimal bound on the knowledge error of the parallel repetition is obtained.

The extraction algorithm $\mathcal{E}$ of [AF22] queries the dishonest prover on uniformly sampled challenges. Instead, when we consider fixed-weight repetitions, challenges must be sampled according to a different distribution, i.e. that obtained by taking the i-th component of a fixed-weight challenge vector. At the core of our result is a generalisation of the knowledge extractor from [AF22] which allows for the sampling of challenges according to an arbitrary distribution $\mathscr{D}$ over the challenge space. More in detail, we show that the extraction probability is given by $\delta_k(\mathcal{P}^*, \mathscr{D})/k$ for a k-special-sound interactive proof, where the probability space is defined by the challenges being sampled according to $\mathscr{D}$. For fixed-weight repetitions, we can then apply a similar approach as before: starting from a dishonest prover for the t-fold repetition with fixed weight w of the interactive proof, we build t dishonest provers on the single instance of the proof. By applying the generalised extractor in parallel, we obtain a bound on the knowledge error of the repeated interactive proof. This bound is obtained by combinatorial results which might be of independent interest.

Although the resulting expression cannot be expressed directly in terms of the knowledge error of the individual instance, the obtained knowledge error coincides with the trivial cheating probability of a dishonest prover, meaning that our result is optimal. A similar strategy is then applied to prove knowledge soundness of fixed-weight repetitions of generic $(k_1, \dots, k_\mu)$-special-sound multi-round interactive proofs. In particular, we first generalise the multi-round extractor from [AF22] over arbitrary distributions and then apply it to the fixed-weight repetitions.

The cheating probability of a dishonest prover is directly derived from the maximum size of the set of challenges to which the prover can answer without actually knowing a witness. We have translated the problem of computing these sizes into finding upper bounds for the cardinality of particular subsets of the Cartesian product of finite sets which satisfy some conditions on the components. In particular, we compute the maximum size of a set of sequences when we limit the number of different values that may appear in any single component. These combinatorial results, from which a bound on the knowledge error of fixed-weight repetitions is deduced, may find application in independent scenarios, and so we have formulated and proved them in full generality.

Organisation. In Section 2 we provide some preliminaries and definitions about interactive proofs, with a focus on multi-round ones. Next, in Section 3 we discuss some combinatorial results that, while interesting on their own, will be essential for Section 4 and Section 5, which contain the core cryptographic results of our work. In particular, Section 4 deals with the easier case of Sigma protocols, while Section 5 deals with the general multi-round case. Lastly, in Section 6 we identify some applications and draw our conclusions.

2 Preliminaries

Notation. We denote by $\mathbb{N}^*$ the set of non-zero natural numbers. For a finite set X, we write $|X|$ for the cardinality of X and by $|x|$ the number of bits necessary to represent an element $x \in X$. We denote with $\{0,1\}^*$ the set of strings of arbitrary length.

When s is a list or a vector, we write $(s)_i$ to denote the i-th element of s. If S is a set whose elements are lists or vectors, we define $(S)_i := \{x : \exists s \in S : (s)_i = x\}$.

Given μ finite sets $\mathsf{Ch}^{[1]}, \ldots, \mathsf{Ch}^{[\mu]}$ and $\mathbf{c} \in \mathsf{Ch}^{[1]} \times \ldots \times \mathsf{Ch}^{[\mu]}$, we will write $\mathbf{c} = (c^{[1]}, \ldots, c^{[\mu]})$ where $c^{[i]} \in \mathsf{Ch}^{[i]}$ for all $i \in \{1, \ldots, \mu\}$. Furthermore, given $t \in \mathbb{N}^*$ and $\mathbf{c} \in (\mathsf{Ch}^{[1]} \times \ldots \times \mathsf{Ch}^{[\mu]})^t$, we will write $\mathbf{c} = ((\mathbf{c})_1, \ldots, (\mathbf{c})_t)$ where $(\mathbf{c})_j \in \mathsf{Ch}^{[1]} \times \cdots \times \mathsf{Ch}^{[\mu]}$ and $(\mathbf{c})_j^{[i]} \in \mathsf{Ch}^{[i]}$ for all $j \in \{1, \ldots, t\}, i \in \{1, \ldots, \mu\}$.

Interactive Proofs. The aim of this work is proving knowledge soundness of fixed-weight repetitions of $(k_1, \ldots, k_\mu)$-special-sound $(2\mu + 1)$-round public-coin protocols, which are specific instances of interactive proofs. In this section we recall the definition of interactive proof, some related notions and usual security requirements. Moreover, we describe the fixed-weight repetition of an interactive proof.

Definition 1 (Binary relation). *A binary relation is a finite set $R \subseteq X \times Y$, where $X, Y \subseteq \{0,1\}^*$. Given $(x, y) \in R$, we say that y is a* witness *for the* statement *x. The set $L_R = \{x \in X \mid \exists y \in Y \text{ s.t. } (x, y) \in R\}$ is called the set of* true statements *for R, or its language.*

Definition 2 (Interactive Proof). *An interactive proof $(\mathcal{P}, \mathcal{V})$ for a binary relation $R \subseteq X \times Y$ is an interactive protocol between two probabilistic polynomial-time machines $\mathcal{P}$ and $\mathcal{V}$. The prover $\mathcal{P}$ takes as input a pair $(x, y) \in R$ while the verifier $\mathcal{V}$ takes as input x. As the output of the protocol - denoted by $(\mathcal{P}(y), \mathcal{V})(x)$ - $\mathcal{V}$ either accepts (outputs 1) or rejects (outputs 0). We say that a transcript, i.e. the set of all messages exchanged in a protocol execution, is accepting (rejecting) if $\mathcal{V}$ accepts (rejects, respectively).*

Definition 3 (Public-Coin). *An interactive proof $(\mathcal{P}, \mathcal{V})$ is* public-coin *if all $\mathcal{V}$'s random choices are made public.*

Throughout this work we assume that, within an execution of an interactive proof $(\mathcal{P}, \mathcal{V})$, the prover $\mathcal{P}$ always sends the first and the last message. Hence, the number of communication rounds is odd, i.e. of the form $2\mu + 1$ with $\mu \in \mathbb{N}^*$. We refer to an interactive proof having $2\mu + 1$ communication rounds with the name $(2\mu + 1)$-*round protocol*. When $\mu = 1$, and thus the rounds are only 3, we call it *Sigma protocol*.

If an interactive proof is public-coin, the verifier needs to send to the prover only their random choices. For this reason, we call *challenges* the messages sent by the verifier and *challenge set* the set from which verifier's messages are sampled. In the case of a $(2\mu + 1)$–round protocol, we define the challenge set Ch as the Cartesian product of μ *round challenge sets* $\mathsf{Ch}^{[i]}$, with $i \in \{1, \dots, \mu\}$, meaning that the challenge for the i-th round is sampled from $\mathsf{Ch}^{[i]}$.

Commonly, an interactive proof is required to satisfy completeness and soundness, as per definitions below.

Definition 4 (Completeness). *An interactive proof* $(\mathcal{P}, \mathcal{V})$ *for a binary relation* $R \subseteq X \times Y$ *is* complete *if, for every* $(x, y) \in R$*, we have*

$$\Pr[(\mathcal{P}(y), \mathcal{V})(x) = 0] \leq \rho(x)$$

where the value $\rho(x)$ *- called* completeness error *- is negligible (in* $|x|$*). If* $\rho(x) = 0$ *for all* $x \in L_R$*, the protocol is said to be* perfectly complete*.*

Definition 5 (Soundness). *An interactive proof* $(\mathcal{P}, \mathcal{V})$ *for a binary relation* $R \subseteq X \times Y$ *is* sound *if, for every* $x \notin L_R$ *and every prover* $\mathcal{P}^*$*, we have*

$$\Pr((\mathcal{P}^*, \mathcal{V})(x) = 1) \leq \sigma(x)$$

where the value $\sigma(x)$ *- called* soundness error *- is negligible (in* $|x|$*).*

We note that an interactive proof which satisfies both the previous properties allows a prover $\mathcal{P}$ to convince the verifier $\mathcal{V}$ that a statement x is true. It does not guarantee anything about $\mathcal{P}$'s knowledge of a witness y such that $(x, y) \in R$. This stronger feature requires *knowledge soundness.*

Definition 6 (Knowledge Soundness). *An interactive proof* $(\mathcal{P}, \mathcal{V})$ *for a binary relation* $R \subseteq X \times Y$ *is* knowledge sound*, with* knowledge error κ*, if there exists an algorithm* $\mathcal{E}$ *that, given as input any* $x \in X$ *and rewindable oracle access to a (potentially dishonest) prover* $\mathcal{P}^*$*, runs in an expected polynomial time (in* $|x|$*) and outputs a witness* $y \in Y$ *for* x *with probability*

$$\Pr[(x, \mathcal{E}^{\mathcal{P}^*}(x)) \in R] \geq \frac{\varepsilon(x, \mathcal{P}^*) - \kappa(x)}{\mathsf{poly}(|x|)},$$

where $\varepsilon(x, \mathcal{P}^*) = \Pr(\mathsf{V}(\mathcal{P}^*(x), x) = 1)$*. The algorithm* $\mathcal{E}$ *is called* knowledge extractor*.*

Remark 1. To simplify the subsequent analysis, where not otherwise specified, we will assume that the prover $\mathcal{P}^*$ is deterministic throughout the sections. In fact, it is possible to show that the extractor is well-defined even when restricted to deterministic provers only [AF22]. Indeed, suppose that $\mathcal{P}^*$ is a probabilistic prover, and denote by $\mathcal{P}^*[r]$ the deterministic prover obtained by setting the randomness of $\mathcal{P}^*$ to r. Then, it is easy to show that $\varepsilon(x, \mathcal{P}^*) = \mathbb{E}[\varepsilon(x, \mathcal{P}^*[r])]$ and $\Pr[(x, \mathcal{E}^{\mathcal{P}^*}(x)) \in R] = \mathbb{E}\Big[\Pr[(x, \mathcal{E}^{\mathcal{P}^*[r]}(x)) \in R]\Big]$, where the expected value is taken over the random choice of r.

Definition 7 (Proof of Knowledge). *An interactive proof* $(\mathcal{P}, \mathcal{V})$ *for a binary relation* $R \subseteq X \times Y$ *which satisfies both completeness with completeness error* ρ *and knowledge soundness with knowledge error* κ *is a* proof of knowledge *if there exists a positive-definite polynomial* p *over the integers such that* $1 - \rho(x) \geq \kappa(x) + \frac{1}{p(|x|)}$ *for all* $x \in X$.

A common strategy to prove the knowledge soundness of a public-coin interactive proof is showing that it enjoys special soundness, which means, informally, that there exists an extracting algorithm able to compute a witness given enough accepting transcripts relative to a true statement x. While the definition for Sigma protocols can be simply stated, for the general $(2\mu + 1)$-round case we need to firstly introduce the notion of tree of transcripts.

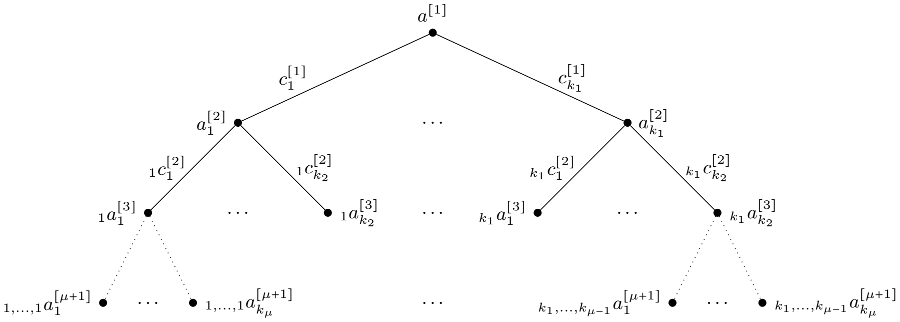

Fig. 1. Graphical representation of a $(k_1, \ldots, k_\mu)$–tree of transcripts for a $(2\mu + 1)$–round public-coin protocol. Left subscripts represent the ancestor nodes, superscripts represent the corresponding round, while right subscripts are used to enumerate edges originating from a node and their corresponding arrival nodes.

Definition 8 (Tree of Transcripts). *Let* $k_1, \ldots, k_\mu, N_1, \ldots, N_\mu \in \mathbb{N}^*$, $R \subseteq X \times Y$ *be a binary relation and* $(\mathcal{P}, \mathcal{V})$ *a* $(2\mu + 1)$*–round public-coin protocol for* R*, where* $\mathcal{V}$ *samples* i*–th challenges* ($i \in \{1, \ldots, \mu\}$) *from a set* $\mathsf{Ch}^{[i]}$ *of cardinality* $N_i \geq k_i$. *A* $(k_1, \ldots, k_\mu)$-tree of transcripts *for* $(\mathcal{P}, \mathcal{V})$ *is a set of* $K = \prod_{i=1}^{\mu} k_i$ *transcripts relative to a given statement* $x \in X$*, arranged in the following tree structure, where nodes correspond to prover's messages while edges to verifier's* *challenges. From every node at level i, with $i \in \{1, \dots, \mu\}$, exactly k_i edges originate, corresponding to k_i pairwise-distinct challenges belonging to $\mathsf{Ch}^{[i]}$. Then, each of the K transcripts corresponds to exactly one path from the root node to a leaf node.*

A graphical representation of a tree of transcripts is provided in Figure 1, where $a^{[1]}$ denotes prover's first message, $c_1^{[1]}, \dots, c_{k_1}^{[1]}$ are sampled from $\mathsf{Ch}^{[1]}$, and so on.

Definition 9 ($(k_1, \dots, k_\mu)$-Special Soundness). *Let $k_1, \dots, k_\mu$, $N_1, \dots, N_\mu \in \mathbb{N}^*$ and $R \subseteq X \times Y$ be a binary relation. A $(2\mu + 1)$-round public-coin protocol $(\mathcal{P}, \mathcal{V})$ for R, where $\mathcal{V}$ samples the i–th challenge ($i \in \{1, \dots, \mu\}$) from a set $\mathsf{Ch}^{[i]}$ of cardinality $N_i \geq k_i$, is $(k_1, \dots, k_\mu)$-out-of-$(N_1, \dots, N_\mu)$ special sound, or simply* $(k_1, \dots, k_\mu)$-special-sound*, if there exists a polynomial-time algorithm that, on input a true statement $x \in X$ and a $(k_1, \dots, k_\mu)$-tree of accepting transcripts for $(\mathcal{P}, \mathcal{V})$ and relative to x, outputs a witness $y \in Y$ for x.*

In the case of a Sigma protocol, it is immediate to prove that k-out-of-N-special soundness implies knowledge soundness with knowledge error $(k - 1)/N$. The general $(2\mu + 1)$–round case is much more involved, and it has only recently been shown [ACK21] that $(k_1, \dots, k_\mu)$-out-of-$(N_1, \dots, N_\mu)$-special soundness tightly implies knowledge soundness, with knowledge error

$$\kappa = 1 - \prod_{i=1}^{\mu} \frac{(N_i - k_i + 1)}{N_i}.$$

A common solution to decrease the knowledge error of a $(2\mu + 1)$-round knowledge sound protocol $(\mathcal{P}, \mathcal{V})$ is to repeat it in parallel multiple times, i.e. the prover and the verifier run t parallel executions of the protocol and the verifier accepts if the resulting t transcripts are accepting. We denote by $(\mathcal{P}^t, \mathcal{V}^t)$ the t-fold parallel repetition of $(\mathcal{P}, \mathcal{V})$. While this technique has been broadly adopted, it was only in 2022 that Attema and Fehr [AF22] proved that the t-fold parallel repetition of any $(k_1, \dots, k_\mu)$-special-sound multi-round public-coin protocol optimally reduces the knowledge error from κ down to κ^t.

Fixed-Weight Repetition. Parallel repetition of knowledge sound protocol improves security at the price of bigger transcripts. When responses to different challenges have very unbalanced sizes and compactness is a bigger concern than computational efficiency, it can be beneficial to use *fixed-weight challenges.*

Definition 10 (Weight). *Let Ch be a finite set, $t \in \mathbb{N}^*$ and $\tilde{c} \in \mathsf{Ch}$. For an element $c = ((c)_1, \dots, (c)_t) \in \mathsf{Ch}^t$, we define the weight of c with respect to $\tilde{c}$ as*

$$\mathsf{wt}_{\tilde{c}}(c) := |\{j \in \{1, ..., t\} : (c)_j = \tilde{c}\}|$$

Definition 11. *Let $t, w, \mu \in \mathbb{N}^*$ such that $t \geq w$, let $\mathsf{Ch}^{[1]}, \dots, \mathsf{Ch}^{[\mu]}$ be finite sets and let $\tilde{c} \in \mathsf{Ch}^{[\mu]}$. Given $\mathsf{Ch} = \mathsf{Ch}^{[1]} \times \dots \times \mathsf{Ch}^{[\mu]}$, we denote by $\mathsf{Ch}_{\tilde{c}}^{t,w}$ the set of elements of Ch^t for which $\mathsf{wt}_{\tilde{c}}\left((c)_1^{[\mu]}, \dots, (c)_t^{[\mu]}\right) = w$, i.e.*

$$\mathsf{Ch}_{\tilde{c}}^{t,w} := \left\{c = \left((c)_1^{[\mu]}, \dots, (c)_t^{[\mu]}\right) : \mathsf{wt}_{\tilde{c}}(c) = w\right\}.$$

When $\tilde{c}$ is clear from the context, we will simplify the notation and write $\mathsf{Ch}^{t,w}$ instead of $\mathsf{Ch}_{\tilde{c}}^{t,w}$. Furthermore, when Ch is not a Cartesian product but a simple set (i.e., $\mu = 1$ and so $\mathsf{Ch} = \mathsf{Ch}^{[\mu]}$), we will simply denote by $\mathsf{Ch}_{\tilde{c}}^{t,w}$ the set

$$\left\{c = ((c)_1, \dots, (c)_t) \in \mathsf{Ch}^t : \mathsf{wt}_{\tilde{c}}(c) = w\right\}.$$

Definition 12 (Fixed-weight Repetition). *Let $k_1, \dots, k_\mu$, $N_1, \dots, N_\mu \in \mathbb{N}^*$, $R \subseteq X \times Y$ be a binary relation and $(\mathcal{P}, \mathcal{V})$ be a $(2\mu+1)-$round public-coin protocol for R, where $\mathcal{V}$ samples the $i-$th challenge ($i \in \{1, \dots, \mu\}$) from a set $\mathsf{Ch}^{[i]}$ of cardinality $N_i \geq k_i$. Therefore, the challenge set of $(\mathcal{P}, \mathcal{V})$ is $\mathsf{Ch} = \prod_{i=1}^{\mu} \mathsf{Ch}^{[i]}$. Let $\tilde{c}$ be a given element of $\mathsf{Ch}^{[\mu]}$. A* (t, w)-fixed-weight parallel repetition *of $(\mathcal{P}, \mathcal{V})$ with respect to $\tilde{c}$, which we denote by $(\mathcal{P}^{t,w}, \mathcal{V}^{t,w})$, is a t-fold parallel repetition of $(\mathcal{P}, \mathcal{V})$ whose challenge set is $\mathsf{Ch}_{\tilde{c}}^{t,w}$.*

Throughout this work, we will consider fixed-weight repetitions only for $(2\mu + 1)-$round public-coin protocols for which there exists a unique element $\tilde{c} \in \mathsf{Ch}^{[\mu]}$ such that, for every possible $\mathbf{c} = (c^{[1]}, \dots, c^{[\mu]}) \in \mathsf{Ch}^{[1]} \times \dots \times \mathsf{Ch}^{[\mu]}$, the response size when $c^{[\mu]} = \tilde{c}$ is significantly higher than when $c^{[\mu]} \neq \tilde{c}$. Under this assumption, a fixed-weight repetition can lead to a more compact protocol compared to a plain parallel repetition, as it is the case for [GPV24; Bar+21; Bal+23; Cho+23; RST23].

Remark 2. In Definition 12, we choose to consider the fixed element $\tilde{c}$ as an element of $\mathsf{Ch}^{[\mu]}$ rather than in the challenge set of previous rounds or a Cartesian product of (a subset of) them. This is consistent with the applications of the fixed-weight technique listed above.

Although the fixed-weight-repetition technique can be considered well established among cryptosystem designers, to the best of our knowledge, its knowledge soundness has not been formally investigated so far. More precisely, when $\mu = 1$ and $k_1 = 2$, 2-special soundness is trivially preserved by the optimisation technique. However, the picture becomes much fuzzier as soon as $k_1 > 2$ and, even more, when $\mu > 1$. For these cases, no formal proof of the knowledge soundness has been provided so far. In Sections 4 and 5 we fill this gap with a positive result, but some preliminary mathematical results are necessary, which will be the focus of the next section.

3 Combinatorial Bounds

To prove that a fixed-weight repetition still enjoys knowledge soundness, we will rely on some combinatorial bounds. These bounds appear to be of independent interest, and for this reason we will state and prove them in full generality in this section. Nevertheless, as they will find a natural application in Sections 4 and 5, we will try to use the same notation that will be used there as much as we can.

Let us consider a finite set Ch with a fixed element $\tilde{c} \in \mathsf{Ch}$, and three positive integers k, t, w such that $|\mathsf{Ch}| \geq k \geq 2$ and $t \geq w$. Our first result regards the maximum cardinality of particular sets $S \subseteq \mathsf{Ch}_{\tilde{c}}^{t,w}$.

Proposition 1. *Given $S \subseteq \mathsf{Ch}_{\tilde{c}}^{t,w}$ such that $|(S)_i| < k$ for all $i \in \{1, \dots, t\}$, we have that, if $t \geq w(k-1)$:*

$$|S| \leq \binom{w(k-1)}{w} (k-2)^{w(k-2)} (k-1)^{t-w(k-1)},$$

and otherwise:

$$|S| \leq \binom{t}{w} (k-2)^{t-w}.$$

Proof. Since $k = 2$ trivially implies $|S| \leq 1 = \binom{w}{w} 0^0 1^{t-w}$, in the remainder we suppose $k \geq 3$.

For $s \in S$, let us define $Z(s)$ as the set of indices $i \in \{1, \dots, t\}$ such that the i-th entry of s is equal to $\tilde{c}$. The set $Z(S) := \bigcup_{s \in S} Z(s)$ is therefore formed by all indices i for which at least one element of S has $\tilde{c}$ as i-th entry. We denote $|Z(S)|$ by h_S, for which holds $h_S \geq w$ by definition of $\mathsf{Ch}_{\tilde{c}}^{t,w}$. As our goal is providing an upper bound for the cardinality of S, we can assume that, for each $i \in \{1, \dots, t\}$, it holds that $|(S)_i| = k - 1$, with $\tilde{c} \in (S)_i$ if and only if $i \in Z(S)$. Every element s of S can be thought as constructed by the following strategy. Choose a subset R of cardinality w from $Z(S)$ and, for every $i \in R$, set the i-th entry of s to $\tilde{c}$; for every $i \in Z(S) \setminus R$ choose a value in $(S)_i \setminus \{\tilde{c}\}$; finally, for every $i \in \{1, \dots, t\} \setminus Z(S)$, choose a value in $(S)_i$. This means that $|S|$ is bounded above by:

$$f(h_S) := \binom{h_S}{w} (k-2)^{h_S - w} (k-1)^{t - h_S}. \tag{1}$$

We note that $\binom{h_S}{w}(k-2)^{h_S-w}$ is monotonically increasing with ratio:

$$\frac{\binom{h_S+1}{w}(k-2)^{h_S+1-w}}{\binom{h_S}{w}(k-2)^{h_S-w}} = \frac{h_S+1}{h_S+1-w}(k-2),$$

while $(k-1)^{t-h_S}$ is monotonically decreasing with ratio:

$$\frac{(k-1)^{t-h_S}}{(k-1)^{t-(h_S+1)}} = k-1.$$

This means that f is increasing as long as

$$\frac{h_S+1}{h_S+1-w}(k-2) > k-1 \quad \Longleftrightarrow \quad h_S < w(k-1) - 1.$$

In conclusion, since $f(w(k-1)-1) = f(w(k-1))$, if $t \geq w(k-1)$ we have

$$|S| \leq f\big(w(k-1)\big) = \binom{w(k-1)}{w}(k-2)^{w(k-2)}(k-1)^{t-w(k-1)}.$$

On the other hand, if $t < w(k-1)$, then f is increasing up to t, so:

$$|S| \leq f(t) = \binom{t}{w}(k-2)^{t-w}. \qquad \square$$

We now want to generalise the above result to a setting where the set Ch is replaced by the Cartesian product of μ finite sets $\mathsf{Ch}^{[1]}, \dots, \mathsf{Ch}^{[\mu]}$, i.e. $\mathsf{Ch} := \prod_{\ell=1}^{\mu} \mathsf{Ch}^{[\ell]}$, and we fix an element $\tilde{c}$ in $\mathsf{Ch}^{[\mu]}$. We formalise such generalisation in the following definitions, by introducing the concept of acceptable set.

In the remainder of this section $k_1, \dots, k_\mu, N_1, \dots, N_\mu$ will denote positive integers such that $|\mathsf{Ch}^{[\ell]}| = N_\ell \geq k_\ell \geq 2 \ \forall \ell \in \{1, \dots, \mu\}$.

Definition 13. *For any $S \subseteq \mathsf{Ch}$, $\ell \in \{2, \dots, \mu\}$ and $(s_1, \dots, s_{\ell-1}) \in \prod_{j=1}^{\ell-1} \mathsf{Ch}^{[j]}$, we define:*

$$S_\ell(s_1, \dots, s_{\ell-1}) := \{s \in \mathsf{Ch}^{[\ell]} : \exists\, (s_1, \dots, s_{\ell-1}, s, r_{\ell+1}, \dots, r_\mu) \in S\}.$$

Informally, $S_\ell(s_1, \dots, s_{\ell-1})$ denotes the set of ℓ-th entries of the elements of S with the first $\ell - 1$ entries equal to $(s_1, \dots, s_{\ell-1})$.

Definition 14. *Given $S \subseteq \mathsf{Ch}$, for any $(a_1, \dots, a_\mu) \in \mathsf{Ch}$ we define the predicate $P_{S,\mu}$ as follows:*

$$P_{S,\mu}((a_1, \dots, a_\mu)) \iff (a_1, \dots, a_\mu) \in S.$$

For $\ell \in \{1, \dots, \mu - 1\}$, the predicate $P_{S,\ell}((a_1, \dots, a_\ell))$ is true if and only if:

$$|\{(a_1, \dots, a_\ell, a_{\ell+1}) : a_{\ell+1} \in S_{\ell+1}(a_1, \dots, a_\ell) \wedge P_{S,\ell+1}(a_1, \dots, a_{\ell+1})\}| \geq k_{\ell+1}.$$

Definition 15 (Acceptable Set). *Given $A \subseteq \mathsf{Ch}_{\tilde{c}}^{t,w}$, we say that it is a $(k_1, \dots, k_\mu)$-out-of-$(N_1, \dots, N_\mu)$ acceptable set if the following condition holds:*

$$|\{a_1 : a_1 \in (A)_i^{[1]} \wedge P_{(A)_i,1}(a_1)\}| < k_1 \qquad \forall i \in \{1, \dots, t\}.$$

Remark 3. The definition of acceptable set is meant to capture the notion of set of challenges which does not define a $(k_1, \dots, k_\mu)$-tree of accepting transcripts in the context of Definition 8.

Given an acceptable set A, it is possible to associate to A a set of t-sequences $\Big\{\big(d(A)_{1,b_1}, \dots, d(A)_{t,b_t}\big) : (b_1, \dots, b_t) \in (\mathsf{Ch}^{[\mu]})_{\tilde{c}}^{t,w}\Big\}$, where we define:

$$d(A)_{i,b_i} := |\Big\{(a)_i \in (A)_i : (a)_i^{[\mu]} = b_i\Big\}| \qquad \forall i \in \{1, \dots, t\}.$$

The result below provides a first upper bound on the cardinality of an acceptable set by building on the t-sequences defined above.

Lemma 1. *For every $(k_1,\ldots,k_\mu)$-out-of-$(N_1,\ldots,N_\mu)$ acceptable set A there exists another acceptable set $\bar{A} \supseteq A$ such that, $\forall i \in \{1,\ldots,t\}$:*

$$\sum_{x \in \mathsf{Ch}^{[\mu]}} d(\bar{A})_{i,x} = \sum_{\ell=1}^{\mu} \left(\prod_{j=\ell+1}^{\mu} N_j \right) (k_\ell - 1) \left(\prod_{j=1}^{\ell-1} (N_j - k_j + 1) \right); \qquad (2)$$

$$d(\bar{A})_{i,\tilde{c}} \geq \sum_{\ell=1}^{\mu-1} \left(\prod_{j=\ell+1}^{\mu-1} N_j \right) (k_\ell - 1) \left(\prod_{j=1}^{\ell-1} (N_j - k_j + 1) \right); \qquad (3)$$

and $|\bar{A}| = \sum_{b \in (\mathsf{Ch}^{[\mu]})^{t,w}_{\tilde{c}}} \prod_{i=1}^{t} d(\bar{A})_{i,(b)_i}$.

Proof. Let A be a $(k_1,\ldots,k_\mu)$-out-of $(N_1,\ldots,N_\mu)$ acceptable set, to construct $\bar{A} \subseteq \mathsf{Ch}^{t,w}_{\tilde{c}}$ we first build $(\bar{A})_i$ for every $i \in \{1,\ldots,t\}$. In particular, we initially set $(\bar{A})_i := \varnothing$ and then iteratively add elements to it.

Let us define $B_i(\oslash) := \{a_1 : a_1 \in (A)^{[1]}_i \wedge P_{(A)_i,1}(a_1)\}$, where $\oslash$ denotes the empty sequence. By definition of acceptable set, we have that $|B_i(\oslash)| \leq k_1 - 1$, so let $\bar{B}_i(\oslash) \subseteq \mathsf{Ch}^{[1]}$ be a set such that $B_i(\oslash) \subseteq \bar{B}_i(\oslash)$ and $|\bar{B}_i(\oslash)| = k_1 - 1$. We add to the set $(\bar{A})_i$ the following set of elements:

$$\mathrm{sat}_i(\oslash) := \left\{ (a_1, a_2, \ldots, a_\mu) : a_1 \in \bar{B}_i(\oslash) \wedge (a_2, \ldots, a_\mu) \in \prod_{j=2}^{\mu} \mathsf{Ch}^{[j]} \right\}.$$

Note that $|\mathrm{sat}_i(\oslash)| = (k_1 - 1) \cdot \prod_{j=2}^{\mu} N_j$.

For each $a_1 \in \mathsf{Ch}^{[1]} \smallsetminus \bar{B}_i(\oslash)$, let $B_i(a_1) := \left\{ a_2 : a_2 \in (A)^{[2]}_i \wedge P_{(A)_i,2}((a_1, a_2)) \right\}$. Again, by definition of acceptable set, we have that $|B_i(a_1)| \leq k_2 - 1$, so let $\bar{B}_i(a_1) \subseteq \mathsf{Ch}^{[2]}$ be a set such that $B_i(a_1) \subseteq \bar{B}_i(a_1) \wedge |\bar{B}_i(a_1)| = k_2 - 1$. We add to the set $(\bar{A})_i$ the following set of elements:

$$\mathrm{sat}_i((a_1)) := \left\{ (a_1, a_2, a_3, \ldots, a_\mu) : a_2 \in \bar{B}_i(a_1) \wedge (a_3, \ldots, a_\mu) \in \prod_{j=3}^{\mu} \mathsf{Ch}^{[j]} \right\}.$$

Note that $|\mathrm{sat}_i((a_1))| = (k_2 - 1) \cdot \prod_{j=3}^{\mu} N_j$ and $|\mathsf{Ch}^{[1]} \smallsetminus \bar{B}_i(\oslash)| = N_1 - k_1 + 1$.

In general, for $\ell \in \{2,\ldots,\mu-1\}$ and any $a_\ell \in \mathsf{Ch}^{[\ell]} \smallsetminus \bar{B}_i((a_1,\ldots,a_{\ell-1}))$, define $B_i((a_1,\ldots,a_\ell)) := \left\{ a_{\ell+1} : a_{\ell+1} \in (A)^{[\ell+1]}_i \wedge P_{(A)_i,\ell+1}((a_1,\ldots,a_\ell,a_{\ell+1})) \right\}$. As before, we have that $|B_i((a_1,\ldots,a_\ell))| \leq k_{\ell+1} - 1$, so it is possible to build a set $\bar{B}_i((a_1,\ldots,a_\ell)) \subseteq \mathsf{Ch}^{[\ell+1]}$ such that:

$$B_i((a_1,\ldots,a_\ell)) \subseteq \bar{B}_i((a_1,\ldots,a_\ell)) \wedge |\bar{B}_i((a_1,\ldots,a_\ell))| = k_{\ell+1} - 1.$$

Again, we add to the set $(\bar{A})_i$ the set of elements:

$$\mathrm{sat}_i((a_1,\ldots,a_\ell)) := \Big\{ (a_1,\ldots,a_\ell,a_{\ell+1},a_{\ell+2},\ldots,a_\mu) : \\ a_{\ell+1} \in \bar{B}_i((a_1,\ldots,a_\ell)) \wedge (a_{\ell+2},\ldots,a_\mu) \in \prod_{j=\ell+2}^{\mu} \mathsf{Ch}^{[j]} \Big\}.$$

In order to count how many elements we are adding to $(\bar{A})_i$, we observe that:

$$|\mathrm{sat}_i((a_1,\dots,a_\ell))| = (k_{\ell+1}-1)\cdot \prod_{j=\ell+2}^{\mu} N_j,$$

$$|\mathsf{Ch}^{[\ell]} \smallsetminus \bar{B}_i((a_1,\dots,a_{\ell-1}))| = N_\ell - k_\ell + 1.$$

The building of $(\bar{A})_i$ ends after μ steps, i.e. when $\ell = \mu - 1$. By construction, $(\bar{A})_i$ contains $(A)_i$. Furthermore, the intersection with $(\bar{A})_i$ of the sets that we are adding to it is always empty. Consequently, at the ℓ-th step, we are adding $\prod_{j=1}^{\ell-1}(N_j - k_j + 1)$ sets $\mathrm{sat}_i((a_1,\dots,a_{\ell-1}))$, each adding $\left(\prod_{j=\ell+1}^{\mu} N_j\right)(k_\ell - 1)$ elements to $(\bar{A})_i$. This results in the following relation:

$$|(\bar{A})_i| = \sum_{\ell=1}^{\mu}\left(\prod_{j=\ell+1}^{\mu} N_j\right)(k_\ell - 1)\left(\prod_{j=1}^{\ell-1}(N_j - k_j + 1)\right). \tag{4}$$

To construct $\bar{A}$ starting from the sets $(\bar{A})_i$, with $i \in \{1,\dots,t\}$, we take every element $((y)_1,\dots,(y)_t) \in \prod_{i=1}^{t}(\bar{A})_i \cap \mathsf{Ch}_{\tilde{c}}^{t,w}$. By construction, $A \subseteq \bar{A}$ and $\bar{A}$ is an acceptable set. Moreover, for every $i \in \{1,\dots,t\}$, we have that:

$$|(\bar{A})_i| = \sum_{x \in \mathsf{Ch}^{[\mu]}} d(\bar{A})_{i,x},$$

as for every $(y)_i \in (\bar{A})_i$ there exist $(y)_1,\dots,(y)_{i-1},(y)_{i-},\dots,(y)_t$ such that $((y)_1,\dots,(y)_t) \in \bar{A}$. A direct consequence of this is that $|\bar{A}| = \sum_{b \in S_{t,w}} \prod_{i=1}^{t} d(\bar{A})_{i,(b)_i}$.

Finally, for any $i \in \{1,\dots,t\}$ we have that:

$$d(\bar{A})_{i,\tilde{c}} \geq \sum_{\ell=1}^{\mu-1}\left(\prod_{j=\ell+1}^{\mu-1} N_j\right)(k_\ell - 1)\left(\prod_{j=1}^{\ell-1}(N_j - k_j + 1)\right),$$

as the right-hand side corresponds to the number of saturated branches in $(\bar{A})_i$, i.e. the number of elements $((y)_i^{[1]},\dots,(y)_i^{[\mu-1]}) \in \prod_{i=1}^{\mu-1}\mathsf{Ch}^{[i]}$ such that, for every x in $\mathsf{Ch}^{[\mu]}$, the element $((y)_i^{[1]},\dots,(y)_i^{[\mu-1]},x)$ belongs to $(\bar{A})_i$.

□

Lemma 2. *Let $w \leq t$, N, Z_0, Z_1, Z_2 be positive integers and consider t sequences of non-negative integers $(d_{i,0},\dots,d_{i,N})_{i\in\{1,\dots,t\}}$ such that, for every $i \in \{1,\dots,t\}$, it holds that:*

$$d_{i,0} \in \{Z_0, Z_2\}, \qquad \sum_{j=0}^{N} d_{i,j} = Z_1.$$

Let $\alpha := |\{i : d_{i,0} = Z_0\}|$, $\ell_0 := \max(0, w - t + \alpha)$, and $\ell_1 := \min(w,\alpha)$. Then:

$$\sum_{b\in S_{t,w}}\prod_{i=1}^{t} d_{i,b_i} = \sum_{\ell=\ell_0}^{\ell_1}\binom{\alpha}{\ell}\binom{t-\alpha}{w-\ell} Z_0^{\ell}\,(Z_1 - Z_0)^{\alpha-\ell}\,(Z_2)^{w-\ell}(Z_1 - Z_2)^{t-\alpha-w+\ell}, \tag{5}$$

where $S_{t,w} := \{0,\dots,N\}_0^{t,w}$ (see Definition 11).

Proof. Given $b \in S_{t,w}$, let us define four support sets:

$$\begin{aligned}
B_{1,b} &:= \{i \in \{1,\dots,t\} : b_i = 0 \wedge d_{i,0} = Z_0\},\\
B_{2,b} &:= \{i \in \{1,\dots,t\} : b_i = 0 \wedge d_{i,0} = Z_2\},\\
B_{3,b} &:= \{i \in \{1,\dots,t\} : b_i \neq 0 \wedge d_{i,0} = Z_0\},\\
B_{4,b} &:= \{i \in \{1,\dots,t\} : b_i \neq 0 \wedge d_{i,0} = Z_2\}.
\end{aligned}$$

It clearly holds that $t = |\bigsqcup_{j=1}^{4} B_{j,b}|$, $\alpha = |B_{1,b} \sqcup B_{3,b}|$, $w = |B_{1,b} \sqcup B_{2,b}|$. Therefore, we have:

$$\begin{aligned}
\sum_{b \in S_{t,w}} \prod_{i=1}^{t} d_{i,b_i} &= \sum_{b \in S_{t,w}} \prod_{j=1}^{4} \left(\prod_{i \in B_{j,b}} d_{i,b_i} \right)\\
&= \sum_{b \in S_{t,w}} \prod_{i \in B_{1,b}} d_{i,0} \prod_{i \in B_{2,b}} d_{i,0} \prod_{i \in B_{3,b}} d_{i,b_i} \prod_{i \in B_{4,b}} d_{i,b_i}\\
&= \sum_{b \in S_{t,w}} \prod_{i \in B_{1,b}} Z_0 \prod_{i \in B_{2,b}} Z_2 \prod_{i \in B_{3,b}} d_{i,b_i} \prod_{i \in B_{4,b}} d_{i,b_i}.
\end{aligned}$$

Now let us consider two disjunct sets $B_1, B_2 \subseteq \{1,\dots,t\}$, with $\ell := |B_1|$. In order for the set $B' := \{b \in S_{t,w} : B_{1,b} = B_1 \wedge B_{2,b} = B_2\}$ to be non-empty, we have that $\ell \leq \min(w, \alpha)$, and also $|B_2| = w - \ell \leq t - \alpha$, i.e., $\ell \geq \max(0, w - t + \alpha)$. Now, we have that:

$$\begin{aligned}
\sum_{b \in B'} \prod_{i=1}^{t} d_{i,b_i} &= \sum_{b \in B'} \prod_{i \in B_{1,b}} Z_0 \prod_{i \in B_{2,b}} Z_2 \prod_{i \in B_{3,b}} d_{i,b_i} \prod_{i \in B_{4,b}} d_{i,b_i}\\
&= \sum_{b \in B'} (Z_0)^{\ell} (Z_2)^{w-\ell} \prod_{i \in B_{3,b}} d_{i,b_i} \prod_{i \in B_{4,b}} d_{i,b_i}.
\end{aligned}$$

It is straightforward to see that, for any $i' \in \{1,\dots,t\}$, the equality below holds:

$$\begin{aligned}
S_{t,w} = &\left(\bigsqcup_{b' \in S_{t-1,w}} \bigsqcup_{j=1}^{N} \{(b'_1,\dots,b'_{i'-1}, j, b'_{i'},\dots,b'_{t-1})\} \right)\\
&\bigsqcup\\
&\left(\bigsqcup_{b' \in S_{t-1,w-1}} \{(b'_1,\dots,b'_{i'-1}, 0, b'_{i'},\dots,b'_{t-1})\} \right).
\end{aligned}$$

Now we want to adapt this partition to our set $B' \subseteq S_{t,w}$ by considering an index i' in $\{1,\dots,t\} \smallsetminus (B_1 \sqcup B_2)$. Let us define an index-translation function $f_{i'} : \{1,\dots,t-1\} \longrightarrow \{1,\dots,t\} \smallsetminus \{i'\}$:

$$f_{i'}(i) := \begin{cases} i & \text{if } i < i';\\ i+1 & \text{if } i \geq i'. \end{cases}$$

Then, we can define:

$$B_1(i') := \{i : f_{i'}(i) \in B_1\}, \qquad B_2(i') := \{i : f_{i'}(i) \in B_2\},$$

and introduce the set:

$$\begin{aligned} B'(i') := \{b \in S_{t-1,w} : \{i \in \{1,\dots,t-1\} : b_i = 0 \land d_{f_{i'}(i),0} = Z_0\} = B_1(i') \land \\ \land \{i \in \{1,\dots,t-1\} : b_i = 0 \land d_{f_{i'}(i),0} = Z_2\} = B_2(i')\}. \end{aligned}$$

We have that:

$$B' = \bigsqcup_{b' \in B'(i')} \bigsqcup_{j=1}^{N} \{(b'_1, \dots, b'_{i'-1}, j, b'_{i'}, \dots, b'_{t-1})\}.$$

Let us define also:

$$\begin{aligned} B_3(i') &:= \{i \in \{1,\dots,t-1\} : f_{i'}(i) \notin B_1 \bigsqcup B_2 \land d_{f_{i'}(i),0} = Z_0\}; \\ B_4(i') &:= \{i \in \{1,\dots,t-1\} : f_{i'}(i) \notin B_1 \bigsqcup B_2 \land d_{f_{i'}(i),0} = Z_2\}. \end{aligned}$$

We can use this partition in our sum. We first assume $d_{i',0} = Z_0$, which leads to:

$$\begin{aligned} \sum_{b \in B'} \prod_{i=1}^{t} d_{i,b_i} &= (Z_0)^{\ell} (Z_2)^{w-\ell} \sum_{b \in B'} \left(\prod_{i \in B_{3,b}} d_{i,b_i} \prod_{i \in B_{4,b}} d_{i,b_i} \right) \\ &= (Z_0)^{\ell} (Z_2)^{w-\ell} \sum_{b' \in B'(i')} \sum_{j=1}^{N} \left(d_{i',j} \prod_{i \in B_3(i')} d_{f_{i'}(i),b'_i} \prod_{i \in B_4(i')} d_{f_{i'}(i),b'_i} \right) \\ &= (Z_0)^{\ell} (Z_2)^{w-\ell} \sum_{b' \in B'(i')} \left(\sum_{j=1}^{N} d_{i',j} \right) \left(\prod_{i \in B_3(i')} d_{i,b'_i} \prod_{i \in B_4(i')} d_{i,b'_i} \right) \\ &= (Z_0)^{\ell} (Z_2)^{w-\ell} \sum_{b' \in B'(i')} \left(\left(\sum_{j=0}^{N} d_{i',j} \right) - d_{i',0} \right) \left(\prod_{i \in B_3(i')} d_{f_{i'}(i),b'_i} \prod_{i \in B_4(i')} d_{f_{i'}(i),b'_i} \right) \\ &= (Z_0)^{\ell} (Z_2)^{w-\ell} \sum_{b' \in B'(i')} (Z_1 - Z_0) \left(\prod_{i \in B_3(i')} d_{f_{i'}(i),b'_i} \prod_{i \in B_4(i')} d_{f_{i'}(i),b'_i} \right) \\ &= (Z_0)^{\ell} (Z_2)^{w-\ell} (Z_1 - Z_0) \sum_{b' \in B'(i')} \left(\prod_{i \in B_3(i')} d_{f_{i'}(i),b'_i} \prod_{i \in B_4(i')} d_{f_{i'}(i),b'_i} \right). \end{aligned}$$

Note that in this way we have effectively extracted the factor corresponding to the index i' without affecting the other indices, and note also that in the case where $d_{i',0} = Z_2$, the only difference is that we can factor out $(Z_1 - Z_2)$ instead of $(Z_1 - Z_0)$. If we repeat this technique starting from $B'(i')$ (whose elements have length $t-1$) instead of B' (whose elements have length t), we can factor out another index. This means that, by repeating the same partition and factoring technique for every $i' \in \{1,\dots,t\} \setminus (B_1 \bigsqcup B_2)$, and remembering that for any $b \in B'$ we have $|B_{3,b}| = \alpha - \ell$ and $|B_{4,b}| = t - \alpha - w + \ell$, we obtain:

$$\sum_{b \in B'} \prod_{i=1}^{t} d_{i,b_i} = (Z_0)^{\ell} (Z_2)^{w-\ell} (Z_1 - Z_0)^{\alpha-\ell} (Z_1 - Z_2)^{t-\alpha w+\ell}.$$

To conclude, note that for ℓ fixed there are $\binom{\alpha}{\ell}$ possible choices for B_1 and $\binom{t-\alpha}{w-\ell}$ possible choices for B_2, and that by varying ℓ, the set of all the possible B' forms a partition of $S_{t,w}$.

□

Proposition 2. *Denote with $n_{t,w}$ the maximal cardinality of a $(k_1,\dots,k_\mu)$-out-of-$(N_1,\dots,N_\mu)$ acceptable set. Then, $n_{t,w}$ is the maximum of the expression:*

$$\sum_{\ell=\max(0,w-t+\alpha)}^{\min(w,\alpha)} \binom{\alpha}{\ell}\binom{t-\alpha}{w-\ell} Z_0^\ell \left(Z_1 - Z_0\right)^{\alpha-\ell} \left(Z_2\right)^{w-\ell} (Z_1 - Z_2)^{t-\alpha-w+\ell},$$

where the maximum is taken over $\alpha \in \{0,\dots,t\}$ and

$$Z_0 := \prod_{\ell=1}^{\mu-1} N_\ell; \tag{6}$$

$$Z_1 := \sum_{\ell=1}^{\mu} \left(\prod_{j=\ell+1}^{\mu} N_j\right)(k_\ell - 1)\left(\prod_{j=1}^{\ell-1}(N_j - k_j + 1)\right); \tag{7}$$

$$Z_2 := \sum_{\ell=1}^{\mu-1} \left(\prod_{j=\ell+1}^{\mu-1} N_j\right)(k_\ell - 1)\left(\prod_{j=1}^{\ell-1}(N_j - k_j + 1)\right). \tag{8}$$

Proof. Notice that, thanks to Lemma 1 we can always limit ourselves to consider acceptable sets $\bar{A}$ such that for every $i \in \{1,\dots,t\}$ the following conditions hold:

$$\sum_{x\in \mathsf{Ch}^{[\mu]}} d_{i,x}(\bar{A}) = Z_1, \qquad d_{i,\tilde{c}}(\bar{A}) \geq Z_2, \tag{9}$$

with Z_1, Z_2 respectively as in Eq. 7 and 8. Then,

$$n_{t,w} := \max_{A}\{|A|\} = \max_{\bar{A}}\left\{|\bar{A}|\right\} = \max_{\bar{A}}\left\{\sum_{b\in(\mathsf{Ch}^{[\mu]})_{\tilde{c}}^{t,w}} \prod_{i=1}^{t} d(\bar{A})_{i,(b)_i}\right\}. \tag{10}$$

For simplicity of notation we remove below the dependence from $\bar{A}$, we biject the elements of $\mathsf{Ch}^{[\mu]}$ with the set $\{0,\dots,N_\mu - 1\}$ mapping $\tilde{c}$ to 0, and again we define $S_{t,w} := \{0,\dots,N_\mu - 1\}_0^{t,w}$. We will also denote with $\{(\bar{d}_{i,0},\dots,\bar{d}_{i,N_\mu-1})\}_{i\in\{1,\dots,t\}}$ a generic set that respects the conditions imposed by Equation (9). We would therefore like to find a valid assignment of $(\bar{d}_{i,j})_{i,j}$ that maximizes the expression above. We show that it is sufficient to consider sets such that, for each index $i \in \{1,\dots,t\}$,

$$\left(\bar{d}_{i,0}, \sum_{j=1}^{N_\mu-1} \bar{d}_{i,j}\right) \in \{(Z_0, Z_1 - Z_0), (Z_2, Z_1 - Z_2)\}. \tag{11}$$

Consider the case $i = 1$ (the extension to the generic case $i \neq 1$ is immediate) and notice that:

$$n_{t,w} = \max \left\{ \bar{d}_{1,0} \sum_{(b_2,\ldots,b_t) \in S_{t-1,w-1}} \prod_{i=2}^{t} \bar{d}_{i,b_i} + \right.$$
$$\left. + \left(\sum_{j=1}^{N_\mu - 1} \bar{d}_{1,j} \right) \sum_{(b_2,\ldots,b_t) \in S_{t-1,w}} \prod_{i=2}^{t} \bar{d}_{i,b_i} \right\}.$$

It is straightforward to see that the best way to maximize $n_{t,w}$ is to maximize either $\bar{d}_{1,0}$ or $\sum_{j=1}^{N_\mu - 1} \bar{d}_{1,j}$. In particular, if we have that:

$$\sum_{(b_2,\ldots,b_t) \in S_{t-1,w-1}} \prod_{i=2}^{t} \bar{d}_{i,b_i} \geq \sum_{(b_2,\ldots,b_t) \in S_{t-1,w}} \prod_{i=2}^{t} \bar{d}_{i,b_i},$$

then the maximum is obtained when we take $\bar{d}_{1,0} = Z_0$ (and consequently $\sum_{j=1}^{N_\mu - 1} \bar{d}_{1,j} = Z_1 - Z_0$). Otherwise, since $\bar{d}_{1,0}$ is always greater or equal than Z_2, the best way to maximize the expression is to choose $\sum_{j=1}^{N_\mu - 1} \bar{d}_{1,j} = Z_1 - Z_2$ and $\bar{d}_{1,0} = Z_2$.

Since we can consider only sets of this type when maximizing Eq. 10, Lemma 2 applies with Z_0, Z_1 and Z_2 respectively as in Eq. 6, 7 and 8, $N := N_\mu - 1$. This concludes the proof. □

4 Fixed-Weight Repetition of a k-Special-Sound Sigma Protocol

Let $(\mathcal{P}, \mathcal{V})$ be a k-special-sound Sigma protocol, with challenge space Ch. We make a two-fold assumption on the protocol:

- the knowledge error $(k-1)/N$ is not negligible in the security parameter;
- the response size for a specific challenge $\tilde{c} \in \mathsf{Ch}$ significantly exceeds the response sizes for the other challenges.

To reduce the knowledge error while limiting the increase in the overall response size, a common technique is to repeat the protocol in parallel t times, with exactly w repetitions using the unfavourable challenge $\tilde{c}$. We denote by $(\mathcal{P}^{t,w}, \mathcal{V}^{t,w})$ the resulting protocol. In this section, we want to prove that such scheme is knowledge sound. To this end, we first slightly generalize the notation and results in [AF22] by, at times, replacing the uniform distribution with an arbitrary one.

A dishonest prover against the Sigma protocol $(\mathcal{P}, \mathcal{V})$ can be described as an arbitrary (possibly probabilistic) algorithm $\mathcal{A}\colon \mathsf{Ch} \to \{0,1\}^*$. Let $\mathsf{V}\colon \mathsf{Ch} \times \{0,1\}^* \to \{0,1\}$ be a verification function. Throughout this section $\mathscr{D}$ will denote a probability distribution over Ch with support Ch. We define the *$\mathscr{D}$-success probability* of $\mathcal{A}$ as

$$\varepsilon^{\mathsf{V}}(\mathcal{A},\mathscr{D}) = \Pr[\mathsf{V}(C,\mathcal{A}(C)) = 1],$$

where the probability space is defined by C being sampled from Ch according to the probability distribution $\mathscr{D}$ and the randomness of $\mathcal{A}$. When not specified, we assume $\mathscr{D}$ is the uniform distribution over Ch and we write $\varepsilon^{\mathsf{V}}(\mathcal{A})$. Similarly, we adapt the worst-case success probability of $\mathcal{A}$ for a random challenge when $k-1$ challenges are removed from Ch, as follows:

$$\delta_k^{\mathsf{V}}(\mathcal{A},\mathscr{D}) = \min_{S\subset\mathsf{Ch}:|S|=k-1} \Pr[\mathsf{V}(C,\mathcal{A}(C)) = 1 \mid C \notin S].$$

It is easily seen that $\delta_1^{\mathsf{V}}(\mathcal{A},\mathscr{D}) = \varepsilon^{\mathsf{V}}(\mathcal{A},\mathscr{D})$. Moreover, in the following lemma we prove that $\delta_k^{\mathsf{V}}(\mathcal{A},\mathscr{D})$ is a decreasing function in k for any choice of $\mathscr{D}$.

Lemma 3. *Let $\mathscr{D}$ be a probability distribution over Ch. Then, for all $k \in \mathbb{N}^*$,*

$$\delta_{k+1}^{\mathsf{V}}(\mathcal{A},\mathscr{D}) \leq \delta_k^{\mathsf{V}}(\mathcal{A},\mathscr{D}).$$

Proof. Let C be a random variable distributed as $\mathscr{D}$ and let $S \subseteq \mathsf{Ch}$ be such that it minimizes $\delta_k^{\mathsf{V}}(\mathcal{A},\mathscr{D})$. Moreover, let $\bar{S} = \mathsf{Ch} \setminus S$ and $\bar{S}' = \{c \in \bar{S} \mid \mathsf{V}(c,\mathcal{A}(c)) = 1\}$. Then, for any $c' \in \bar{S}'$, we have

$$\begin{aligned}\delta_{k+1}^{\mathsf{V}}(\mathcal{A},\mathscr{D}) &\leq \Pr[\mathsf{V}(C,\mathcal{A}(C)) = 1 \mid C \notin S \cup \{c'\}] = \frac{(\sum_{c\in\bar{S}'} \Pr[C=c]) - \Pr[C=c']}{(\sum_{c\in\bar{S}} \Pr[C=c]) - \Pr[C=c']} \\ &\leq \frac{\sum_{c\in\bar{S}'} \Pr[C=c]}{\sum_{c\in\bar{S}} \Pr[C=c]} = \delta_k^{\mathsf{V}}(\mathcal{A},\mathscr{D}).\end{aligned}$$

□

In the following, we also consider the restriction $\mathscr{D}|_S$ of $\mathscr{D}$ to a subset $S \subseteq \mathsf{Ch}$.

Definition 16 (Distribution Restriction). *Let $\mathscr{D}$ be a probability distribution over Ch and let $X \sim \mathscr{D}$. For any subset $S \subseteq \mathsf{Ch}$, the* restriction *$\mathscr{D}|_S$ of $\mathscr{D}$ to S is defined by the following density function*

$$\Pr[X|_S = x] = \frac{\Pr[X=x]}{\sum_{x'\in S} \Pr[X=x']}, \qquad \textit{for all } x \in S.$$

A simple adaptation of [AF22, Lemma 2] proves the existence of an extraction algorithm $\mathcal{E}^{\mathcal{A}}(\mathscr{D})$, with oracle access to $\mathcal{A}$ and that samples challenges from Ch following the distribution $\mathscr{D}$, which runs in expected polynomial time and succeeds with probability at least $\delta_k^{\mathsf{V}}(\mathcal{A},\mathscr{D})/k$. The extraction algorithm is described in Figure 2.

Lemma 4. *Let $k \in \mathbb{N}^*$, Ch be a finite set with cardinality $N \geq k$, $\mathsf{V}\colon \mathsf{Ch}\times\{0,1\}^* \to \{0,1\}$ an arbitrary function and $\mathscr{D}$ an arbitrary probability distribution over Ch. Then there exists an algorithm $\mathcal{E}^{\mathcal{A}}(\mathscr{D})$ so that, given oracle access to any (probabilistic) algorithm $\mathcal{A}\colon \mathsf{Ch} \to \{0,1\}^*$, $\mathcal{E}^{\mathcal{A}}(\mathscr{D})$ requires an expected number of at most $2k-1$ queries to $\mathcal{A}$ and, with probability at least $\delta_k^{\mathsf{V}}(\mathcal{A},\mathscr{D})/k$, it outputs k pairs $(c_1,y_1),(c_2,y_2),\ldots,(c_k,y_k) \in \mathsf{Ch}\times\{0,1\}^*$ with $\mathsf{V}(c_i,y_i) = 1$ for all i and $c_i \neq c_j$ for all $i \neq j$.*

Input: $k \in \mathbb{N}^*$, Ch a finite set with $|\mathsf{Ch}| = N \geq k$ and $S \subseteq \mathsf{Ch}$ with $|S| \geq k$.
Oracle access: algorithm $\mathcal{A}\colon \mathsf{Ch} \to \{0,1\}^*$ and verification function $\mathsf{V}\colon \mathsf{Ch} \times \{0,1\}^* \to \{0,1\}$.
Output: if successful, $(c_1, y_1), \dots, (c_k, y_k) \in \mathsf{Ch} \times \{0,1\}^*$ with $\mathsf{V}(c_i, y_i) = 1$ for all i and $c_i \neq c_j$ for $i \neq j$, otherwise $\perp$.

```
Sample $c_1 \in S$ according to $\mathscr{D}|_S$ and obtain $y_1 \leftarrow \mathcal{A}(c_1)$
if $\mathsf{V}(c_1, y_1) = 0$ then abort and output $\perp$
if $\mathsf{V}(c_1, y_1) = 1$ and $k = 1$ then output $(c_1, y_1) \in \mathsf{Ch} \times \{0,1\}^*$
else
  repeat
    set $S' = S \setminus \{c_1\}$ and run $\mathcal{E}^{\mathcal{A}}(\mathscr{D}|_{S'})$
    set $\mathsf{coin} \leftarrow \mathsf{V}(d, \mathcal{A}(d))$ with $d \in S$ sampled according to $\mathscr{D}|_S$
  until $\mathcal{E}^{\mathcal{A}}(\mathscr{D}|_{S'})$ outputs $(c_2, y_2), \dots, (c_k, y_k)$ or $\mathsf{coin} = 1$
if $\mathsf{coin} = 1$ then return $\perp$
else return $(c_1, y_1), \dots, (c_k, y_k)$
```

Fig. 2. Extractor $\mathcal{E}^{\mathcal{A}}(\mathscr{D}|_S)$

Proof. The proof is similar to the proof of [AF22, Lemma 2]. In the original proof, the extractor samples the challenges uniformly from a subset $S \subseteq \mathsf{Ch}$. Here, we need to consider the natural restriction of $\mathscr{D}$ to S as per Definition 16. Since we are assuming that $\mathscr{D}$ has support equal to Ch, the restriction is well-defined. Then Lemma 3 is enough to adapt the proof of [AF22, Lemma 2] and obtain the claim. □

4.1 Knowledge Soundness of Fixed-Weight Repetitions

We now consider the (t, w)-fixed-weight repetition $(\mathcal{P}^{t,w}, \mathcal{V}^{t,w})$ of a k-out-of-N special-sound Sigma protocol $(\mathcal{P}, \mathcal{V})$. With reference to Definitions 10 and 12, we assume that the challenge space for $(\mathcal{P}, \mathcal{V})$ is $\mathsf{Ch} = \{0, \dots, N-1\}$ and the unfavourable challenge in $\tilde{c} = 0$, and we write $\mathsf{wt}(c)$ in place of $\mathsf{wt}_0(c)$.

The uniform distribution on $\mathsf{Ch}^{t,w} = \mathsf{Ch}_0^{t,w}$ induces t probability distributions $\mathscr{D}_i$ on Ch, obtained by taking the i-th component of a challenge uniformly sampled from $\mathsf{Ch}^{t,w}$.

Definition 17. *For every $i \in \{1, \dots, t\}$ we define the probability distribution $\mathscr{D}_i$ over Ch as the probability distribution having the following density function:*

$$\Pr[X_i = a] = \frac{|\{c \in \mathsf{Ch}^{t,w} \mid (c)_i = a\}|}{|\mathsf{Ch}^{t,w}|}.$$

An adversary against $(\mathcal{P}^{t,w}, \mathcal{V}^{t,w})$ is described by a (possibly probabilistic) algorithm $\mathcal{A}\colon \mathsf{Ch}^{t,w} \to \{0,1\}^*$. The success probability of $\mathcal{A}$ is defined as

$$\varepsilon^V(\mathcal{A}) = \Pr[\mathsf{V}(C, \mathcal{A}(C)) = 1],$$

for some verification algorithm $\mathsf{V}\colon \mathsf{Ch}^{t,w} \times \{0,1\}^* \to \{0,1\}$, where C is a random variable uniformly distributed over $\mathsf{Ch}^{t,w}$.

From $\mathcal{A}$, we can define t algorithms $\mathcal{A}_1, \dots, \mathcal{A}_t$, considering only a single invocation of $(\mathcal{P}, \mathcal{V})$. In particular, each $\mathcal{A}_i$ takes as input a challenge $c_i \in \mathsf{Ch}$ and runs $y \leftarrow \mathcal{A}(c = (c_i, \bar{c}))$, where $\bar{c}$ is sampled uniformly at random from $\mathsf{Ch}^{t-1,w-1}$ if $c_i = 0$ or from $\mathsf{Ch}^{t-1,w}$ otherwise, and $\mathcal{A}$ appropriately reorder its input so that c_i is the i-th component of c (i.e. $(c)_i = c_i$). Finally, $\mathcal{A}_i$ returns y along with $\bar{c}$.

Notice that, when the input challenge c_i for $\mathcal{A}_i$ is sampled according to the probability distribution $\mathscr{D}_i$ over Ch (see Definition 17), then the inputs passed to $\mathcal{A}$ are uniformly distributed over $\mathsf{Ch}^{t,w}$. In this case, for each $\mathcal{A}_i$, we can run the extractor $\mathcal{E}^{\mathcal{A}_i}(\mathscr{D}_i)$ of Figure 2. From Lemma 4, the extraction succeeds with probability at least $\delta_k^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i)/k$, where

$$\delta_k^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i) = \min_{S_i \subset \mathsf{Ch}:|S_i|=k-1} \Pr[\mathsf{V}(D_i, \mathcal{A}(D_i)) = 1 \mid D_i \notin S_i\,],$$

D_i is distributed as $\mathscr{D}_i$ and V appropriately reorder its input[8].

In the following lemma we show that, when executed in parallel, at least one of the extractors $\mathcal{E}^{\mathcal{A}_i}(\mathscr{D}_i)$ succeeds with high probability in producing k challenge-response pairs that verify V and such that the i-th components of the challenges are all distinct.

Lemma 5. *Let $k, t \in \mathbb{N}^*$, $1 \le w \le t$ and Ch a finite set with cardinality $N \ge k$. Let $\mathsf{V}\colon \mathsf{Ch}^{t,w} \times \{0,1\}^* \to \{0,1\}$ and let $\mathcal{A}$ be a (probabilistic) algorithm that takes as input $c \in \mathsf{Ch}^{t,w}$ and returns a string $y \in \{0,1\}^*$. Then*

$$\sum_{i=1}^{t} \delta_k^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i) \ge \frac{\varepsilon^V(\mathcal{A}) - \kappa_{t,w}}{1 - \kappa^{(1)}},$$

where

- $\kappa^{(1)} = \min\left\{\frac{w}{t} + (k-2)\frac{t-w}{t(N-1)}, (k-1)\frac{t-w}{t(N-1)}\right\}$;
- $\kappa_{t,w} = \binom{t}{w}^{-1} \frac{\eta_{t,w}}{(N-1)^{t-w}}$, *with*

$$\eta_{t,w} = \begin{cases} \binom{w(k-1)}{w}(k-2)^{w(k-2)}(k-1)^{t-w(k-1)} & \text{if } t \ge w(k-1) \\ \binom{t}{w}(k-2)^{t-w} & \text{otherwise} \end{cases}.$$

Proof. Let $(C)_i$ be the i-th component of the random variable C uniformly distributed over $\mathsf{Ch}^{t,w}$ and let Λ denote the event $\mathsf{V}(C, \mathcal{A}(C)) = 1$. Therefore $\Pr[\Lambda] = \varepsilon^{\mathsf{V}}(\mathcal{A})$. For $i \in \{1, \dots, t\}$, let $S_i \subset \mathsf{Ch}$ be such that it minimizes $\delta_k^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i)$. Then,

$$\sum_{i=1}^{t} \delta_k^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i) = \sum_{i=1}^{t} \Pr[\mathsf{V}(D_i, \mathcal{A}_i(D_i)) = 1 \mid D_i \notin S_i\,] = \sum_{i=1}^{t} \Pr[\Lambda \mid (C)_i \notin S_i\,]$$

[8] The verification function for $\mathcal{A}_i$ is the same V considered for $\mathcal{A}$, but seen as a function of the form $\mathsf{Ch} \times (\mathsf{Ch}^{t-1} \times \{0,1\}^*)$.

as, for any $i \in \{1, \ldots, t\}$, D_i and $(C)_i$ are identically distributed and it holds that

$$\begin{aligned}
&\Pr[\mathsf{V}(D_i, \mathcal{A}_i(D_i)) = 1 \mid D_i \notin S_i\,] = \Pr[\mathsf{V}((C)_i, \mathcal{A}_i((C)_i)) = 1 \mid (C)_i \notin S_i\,] = \\
&\quad = \sum_{c \in \mathsf{Ch}^{t,w}} \Pr[\mathsf{V}((c)_i, \mathcal{A}_i((c)_i)) = 1 \mid C = c\,] \Pr[C = c \mid (C)_i \notin S_i\,] \\
&\quad = \sum_{c \in \mathsf{Ch}^{t,w}} \Pr[\mathsf{V}(c, \mathcal{A}(c)) = 1 \mid C = c\,] \Pr[C = c \mid (C)_i \notin S_i\,] = \Pr[\Lambda \mid (C)_i \notin S_i\,].
\end{aligned}$$

From elementary probability, it follows that

$$\begin{aligned}
\sum_{i=1}^{t} \Pr[\Lambda \mid (C)_i \notin S_i\,] &= \sum_{i=1}^{t} \frac{\Pr[\Lambda \wedge (C)_i \notin S_i]}{\Pr[(C)_i \notin S_i]} = \sum_{i=1}^{t} \frac{\Pr[\Lambda \wedge (C)_i \notin S_i]}{1 - \Pr[(C)_i \in S_i]} \\
&\geq \frac{\Pr[\Lambda \wedge \bigcup_i (C)_i \notin S_i]}{1 - \Pr[(C)_1 \in S_1]} \geq \frac{\Pr[\Lambda] - \Pr[\bigcap_i (C)_i \in S_i]}{1 - \Pr[(C)_1 \in S_1]},
\end{aligned}$$

where in the first inequality we can take $1/(1 - \Pr[(C)_1 \in S_1])$ out of the sum by observing that, for any $i \in \{1, \ldots, t\}$,

$$\Pr[(C)_i \in S_i] = \begin{cases} \frac{w}{t} + (k-2)\frac{t-w}{t(N-1)} & \text{if } 0 \in S_i \\ (k-1)\frac{t-w}{t(N-1)} & \text{otherwise} \end{cases}.$$

In addition, $\Pr[(C)_i \in S_i] \geq \min_{S_1} \Pr[(C)_1 \in S_1] =: \kappa^{(1)}$.

Moreover, let us define

$$\kappa_{t,w} = \max_{S_1, \ldots, S_t} \Pr[(C)_1 \in S_1 \wedge (C)_2 \in S_2 \wedge \ldots \wedge (C)_t \in S_t],$$

where the maximum is over all sets $S_i \subset \mathsf{Ch}$ with $|S_i| = k - 1$. Notice that, equivalently, $\kappa_{t,w} = \Pr[C \in S]$, where $S \subset \mathsf{Ch}^{t,w}$ depends on the sets $S_1, \ldots, S_t$ that maximize the probability. The maximal size $\eta_{t,w}$ of S is computed in Proposition 1 as

$$\eta_{t,w} = \begin{cases} \binom{w(k-1)}{w}(k-2)^{w(k-2)}(k-1)^{t-w(k-1)} & \text{if } t \geq w(k-1) \\ \binom{t}{w}(k-2)^{t-w} & \text{otherwise} \end{cases}.$$

Therefore

$$\kappa_{t,w} = \Pr[C \in S] \leq \frac{\eta_{t,w}}{|\mathsf{Ch}^{t,w}|} = \binom{t}{w}^{-1} \frac{\eta_{t,w}}{(N-1)^{t-w}},$$

which completes the proof. □

In light of Lemma 5, we can bound the probability that at least one extractor $\mathcal{E}^{\mathcal{A}_i}(\mathscr{D}_i)$ is successful as follows:

$$\max_{1 \leq i \leq t} \delta_k^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i) \geq \frac{1}{t} \sum_{i=1}^{t} \delta_k^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i) \geq \frac{\varepsilon^{\mathsf{V}}(\mathcal{A}) - \kappa_{t,w}}{t(1 - \kappa^{(1)})}.$$

As a consequence, the (t, w)-fixed-weight repetition $(\mathcal{P}^{t,w}, \mathcal{V}^{t,w})$ of a k-special-sound Sigma protocol $(\mathcal{P}, \mathcal{V})$ is knowledge sound with knowledge error $\kappa_{t,w}$.

Theorem 1 (Fixed-Weight Repetition of a k-Special-Sound Sigma Protocol). *Let $(\mathcal{P},\mathcal{V})$ be a k-out-of-N special-sound Sigma protocol. Let $(\mathcal{P}^{t,w},\mathcal{V}^{t,w})$ be the (t,w)-fixed-weight repetition of $(\mathcal{P},\mathcal{V})$, where $k,t\in\mathbb{N}^*$ and $1\leq w\leq t$. Then $(\mathcal{P}^{t,w},\mathcal{V}^{t,w})$ is knowledge sound with knowledge error $\kappa^{t,w}$, where*

$$\kappa_{t,w}=\binom{t}{w}^{-1}\frac{\eta_{t,w}}{(N-1)^{t-w}},$$

with

$$\eta_{t,w}=\begin{cases}\binom{w(k-1)}{w}(k-2)^{w(k-2)}(k-1)^{t-w(k-1)} & \text{if } t\geq w(k-1)\\ \binom{t}{w}(k-2)^{t-w} & \text{otherwise}\end{cases}.$$

Remark 4. Recently, [AFR23] considered a further generalisation, named Γ-special soundness, of the notion of k-special soundness, where the subset of challenges from which it is possible to extract a witness is determined by an arbitrary access structure Γ, i.e. a monotone set of subsets of the challenge space. The authors proved that, for any Γ-special-sound Sigma protocol, it is possible to build an extractor that has knowledge error κ_Γ and an expected running time that scales with t_Γ, where κ_Γ, t_Γ are positive integers determined by Γ. Then, if t_Γ is polynomial, Γ-special-soundness implies knowledge soundness. Moreover, they showed that both a k-special-sound Sigma protocol and its t-fold parallel repetition are Γ-special sound for a suitable access structure Γ, which led them to re-discover the results of [AF22].
The (t,w)-fixed-weight repetition of a k-special sound protocol can also be described within this framework, and the results of Theorem 1 can be obtained by techniques similar to that of [AFR23]. Unfortunately, it is not possible to find an access structure that suitably describes the (t,w)-fixed-weight repetition of a $(k_1,\ldots,k_\mu)$-special sound protocol. Therefore, with the goal of providing a clearer intuition, we have made the description of the extractor for Sigma protocols explicit, building on the techniques of [AF22] rather than those of [AFR23].

5 Fixed-Weight Repetition of a $(k_1,\ldots,k_\mu)$-Special-Sound Interactive Proof

In the following, we extend the result of Section 4 to multi-round protocols. Let $(\mathcal{P},\mathcal{V})$ be a $(k_1,\ldots,k_\mu)$-special-sound multi-round interactive proof with challenge space $\mathsf{Ch}^{[1]}\times\cdots\times\mathsf{Ch}^{[\mu]}$. We define $K=\prod_{i=1}^{\mu}k_i$ and write $\mathbf{c}=(c^{[1]},\ldots,c^{[\mu]})$ for an element $\mathbf{c}\in\mathsf{Ch}^{[1]}\times\cdots\times\mathsf{Ch}^{[\mu]}$.

Similarly to the case of 3-round protocols, with the aim of reducing the knowledge error while limiting the increase in the overall response size, we consider the t-fold parallel repetition of the protocol $(\mathcal{P},\mathcal{V})$, where exactly w repetitions use the unfavourable challenge $\tilde{c}$ in the last round. $(\mathcal{P}^{t,w},\mathcal{V}^{t,w})$ is the resulting protocol. To show that this protocol is knowledge sound, we again start by slightly generalising the notation and results in [AF22].

A dishonest prover against $(\mathcal{P}, \mathcal{V})$ can be described as an arbitrary (probabilistic) algorithm $\mathcal{A}\colon \mathsf{Ch}^{[1]} \times \cdots \times \mathsf{Ch}^{[\mu]} \to \{0,1\}^*$. Let $\mathsf{V}\colon \mathsf{Ch}^{[1]} \times \cdots \times \mathsf{Ch}^{[\mu]} \times \{0,1\}^* \to \{0,1\}$ be a verification function and $\mathscr{D} = (\mathscr{D}^{[1]}, \dots, \mathscr{D}^{[\mu]})$ a collection of probability distributions, where $\mathscr{D}^{[i]}$ is over $D^{[i]} \subseteq \mathsf{Ch}^{[i]}$ with $|D^{[i]}| \geq k_i$. We define the *$\mathscr{D}$-success probability* of $\mathcal{A}$ as

$$\varepsilon^V(\mathcal{A}, \mathscr{D}) = \Pr[\mathsf{V}(C, \mathcal{A}(C)) = 1],$$

where $C = (C^{[1]}, \dots, C^{[\mu]})$ is a random variable, with $C^{[i]}$ being distributed as $\mathscr{D}^{[1]}$. If C is uniformly distributed over $\mathsf{Ch}^{[1]} \times \cdots \times \mathsf{Ch}^{[\mu]}$, we write $\varepsilon^V(\mathcal{A})$. Similarly, we adapt the punctured success probability of $\mathcal{A}$ as

$$\delta^{\mathsf{V}}_{\mathbf{k}}(\mathcal{A}, \mathscr{D}) = \min_{S^{[1]}, S^{[2]}(\cdot), \dots, S^{[\mu]}(\cdot)} \Pr\left[\mathsf{V}(C, \mathcal{A}(C)) = 1 \,\middle|\, \substack{C^{[1]} \notin S^{[1]} \wedge C^{[2]} \notin S^{[2]}(C^{[1]}) \wedge \cdots \\ \cdots \wedge C^{[\mu]} \notin S^{[\mu]}(C^{[1]}, \dots, C^{[\mu-1]})}\right],$$

where the minimum is over all sets $S^{[1]} \in \mathsf{Ch}^{[1]}|_{k_1-1}$, and over all functions $S^{[i]}\colon \mathsf{Ch}^{[1]} \times \cdots \times \mathsf{Ch}^{[i-1]} \to \mathsf{Ch}^{[i]}|_{k_i-1}$, with $i = 2, \dots, \mu$. Here, for any $i \in \{1, \dots, t\}$, $\mathsf{Ch}^{[i]}|_{k_i-1}$ denotes the set of subsets of $\mathsf{Ch}^{[i]}$ with cardinality $k_i - 1$.

Next, we define an extraction algorithm $\mathcal{E}^{\mathcal{A}}(\mathscr{D})$ with oracle access to $\mathcal{A}$ that samples the challenges according to the distribution $\mathscr{D}$. Building on [AF22, Lemma 4], it is possible to show that $\mathcal{E}^{\mathcal{A}}(\mathscr{D})$ runs in expected polynomial time and succeeds with probability at least $\delta^{\mathsf{V}}_{k}(\mathcal{A}, \mathscr{D})/K$.

Lemma 6. *Let $k_1, \dots, k_\mu \in \mathbb{N}^*$, $K = \prod_{i=1}^{\mu} k_i$, $\mathsf{Ch}^{[1]}, \dots, \mathsf{Ch}^{[\mu]}$ finite sets with $\mathsf{Ch}^{[j]}$ having cardinality $N_j \geq k_j$, $\mathsf{V}\colon \mathsf{Ch}^{[1]} \times \cdots \times \mathsf{Ch}^{[\mu]} \times \{0,1\}^* \to \{0,1\}$ an arbitrary function and $\mathscr{D} = (\mathscr{D}^{[1]}, \dots, \mathscr{D}^{[\mu]})$ a collection of probability distributions $\mathscr{D}^{[j]}$ with support equal to $\mathsf{Ch}^{[j]}$. Then, there exists an algorithm $\mathcal{E}^{\mathcal{A}}(\mathscr{D})$ that, given oracle access to a (probabilistic) algorithm $\mathcal{A}\colon \mathsf{Ch}^{[1]} \times \cdots \times \mathsf{Ch}^{[\mu]} \to \{0,1\}^*$, with an expected number of at most $2^\mu K$ queries to $\mathcal{A}$ and with probability at least $\delta^{\mathsf{V}}_{\mathbf{k}}(\mathcal{A}, \mathscr{D})/K$, it outputs K pairs $(\mathbf{c}_1, y_1), \dots, (\mathbf{c}_K, y_K) \in \mathsf{Ch}^{[1]} \times \cdots \times \mathsf{Ch}^{[\mu]} \times \{0,1\}^*$ with $\mathsf{V}(\mathbf{c}_i, y_i) = 1$ for all $i \in \{1, \dots, \mu\}$ and such that the vectors $\mathbf{c}_i$ form a $(k_1, \dots, k_\mu)$-tree of transcripts.*

Proof. The proof resembles that of [AF22, Lemma 4], with the only difference that the single-instance extractor used internally is an instantiation of the one described in Figure 2. □

5.1 Knowledge-Soundness of Fixed-Weight Repetitions

Let $(\mathcal{P}^{t,w}, \mathcal{V}^{t,w})$ be the (t,w)-fixed-weight repetition – with respect to an unfavourable challenge $\tilde{c} \in \mathsf{Ch}^{[\mu]}$ – of a $(k_1, \dots, k_\mu)$-special-sound proof $(\mathcal{P}, \mathcal{V})$ with challenge space $\mathsf{Ch} = \mathsf{Ch}^{[1]} \times \cdots \mathsf{Ch}^{[\mu]}$.

For ease of notation, in the following we assume that the challenge space for the i-th round of $(\mathcal{P}, \mathcal{V})$ is $\mathsf{Ch}^{[i]} = \{0, \dots, N_i - 1\}$ while the unfavourable challenge for the last round is $\tilde{c} = 0$.

Definition 18. *For each $j \in \{1, \dots, \mu - 1\}$, let $\mathscr{U}^{[j]}$ be the uniform distribution over $\mathsf{Ch}^{[i]}$. For every $i \in \{1, \dots, t\}$, let $\mathscr{D}_i^{[\mu]}$ be the probability distribution having the following density function:*

$$\Pr[X_i = k] = \frac{|\{c \in (\mathsf{Ch}^{[\mu]})_0^{t,w} \mid (c)_i = k\}|}{|(\mathsf{Ch}^{[\mu]})_0^{t,w}|}.$$

Finally, let $\mathscr{D}_i = (\mathscr{U}^{[1]}, \dots, \mathscr{U}^{[\mu-1]}, \mathscr{D}_i^{[\mu]})$.

An adversary against $(\mathcal{P}^{t,w}, \mathcal{V}^{t,w})$ is described as a (possibly probabilistic) algorithm which, on input a row $\mathbf{c} = ((\mathbf{c})_1, \dots, (\mathbf{c})_t)$ of columns $(\mathbf{c})_i = ((c)_i^{[1]}, \dots, (c)_i^{[\mu]}) \in \mathsf{Ch}^{[1]} \times \dots \times \mathsf{Ch}^{[\mu]}$ of challenges such that $\mathsf{wt}_0((c)_1^{[\mu]}, \dots, (c)_t^{[\mu]}) = w$, outputs a string $y \in \{0,1\}^*$. The success probability of $\mathcal{A}$ is defined as

$$\varepsilon^V(\mathcal{A}) = \Pr[\mathsf{V}(C, \mathcal{A}(C)) = 1],$$

for some verification algorithm $\mathsf{V} \colon \mathsf{Ch}_0^{t,w} \times \{0,1\}^* \to \{0,1\}$, with C being a random variable uniformly distributed over $\mathsf{Ch}_0^{t,w}$.

Such an algorithm $\mathcal{A}$ induces t algorithms $\mathcal{A}_1, \dots, \mathcal{A}_t$, analogous to those considered in the context of a single repetition of $(\mathcal{P}, \mathcal{V})$. Each $\mathcal{A}_i$ takes as input a column $(\mathbf{c})_i \in \mathsf{Ch}^{[1]} \times \dots \times \mathsf{Ch}^{[\mu]}$. Then $\mathcal{A}_i$ runs $y \leftarrow \mathcal{A}(\mathbf{c} = ((\mathbf{c})_i, \bar{\mathbf{c}}))$, where $\bar{\mathbf{c}}$ is sampled uniformly at random from $\mathsf{Ch}_0^{t-1,w-1}$ if $(c)_i^{[\mu]} = 0$ or from $\mathsf{Ch}_0^{t-1,w}$ otherwise, and $\mathcal{A}$ is understood to appropriately reorder its input so that $(\mathbf{c})_i$ is the i-th component of $\mathbf{c}$. Finally $\mathcal{A}_i$ returns y along with $\bar{\mathbf{c}}$.

Notice that, when the input challenge for $\mathcal{A}_i$ is sampled according to the probability distribution $\mathscr{D}_i = (\mathscr{U}^{[1]}, \dots, \mathscr{U}^{[\mu-1]}, \mathscr{D}_i^{[\mu]})$ over $\mathsf{Ch}^{[1]} \times \dots \times \mathsf{Ch}^{[\mu]}$, then the inputs passed to $\mathcal{A}$ are uniformly distributed over $\mathsf{Ch}_0^{t,w}$. Hence, for each $\mathcal{A}_i$, we can consider the extractor $\mathcal{E}^{\mathcal{A}_i}(\mathscr{D}_i)$ of Lemma 6, which succeeds with probability at least $\delta_{\mathbf{k}}^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i)/K$, where

$$\delta_{\mathbf{k}}^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i) = \min_{S_i^{[1]}, S_i^{[2]}(\cdot), \dots, S_i^{[\mu]}(\cdot)} \Pr\left[\mathsf{V}(D_i, \mathcal{A}_i(D_i)) = 1 \,\middle|\, \begin{smallmatrix} D_i^{[1]} \notin S_i^{[1]} \wedge D_i^{[2]} \notin S_i^{[2]}(D_i^{[1]}) \wedge \cdots \\ \cdots \wedge D_i^{[\mu]} \notin S_i^{[\mu]}(D_i^{[1]}, \dots, D_i^{[\mu-1]}) \end{smallmatrix}\right],$$

and D_i is distributed as $\mathscr{D}_i$.

In the following lemma we show that, when executed in parallel, at least one of the extractors $\mathcal{E}^{\mathcal{A}_i}(\mathscr{D}_i)$ succeeds with high probability in producing $\prod_{i=1}^{\mu} k_i$ challenge-response pairs that verify V and such that the challenges form a $(k_1, \dots, k_\mu)$-tree of transcripts.

Lemma 7. *Let $k_1, \dots, k_\mu, t, w \in \mathbb{N}^*$ such that $1 \le w \le t$ and let $\mathsf{Ch}^{[1]}, \dots, \mathsf{Ch}^{[\mu]}$ be finite sets with $\mathsf{Ch}^{[j]}$ having cardinality $N_j \ge k_j$. Let $\mathsf{V} \colon \mathsf{Ch}_0^{t,w} \times \{0,1\}^* \to \{0,1\}$ and let $\mathcal{A}$ be a (probabilistic) algorithm that takes as input an element $\mathbf{c}$ of $\mathsf{Ch}_0^{t,w}$ and outputs a string $y \in \{0,1\}^*$. Then*

$$\sum_{i=1}^{t} \delta_{\mathbf{k}}^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i) \ge \frac{\varepsilon^V(\mathcal{A}) - \kappa_{t,w}}{1 - \kappa^{(1)}},$$

where $\kappa_{t,w}$ is the maximum, taken over $\alpha \in \{0,\ldots,t\}$, of the expression:

$$\frac{\sum_{\ell=\max(0,w-t+\alpha)}^{\min(w,\alpha)} \binom{\alpha}{\ell}\binom{t-\alpha}{w-\ell} Z_0^{\ell}\,(Z_1 - Z_0)^{\alpha-\ell}\,(Z_2)^{w-\ell}(Z_1 - Z_2)^{t-\alpha-w+\ell}}{|\mathsf{Ch}_0^{t,w}|},$$

where $|\mathsf{Ch}_0^{t,w}| = \binom{t}{w}(N_\mu - 1)^{t-w}(\prod_{i=1}^{\mu-1} N_i)^t$ *and*

$$\begin{aligned}
Z_0 &:= \prod_{\ell=1}^{\mu-1} N_\ell, \\
Z_1 &:= \sum_{\ell=1}^{\mu} \left(\prod_{j=\ell+1}^{\mu} N_j\right)(k_\ell - 1)\left(\prod_{j=1}^{\ell-1}(N_j - k_j + 1)\right), \\
Z_2 &:= \sum_{\ell=1}^{\mu-1} \left(\prod_{j=\ell+1}^{\mu-1} N_j\right)(k_\ell - 1)\left(\prod_{j=1}^{\ell-1}(N_j - k_j + 1)\right).
\end{aligned}$$

Moreover, it holds that

$$\kappa^{(1)} \geq 1 - \left(\prod_{j-1}^{\mu-1} \frac{N_j - k_j + 1}{N_j}\right)\left(\frac{N_\mu - k_\mu + 1}{N_\mu - 1}\frac{t-w}{w} + \frac{w}{t}\right).$$

Proof. Let $(C)_i$ be the i-th component of the random variable C uniformly distributed over $\mathsf{Ch}_0^{t,w}$ and let $\varLambda$ be the event $\mathsf{V}(C, \mathcal{A}(C)) = 1$. Therefore $\Pr[\varLambda] = \varepsilon^V(\mathcal{A})$. For $i \in \{1,\ldots,t\}$, let $S_i^{[1]}$ and $S_i^{[2]}(\cdot),\ldots,S_i^{[\mu]}(\cdot)$ be such that they minimize $\delta_{\mathbf{k}}^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i)$. Moreover, we denote by $\varGamma_i$ the event

$$(C)_i^{[1]} \notin S_i^{[1]} \wedge (C)_i^{[2]} \notin S_i^{[2]}((C)_i^{[1]}) \wedge \cdots \wedge (C)_i^{[\mu-1]} \notin S_i^{[\mu-1]}((C)_i^{[1]},\ldots,(C)_i^{[\mu-2]})$$

and by $\varOmega_i$ the event $(C)_i^{[\mu]} \notin S_i^{[\mu]}((C)_i^{[1]},\ldots,(C)_i^{[\mu-1]})$. Moreover, we consider the probability distribution D_i which is distributed as $\mathscr{D}_i = (\mathscr{U}^{[1]},\ldots,\mathscr{U}^{[\mu-1]},\mathscr{D}_i^{[\mu]})$ over $\mathsf{Ch}^{[1]} \times \cdots \times \mathsf{Ch}^{[\mu]}$. Therefore, similarly to the proof of Lemma 5, D_i and $(C)_i$ are identically distributed for any $i \in \{1,\ldots,t\}$ and, by construction of the $\mathcal{A}_i$'s, it holds that

$$\begin{aligned}
\sum_{i=1}^{t} \delta_{\mathbf{k}}^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i) &= \sum_{i=1}^{t} \Pr\left[\mathsf{V}(D_i, \mathcal{A}_i(D_i)) = 1 \,\middle|\, \substack{D_i^{[1]}\notin S_i^{[1]}\wedge D_i^{[2]}\notin S_i^{[2]}(D_i^{[1]})\wedge\cdots \\ \cdots\wedge D_i^{[\mu]}\notin S_i^{[\mu]}(D_i^{[1]},\ldots,D_i^{[\mu-1]})}\right] \\
&= \sum_{i=1}^{t} \Pr[\varLambda \mid \varGamma_i \cap \varOmega_i\,].
\end{aligned}$$

From elementary probability, it follows that

$$\begin{aligned}
\sum_{i=1}^{t} \Pr[\varLambda \mid \varGamma_i \cap \varOmega_i\,] = \sum_{i=1}^{t} \frac{\Pr[\varLambda \wedge (\varGamma_i \cap \varOmega_i)]}{\Pr[\varGamma_i \cap \varOmega_i]} &= \sum_{i=1}^{t} \frac{\Pr[\varLambda \wedge (\varGamma_i \cap \varOmega_i)]}{\Pr[\varGamma_1 \cap \varOmega_1]} \\
\geq \frac{\Pr[\varLambda \wedge \bigcup_i (\varGamma_i \cap \varOmega_i)]}{\Pr[\varGamma_1 \cap \varOmega_1]} &\geq \frac{\Pr[\varLambda] - \Pr\left[\bigcap_i \overline{(\varGamma_i \cap \varOmega_i)}\right]}{\Pr[\varGamma_1 \cap \varOmega_1]},
\end{aligned}$$

where the second equality is obtained by observing that $\Pr[\mathit{\Gamma}_1 \cap \mathit{\Omega}_1] = \cdots = \Pr[\mathit{\Gamma}_t \cap \mathit{\Omega}_t]$.

Now, let $\kappa_{t,w} = \Pr\Big[\bigcap_{i=1}^{t} \overline{(\mathit{\Gamma}_i \cap \mathit{\Omega}_i)}\Big]$. For any $i \in \{1, \dots, t\}$, the set $S_i^{[1]}$ and the maps $S_i^{[2]}(\cdot), \dots, S_i^{[\mu]}(\cdot)$ identify a subset $(\bar{A})_i$ of $\mathsf{Ch}^{[1]} \times \cdots \times \mathsf{Ch}^{[\mu]}$ defined in the following way. The set $S_i^{[1]}$ dictates that $(\bar{A})_i$ contains

$$\left\{ (c^{[1]}, c^{[2]}, \dots, c^{[\mu]}) : c^{[1]} \in S_i^{[1]} \wedge (c^{[2]}, \dots, c^{[\mu]}) \in \prod_{j=2}^{\mu} \mathsf{Ch}^{[j]} \right\}.$$

Furthermore, the set $S_i^{[1]}$ and the map $S_i^{[2]}(\cdot)$ dictate that $(\bar{A})_i$ also contains

$$\left\{ (c^{[1]}, c^{[2]}, \dots, c^{[\mu]}) : c^{[1]} \notin S_i^{[1]} \wedge c^{[2]} \in S_i^{[2]}(c^{[1]}) \wedge (c^{[3]}, \dots, c^{[\mu]}) \in \prod_{j=3}^{\mu} \mathsf{Ch}^{[j]} \right\}.$$

By iterating this argument, we deduce that the sets $(\bar{A})_i$ have a form identical to the sets in the proof of Lemma 1 which have the same names, the only difference being that within that proof the sets $(\bar{A})_i$ were determined by a starting acceptable set A, while here they are determined by $S_i^{[1]}$ and $S_i^{[2]}(\cdot), \dots, S_i^{[\mu]}(\cdot)$. As a consequence, $\kappa_{t,w}$ corresponds to the probability of belonging to the set $\bar{A}$, which is defined as the set containing every element $((y)_1, \dots, (y)_t) \in \prod_{i=1}^{t} (\bar{A})_i$ which respects the first condition of Definition 15, i.e. $((y)_1^{[\mu]}, \dots, (y)_t^{[\mu]}) \in (\mathsf{Ch}^{[\mu]})_0^{t,w}$. By applying (the proof of) Proposition 2 to the set $\bar{A}$, we conclude that the probability $\kappa_{t,w}$ is exactly the one in the claim.

Finally, let $\kappa^{(1)} = 1 - \Pr[\mathit{\Gamma}_1 \cap \mathit{\Omega}_1]$ and write $\Pr[\mathit{\Gamma}_1 \cap \mathit{\Omega}_1] = \Pr[\mathit{\Gamma}_1] \cdot \Pr[\mathit{\Omega}_1 \mid \mathit{\Gamma}_1\ ]$. Notice that

$$\Pr[\mathit{\Gamma}_1] = \prod_{j=1}^{\mu-1} \frac{N_j - k_j + 1}{N_j}.$$

Moreover, observe that $\Pr[\mathit{\Omega}_1 \mid \mathit{\Gamma}_1\ ] = \Pr\Big[(C)_1^{[\mu]} \notin S_1^{[\mu]}\Big]$ for some set $S_1^{[\mu]} \subset \mathsf{Ch}^{[\mu]}$ with $|S_1^{[\mu]}| = k_\mu - 1$. Now, let $\bar{S}_1^{[\mu]} = \mathsf{Ch}^{[\mu]} \setminus S_1^{[\mu]}$, then

$$\Pr\Big[(C)_1^{[\mu]} \notin S_1^{[\mu]}\Big] = \Pr\Big[(C)_1^{[\mu]} \in \bar{S}_1^{[\mu]}\Big] = \frac{\eta_1}{|(\mathsf{Ch}^{[\mu]})_0^{t,w}|},$$

where the value of η_1 is given by the size of a maximal $\bar{S} \subseteq (\mathsf{Ch}^{[\mu]})_0^{t,w}$ such that $|(\bar{S})_1| \leq N_\mu - k_\mu + 1$. Following the same techniques of Proposition 1, we can explicitly compute η_1 depending on whether $0 \in \bar{S}_1^{[\mu]}$. It holds that

$$\begin{aligned}
\eta_1 &= \max \left\{ \begin{matrix} \binom{t-1}{w}(N_\mu - k_\mu + 1)(N_\mu - 1)^{t-w-1} & \text{If } 0 \notin \bar{S}_1^{[\mu]} \\ \binom{t-1}{w}(N_\mu - k_\mu)(N_\mu - 1)^{t-w-1} + \binom{t-1}{w-1}(N_\mu - 1)^{t-w} & \text{If } 0 \in \bar{S}_1^{[\mu]} \end{matrix} \right\} \\
&\leq \binom{t-1}{w}(N_\mu - k_\mu + 1)(N_\mu - 1)^{t-w-1} + \binom{t-1}{w-1}(N_\mu - 1)^{t-w} \\
&= \binom{t}{w}(N_\mu - 1)^{t-w} \left(\frac{N_\mu - k_\mu + 1}{N_\mu - 1} \frac{t-w}{w} + \frac{w}{t} \right).
\end{aligned}$$

Since $|(\mathsf{Ch}^{[\mu]})_0^{t,w}| = \binom{t}{w}(N_\mu - 1)^{t-w}$, we obtain

$$\Pr[\Gamma_1 \cap \Omega_1] \leq \left(\prod_{j=1}^{\mu-1} \frac{N_j - k_j + 1}{N_j}\right)\left(\frac{N_\mu - k_\mu + 1}{N_\mu - 1}\frac{t-w}{w} + \frac{w}{t}\right). \qquad \square$$

As for the fixed-weight repetition of a Sigma protocol, following Lemma 7 we can bound the probability that at least one extractor $\mathcal{E}^{\mathcal{A}_i}(\mathscr{D}_i)$ is successful:

$$\max_{1 \leq i \leq t} \delta_{\mathbf{k}}^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i) \geq \frac{1}{t}\sum_{i=1}^{t} \delta_{\mathbf{k}}^{\mathsf{V}}(\mathcal{A}_i, \mathscr{D}_i) \geq \frac{\varepsilon^{\mathsf{V}}(\mathcal{A}) - \kappa_{t,w}}{t \cdot (1 - \kappa^{(1)})}.$$

It follows that the (t,w)-fixed-weight repetition $(\mathcal{P}^{t,w}, \mathcal{V}^{t,w})$ of a $(k_1, \ldots, k_\mu)$-special-sound proof $(\mathcal{P}, \mathcal{V})$ is knowledge sound with knowledge error $\kappa_{t,w}$.

Theorem 2 (Fixed-Weight Repetition of a $(k_1, \ldots, k_\mu)$-Special-Sound Multi-Round Proof). *Let $(\mathcal{P}, \mathcal{V})$ be a $(k_1, \ldots, k_\mu)$-special-sound interactive proof and $(\mathcal{P}^{t,w}, \mathcal{V}^{t,w})$ be the (t,w)-fixed-weight repetition of $(\mathcal{P}, \mathcal{V})$, where $k, t \in \mathbb{N}^*$ and $1 \leq w \leq t$. Then $(\mathcal{P}^{t,w}, \mathcal{V}^{t,w})$ is knowledge sound with knowledge error $\kappa_{t,w}$, where $\kappa_{t,w}$ is the maximum, taken over $\alpha \in \{0, \ldots, t\}$, of the expression*

$$\frac{\sum_{\ell=\max(0,w-t+\alpha)}^{\min(w,\alpha)} \binom{\alpha}{\ell}\binom{t-\alpha}{w-\ell} Z_0^{\ell} (Z_1 - Z_0)^{\alpha-\ell} (Z_2)^{w-\ell} (Z_1 - Z_2)^{t-\alpha-w+\ell}}{\binom{t}{w}(N_\mu - 1)^{t-w}(\prod_{i=1}^{\mu-1} N_i)^t},$$

where Z_0, Z_1, Z_2 are defined as in Lemma 7.

6 Applications and Conclusions

In this paper, we have established a positive result about the security of fixed-weight parallel repetitions of special-sound multi-round interactive proofs. We have given an in-depth description of the optimal strategy of a dishonest prover attacking the fixed-weight repetition of the protocol. In particular, we provided an explicit expression of the adversary's cheating probability, for both the three-round and multi-round cases. Next, we generalized the knowledge extractor from [AF22], applying it to the (t,w)-fixed-weight repetition of a $(k_1, \ldots, k_\mu)$-special-sound multi-round interactive proof. We obtained a strong result on the knowledge soundness of the fixed-weight optimization, proving that the knowledge error of the protocol matches the optimal cheating probability of a dishonest prover. To the best of our knowledge, this is the first time the security of this standard optimization has been analysed, beyond 2-special-sound Sigma protocols.

Our work gives direct, tight results on the security of the protocols underlying many recent signatures. For instance, they provide an explicit knowledge error for the fixed-weight repetition of q2-identification schemes [Che+16], such as the 5-round protocol underlying CROSS [Bal+23]. Similarly, they can be applied to k-special-sound Sigma protocols, with $k > 2$, such as the recent SIDH-based signature of [GPV24].

When dealing with multi-round proofs, our results cover the fixed-weight optimization of challenges in the last round. This is a seemingly arbitrary choice, as we might consider fixed-weight challenges in intermediate rounds or in a subset of multiple rounds, but it is closely tailored to concrete applications of interactive proofs for building digital signatures. Indeed, fixed-weight optimization is motivated by the presence of challenges with larger response sizes, while intermediate rounds have typically constant-size responses. However, an extension of our results to a "generalized" fixed-weight optimization might be of interest for future protocols with different approaches from the current ones.

On the negative side, our result does not directly translate to the non-interactive case. As shown in [AFK22], the Fiat-Shamir transform of a t-fold parallel repetition of a $(k_1, \ldots, k_\mu)$-special-sound interactive proof incurs in a security loss that is exponential in the number of rounds. While the attack of [AFK22] does not specifically target fixed weight repetitions, the same heuristic could be applied to our scenario. Adapting the attack to find precise bounds for the security loss is an interesting aspect for future research, since they are crucial to determine precisely the parameters of multi-round-based signatures, such as CROSS [Bal+23].

Acknowledgments This work has been partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

The first author is supported by the Italian Ministry of University's PRIN 2022 program under the "Mathematical Primitives for Post Quantum Digital Signatures" (P2022J4HRR) and "POst quantum Identification and eNcryption primiTives: dEsign and Realization (POINTER)" (2022M2JLF2) projects funded by the European Union - Next Generation EU.

The third author acknowledges support from Ripple's University Blockchain Research Initiative and from the INDAM group GNSAGA.

Authors wish to thank Paolo Santini for the feedback and the valuable discussion about CROSS.

References

[ACK21] T. Attema, R. Cramer, and L. Kohl. "A Compressed Σ-Protocol Theory for Lattices". In: *CRYPTO 2021, Part II.* Ed. by T. Malkin and C. Peikert. Vol. 12826. LNCS. Virtual Event: Springer, Heidelberg, Aug. 2021, pp. 549–579. DOI: 10.1007/978-3-030-84245-1_19.

[AF22] T. Attema and S. Fehr. "Parallel Repetition of $(k_1, \ldots, k_\mu)$-Special-Sound Multi-round Interactive Proofs". In: *CRYPTO 2022, Part I.* Ed. by Y. Dodis and T. Shrimpton. Vol. 13507. LNCS. Springer, Heidelberg, Aug. 2022, pp. 415–443. DOI: 10.1007/978-3-031-15802-5_15.

[AFK22] T. Attema, S. Fehr, and M. Klooß. “Fiat-Shamir Transformation of Multi-round Interactive Proofs”. In: *TCC 2022, Part I.* Ed. by E. Kiltz and V. Vaikuntanathan. Vol. 13747. LNCS. Springer, Heidelberg, Nov. 2022, pp. 113–142. DOI: 10.1007/978-3-031-22318-1_5.

[AFR23] T. Attema, S. Fehr, and N. Resch. “Generalized Special-Sound Interactive Proofs and Their Knowledge Soundness”. In: *TCC 2023, Part III.* Ed. by G. N. Rothblum and H. Wee. Vol. 14371. LNCS. Springer, Heidelberg, Nov.–Dec. 2023, pp. 424–454. DOI: 10.1007/978-3-031-48621-0_15.

[Bal+23] M. Baldi et al. *CROSS — Codes and Restricted Objects Signature Scheme.* Tech. rep. available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures. National Institute of Standards and Technology, 2023.

[Bar+21] A. Barenghi, J.-F. Biasse, E. Persichetti, and P. Santini. “LESS-FM: Fine-Tuning Signatures from the Code Equivalence Problem”. In: *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021.* Ed. by J. H. Cheon and J.-P. Tillich. Springer, Heidelberg, 2021, pp. 23–43. DOI: 10.1007/978-3-030-81293-5_2.

[Beu+23] W. Beullens, S. Dobson, S. Katsumata, Y.-F. Lai, and F. Pintore. “Group signatures and more from isogenies and lattices: generic, simple, and efficient”. In: *DCC* 91.6 (2023), pp. 2141–2200. DOI: 10.1007/s10623-023-01192-x.

[BKP20] W. Beullens, S. Katsumata, and F. Pintore. “Calamari and Falafl: Logarithmic (Linkable) Ring Signatures from Isogenies and Lattices”. In: *ASIACRYPT 2020, Part II.* Ed. by S. Moriai and H. Wang. Vol. 12492. LNCS. Springer, Heidelberg, Dec. 2020, pp. 464–492. DOI: 10.1007/978-3-030-64834-3_16.

[BKV19] W. Beullens, T. Kleinjung, and F. Vercauteren. “CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations”. In: *ASIACRYPT 2019, Part I.* Ed. by S. D. Galbraith and S. Moriai. Vol. 11921. LNCS. Springer, Heidelberg, Dec. 2019, pp. 227–247. DOI: 10.1007/978-3-030-34578-5_9.

[Che+16] M.-S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, and P. Schwabe. “From 5-Pass MQ-Based Identification to MQ-Based Signatures”. In: *ASIACRYPT 2016, Part II.* Ed. by J. H. Cheon and T. Takagi. Vol. 10032. LNCS. Springer, Heidelberg, Dec. 2016, pp. 135–165. DOI: 10.1007/978-3-662-53890-6_5.

[Cho+23] T. Chou, R. Niederhagen, E. Persichetti, T. H. Randrianarisoa, K. Reijnders, S. Samardjiska, and M. Trimoska. “Take Your MEDS: Digital Signatures from Matrix Code Equivalence”. In: *AFRICACRYPT 23.* Ed. by N. El Mrabet, L. De Feo, and S. Duquesne. Vol. 14064. LNCS. Springer Nature, July 2023, pp. 28–52. DOI: 10.1007/978-3-031-37679-5_2.

[De +20] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. “SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies”.

In: *ASIACRYPT 2020, Part I*. Ed. by S. Moriai and H. Wang. Vol. 12491. LNCS. Springer, Heidelberg, Dec. 2020, pp. 64–93. DOI: `10.1007/978-3-030-64837-4_3`.

[DG19] L. De Feo and S. D. Galbraith. "SeaSign: Compact Isogeny Signatures from Class Group Actions". In: *EUROCRYPT 2019, Part III*. Ed. by Y. Ishai and V. Rijmen. Vol. 11478. LNCS. Springer, Heidelberg, May 2019, pp. 759–789. DOI: `10.1007/978-3-030-17659-4_26`.

[Duc+18] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé. "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme". In: *IACR TCHES* 2018.1 (2018). `https://tches.iacr.org/index.php/TCHES/article/view/839`, pp. 238–268. DOI: `10.13154/tches.v2018.i1.238-268`.

[FS87] A. Fiat and A. Shamir. "How to Prove Yourself: Practical Solutions to Identification and Signature Problems". In: *CRYPTO'86*. Ed. by A. M. Odlyzko. Vol. 263. LNCS. Springer, Heidelberg, Aug. 1987, pp. 186–194. DOI: `10.1007/3-540-47721-7_12`.

[GPV24] W. Ghantous, F. Pintore, and M. Veroni. "Efficiency of SIDH-based signatures (yes, SIDH)". In: *J. Math. Cryptol.* 18.1 (2024). DOI: `10.1515/JMC-2023-0023`. URL: `https://doi.org/10.1515/jmc-2023-0023`.

[NIS17] NIST. *Post-Quantum Cryptography Standardization*. URL: `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`. 2017.

[NIS23] NIST. *Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process*. URL: `https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals`. 2023.

[RST23] L. Ran, S. Samardjiska, and M. Trimoska. "Algebraic Algorithm for the Alternating Trilinear Form Equivalence Problem". In: *Code-Based Cryptography - 11th International Workshop, CBCrypto 2023, Lyon, France, April 22-23, 2023, Revised Selected Papers*. Ed. by A. Esser and P. Santini. Vol. 14311. Lecture Notes in Computer Science. Springer, 2023, pp. 84–103. DOI: `10.1007/978-3-031-46495-9\_5`. URL: `https://doi.org/10.1007/978-3-031-46495-9\_5`.