On Time-Lock Cryptographic Assumptions in Abelian Hidden-Order Groups

Aron van Baarsen and Marc Stevens
aron.van.baarsen@cwi.nl

CWI, Cryptology Group, Amsterdam, The Netherlands

Abstract. In this paper we study cryptographic finite abelian groups of unknown order and hardness assumptions in these groups. Abelian groups necessitate multiple group generators, which may be chosen at random. We formalize this setting and hardness assumptions therein. Furthermore, we generalize the algebraic group model and strong algebraic group model from cyclic groups to arbitrary finite abelian groups of unknown order. Building on these formalizations, we present techniques to deal with this new setting, and prove new reductions. These results are relevant for class groups of imaginary quadratic number fields and time-lock cryptography build upon them.

Keywords: cryptographic abelian groups, hidden order groups, algebraic group model, time-lock cryptography

1 Introduction

Abelian groups of hidden order have recently been gaining more attention in cryptography, due to their applications in, for example, time-lock cryptography [30, 22, 6], cryptographic accumulators [6] and zero-knowledge arguments [10, 3]. Both RSA groups and class groups of imaginary quadratic number fields have been proposed as hidden order groups for these applications. A trusted setup is required in the RSA group setting to hide the order, but the class group setting does not suffer from this restriction. In contrast to RSA groups, class groups are abelian groups which are not always cyclic, i.e., they may require more than one generator to generate the full group. In particular, this implies prime divisors of the group order may have multiplicity larger than one. Moreover, there are no known generic efficient algorithms for abelian groups to compute a smallest set of generators or to certify a set of elements generate the full group.

There has been significantly less study of computational assumptions in abelian groups compared to cyclic groups. This paper aims to address this gap by studying the relation between various computational problems in finite abelian groups in the (strong) algebraic group model. The algebraic group model (AGM), introduced by Fuchsbauer, Kiltz and Loss [16], requires algorithms to output an algebraic representation of their output elements in terms of input group elements. The strong algebraic group model (SAGM), introduced by Katz, Loss and Xu [17], additionally requires any algorithm to expose the circuit of group operations it computed for output group elements. Both these models have predominantly been used to study computational assumptions in cyclic groups, mainly those of prime order [16] and semiprime order [17]. Another aim of this paper is therefore to generalize the AGM and the SAGM to the setting of finite abelian groups which are not necessarily cyclic.

Restricted Group Models. There has been a relatively long history of studying computational problems in groups in a restricted model of computation. Starting with Nechaev [21] and Shoup [29] introducing the generic group model (GGM). The two main computational models relevant to this paper are the algebraic group model (AGM) [16] and the strong algebraic group model (SAGM) [17].

Intuitively speaking, in contrast to the GGM, an algorithm in the AGM is allowed to exploit any additional group structure and representation of group elements like in the standard model. However, the AGM is not equivalent to the standard model, as algorithms in the AGM are required to provide an algebraic representation of their output group elements in terms of input group

Name	Game $((\mathbb{G}, g) \xleftarrow{\$} \mathcal{G}_\kappa)$	Outcome
$\mathsf{MO}_{\mathcal{C}}$	$N \xleftarrow{\$} \mathcal{A}(g)$	$N \equiv 0 \pmod{\lvert\mathbb{G}\rvert}$
$\mathsf{HO}_{\mathcal{C}}$	$N \xleftarrow{\$} \mathcal{A}(g)$	$N = \lvert\mathbb{G}\rvert$
$\mathsf{DLog}/\mathsf{DLog}_1$	$X \xleftarrow{\$} \mathbb{G},\ e \xleftarrow{\$} \mathcal{A}(g, X)$	$g^e = X$
DLog_2	$X \xleftarrow{\$} \mathbb{G},\ Y \xleftarrow{\$} \langle X\rangle,\ e \xleftarrow{\$} \mathcal{A}(g, X, Y)$	$X^e = Y$
$\mathsf{CDH}/\mathsf{CDH}_1$	$a, b \xleftarrow{\$} \mathcal{U}_{\lvert\mathbb{G}\rvert},\ Y \xleftarrow{\$} \mathcal{A}(g, g^a, g^b)$	$Y = g^{ab}$
CDH_2	$X \xleftarrow{\$} \mathbb{G},\ a, b \xleftarrow{\$} \mathcal{U}_{\lvert\langle X\rangle\rvert},\ Y \xleftarrow{\$} \mathcal{A}(g, X, X^a, X^b)$	$Y = X^{ab}$

Here $\mathcal{G} = (\mathcal{G}_\kappa)_{\kappa=1}^{\infty}$ is a cyclic group family with security parameter κ, and $\mathcal{A}$ is an adversary playing the game. Each game starts by sampling $(\mathbb{G}, g)$. See Section 3.

Table 1. Overview of the relevant computational games in cyclic groups

Name	Game $(\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa,\ \boldsymbol{g} := (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G}^n)$	$\mathcal{A}$ wins if
MO	$N \xleftarrow{\$} \mathcal{A}(\boldsymbol{g})$	$N \equiv 0 \pmod{\lvert\mathbb{G}\rvert} \wedge N \neq 0$
HO	$N \xleftarrow{\$} \mathcal{A}(\boldsymbol{g})$	$N = \lvert\mathbb{G}\rvert$
LO	$(X, d) \xleftarrow{\$} \mathcal{A}(\boldsymbol{g})$	$X \neq 1_{\mathbb{G}} \wedge 1 < d < 2^\kappa \wedge X^d = 1_{\mathbb{G}}$
DLog_1	$X \xleftarrow{\$} \mathbb{G},\ \boldsymbol{e} \xleftarrow{\$} \mathcal{A}(\boldsymbol{g}, X)$	$\boldsymbol{g}^{\boldsymbol{e}} = X$
DLog_2	$X \xleftarrow{\$} \mathbb{G},\ Y \xleftarrow{\$} \langle X\rangle,\ e \xleftarrow{\$} \mathcal{A}(\boldsymbol{g}, X, Y)$	$X^e = Y$
CDH_2	$X \xleftarrow{\$} \mathbb{G},\ \ a, b \xleftarrow{\$} \mathcal{U}_{\lvert\langle X\rangle\rvert},\ Y \xleftarrow{\$} \mathcal{A}(\boldsymbol{g}, X, X^a, X^b)$	$Y = X^{ab}$
e-RT	$X \xleftarrow{\$} \mathbb{G},\ Y \xleftarrow{\$} \mathcal{A}(\boldsymbol{g}, X^e)$	$Y^e = X \wedge e > 1$
StRoot	$X \xleftarrow{\$} \mathbb{G},\ (Y, e) \xleftarrow{\$} \mathcal{A}(\boldsymbol{g}, X)$	$Y^e = X \wedge e > 1$
ARoot	$X \xleftarrow{\$} \mathcal{A}(\boldsymbol{g}),\ \ell \xleftarrow{\$} \mathrm{Primes}(2\kappa),\ Y \xleftarrow{\$} \mathcal{A}(X, \ell)$	$X \neq 1_{\mathbb{G}} \wedge Y^\ell = X$
T-RSW	$\mathcal{A}_2 \leftarrow \mathcal{A}_1(\boldsymbol{g}),\ X \xleftarrow{\$} \mathbb{G},\ Y \xleftarrow{\$} \mathcal{A}_2(\boldsymbol{g}, X)$	$Y = X^{2^T} \wedge \mathsf{ATime}(\mathcal{A}_2) < T$

Here $\mathcal{G} = (\mathcal{G}_\kappa)_{\kappa=1}^{\infty}$ is a group family with security parameter κ, and $\mathcal{A}$ is an adversary playing the game. Each game starts by sampling $\mathbb{G}, g_1, \ldots, g_n$. See Section 4.

Table 2. Overview of the relevant computational games in finite abelian groups

elements. The SAGM lies between the AGM and the GGM as it requires that the algorithm exposes the circuit of group operations it computed for output group elements.

In the (S)AGM one can study the hardness of computational problems through reductions to other computational problems, just as in the standard model (SM). The generic group model also allows for the proving of information-theoretic lower bounds on the complexity of computational problems. See for instance, the lower bounds on the discrete logarithm and the computational Diffie-Hellman problem by Shoup [29], and the lower bound on any generic reduction from the discrete logarithm problem to the computational Diffie-Hellman problem when the group order has a multiple prime factor by Maurer and Wolff [20].

Since reductions in the (S)AGM are typically *generic*, i.e. the reduction itself only uses generic group operations, computational lower bounds in the GGM can imply the impossibility of efficient generic reductions in the AGM.

1.1 Our Contributions

The main contributions of this paper consist of (1) a formalization of the finite abelian hidden order setting and the respective generalizations of the (S)AGM, and (2) proving security reductions in this setting as further detailed below.

In Section 4, we first formalize the setting of working with *finite abelian groups of hidden order* and introduce a framework to study computational problems therein. An important example are class groups of imaginary quadratic number fields. Instead of assuming the existence of a canonical set of generators, a sufficiently large set of random group elements is used to generate the full group. Hence, each game in Table 2 includes sampling a set of random generators.

We generalize both the AGM and SAGM to this setting, as earlier related works were restricted to prime order cyclic groups [16] and hidden order RSA groups [17], respectively. We will refer to these generalized models as the *abelian hidden order (strong) algebraic group model* (AHO-AGM and AHO-SAGM, respectively, for short).

An overview of the computational problems we consider in finite abelian hidden order groups is given in Table 2. These are (including some works that depend on them):

A \ B	DLog_1	DLog_2	CDH_2	HO	MO	T-RSW	StRoot	ARoot	e-RT	LO
DLog_1				[29], 6.6	[29], 6.6	[29], 6.6	[29], 6.6	[29], 6.6	[29], 6.6	[29], 6.6
DLog_2				[29], 6.6	[29], 6.6	[29], 6.6	[29], 6.6	[29], 6.6	[29], 6.6	[29], 6.6
CDH_2		6.3		[29], 6.8	[29], 6.8	[29], 6.8	[29], 6.8	[29], 6.8	[29], 6.8	[29], 6.8
HO										
MO	6.5	6.4	7.5	Trivial		8.2	7.1	7.2	7.4	7.3
T-RSW	6.5	6.4	7.5	[17], 6.1	[17], 6.1		7.1	7.2	7.4	7.3
StRoot	6.5	6.4	7.5	[13], 6.1	[13], 6.1	8.2		7.2	7.4	7.3
ARoot	6.5	6.4	7.5	[30], 6.1	[30], 6.1	8.2	7.1		7.4	[6]
e-RT	†[2], 6.1	†[2], 6.1	†[2], 6.1	†[2], 6.1	†[2], 6.1	†[2], 6.1	†[2], 6.1	†[2], 6.1		†[2], 6.1
LO	‡6.2,6.5	‡6.2,6.4	‡6.2,7.5	‡6.2	‡6.2	‡6.2,8.2	‡6.2,7.1	‡6.2,7.2	‡6.2,7.4	

Fig. 1. Overview of the relevant reductions $A \xrightarrow[\text{AHO-GM}]{} B$ in the finite abelian hidden order group model, where GM is in the set $\{\text{SM}, \text{AGM}, \text{SAGM}\}$. The colors and symbols in the cells mean the following:
- new results (in SM/AGM/SAGM) (■), partial results (■), no *generic* reduction (■)
- †: conditioned on e coprime with group order
- ‡: assuming an oracle for small prime subdivisor of group order

MO/HO: the *(multiple/exact) order problem* ([12, 2, 30, 22, 6, 5, 10, 17, 3]);
LO: the *low order problem* ([22, 6]);
ARoot: the *adaptive root problem* ([30, 6, 5, 10]);
StRoot: the *strong root problem* ([12, 5, 10]);
e-RT: the *e-th root problem* ([23, 2],[8, Ch. 12]);
T-RSW: the *T-repeated squaring problem* ([25, 30, 22, 6, 17]);
DLog_1: the *generalized discrete logarithm problem* ([7]);
DLog_2: the *subgroup discrete logarithm problem* ([2],[8, Ch. 12]);
CDH_2: the *subgroup computational Diffie-Hellman problem* ([9],[8, Ch. 12]).

An overview of the relevant counterparts of these computational games in cyclic groups is given in Table 1.

For *cyclic groups of hidden order*, we show in Section 3 the simple reduction $\mathsf{MO}_{\mathcal{C}} \Rightarrow \mathsf{DLog}$ in the *hidden order cyclic group model* (HO-SM). Subsequently, we prove a novel reduction $\mathsf{HO}_{\mathcal{C}} \Rightarrow \mathsf{DLog}$ in the HO-SM (see Theorem 3.5).

For *finite abelian hidden order groups*, our contributions are outlined in Figure 1 and detailed in Sections 5, 6, 7 and 8. In the AHO-SM, we prove reductions of MO to DLog_1 and DLog_2, and of LO to MO in the case where an oracle for a small prime divisor of the group order exists. We provide an example of such an oracle for the class group setting.

In the AHO-AGM, we prove that MO is equivalent to ARoot as well as StRoot. Furthermore, we prove reductions of MO to e-RT, LO and CDH_2. Lastly, in the AHO-SAGM, we prove that T-RSW is equivalent to MO.

Overview of Techniques. The main results of this paper are reductions from the problem of computing a multiple of the order of a finite abelian group to other computational problems. A key observation here is that when $\mathbb{G}$ is a finite abelian group generated by $\boldsymbol{g} = (g_1, \ldots, g_n)$, then the integer vectors $\boldsymbol{e} = (e_1, \ldots, e_n)$ with $g_1^{e_1} \cdots g_n^{e_n} = 1_{\mathbb{G}}$ form a lattice, called the *relationship lattice* of $\boldsymbol{g}$. We show in Lemma 5.1 that if one can find relations $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ which form a full rank sublattice of $L(\boldsymbol{g})$, then $|\det(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)|$ is an integer multiple of the order of $\mathbb{G}$.

In Lemma 5.4 we prove a template reduction to obtain a multiple of the group order with specified bounded loss in time and success probability, based on a given simple transformation from an adversary to a relation sampler with the following requirements: (1) repeated calls have independent and identical success probability, which may not hold for the underlying adversary; (2) n relations from n successful executions of the resulting relation sampler have negligible probability to be linearly dependent. The reduction succeeds when n linearly independent relations are obtained among $\lceil Sn/p \rceil$ calls to the sampler, where S is an oversampling parameter and p is the adversary's

advantage. Lemmas 2.6 and 2.7 on probability distribution ensembles allow us to bound the success probability loss of the reduction.

To use the template reduction for several of our results, in each case we need to construct such a relation sampler and prove it satisfies these requirements. To show that the determinant $|\det(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)|$ is non-zero, one can pick a suitable large prime p and show that the determinant is non-zero modulo p with all but negligible probability. This can be achieved by demonstrating that the relationship coefficients modulo p (i.e., the coefficients of the matrix $E = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n) \bmod p$) are distributed close, i.e., at negligible statistical distance, to uniform (see Lemma 2.5). Subsequently, we can apply the Schwartz-Zippel lemma [28, 31] to conclude that the determinant of E will be zero modulo p with negligible probability.

In order to obtain these relations with close to uniformly distributed coefficients modulo p, we query an adversary $\mathcal{A}$, which solves a given computational problem G, a number of times on independent random inputs from a fixed group $\mathbb{G}$, i.e., a new set of generators and challenge group elements. Note that by each time freshly sampling a set of generators and input challenge it also satisfies the requirement for independent and identical success probabilities.

From a correct input and output instance (and algebraic representations of these instances with respect to $\boldsymbol{g}$), we need to show one can obtain a relation with respect to $\boldsymbol{g}$. To construct relations which are distributed sufficiently close to uniform modulo p, a main observation is that if we pass an element $X = g_1^{r_1} \cdots g_n^{r_n}$ to the adversary $\mathcal{A}$, and write $r_i = r_i' + r_i'' \cdot |\langle g_i \rangle|$ with $0 \leq r_i' < |\langle g_i \rangle|$, then the group element X is independent of the values of r_i'' (as $g_i^{|\langle g_i \rangle|} = 1_{\mathbb{G}}$) and thus any execution of $\mathcal{A}$ is independent of these r_i''. If we sample r_i uniformly from a sufficiently large set, then their modular reduction $r_i'' \mod p$ is going to be distributed negligibly close to uniform modulo p as desired.

In the case of cyclic groups, we show one can obtain the *exact* group order with high probability from several multiples of the group order obtained from a discrete logarithm adversary (Theorem 3.5). The main ingredient in this proof is a theorem which states that independent uniformly sampled integers, shifted by some bounded independent integers, have greatest common divisor equal to one with high probability (Theorem 3.4).

1.2 Related Work

Damgård and Koprowski [13] considered a variant of the strong root problem StRoot and the e-th root problem e-RT in the GGM. The main difference is that our work considers these assumptions in the AGM, and the methods we use are mostly incomparable. This paper [13] did however introduce a version of the GGM in which the group order is *hidden* and introduced the notion of a *(hard) group family*, on which our definitions in Section 4 are based.

Katz et al. [17] showed a reduction from the integer factorization problem to the T-repeated squaring problem T-RSW for RSA groups in the SAGM. Their reduction is in fact a reduction from the exact order problem HO to the T-RSW problem. They show this through a reduction from HO to the multiple order problem MO, which happen to be equivalent in RSA groups [17, Lemma 1]. Although Lemma 8.1 and Theorem 8.2 of our work can be seen as a generalization of [17, Theorem 2] from the family of RSA groups to *all* finite abelian groups, the techniques we use to prove these results are distinct and novel. Additionally, our work in the finite abelian group setting investigates more relations between more computational problems. The motivation to do so is that class groups of imaginary quadratic number fields are not covered by [17], while this is one of the main candidate group families for hidden order cryptography like VDFs.

Finally, the line of work by Rotem, Segev and Shahaf [27] and Rotem and Segev [26] considers generic-group delay functions and generic-ring delay functions, respectively. In particular, they show that generically speeding up repeated squaring is equivalent to factoring [26]. Their work [26] is however again limited to rings of the form $\mathbb{Z}_N$ with $N = pq$ an RSA modulus. Moreover, the works are in the setting of the generic group model (for cyclic groups) [27] and the generic ring model [26], and their methods are unlike this work.

1.3 Applications of Hidden-Order Groups

Verifiable Delay Functions. Verifiable delay functions (VDFs) were introduced by Boneh, Bonneau, Bünz and Fisch [4] as a cryptographic primitive with proposed applications in, for

example, public randomness beacons [24, 6, 15] and computational timestamping [6, 18]. The most popular VDF constructions are those introduced by Weselowski [30] and Pietrzak [22], both are based on the notion of time-lock puzzles from Rivest, Shamir and Wagner [25]. Time-lock puzzles assume that no efficient adversary can compute X^{2^T} faster than by computing T sequential squarings, which translates to the T-RSW hardness assumption in the AHO-SAGM. We show in Theorem 8.2 that T-RSW is hard in the AHO-SAGM if it is hard to compute a multiple of the group order (i.e., MO is hard). Furthermore, these constructions assume the hardness of the adaptive root problem ARoot (for Weselowski's construction) and the low order problem LO (for Pietrzak's construction). We show in Theorem 7.2 that ARoot is hard in the AHO-AGM if MO is hard. It follows from the known standard model reduction ARoot $\Rightarrow$ LO [6] that LO is hard in the AHO-AGM if MO is hard (Corollary 7.3).

Cryptographic Accumulators. Boneh, Bünz and Fisch [5] propose a construction for a universal accumulator in a distributed setting, together with batching and aggregation techniques, in hidden order groups. The security of the accumulator is based on a variant of the strong root problem StRoot. We show in Theorem 7.1 that StRoot is hard in the AHO-AGM if MO is hard. The authors moreover construct succinct arguments for knowledge of discrete logarithms in hidden order groups based on the adaptive root problem ARoot [5].

Zero-Knowledge Arguments. Bünz et al. [10] construct transparent SNARKs based on hidden order groups, where its security depends on a variant of the strong root problem StRoot and the adaptive root problem ARoot. Block et al. [3] adapt this scheme from [10] to overcome a gap in the proof of security in order to construct time and space efficient non-interactive zero-knowledge arguments. Their construction is based on the hardness of computing a multiple of the order of a random group element, which is closely related to the MO/HO problems.

2 Preliminaries

For integers $a \leq b$, let $[a, b]$ denote the set $\{a, a+1, \ldots, b-1, b\}$ and for $a < b$ let $[a, b)$ denote $[a, b-1]$. For a positive integer n, let Primes(n) denote the set of the first 2^n primes.

Let $\mathbb{G}$ be a finite abelian group. For $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{G}^n$ and $\boldsymbol{e} = (e_1, \ldots, e_n) \in \mathbb{Z}^n$, we use the shorthand $\langle \boldsymbol{g} \rangle := \langle g_1, \ldots, g_n \rangle$ for the subgroup generated by $g_1, \ldots, g_n$, and $\boldsymbol{g}^{\boldsymbol{e}} := \prod_{i=1}^n g_i^{e_i}$ for coordinate-wise exponentiation and multiplication of the results. Furthermore, for $A = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \in \mathbb{Z}^{n \times n}$, we denote $\boldsymbol{g}^A := (\boldsymbol{g}^{\boldsymbol{a}_1}, \ldots, \boldsymbol{g}^{\boldsymbol{a}_n})$.

For a finite set S, let $\mathcal{U}_S$ denote the uniform distribution on S. Moreover, for any $0 < M \leq N$, we define $\mathcal{U}_M := \mathcal{U}_{[0,M)}$ and $\mathcal{R}_{N,M} := [x \bmod M \mid x \xleftarrow{\$} \mathcal{U}_N]$ for the probability distribution on the set $[0, M)$ obtained by reducing samples from $\mathcal{U}_N$ modulo M. For sets and probability distributions, we use $\prod$ to denote the cartesian product. In particular, for probability distributions $\mathcal{D}_i$ over domains S_i, the cartesian product $\mathcal{D} = \prod_{i=1}^n \mathcal{D}_i$ is the probability distribution over $\prod_{i=1}^n \mathcal{S}_i$ defined by the probability function: $p((x_i)_{i=1}^n) := \prod_{i=1}^n \Pr_{X_i \sim \mathcal{D}_i}[X_i = x_i]$.

We assume that all algorithms receive 1^κ as input, where κ is the security parameter. Furthermore, we assume the asymptotic runtime of our reductions is dominated by the runtime of the original adversary it calls as subroutine. To avoid unnecessary clutter, we omit asymptotic lower order additive terms in the running time analyses of our reductions. These generally include very simple operations such as sampling of integers, passing arguments between algorithms, and simple bit-wise operations. Also, we scale time units such that multiplication in the group $\mathbb{G}$ under consideration takes unit time.

2.1 Statistical Distance and Approximate Uniform Sampling

We introduce several lemmas on probability distributions that we use later on.

Lemma 2.1. *For a given positive integer $M \geq 1$, let X and Y be independent random variables on $[0, M)$ and define the random variable $Z := [X + Y \bmod M]$. If $X \sim \mathcal{U}_M$ or $Y \sim \mathcal{U}_M$, then $Z \sim \mathcal{U}_M$ is uniformly distributed on $[0, M)$ as well.*

Definition 2.2. *For given probability distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ over a finite set S, the statistical distance between $\mathcal{D}_1$ and $\mathcal{D}_2$ is defined as*

$$\delta(\mathcal{D}_1, \mathcal{D}_2) := \frac{1}{2} \sum_{x \in S} \left| \Pr_{X \sim \mathcal{D}_1}[X = x] - \Pr_{Y \sim \mathcal{D}_2}[Y = x] \right|.$$

An equivalent definition we use is the maximal absolute difference that can occur between both probability distributions over all possible events:

$$\delta(\mathcal{D}_1, \mathcal{D}_2) = \max_{T \subseteq S} \left| \Pr_{X \sim \mathcal{D}_1}[X \in T] - \Pr_{Y \sim \mathcal{D}_2}[Y \in T] \right|.$$

Lemma 2.3. *Let $M \leq N$ be positive integers and let $X \sim \mathcal{U}_N$. Then*

$$\forall y \in [0, M) : \left| \Pr[X \equiv y \bmod M] - 1/M \right| \leq 1/N,$$

hence the statistical distance between $[X \bmod M] = \mathcal{R}_{N,M}$ and $\mathcal{U}_M$ is bounded as

$$\delta\left(\mathcal{R}_{N,M}, \mathcal{U}_M\right) \leq M/2N.$$

Lemma 2.4. *Let $M \leq N$ be positive integers and let $X \sim \mathcal{U}_N$. For any $x \in [0, N)$ there are unique $y \in [0, M)$, $z \in [0, \lceil N/M \rceil)$ such that $x = y + zM$. Let $Z_y := [\lfloor X/M \rfloor \mid X \equiv y \bmod M]$ be the random variable related to z obtained by dividing X by M and rounding down, conditioned on $X \equiv y \bmod M$. Then*

$$\Pr[Z_y = z] = \begin{cases} 1/\lceil N/M \rceil & \text{if } y < (N \bmod M) \wedge y + zM \in [0, N); \\ 1/\lfloor N/M \rfloor & \text{if } y \geq (N \bmod M) \wedge y + zM \in [0, N); \\ 0 & \text{otherwise.} \end{cases}$$

Hence $Z_y \sim \mathcal{U}_{\lceil N/M \rceil}$ if $y < (N \bmod M)$ and $Z_y \sim \mathcal{U}_{\lfloor N/M \rfloor}$ otherwise. Moreover, the statistical distance between those two distributions is bounded:

$$\delta(Z_y, \mathcal{U}_{\lceil N/M \rceil}) \leq \delta(\mathcal{U}_{\lfloor N/M \rfloor}, \mathcal{U}_{\lceil N/M \rceil}) \leq 1/\lceil N/M \rceil.$$

Lemma 2.5. *Let $\mathcal{U}_M$ be the uniform distribution on the set $[0, M)$ and let $\mathcal{D}_i$ be probability distributions over the same set for $i = 1, \ldots, \ell$. Assume that there exists a constant $0 < \delta \leq 1/M\ell$ such that for all instances $x \in [0, M)$*

$$\left| \Pr_{X \sim \mathcal{D}_i}[X = x] - \Pr_{Y \sim \mathcal{U}_M}[Y = x] \right| \leq \delta.$$

Then the statistical distance between the cartesian products $\prod_{i=1}^{\ell} \mathcal{D}_i$ and $\prod_{i=1}^{\ell} \mathcal{U}_M$ is upper bounded by $\frac{1}{2}\left(\delta\ell M + (\delta\ell M)^2\right)$.

Proof. See Appendix A. □

We prove the following Lemma that we use in reductions to analyze repeatedly calling adversaries with inputs belonging to the same group.

Lemma 2.6. *Let $\mathcal{X} = \{X_i\}_{i \in I}$ be a finite probability distribution ensemble, where $X_i \sim B(N, p_i)$ follows the binomial distribution with N samples with probability p_i. Let the set $\mathcal{X}$ itself be endowed with the uniform distribution. Given $n \geq 1$, $S \geq 4$ and the average probability $p = \mathrm{E}[p_i]$, if $N = \lceil Sn/p \rceil$ then*

$$\Pr_{X \in \mathcal{X}}[X \geq n] \geq (p/2) \cdot (1 - e^{-n \cdot C_S})$$

where $C_S := (S-3)/2 + 1/S - \log(S/2)$. Note that $C_S \geq 1$ for $S \geq 8$.

Proof (sketch). The claim can be shown by analyzing the subset $\mathcal{X}_2 = \{X_i \in \mathcal{X} \mid p_i > p/2\}$ and bounding its size $|\mathcal{X}_2| \geq (p/2) \cdot |\mathcal{X}|$. For each $X_i \in \mathcal{X}_2$, one can then upper bound $\Pr[X_i \leq n]$ using Chernoff's bound and the fact that $p_i > p/2$. See Appendix A for a full version of the proof. □

Lemma 2.7. *Let $B(N,p)$ and $B(N,p')$ be binomial distributions with N samples and respective success probabilities p and p'. Then the statistical distance between these distributions is bounded by $(N^2/2) \cdot |p - p'|$.*

Proof (sketch). Define $x_{i,j} := \Pr[B(i,p) = j]$, $y_{i,j} := \Pr[B(i,p') = j]$ and $\alpha_i := \max_j |x_{i,j} - y_{i,j}|$. Then the statistical distance is bounded by $1/2 \cdot N \cdot \alpha_N$. One can show that $\alpha_1 = |p - p'|$, and for $i \geq 1$ that $\alpha_{i+1} \leq \alpha_i + \alpha_1$ since for any j:

$$\begin{aligned}
&|x_{i+1,j} - y_{i+1,j}| = \\
&|y_{1,1}(x_{i,j-1} - y_{i,j-1}) + y_{1,0}(x_{i,j} - y_{i,j}) + x_{i,j-1}(x_{1,1} - y_{1,1}) + x_{i,j}(x_{1,0} - y_{1,0})| \\
&\leq y_{1,1}\alpha_i + y_{1,0}\alpha_i + x_{i,j-1}\alpha_1 + x_{i,j}\alpha_1 \leq \alpha_i + \alpha_1,
\end{aligned}$$

It follows that $\alpha_N \leq N \cdot |p - p'|$, which proves the claim. □

2.2 Security Games and Adversaries

Definition 2.8. *A security game* G *is defined with respect to a set of parameters* par *(defining the group family) and an adversary* $\mathcal{A}$ *that plays the game. A game consists of a main procedure that receives as input a security parameter $\kappa \in \mathbb{Z}_{\geq 1}$ and at the end outputs a single bit 0 ($\mathcal{A}$ loses) or 1 ($\mathcal{A}$ wins). We denote the output of a game* G *executed with parameters* par *and adversary* $\mathcal{A}$ *as* $\mathsf{G}^{\mathcal{A}}_{\mathrm{par}}(\kappa)$*. We define the* advantage *of* $\mathcal{A}$ *in* G *as*

$$\mathsf{Adv}^{\mathsf{G}}_{\mathrm{par},\mathcal{A}}(\kappa) := \Pr[\mathsf{G}^{\mathcal{A}}_{\mathrm{par}}(\kappa) = 1].$$

We denote the (expected) running time *of* $\mathsf{G}^{\mathcal{A}}_{\mathrm{par}}(\kappa)$ *by* $\mathsf{Time}^{\mathsf{G}}_{\mathrm{par},\mathcal{A}}(\kappa)$*. We extend this notation to be able to denote the advantage conditional on an event E in* G*:*

$$\mathsf{Adv}^{\mathsf{G}}_{\mathrm{par},\mathcal{A}}|_E(\kappa) := \Pr[\mathsf{G}^{\mathcal{A}}_{\mathrm{par}}(\kappa) = 1 \mid E].$$

Definition 2.9. *Let* G, H *be security games. We write* $\mathsf{H} \xrightarrow{(\Delta_\varepsilon,\Delta_t)} \mathsf{G}$ *if there exists an algorithm* $\mathcal{R}$ *(called a $(\Delta_\varepsilon, \Delta_t)$-reduction) such that for all algorithms* $\mathcal{A}$ *playing game* G*, the algorithm* $\mathcal{B} := \mathcal{R}^{\mathcal{A}}$ *playing game* H *satisfies*

$$\mathsf{Adv}^{\mathsf{H}}_{\mathrm{par},\mathcal{B}}(\kappa) \geq \Delta_\varepsilon \cdot \mathsf{Adv}^{\mathsf{G}}_{\mathrm{par},\mathcal{A}}(\kappa) - \mathrm{negl}(\kappa),\ \mathsf{Time}^{\mathsf{H}}_{\mathrm{par},\mathcal{B}}(\kappa) \leq \Delta_t \cdot \mathsf{Time}^{\mathsf{G}}_{\mathrm{par},\mathcal{A}}(\kappa) + T(\kappa),$$

where $T(\kappa)$ is an insignificant overhead, i.e., $\lim_{\kappa\to\infty} T(\kappa)/\mathsf{Time}^{\mathsf{G}}_{\mathrm{par},\mathcal{A}}(\kappa) \to 0$.
This notation can be extended, e.g., as $\mathsf{H} \xrightarrow[\mathrm{AGM}]{(\Delta_\varepsilon,\Delta_t)} \mathsf{G}$ *to specify the reduction holds within the mentioned restricted model (*AGM *in the example).*

2.3 Algebraic Group Model

The *algebraic group model* (AGM) is a simplified model of computation introduced by Fuchsbauer et al. [16]. It lies between the generic group model (GGM), first introduced by Nechaev [21] and Shoup [29], and the standard (Turing machine) model. In the AGM all algorithms are modeled as *algebraic*. This means that for any group element $X \in \mathbb{G}$ an algorithm may output, it additionally has to output an algebraic representation $\boldsymbol{a} = (a_1, \ldots, a_\ell) \in \mathbb{Z}^\ell$ such that $X = \prod_{i=1}^{\ell} g_i^{a_i}$ in terms of the group elements $\boldsymbol{g} = (g_1, \ldots, g_\ell) \in \mathbb{G}^\ell$ the algorithm has received as input. We will denote such a representation by $[X]_{\boldsymbol{g}}$. In the GGM every algorithm only receives random identifiers of group elements and can only perform group operations through oracle queries. In contrast to the generic group model GGM, the AGM does not let us prove information-theoretic lower bounds on the complexity of algebraic adversaries trying to solve a given problem. Just as in the standard model, security implications in the AGM are proven through reductions.

The AGM has originally only been defined for *cyclic groups* $\mathbb{G}$ of *known* prime order [16]. In this work, we will generalize this to the setting where $\mathbb{G}$ is an arbitrary *finite abelian group* of *unknown* order $|\mathbb{G}|$. The formal definition will be given in Subsection 4.1.

2.4 Strong Algebraic Group Model

The *strong* algebraic group model (SAGM) has been introduced by Katz et al. [17] as a strengthened version of the algebraic group model (AGM). The SAGM lies between the GGM and the AGM. Any SAGM algorithm is algebraic, but it must expose the algebraic representation of output group elements instead as an algebraic circuit more similar to the GGM. More specifically, algorithms in the SAGM may use one or more output rounds, where in each output round any output group element must be described as a primitive group operation on one or two group elements that were input or were output in a previous round. Our definition of the SAGM is completely identical to the definition from Katz et al. [17]. However, since the definition depends on our generalized definition of the AGM, we will postpone giving the formal definition until Section 4.2.

3 Hidden Order Cyclic Group Model (HO-SM)

As a stepping stone to the theory of finite (not necessarily cyclic) abelian groups, we first consider a simple reduction of the multiple order problem $\mathsf{MO}_{\mathcal{C}}$ to the discrete logarithm problem DLog for *cyclic groups of unknown order*. Then we prove a novel reduction from $\mathsf{HO}_{\mathcal{C}}$ to DLog in Theorem 3.5, which will also illustrate some of the main techniques used in the rest of this paper.

Definition 3.1. *A* cyclic group family $\mathcal{G} = (\mathcal{G}_\kappa)_{\kappa=1}^{\infty}$ *is a family of probability distributions over finite cyclic groups defined with:*

1. *An efficient sampling algorithm* GGen *that, on input* 1^κ*, randomly samples a group* $\mathbb{G} \in \mathcal{G}_\kappa$ *and outputs a group description of* $\mathbb{G}$*, a generator* g *and* $1_{\mathbb{G}}$*.*
2. *An efficient sampling algorithm* $\mathsf{GSample}$ *which, given a group description of* $\mathbb{G}$*, outputs a group element* $x \in \mathbb{G}$ *sampled uniformly at random.*
3. *Efficient algorithms* GMul *and* GInv *that, respectively, multiplies two group elements, and inverts a group element.*
4. *A group order upper bound* $U(\kappa)$*:* $\forall\kappa\forall\mathbb{G} \in \mathcal{G}_\kappa : U(\kappa) \geq |\mathbb{G}|$*, such that* $\log U(\kappa) \in \mathrm{poly}(\kappa)$ *and* $1/U(\kappa) \in \mathrm{negl}(\kappa)$*.*

Remark 3.2. Note that the bit size of the representations of the group elements of all $\mathbb{G} \in \mathcal{G}_\kappa$ should be polynomial in the security parameter κ, since otherwise it would not be possible to construct efficient algorithms on $\mathbb{G}$. If we assume that an upper bound $p(\kappa)$ on the bit size of the representations is known, this automatically gives an upper bound $U_\kappa = 2^{p(\kappa)}$ on the order of $\mathbb{G}$, for which $\log(U_\kappa)$ is polynomial in κ.

Lemma 3.3. *For any cyclic group family* $\mathcal{G} = (\mathcal{G}_\kappa)_{\kappa=1}^{\infty}$*:*

$$\mathsf{MO}_{\mathcal{C}} \xrightarrow[\text{HO-SM}]{1,1} \mathsf{DLog}.$$

Proof. Given a DLog adversary $\mathcal{A}$, we construct an $\mathsf{MO}_{\mathcal{C}}$ adversary $\mathcal{B}^{\mathcal{A}}$ as follows, which takes inputs $\mathbb{G}, g, U$.

$r \xleftarrow{\$} \mathcal{U}_{U^2}, \quad d \leftarrow \mathcal{A}(g, g^r)$
if $g^d = g^r$ **then return** $|r - d|$ **else return** $\perp$

By Lemma 2.3, the statistical distance between $r \bmod |\mathbb{G}|$ and the uniform distribution on $[0, |\mathbb{G}|)$ has negligible bound $\varepsilon_1 := 1/U \in \mathrm{negl}(\kappa)$. Since $\mathcal{A}$ succeeds with probability $p := \mathsf{Adv}^{\mathsf{DLog}}_{(\mathbb{G},g),\mathcal{A}}$ when g^r is distributed uniformly in $\mathbb{G}$, it follows that $\mathcal{A}$ succeeds on each instance (g, g^r) with probability at least $p - \varepsilon_1$. Moreover, if $\mathcal{A}$ succeeds and $g^d = g^r$, then $\mathcal{B}^{\mathcal{A}}$ outputs $|r - d|$ which is indeed an integer multiple of the group order, but potentially zero if $r = d$.

To bound the probability that $r = d$, write $r = r' + r''|\mathbb{G}|$ with $0 \leq r' < |\mathbb{G}|$ and $r'' \in [0, N)$, where $N := \lceil U^2/|\mathbb{G}| \rceil \geq U$. Then $g^r = g^{r'}$ only depends on r', thus the execution and output d of $\mathcal{A}$ only depends on r' as well. This implies that we can view the experiment as if r is sampled, conditioned on $r \equiv r' \bmod |\mathbb{G}|$, only after we receive the output d of $\mathcal{A}(g, g^{r'})$. Note that $r'' = (r - r')/|\mathbb{G}|$ is

distributed as Z_y in Lemma 2.4, and thus r'' has statistical distance at most $1/N$ to $\mathcal{U}_N$. Since furthermore, the probability that any particular value is sampled from $\mathcal{U}_N$ is at most $1/N$, it follows that $\Pr[r = d] = \Pr[r'' = (d - r')/|\mathbb{G}|] \leq 2/N =: \varepsilon_2$, then $\varepsilon_2 \leq 2/U \in \mathrm{negl}(\kappa)$. Hence, $\mathcal{B}^{\mathcal{A}}$ outputs a non-zero multiple of the group order with probability at least $(p - \varepsilon_1)(1 - \varepsilon_2) = p - \mathrm{negl}(\kappa)$ and with the same Time complexity as $\mathcal{A}$ plus some insignificant overhead. □

The above Lemma shows that we can leverage a DLog adversary to obtain a multiple of the group order with non-negligible probability. By repeating this process with independently randomly chosen g^r, we can obtain various multiples of the group order, and using the following theorem we can show that in this way we can obtain the *exact* group order with high probability.

Theorem 3.4. *Let $k \geq 2$, $n \geq 2^{23}$, and $1 \leq d < n$ be positive integers, and let $s_1, \ldots, s_k$ be arbitrary integers with $|s_i| \leq n^d$. Let $X_1, \ldots, X_k$ be independent random variables with distribution $\mathcal{U}_n$, then:*

$$\Pr[\gcd(s_1 + X_1, \ldots, s_k + X_k) = 1] \geq (1 - (d/n)^{k-1}) \cdot (1 - \epsilon_k) \cdot 1/\zeta(k) =: \sigma(k, d/n),$$

where $\zeta(k)$ is the Riemann zeta function, $\epsilon_k \leq .077$ for $k = 2$ and $\epsilon_k \leq 2.9 \cdot 10^{-5}$ for $k \geq 3$. When $d \leq n/10$, this probability is at least .505 for $k \geq 2$, at least .92 for $k \geq 4$, and at least .99 for $k \geq 7$.

Proof. The proof is given in Appendix A. □

Theorem 3.5. *For any cyclic group family $\mathcal{G} = (\mathcal{G}_\kappa)_{\kappa=1}^{\infty}$, integers $k \geq 2$, $S \geq 4$:*

$$\mathsf{HO}_{\mathcal{C}} \xrightarrow[\text{HO-SM}]{\frac{c_k(1-e^{-k \cdot C_S})/2,\ \lceil Sk/p \rceil}{\dashrightarrow}} \mathsf{DLog}, \quad \textit{e.g.,}\ \mathsf{HO}_{\mathcal{C}} \xrightarrow[\text{HO-SM}]{\frac{.49,\ \lceil 56/p \rceil}{\dashrightarrow}} \mathsf{DLog},$$

where $p := \mathsf{Adv}^{\mathsf{DLog}}_{\mathcal{G},\mathcal{A}}(\kappa)$, C_S as in Lemma 2.6, and $c_k := \sigma(k, 1/10) \geq 0.505$. The example uses $S = 8$ and $k = 7$.

Proof. Given a DLog adversary $\mathcal{A}$ with advantage $p(\kappa) := \mathsf{Adv}^{\mathsf{DLog}}_{\mathcal{G},\mathcal{A}}(\kappa)$, then given $k \geq 2$, $S \geq 4$ we construct an $\mathsf{HO}_{\mathcal{C}}$ adversary $\mathcal{B}^{\mathcal{A}}$ which takes input $(1^\kappa, \mathbb{G}, g)$ with $(\mathbb{G}, g) \in \mathcal{G}_\kappa$ as follows.

$M := \emptyset$
for $i = 1, \ldots, \lceil Sk/p(\kappa) \rceil$
  $r_i \xleftarrow{\$} \mathcal{U}_{U^2}$, $d_i \leftarrow \mathcal{A}(g, g^{r_i})$
  if $g^{r_i} = g^{d_i}$ **then** $M \leftarrow M \cup \{|d_i - r_i|\}$
if $M \neq \emptyset$ **then return** $\gcd(M)$ **else return** $\perp$

This adversary is similar to the one in the proof of Lemma 3.3, except it performs $\lceil Sk/p(\kappa) \rceil$ such sample & queries and returns the gcd of the obtained differences $|r_i - d_i|$. This corresponds to the time complexity factor $\lceil Sk/p(\kappa) \rceil$ in the claim.

We have already shown that for each sample & query the probability that $g^r = g^d$ depends on $(\mathbb{G}, g)$ and is $p'_{\mathbb{G}} := p_{\mathbb{G}} - negl(\kappa)$, where $p_{\mathbb{G}} := \mathsf{Adv}^{\mathsf{DLog}}_{(\mathbb{G},g),\mathcal{A}}$. Let $p' := E_{\mathbb{G} \in \mathcal{G}_\kappa}[p'_{\mathbb{G}}]$ be the average success probability of a successful sample & query for a random group $\mathbb{G} \in \mathcal{G}_\kappa$, then $p' = p(\kappa) - negl(\kappa)$.

Next we bound the probability we find at least k successful samples for a random group $\mathbb{G} \in \mathcal{G}_\kappa$. We apply Lemma 2.6 on $\mathcal{X} = \{B(\lceil Sk/p(\kappa) \rceil, p_{\mathbb{G}})\}_{\mathbb{G} \in \mathcal{G}_\kappa}$ and use Lemma 2.7 to find that

$$\Pr_{\mathbb{G} \in \mathcal{G}_\kappa}[|M| \geq k] = \Pr_{X \in \mathcal{X}}[X \geq k] - \mathrm{negl}(\kappa) \geq p \cdot (1 - e^{-k \cdot C_S})/2 - \mathrm{negl}(\kappa).$$

For any given $(\mathbb{G}, g)$, consider any successful sample & query $g^{r_i} = g^{d_i}$ and let $N := \lceil U^2/|\mathbb{G}| \rceil$. As the size of the outputs d_i of $\mathcal{A}$ are polynomially bounded in κ, there is an integer K such that for all $\kappa \geq K$ the outputs of $\mathcal{A}$ are bounded by $|d_i| \leq N^{N/10}$. Assume that indeed $|d_i| \leq N^{N/10}$ and $N \geq U \geq |\mathbb{G}| \geq 2^{23}$.

We have already shown that $r''_i = \lfloor r_i/|\mathbb{G}| \rfloor$ is distributed independently from d_i and has negligible statistical distance ε_1 to $\mathcal{U}_N$. By Theorem 3.4 it follows that if we have k successful samples $|r_1 - d_1|, \ldots, |r_k - d_k|$ then

$$\Pr\left[\gcd\left(|r_1 - d_1|/|\mathbb{G}|, \ldots, |r_k - d_k|/|\mathbb{G}|\right) = 1\right] \geq \sigma(k, 1/10) - k\varepsilon_1 = c_k - \mathrm{negl}(\kappa).$$

Finally, we can conclude that indeed:
$\Pr_{(\mathbb{G},g) \in \mathcal{G}_\kappa}\left[\mathcal{B}^{\mathcal{A}}(1^\kappa, \mathbb{G}, g) = |\mathbb{G}|\right] \geq p \cdot (c_k(1 - e^{-k \cdot C_S})/2) - \mathrm{negl}(\kappa)$. □

4 Abelian Hidden Order Standard Model (AHO-SM)

In this section we propose a computational framework for working in finite abelian groups of hidden order. We first generalize the notion of a (hard) group family from Damgård and Koprowski [13], and later introduce generalized notions of the algebraic group model from Fuchsbauer et al. [16] as well as of the strong algebraic group model from Katz et al. [17].

In our definition of an abelian group family below we do not assume sampled groups come with a canonical set of generators. Instead a sufficiently large set of random group elements can always be used as generator set. Hence, for the computational problems considered in Table 2, each game starts with sampling a group $\mathbb{G}$ as well as a set of random generators $(g_1, \ldots, g_n)$.

Definition 4.1. *An* abelian group family $\mathcal{G} = (\mathcal{G}_\kappa)_{\kappa=1}^{\infty}$ *is a family of probability distributions over finite abelian groups defined with:*

1. *An efficient sampling algorithm* GGen *that, on input* 1^κ*, samples uniformly at random a group* $\mathbb{G} \in \mathcal{G}_\kappa$ *and outputs a group description of* $\mathbb{G}$ *and* $1_\mathbb{G}$*.*
2. *An efficient sampling algorithm* $\mathsf{GSample}$ *which, given a group description of* $\mathbb{G}$*, outputs a group element* $x \in \mathbb{G}$ *sampled uniformly at random.*
3. *Efficient algorithms* GMul *and* GInv *that, respectively, multiplies two group elements, and inverts a group element.*
4. *A group order upper bound* $U(\kappa)$*:* $\forall\kappa\forall\mathbb{G} \in \mathcal{G}_\kappa : U(\kappa) \geq |\mathbb{G}|$*, such that* $\log U(\kappa) \in \mathrm{poly}(\kappa)$ *and* $1/U(\kappa) \in \mathrm{negl}(\kappa)$*.*
5. *A random group generator count* $n(\kappa) \in \mathbb{Z}_{>0}$ *and* $n(\kappa) \in \mathrm{poly}(\kappa)$ *such that*

$$\Pr[\langle \boldsymbol{g} \rangle \neq \mathbb{G} \mid \mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa, \boldsymbol{g} \xleftarrow{\$} \mathbb{G}^{n(\kappa)}] \in \mathrm{negl}(\kappa).$$

When the security parameter κ *is clear from the context, we will usually omit* κ *and simply denote* U *and* n *instead of* $U(\kappa)$ *and* $n(\kappa)$*, respectively.*

Note that by the same arguments as in Remark 3.2, for any tuple of abelian group family algorithms (GGen, $\mathsf{GSample}$, GMul, GInv) there always exists a candidate $U(\kappa)$ that satisfies Definition 4.1. Moreover, the following Lemma also provides a candidate $n(\kappa)$.

Lemma 4.2. *For any abelian group* $\mathbb{G}$ *and* $U \geq |\mathbb{G}|$*, let* $n := \lceil \log_2 U \rceil$ *then there exist* $g_1, \ldots, g_n$ *such that* $\langle g_1, \ldots, g_n \rangle = \mathbb{G}$*. Moreover,* $2n$ *random elements fail to generate the full group with exponentially small probability in* n*, i.e.,*

$$\Pr[\langle \boldsymbol{g} \rangle \neq \mathbb{G} \mid \boldsymbol{g} \xleftarrow{\$} \mathbb{G}^{2n}] \leq 2^{-n} (\leq 1/U).$$

Proof. The first part of the lemma follows directly from the observation that if $g_{i+1} \notin \langle g_1, \ldots, g_i \rangle$ then we have that $|\langle g_1, \ldots, g_{i+1} \rangle| = k \cdot |\langle g_1, \ldots, g_i \rangle|$ with $k \in \mathbb{Z}_{\geq 2}$. The second part of the lemma follows from two observations. First, that for all $g_1, \ldots, g_i$ that generate a strict subgroup $\mathbb{G}' := \langle g_1, \ldots, g_i \rangle \neq \mathbb{G}$ the probability that a randomly sampled element lies in the subgroup is bounded as $\Pr[x \in \mathbb{G}' \mid x \xleftarrow{\$} \mathbb{G}] \leq 1/2$. Second, for $\boldsymbol{g} \in \mathbb{G}^{2n}$ with $\langle \boldsymbol{g} \rangle \neq \mathbb{G}$, it follows that for at least n indices i it holds that $g_{i+1} \in \langle g_1, \ldots, g_i \rangle \neq \mathbb{G}$. □

We generalize the notion of a *hard group family* from Damgård and Koprowski [13, Definition 1] to the abelian hidden order setting as follows.

Definition 4.3. *Let* $\mathsf{lp}(N)$ *denote the largest prime divisor of* N*. Sampling a group* $\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa$ *and considering* $\mathsf{lp}(|\mathbb{G}|)$*, induces a distribution* $\mathcal{D}_\kappa$ *on the primes. Define* $\alpha(\mathcal{G}_\kappa) := \max_p \Pr_\mathbb{G}[p = \mathsf{lp}(|\mathbb{G}|)]$ *to be the maximal probability in* $\mathcal{D}_\kappa$*. For a positive integer* M*, define the probability* $\beta(\mathcal{G}_\kappa, M) := \Pr_\mathbb{G}[\mathsf{lp}(|\mathbb{G}|) \leq M]$ *that the largest prime divisor of the group order is at most* M*.*

Definition 4.4. *A* hard abelian group family *is an abelian group family* $(\mathcal{G}_\kappa)_{\kappa \in \mathbb{Z}_{>0}}$ *which satisfies the following conditions:*

1. $\alpha(\mathcal{G}_\kappa)$ *is negligible in* κ*;*
2. *There exists* $B(\kappa)$ *such that* $\forall\mathbb{G} \in \mathcal{G}_\kappa : B(\kappa) \leq |\mathbb{G}|$ *and* $1/B(\kappa) \in \mathrm{negl}(\kappa)$*.*

Moreover, Damgård and Koprowski noted that if $(\mathcal{G}_\kappa)_{\kappa\in\mathbb{Z}_{>0}}$ is a hard abelian group family, then setting $M_\kappa = 1/\sqrt{\alpha(\mathcal{G}_\kappa)}$ leads to $\beta(\mathcal{G}_\kappa, M_\kappa)$ as well as $1/M_\kappa$ being negligible [13, Fact 1].

The order of elements sampled uniformly at random will in general be superpolynomially large, which we will show using the following two lemmas.

Lemma 4.5. *Let $|\mathbb{G}| = \prod_p p^{e(p)}$ be the prime factorization of $|\mathbb{G}|$. Then the probability for a prime $p \mid |\mathbb{G}|$ to divide the order of a uniformly random element of $\mathbb{G}$ is $1 - 1/p^{e(p)}$.*

Proof. By the fundamental theorem of finite abelian groups we can write $\mathbb{G} \cong \bigoplus_{i=1}^{t}(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$, where $p_1, \dots p_t$ are (not necessarily distinct) prime numbers. The order of an element $X \in \mathbb{G}$ is *not* divisible by a prime $p \mid |\mathbb{G}|$ if and only if X has trivial components in all subgroups corresponding to $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})$ with $p_i = p$. There are exactly $\prod_{p_i \neq p} p_i^{e_i} = |\mathbb{G}|/p^{e(p)}$ such elements. □

Lemma 4.6. *Let $(\mathcal{G}_\kappa)_{\kappa=1}^{\infty}$ be a hard abelian group family. Then there exists a superpolynomial bound M_κ such that the order of a random element $X \in \mathbb{G} \in \mathcal{G}_\kappa$ will have order greater than M_κ with all but negligible probability, i.e.:*

$$\Pr\left[|\langle X\rangle| < M_\kappa \mid X \xleftarrow{\$} \mathbb{G},\, \mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa\right] \in \mathrm{negl}(\kappa).$$

Proof. As mentioned above, for $M_\kappa = 1/\sqrt{\alpha(\mathcal{G}_\kappa)}$ the bound $\beta(\mathcal{G}_\kappa, M_\kappa)$ is negligible, since $\alpha(\mathcal{G}_\kappa) \in \mathrm{negl}(\kappa)$ [13, Fact 1]. Assume that the largest prime divisor p of $|\mathbb{G}|$ is at least M_κ, which happens with probability $1 - \mathrm{negl}(\kappa)$. Now, sampling $X \xleftarrow{\$} \mathbb{G}$, we see that p divides the order of X with probability $\geq 1 - 1/p$ by Lemma 4.5, i.e. with all but negligible probability. □

Note that even without knowing the exact group structure or the exact group order we can efficiently sample group elements as $\boldsymbol{g}^{\boldsymbol{r}}$ close to uniform, as shown in the following two lemmas.

Lemma 4.7. *Let $\mathbb{G}$ be a finite abelian group and let $g_1, \dots, g_n \in \mathbb{G}$ be a system of generators. Put $O_i := |\langle g_i\rangle|$ for $i = 1, \dots, n$. If we sample $(r_i)_{i=1}^n \xleftarrow{\$} \prod_{i=1}^n \mathcal{U}_{O_i}$ and set $X := g_1^{r_1} \cdots g_n^{r_n}$, then X is uniformly distributed in $\mathbb{G}$.*

Lemma 4.8. *Let $\mathbb{G}$ be a finite abelian group and $\langle g_1, \dots, g_n\rangle = \mathbb{G}$, and let ℓ, v be positive integers. If we sample $(r_{ij})_{i,j=1}^{\ell,n} \xleftarrow{\$} (\mathcal{U}_{U^v})^{\ell n}$ and set $X_i := g_1^{r_{i1}} \cdots g_n^{r_{in}}$ for $i = 1, \dots, \ell$. Then the statistical distance between the distribution of $(X_i)_{i=1}^{\ell}$ and the uniform distribution $\mathcal{U}_{\mathbb{G}^\ell}$ is upper bounded by $\ell n/2U^{v-1} + \ell^2 n^2/2U^{2v-2}$.*

Proofs of Lemmas 4.7 and 4.8 can be found in Appendix A.

4.1 Abelian Hidden Order Algebraic Group Model (AHO-AGM)

In this subsection we generalize the algebraic group model (AGM) of Fuchsbauer et al. [16] to the setting of finite abelian groups of hidden order. We call this model the *abelian hidden order algebraic group model* (AHO-AGM). In the AHO-AGM, all algorithms must satisfy the following definition.

Definition 4.9. *An algorithm $\mathcal{A}$ executed in an algebraic game* G *is called* algebraic *if for all group elements $X \in \mathbb{G}$ that $\mathcal{A}$ outputs, it also outputs a representation $\boldsymbol{a} = (a_1, \dots, a_\ell) \in \mathbb{Z}^\ell$ such that $X = \prod_{i=1}^{\ell} g_i^{a_i}$, where $\boldsymbol{g} = (g_1, \dots, g_\ell) \in \mathbb{G}^\ell$ is the list of all group elements that have been given to $\mathcal{A}$ so far. We will denote such a representation by $[X]_{\boldsymbol{g}}$. (Here, typically, $g_1, \dots, g_n$ are the uniformly randomly chosen generators for $\mathbb{G}$.)*

Surprisingly, a standard model reduction and an algebraic group model reduction can compose to a standard model reduction under certain conditions. That is $\mathsf{Z} \xRightarrow[\text{AHO-SM}]{} X$ may follow from $\mathsf{Z} \xRightarrow[\text{AHO-AGM}]{} Y$ and $\mathsf{Y} \xRightarrow[\text{AHO-SM}]{} X$.

Note that *any* standard model algorithm for any game $\mathsf{X} \in \{\mathsf{MO}, \mathsf{HO}, \mathsf{DLog}_1, \mathsf{DLog}_2\}$ is by definition also algebraic, since no group elements are output. In that case any *generic* reduction $\mathsf{Y} \Rightarrow \mathsf{X}$ results in an algebraic adversary for Y. Hence, such generic reductions $\mathsf{Y} \Rightarrow \mathsf{X}$ in the standard model can be composed with any algebraic group model reduction from $\mathsf{Z} \Rightarrow \mathsf{Y}$ to obtain a *standard model* reduction $\mathsf{Z} \Rightarrow \mathsf{X}$. (see e.g. Corollary 6.4.)

4.2 Abelian Hidden Order Strong Algebraic Group Model (AHO-SAGM)

In this subsection we extend the strong algebraic group model (SAGM) to finite abelian (not necessarily cyclic) groups. In the SAGM the running time of an algorithm is measured by the number of algebraic rounds and the "normal" running time measured in some underlying computational model (e.g. the Turing machine model). The SAGM is similar to the AGM, but in the case of the repeated squaring problem with timing parameter T, an adversary can simply output g^{2^T} in one algebraic round. Therefore the AGM is not the right model to study the hardness of the repeated squaring problem. This is made formal in [17, Theorem 3]. Moreover, note that this model allows for arbitrary parallelism, since strongly algebraic algorithms are allowed to output multiple tuples per round. Of course efficient algebraic algorithms are only allowed to output a polynomial number of tuples in each round.

Note that a strong algebraic algorithm is automatically an algebraic algorithm. Conversely, assuming that the output length is polynomial, any algebraic algorithm can be turned into a strongly algebraic algorithm with a polylogarithmic time loss (see [17, Theorem 1]).

Our definition is a generalization of the original definition introduced by Katz et al. [17]. Contrary to Katz et al. [17], we let $\mathbb{G}$ be any *finite abelian group*, which is sampled according to some group family $\mathcal{G} = (\mathcal{G}_\kappa)_{\kappa=1}^{\infty}$. Here κ can be seen as the security parameter of the corresponding game. We call this model the *abelian hidden order strong algebraic group model* (AHO-SAGM). In the AHO-SAGM, all algorithms must satisfy the following definition.

Definition 4.10. *An algorithm $\mathcal{A}$ over a group $\mathbb{G}$ is called* strongly algebraic *if it has one or more output rounds (between which it may perform arbitrary local computation). An output round is called algebraic if it contains one or more group elements. For each group element X it outputs it must also output a tuple of one of the following forms:*

1. *$(X, X_1, X_2) \in \mathbb{G}^3$ such that $X = X_1 X_2$, where X_1, X_2 were either previously given to $\mathcal{A}$ or previously output by $\mathcal{A}$.*
2. *$(X, X_1) \in \mathbb{G}^2$ such that $X = X_1^{-1}$, where X_1 was either previously given to $\mathcal{A}$ or previously output by $\mathcal{A}$.*

In the AHO-SAGM*, we will denote a tuple of one of the above forms by $[X]$. The* algebraic running time *of $\mathcal{A}$ is the number of algebraic rounds it takes, and is denoted by* ATime*. We denote the running time of $\mathcal{A}$ by a pair* $(\mathsf{ATime}, \mathsf{Time})$*.*

5 Computing (a Multiple of) the Group Order

Following [7], given a system of generators $\boldsymbol{g} = (g_1, \ldots, g_n)$ of a finite abelian group $\mathbb{G}$, we call any vector $\boldsymbol{e} = (e_1, \ldots, e_n)$ with the property that $\boldsymbol{g}^{\boldsymbol{e}} = 1_{\mathbb{G}}$ a *relation* for $\boldsymbol{g}$. The relations for $\boldsymbol{g}$ form a lattice in $\mathbb{Z}^n$, which we will denote by $L(\boldsymbol{g})$. Since this lattice is the kernel of the surjective homomorphism

$$\mathbb{Z}^n \to \mathbb{G}, \quad \boldsymbol{e} \mapsto \boldsymbol{g}^{\boldsymbol{e}}, \tag{1}$$

its dimension is n. Let $B = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ be a basis for the lattice $L(\boldsymbol{g})$, then $\mathbb{Z}^n / B\,\mathbb{Z}^n \cong \mathbb{G}$ by (1), from which it follows that [7, Lemma 3.1]

$$|\det(B)| = |\mathbb{Z}^n / B\,\mathbb{Z}^n| = |\mathbb{G}|. \tag{2}$$

We can show that if you find a full rank *sublattice* of $L(\boldsymbol{g})$ then you obtain a *multiple* of the group order:

Lemma 5.1. *Let $\mathbb{G}$ be a finite abelian group, let $\boldsymbol{g} = (g_1, \ldots, g_n)$ be a system of generators of $\mathbb{G}$, and let $B = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ be a basis for the relationship lattice $L(\boldsymbol{g})$. Let $R = (\boldsymbol{r}_1, \ldots, \boldsymbol{r}_n)$ be a system of relations for $\boldsymbol{g}$, which are linearly independent as vectors over $\mathbb{R}$. This implies these form a full rank sublattice $\Lambda := R\mathbb{Z}^n \subset L(\boldsymbol{g})$. Then $|\det(R)|$ is an integer multiple of $|\mathbb{G}|$.*

Proof. Since both lattice bases B and R generate $\mathbb{R}^n$ as a vector space, we know that there is a matrix $T = (t_{ij})_{i,j=1}^n$ such that $R = BT$, with $d := \det(T) \neq 0$. Since a change of basis on either $L(\boldsymbol{g})$ or Λ multiplies d by ± 1, the absolute value of d is uniquely determined by $L(\boldsymbol{g})$ and Λ, and

we will also refer to this as the *relative determinant* $d(\Lambda/L(\boldsymbol{g})) := |d|$. Since $\boldsymbol{r}_i \in \Lambda \subset L(\boldsymbol{g})$, we can write $\boldsymbol{r}_i = \sum_{j=1}^{n} a_{ij}\boldsymbol{b}_j$ for some $a_{ij} \in \mathbb{Z}$. Hence from the expression $\boldsymbol{r}_i = \sum_{j=1}^{n} t_{ij}\boldsymbol{b}_j$, we deduce that $t_{ij} \in \mathbb{Z}$ (since otherwise we would obtain a linear relation between the $\boldsymbol{b}_j$). This implies that $d = \det(T) \in \mathbb{Z}$. Together with equation (2), we see that $|\det(R)| = |d \cdot \det(B)|$ is an integer multiple of $|\mathbb{G}|$. □

Given a distribution over $\mathbb{Z}^{n\times n}$ resulting in the uniform distribution over $\mathbb{Z}_p^{n\times n}$ when reducing matrices modulo a prime p, then one can use the Schwartz-Zippel lemma [28, 31] to upper bound the probability of sampling a singular matrix.

Lemma 5.2 ([28, 31]). *Let p be prime. Let $F(X_1, \ldots, X_k) \in \mathbb{Z}_p[X_1, \ldots, X_k]$ be a nonzero polynomial of total degree d. Then for uniformly random $x_1, \ldots, x_k \xleftarrow{\$} \mathbb{Z}_p$, the probability that $F(x_1, \ldots, x_k) = 0$ is at most d/p.*

Corollary 5.3. *Let p be a prime and $n \geq 1$ an integer. Then we have* $\Pr[\det(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = 0 \mid \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \xleftarrow{\$} \mathbb{Z}_p^n] \leq n/p$.

5.1 Reduction Template for MO

Using the previous results, we construct a template reduction $\mathsf{MO} \Rightarrow \mathsf{G}$ for some computational game G, and specify certain conditions G needs to satisfy in order for such a reduction to succeed with sufficiently high probability.

We have seen in Lemma 5.1 that if we can find n linearly independent relations $R = (\boldsymbol{r}_1, \ldots, \boldsymbol{r}_n)$, then $|\det(R)|$ is going to be an integer multiple of the order of $\mathbb{G}$. Therefore to show that we can reduce the multiple order problem MO to some computational problem G, it suffices to show that we can use any adversary $\mathcal{A}$ for game G to obtain n linearly independent relations for a given system of generators with a reasonable probability.

We are now ready to formulate the necessary conditions on the game G for a reduction $\mathsf{MO} \Rightarrow \mathsf{G}$ to exist, and construct a template for such a reduction.

Lemma 5.4. *Let $\mathcal{G} = (\mathcal{G}_\kappa)_{\kappa=1}^{\infty}$ be a group family with security parameter $\kappa \in \mathbb{Z}_{>0}$. Let G be some computational game, which, given κ, is based on sampling a group $\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa$ and $\boldsymbol{g} = (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G}^n$ uniformly at random. Let $\mathsf{Rel}^{\mathcal{A}}$ be a* relation sampler *that takes as input a group $\mathbb{G} \in \mathcal{G}_\kappa$, $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{G}^n$, and has oracle access to an adversary $\mathcal{A}$ for game G. Assume $\mathsf{Rel}^{\mathcal{A}}$ satisfies the following properties for any given adversary $\mathcal{A}$ in a given group model* AHO-GM *(i.e.,* AHO-SM, AHO-AGM, AHO-SAGM*):*

(i) $\mathsf{Rel}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$ *outputs either $\perp$ (failure) or a relation $\boldsymbol{e}$ s.t. $\boldsymbol{g}^{\boldsymbol{e}} = 1_{\mathbb{G}}$ (success).*
(ii) *When $\mathbb{G} = \langle \boldsymbol{g} \rangle$, each execution of $\mathsf{Rel}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$ is independent and has identical success probability $p'_{\mathbb{G},\boldsymbol{g}}$ with $|p'_{\mathbb{G},\boldsymbol{g}} - p_{\mathbb{G},\boldsymbol{g}}| \leq \varepsilon_1 \in \mathrm{negl}(\kappa)$.*
(iii) *When $\mathbb{G} = \langle \boldsymbol{g} \rangle$, given n relation outputs $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ of n independent and successful executions of $\mathsf{Rel}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$, then* $\Pr[\det(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n) = 0] \in \mathrm{negl}(\kappa)$.
(iv) $\mathsf{Time}_{\mathcal{G},\mathsf{Rel}} \sim \mathsf{Time}^{\mathsf{G}}_{\mathcal{G},\mathcal{A}}$*, i.e., the time complexity of* Rel *is asymptotically equivalent to that of $\mathcal{A}$.*

Then for $S \geq 4$:

$$\mathsf{MO} \xRightarrow[\text{AHO-GM}]{(1-e^{-n\cdot C_S})/2,\, \lceil Sn/p \rceil} \mathsf{G},$$

where $p := \mathsf{Adv}^{\mathsf{G}}_{\mathcal{G},\mathcal{A}}(\kappa)$, $p_{\mathbb{G},\boldsymbol{g}} := \mathsf{Adv}^{\mathsf{G}}_{\mathcal{G},\mathcal{A}}|_{\mathbb{G},\boldsymbol{g}}(\kappa)$ and C_S is defined as in Lemma 2.6.

Proof. Given an adversary $\mathcal{A}$ for game G, we construct an MO adversary $\mathcal{B}^{\mathcal{A}}$ which takes input $(1^\kappa, \mathbb{G}, \boldsymbol{g})$ where $\mathbb{G} \in \mathcal{G}_\kappa$, $\boldsymbol{g} \in \mathbb{G}^n$ as given in Figure 2. The adversary $\mathcal{B}$ calls $\mathcal{A}$ exactly $l := \lceil Sn/p \rceil$ times, which explains the time factor. For the advantage of $\mathcal{B}$ our proof is based on the following inequality:

$$\begin{aligned}
\mathsf{Adv}^{\mathsf{MO}}_{\mathcal{G},\mathcal{B}}(\kappa) &\geq \Pr_{\mathbb{G},\boldsymbol{g}}[\mathcal{B}^{\mathcal{A}}(1^\kappa, \mathbb{G}, \boldsymbol{g}) \in \mathbb{Z}_{>0} \mid \mathsf{Columns}(E) = n \wedge \langle \boldsymbol{g} \rangle = \mathbb{G}] \\
&\quad \cdot \Pr_{\mathbb{G},\boldsymbol{g}}[\mathsf{Columns}(E) = n \mid \langle \boldsymbol{g} \rangle = \mathbb{G}] \cdot \Pr_{\mathbb{G},\boldsymbol{g}}[\langle \boldsymbol{g} \rangle = \mathbb{G}] \\
&\geq p \cdot (1 - e^{-n\cdot C_S})/2 - \mathrm{negl}(\kappa) \qquad (3)
\end{aligned}$$

$E := ()$
for $i = 1, \ldots, \lceil Sn/p \rceil$
  $\boldsymbol{e}_i \leftarrow \mathsf{Rel}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$
  if $\boldsymbol{e}_i \neq \perp$ **then**
    $E \leftarrow (E \| \boldsymbol{e}_i^T)$
    if $\mathsf{Columns}(E) = n$ **then return** $|\det(E)|$
return $\perp$

Fig. 2. Template for MO adversary $\mathcal{B}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$

First, recall that by Definition 4.1(5.):

$$\Pr_{\mathbb{G},\boldsymbol{g}}[\langle \boldsymbol{g} \rangle = \mathbb{G}] = 1 - \mathrm{negl}(\kappa). \tag{4}$$

Second, by condition (iii), over all $\mathbb{G}, \boldsymbol{g}$ with $\langle \boldsymbol{g} \rangle = \mathbb{G}$:

$$\Pr_{\mathbb{G},\boldsymbol{g}}[\mathcal{B}^{\mathcal{A}}(1^{\kappa}, \mathbb{G}, \boldsymbol{g}) \in \mathbb{Z}_{>0} \mid \mathsf{Columns}(E) = n \wedge \langle \boldsymbol{g} \rangle = \mathbb{G}] = 1 - \mathrm{negl}(\kappa). \tag{5}$$

Third, for any given $\mathbb{G}, \boldsymbol{g}$ with $\langle \boldsymbol{g} \rangle = \mathbb{G}$, the success probability of each call to Rel is $p'_{\mathbb{G},\boldsymbol{g}}$ and the amount of successful calls has distribution $B(l, p'_{\mathbb{G},\boldsymbol{g}})$ by condition (ii). From condition (ii) and Lemma 2.7 it follows that the statistical distance between $B(l, p'_{\mathbb{G},\boldsymbol{g}})$ and $B(l, p_{\mathbb{G},\boldsymbol{g}})$ is at most $\varepsilon_2 := (l^2/2) \cdot \varepsilon_1 \in \mathrm{negl}(\kappa)$.

By applying Lemma 2.6 on $\mathcal{X} = \{B(l, p_{\mathbb{G},\boldsymbol{g}})\}_{\mathbb{G}=\langle \boldsymbol{g} \rangle}$, we find that

$$\Pr_{\mathbb{G},\boldsymbol{g}}[\mathsf{Columns}(E) = n \mid \mathbb{G} = \langle \boldsymbol{g} \rangle] \geq \Pr_{X \in \mathcal{X}}[X \geq n] - \varepsilon_2 \geq p \cdot (1 - e^{-n \cdot C_S})/2 - \varepsilon_2. \tag{6}$$

The desired inequality (3) is obtained by multiplying Eqs. (4), (5) and (6). □

6 Security Reductions in the AHO-SM

In this section we prove reductions in the abelian hidden order standard model. Firstly, {StRoot, ARoot, e-RT, T-RSW} ⇒ MO were previously shown. Using an assumed small prime divisor of group order oracle $\mathcal{O}$, we can prove $\mathsf{LO}^{\mathcal{O}} \Rightarrow \mathsf{MO}$ as well. Followed by reductions $\mathsf{MO} \Rightarrow \mathsf{DLog}_1$ and $\mathsf{MO} \Rightarrow \mathsf{DLog}_2$, where the latter follows from the straightforward reduction $\mathsf{CDH}_2 \Rightarrow \mathsf{DLog}_2$ and the reduction $\mathsf{MO} \Rightarrow \mathsf{CDH}_2$ from Theorem 7.5. An impossibility of efficient *generic* reductions in the opposite direction for DLog_1, DLog_2 and CDH_2 is treated in section 6.1.

Lemma 6.1 ([13, 30, 17, 2]).

$$\{\mathsf{StRoot}, \mathsf{ARoot}, T\text{-}\mathsf{RSW}, e\text{-}\mathsf{RT}\} \xrightarrow[\text{AHO-SM}]{1,1} \mathsf{MO}, \quad \textit{for } \gcd(e, |\mathbb{G}|) = 1.$$

Proof (sketch). Let N denote the multiple of the group order $|\mathbb{G}|$. For e-RT this is a trivial generalization over [13, 2]. Given N, one can determine $N' = N/\gcd(e^{\lfloor \log_e(N) \rfloor}, N)$. The resulting value N' will still be a multiple of $|\mathbb{G}|$ and coprime with e, hence one can compute an e-th root of $X \in \mathbb{G}$ as $Y := X^d$ where $ed \equiv 1 \bmod N'$. Now the first two reductions can be easily shown using the e-RT reduction: for StRoot one can pick an exponent coprime to N (e.g., by picking a prime $> N$). For ARoot the adversary receives a random large prime e which is coprime to N with all but negligible probability. Finally, T-RSW ⇒ MO since $\log_2(2^T) > \log_2(2^T \bmod N)$ for any $T \gg N$. □

Note that for e-RT with $\gcd(e, |\mathbb{G}|) > 1$ the situation is less straightforward. For cyclic groups and some more general forms of finite abelian groups, Shank's algorithm can be extended to compute

e-th roots [19, Chapter 3]. However, this holds in the known group order setting, it remains an open question whether it is possible to compute e-th roots given only a multiple of the order.

The situation for the reduction $\mathsf{LO} \Rightarrow \mathsf{MO}$ is also complex. First of all, there need to be elements or order $< 2^\kappa$ in the group $\mathbb{G}$ in order for the reduction to be possible at all. An algebraic method that works in any finite abelian group which contains elements of low order, is not known to the authors at this time. However, if one has access to an oracle which provides a small prime divisor of the group order then it is possible to construct such a reduction as we prove below. Note that a concrete example of such an oracle can be given in the setting of class groups of imaginary quadratic number fields. Here the Cohen-Lenstra heuristics [11] predict that the group order is divisible by an odd prime q with probability $\mho(q) = 1 - \prod_{n=1}^{\infty}(1 - 1/q^n)$. For example: $\mho(3) \approx 0.439874$.

Proposition 6.2. *Let $\mathcal{O}$ be an oracle that on input a finite abelian group $\mathbb{G} \in \mathcal{G}_\kappa$, outputs a prime $q < 2^\kappa$ which divides the order $|\mathbb{G}|$ with non-negligible probability p. Let $\mathsf{LO}^{\mathcal{O}}$ denote the low order game where an adversary playing the game has access to $\mathcal{O}$. Then*

$$\mathsf{LO}^{\mathcal{O}} \xRightarrow[\text{AHO-SM}]{p/2,\,1} \mathsf{MO}.$$

Proof. Given an MO adversary $\mathcal{A}$, we construct an LO adversary $\mathcal{B}^{\mathcal{A},\mathcal{O}}$, which takes input $(\mathbb{G}, \boldsymbol{g})$ with $\mathbb{G} \in \mathcal{G}_\kappa$ and $\boldsymbol{g} \in \mathbb{G}^n$, as defined below:

$q \leftarrow \mathcal{O}(\mathbb{G}), \quad N \leftarrow \mathcal{A}(\boldsymbol{g}), \quad \boldsymbol{r} \xleftarrow{\$} (\mathcal{U}_{U^2})^n, \quad X := \boldsymbol{g}^{\boldsymbol{r}}$
for $i = 1, \ldots, \lfloor \log_q(N) \rfloor$
  if $N \not\equiv 0 \bmod q^i$ **then return** $\perp$
  if $X^{N/q^i} \neq 1_{\mathbb{G}}$ **then return** $(X^{N/q^i}, q)$
return $\perp$

For random $\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa$ and $\boldsymbol{g} \xleftarrow{\$} \mathbb{G}^n$, if the output of $\mathcal{A}$ is correct and q divides the order of X, then we claim that $\mathcal{B}^{\mathcal{A},\mathcal{O}}$ outputs a correct element of low order. Indeed, we know that $X^N = 1_{\mathbb{G}}$ and since $N/q^{\lfloor \log_q(N) \rfloor}$ is not divisible by q, there must be an $1 \leq i \leq \lfloor \log_q(N) \rfloor$ for which $X^{N/q^i} \neq 1_{\mathbb{G}}$. Let i^* be the first i for which this happens, then $(X^{N/q^{i^*}})^q = X^{N/q^{i^*-1}} = 1_{\mathbb{G}}$, so the output of $\mathcal{B}^{\mathcal{A},\mathcal{O}}$ is indeed correct in this case.

By definition of the oracle $\mathcal{O}$, the group order $|\mathbb{G}|$ is divisible by q with probability p. If q divides the group order, then by Lemma 4.5 the probability that q divides the order of a uniformly chosen $X \in \mathbb{G}$ is at least $1 - 1/q \geq 1/2$.

By Lemma 4.8, the distribution of X has negligible statistical distance to the uniform distribution $\mathcal{U}_{\mathbb{G}}$ when $\boldsymbol{g}$ form a system of generators for $\mathbb{G}$, and we assume the latter to happen with all but negligible probability. Hence $\mathcal{B}^{\mathcal{A},\mathcal{O}}$ succeeds with probability $\mathsf{Adv}^{\mathsf{LO}}_{\mathcal{G},\mathcal{B}^{\mathcal{A},\mathcal{O}}}(\kappa) \geq (p/2 + \varepsilon) \cdot \mathsf{Adv}^{\mathsf{MO}}_{\mathcal{G},\mathcal{A}}(\kappa)$, for some negligible ε. □

Lemma 6.3.

$$\mathsf{CDH}_2 \xRightarrow[\text{AHO-SM}]{1,\,1} \mathsf{DLog}_2$$

Proof (sketch). Given a CDH_2 instance (X, A, B), one can simply query a DLog_2 adversary on (X, A) and raise B to the resulting output. □

Note that any standard model DLog_2 adversary is algebraic as well, hence the above generic reduction produces an algebraic CDH_2 adversary which can be composed with the algebraic reduction in Theorem 7.5 to obtain:

Corollary 6.4.

$$\mathsf{MO} \xRightarrow[\text{AHO-SM}]{(1-e^{-n\cdot C_S})/2,\,\lceil Sn/p \rceil} \mathsf{DLog}_2, \quad \textit{for } S \geq 4,$$

where $p := \mathsf{Adv}^{\mathsf{DLog}_2}_{\mathcal{G},\mathcal{A}}(\kappa)$ and C_S is defined as in Lemma 2.6.

Theorem 6.5.

$$\mathsf{MO} \xrightarrow[\text{AHO-SM}]{(1-e^{-n\cdot C_S})/2,\,\lceil Sn/p\rceil} \mathsf{DLog}_1, \quad \textit{for } S \geq 4,$$

where $p := \mathsf{Adv}^{\mathsf{DLog}_1}_{\mathcal{G},\mathcal{A}}(\kappa)$ *and* C_S *is defined as in Lemma 2.6.*

Proof. Given a DLog_1 adversary $\mathcal{A}$, we construct an MO adversary $\mathcal{B}^{\mathcal{A}}$, which takes input $(\mathbb{G}, \boldsymbol{g})$ with $\mathbb{G} \in \mathcal{G}_\kappa$ and $\boldsymbol{g} \in \mathbb{G}^n$, according to the template in Lemma 5.4. We define a relation sampler $\mathsf{Rel}^{\mathcal{A}}$ as follows, where we assume that a state is maintained in which all internal variables are stored and which is passed between the subroutines.

$\mathsf{Rel}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$	$\mathsf{Samp}(\mathbb{G})$	$\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$
$(\tilde{\boldsymbol{g}}_i, X_i) \leftarrow \mathsf{Samp}(\mathbb{G})$	$A_i \xleftarrow{\$} (\mathcal{U}_{U^2})^{n^2}$	**if** $\tilde{\boldsymbol{g}}_i^{\tilde{\boldsymbol{d}}_i} = X_i$ **then**
$\tilde{\boldsymbol{d}}_i \leftarrow \mathcal{A}(\tilde{\boldsymbol{g}}_i, X_i)$	$\boldsymbol{r}_i \xleftarrow{\$} (\mathcal{U}_{U^3})^n$	**return** $\boldsymbol{r}_i - A_i\tilde{\boldsymbol{d}}_i$
return $\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$	**return** $(\boldsymbol{g}^{A_i}, \boldsymbol{g}^{\boldsymbol{r}_i})$	**else return** $\perp$

Assume $\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa$ and $\boldsymbol{g} \xleftarrow{\$} \mathbb{G}^n$ are sampled uniformly at random. It is straightforward to check that $\boldsymbol{r}_i - A_i\tilde{\boldsymbol{d}}_i$ do indeed form relations with respect to $\boldsymbol{g}$; hence Lemma 5.4(i) is satisfied.

By assumption, $\boldsymbol{g}$ forms a system of generators with all but negligible probability. Conditioned on the event that $\mathbb{G} = \langle \boldsymbol{g} \rangle$, the instances $(\tilde{\boldsymbol{g}}_i, X_i)$ have negligible statistical distance to the uniform distribution $\mathcal{U}_{\mathbb{G}^{n+1}}$ by Lemma 4.8, which is the way problem instances are distributed in the definition of DLog_1. Hence each execution of $\mathsf{Rel}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$ is independent and has identical success probability

$$p'_{\mathbb{G},\boldsymbol{g}} := \mathsf{Adv}^{\mathsf{DLog}_1}_{\mathcal{G},\mathcal{A}}|_{\mathbb{G},\boldsymbol{g}}(\kappa) + \varepsilon_1$$

for some negligible ε_1; thus Lemma 5.4(ii) is satisfied. Moreover, Lemma 5.4(iv) is also clear under the assumption that the runtime of Rel is asymptotically dominated by the runtime of $\mathcal{A}$.

It remains to show that Lemma 5.4(iii) is satisfied. Let $O_j := |\langle g_j \rangle|$ and write $r_{ij} = r'_{ij} + r''_{ij}O_j$ with $0 \leq r'_{ij} < O_j$. Furthermore, write $A_i = (\boldsymbol{a}_{i1}, \ldots, \boldsymbol{a}_{in})$ and let $d_{ij} = \sum_{k=1}^n a_{ikj}\tilde{d}_{ik}$. We can split the relationship coefficients as

$$\hat{r}_{ij} - \hat{d}_{ij} \quad \text{with} \quad \hat{r}_{ij} := r''_{ij}O_j, \quad \hat{d}_{ij} := d_{ij} - r'_{ij}.$$

Without loss of generality, we assume $\mathcal{A}$ succeeds on the instances $i = 1, \ldots, n$. Our goal will be to show that the $\hat{r}_{ij}$ are distributed negligibly close to uniform modulo p given arbitrary values of the shifts $\hat{d}_{ij}$, so that we can conclude that the coefficients $\hat{r}_{ij} - \hat{d}_{ij} = r_{ij} - d_{ij}$ are distributed negligibly close to uniform modulo p by Lemma 2.1. Ultimately, we conclude that the probability that $\det(r_{ij} - d_{ij})_{i,j=1}^n = 0$ is negligible by Corollary 5.3.

Since $g_j^{r_{ij}} = g_j^{r'_{ij}}$, the execution of $\mathcal{A}$ is independent from the r''_{ij}. So despite the distribution of the $\boldsymbol{r}_i$ being conditioned on $\mathcal{A}$ succeeding on input $(\boldsymbol{g}^{A_i}, \boldsymbol{g}^{\boldsymbol{r}_i})$, the distribution of the r''_{ij} is independent from that of the d_{ij}. It therefore suffices to show that the $\hat{r}_{ij}$ are distributed negligibly close to uniform modulo p given arbitrary values of the $r'_{ij} \in [0, O_j)$. We pick p to be a prime $|\mathbb{G}|/2 < p < |\mathbb{G}|$, which exists by Bertrand's postulate (see e.g., [1, Chapter 2]), so that p is coprime to O_j for each $j = 1, \ldots, n$. Hence it suffices to show that the r''_{ij} are distributed negligibly close to uniform modulo p given arbitrary values of the $r'_{ij} \in [0, O_j)$.

Let $y \in [0, p)$ and fix $x \in [0, O_j)$. We can bound the probability as

$$\frac{1}{p} - \frac{O_j}{U^3 - O_j} \leq \Pr[r''_{ij} \equiv y \bmod p \,|\, r'_{ij} = x] \leq \frac{1}{p} + \frac{O_j}{U^3 - O_j},$$

and denote this distribution by $\mathcal{R}_{U^3,ij,p,x}$. Hence we can apply Lemma 2.5 with $\delta = O_j/(U^3 - O_j)$ to find that, for fixed $(x_{ij})_{i,j=1}^n \in \prod_{i,j=1}^n [0, O_j)$, the statistical distance Δ between $(\mathcal{U}_p)^{n^2}$ and $\prod_{i,j=1}^n \mathcal{R}_{U^3,ij,p,x_{ij}}$ is bounded as

$$\Delta \leq \frac{1}{2}\left(\frac{n^2 p\, O_j}{U^3 - O_j} + \left(\frac{n^2 p\, O_j}{U^3 - O_j}\right)^2\right) \leq \frac{1}{2}\left(\frac{n^2}{U-1} + \left(\frac{n^2}{U-1}\right)^2\right)$$

which is negligible. Hence the probability that $\det(E) = \det(r_{ij} - d_{ij})_{i,j=1}^n = 0$ is negligible by Corollary 5.3; thus Lemma 5.4(iii) is satisfied. □

6.1 Impossibility Results for Generic Reductions

Corollary 6.6. *There do not exist efficient* generic *reductions from* DLog_1 *to* MO *and from* CDH_1 *to* MO*: solving these problems in the generic group model for prime cyclic groups* $\mathbb{G}$ *takes time* $\sqrt{|\mathbb{G}|}$ *with known group order [29, Theorem 1 and 3]. Since* DLog_2 *is equivalent to* DLog_1 *in the case of cyclic groups of prime order, it also follows that no efficient* generic *reduction from* DLog_2 *to* MO *exists.*

Lemma 6.7. *For a group family of (hidden) cyclic large prime order, we have*

$$\mathsf{CDH}_1 \xRightarrow[\text{HO-SM}]{1,1} \mathsf{CDH}_2$$

Proof (sketch). On CDH_1 input tuple (g, g^a, g^b), choose random exponent r and let $s = r^{-1} \bmod p$. Let $X = g^r$, $Y = (g^a)^r = X^a$, $Z = g^b = X^{bs}$ and we return $R = \mathcal{A}(g, X, Y, Z)$. If $\mathcal{A}$ is successful then $R = X^{abs} = g^{absr} = g^{ab}$ as desired. Note that it does not need to know the prime order p. □

Corollary 6.8. *There does not exist an efficient* generic *reduction from* CDH_2 *to* MO*, as otherwise this would contradict Corollary 6.6 using Lemma 6.7.*

7 Security Reductions in the AHO-AGM

Theorem 7.1.

$$\mathsf{MO} \xRightarrow[\text{AHO-AGM}]{(1-e^{-n\cdot C_S})/2,\ \lceil Sn/p \rceil} \mathsf{StRoot}, \quad \text{for } S \geq 4,$$

where $p := \mathsf{Adv}^{\mathsf{StRoot}}_{\mathcal{G},\mathcal{A}}(\kappa)$ *and* C_S *is defined as in Lemma 2.6.*

Proof. Again we will use the template from Lemma 5.4 to construct an MO adversary $\mathcal{B}^{\mathcal{A}}$, which takes input $(\mathbb{G}, \boldsymbol{g})$ with $\mathbb{G} \in \mathcal{G}_\kappa$ and $\boldsymbol{g} \in \mathbb{G}^n$, given an *algebraic* StRoot adversary $\mathcal{A}$. We define a relation sampler $\mathsf{Rel}^{\mathcal{A}}$ as follows, where we assume that a state is maintained in which all internal variables are stored and which is passed between the subroutines.

$\mathsf{Rel}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$	$\mathsf{Samp}(\mathbb{G})$	$\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$
$(\tilde{\boldsymbol{g}}_i, X_i) \leftarrow \mathsf{Samp}(\mathbb{G})$	$A_i \xleftarrow{\$} (\mathcal{U}_{U^2})^{n^2}$	**if** $(Y_i^{e_i} = X_i \wedge e_i > 1)$ **then**
$([Y_i]_{(\tilde{\boldsymbol{g}}_i, X_i)}, e_i) \leftarrow \mathcal{A}(\tilde{\boldsymbol{g}}_i, X_i)$	$\boldsymbol{r}_i \xleftarrow{\$} (\mathcal{U}_{U^3})^n$	**return** $\boldsymbol{r}_i(1 - c_i e_i) - e_i A_i \boldsymbol{b}_i$
$(\boldsymbol{b}_i, c_i) := [Y_i]_{(\tilde{\boldsymbol{g}}_i, X_i)}$	**return** $(\boldsymbol{g}^{A_i}, \boldsymbol{g}^{\boldsymbol{r}_i})$	**else return** $\perp$
return $\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$		

Assume $\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa$ and $\boldsymbol{g} \xleftarrow{\$} \mathbb{G}^n$ are sampled uniformly at random. Again it is straightforward to check that $\boldsymbol{r}_i(1 - c_i e_i) - e_i A_i \boldsymbol{b}_i$ do indeed form relations with respect to $\boldsymbol{g}$; hence Lemma 5.4(i) is satisfied. Completely analogous to Theorem 6.5 conditions (ii) and (iv) of Lemma 5.4 are satisfied.

Our approach to show that Lemma 5.4(iii) is satisfied will be similar to the one in Theorem 6.5. Without loss of generality, we assume that $\mathcal{A}$ succeeds on instances $i = 1, \ldots, n$. Write $A_i = (\boldsymbol{a}_{i1}, \ldots, \boldsymbol{a}_{in})$ and $r_{ij} = r'_{ij} + r''_{ij} O_j$ with $0 \leq r'_{ij} < O_j$, and split the relationship coefficients as

$$\hat{r}_{ij} - \hat{d}_{ij} \quad \text{with} \quad \hat{r}_{ij} := r''_{ij}(1 - c_i e_i) O_j, \quad \hat{d}_{ij} := e_i \sum_{k=1}^{n} a_{ikj} b_{ik} + r'_{ij}(c_i e_i - 1).$$

We claim that we can now pick a prime p such that it is coprime to each O_j for $j = 1, \ldots, n$, and additionally coprime to $1 - c_i e_i$ for all $i = 1, \ldots, n$ (note that $1 - c_i e_i \neq 0$ since $e_i > 1$). This is possible since by [14, Théorème 1.10: 4 & 5], for $|\mathbb{G}| \geq 120368 \approx 2^{17}$, there are superpolynomially many, namely at least

$$\frac{|\mathbb{G}|\,(\log(|\mathbb{G}|/4) - 1.2)}{2(\log|\mathbb{G}| - 1)(\log(|\mathbb{G}|/2) - 1.1)},$$

primes between $|\mathbb{G}|/2$ and $|\mathbb{G}|$. As mentioned before, these are coprime to each O_j for $j = 1, \ldots, n$. Moreover, the number of prime factors of $1 - c_i e_i$ is bounded polynomially for each $i = 1, \ldots, n$, and n is bounded polynomially; hence there are superpolynomially many primes meeting our criteria.

From Theorem 6.5 we know that the distribution of $(r''_{ij} \bmod p)_{i,j=1}^n$, conditioned on arbitrary values of $(r'_{ij})_{i,j=1}^n \in \prod_{i,j=1}^n [0, O_j)$, has negligible statistical distance to $(\mathcal{U}_p)^{n^2}$ and is independent of e_i, $\boldsymbol{b}_i$ and c_i for $i = 1, \ldots, n$. Hence we can conclude that $(\hat{r}_{ij} - \hat{d}_{ij} \bmod p)_{i,j=1}^n$ has negligible statistical distance to $(\mathcal{U}_p)^{n^2}$, and thus that the probability that $\det(E) = \det(\hat{r}_{ij} - \hat{d}_{ij})_{i,j=1}^n = 0$ is negligible by Corollary 5.3; hence Lemma 5.4(iii) is satisfied. □

Theorem 7.2.

$$\mathsf{MO} \xrightarrow[\text{AHO-AGM}]{(1-e^{-n \cdot C_S})/2,\, \lceil Sn/p \rceil} \mathsf{ARoot}, \quad \textit{for } S \geq 4,$$

where $p := \mathsf{Adv}^{\mathsf{ARoot}}_{\mathcal{G},\mathcal{A}}(\kappa)$ *and* C_S *is defined as in Lemma 2.6.*

Proof. Given an *algebraic* ARoot adversary $\mathcal{A}$, we will again use the template from Lemma 5.4 to construct an MO adversary $\mathcal{B}^{\mathcal{A}}$, which takes input $(\mathbb{G}, \boldsymbol{g})$ with $\mathbb{G} \in \mathcal{G}_\kappa$ and $\boldsymbol{g} \in \mathbb{G}^n$. We define a relation sampler $\mathsf{Rel}^{\mathcal{A}}$ as follows, where we assume that a state is maintained in which all internal variables are stored and which is passed between the subroutines.

$\mathsf{Rel}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$	$\mathsf{Samp}(\mathbb{G})$	$\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$
$(\tilde{\boldsymbol{g}}_i, X_i, \ell_i) \leftarrow \mathsf{Samp}(\mathbb{G})$	$A_i \xleftarrow{\$} (\mathcal{U}_{U^3})^{n^2}$	**if** $(Y_i^{\ell_i} = X_i \wedge X_i \neq 1_{\mathbb{G}})$ **then**
$[Y_i]_{(\tilde{\boldsymbol{g}}_i, X_i)} \leftarrow \mathcal{A}(\tilde{\boldsymbol{g}}_i, X_i, \ell_i)$	$[X_i]_{\boldsymbol{g}_i^{A_i}} \leftarrow \mathcal{A}(\boldsymbol{g}^{A_i})$	**return** $A_i(\boldsymbol{b}_i(1 - d_i\ell_i) - \boldsymbol{c}_i\ell_i)$
$(\boldsymbol{c}_i, d_i) := [Y_i]_{(\tilde{\boldsymbol{g}}_i, X_i)}$	$\boldsymbol{b}_i := [X_i]_{\boldsymbol{g}_i^{A_i}}$	**else return** $\perp$
return $\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$	$\ell_i \xleftarrow{\$} \text{Primes}(2\kappa)$	
	return $(\boldsymbol{g}^{A_i}, X_i, \ell_i)$	

It is straightforward to check that $A_i(\boldsymbol{b}_i(1 - d_i\ell_i) - \boldsymbol{c}_i\ell_i)$ do indeed form relations with respect to $\boldsymbol{g}$; hence Lemma 5.4(i) is satisfied. Completely analogous to Theorem 6.5 conditions (ii) and (iv) of Lemma 5.4 are satisfied.

To show that Lemma 5.4(iii) is satisfied, we again take a similar approach as in the proof of Theorem 6.5. Without loss of generality, we assume that $\mathcal{A}$ succeeds on instances $i = 1, \ldots, n$. Write $A_i = (\boldsymbol{a}_{i1}, \ldots, \boldsymbol{a}_{in})$ and $a_{ikj} = a'_{ikj} + a''_{ikj} O_j$ with $0 \leq a_{ikj} < O_j$. Note that for every $i = 1, \ldots, n$, there is at least one $k \in \{1, \ldots, n\}$ for which $b_{ik} \neq 0$ since $\mathcal{A}$ needs to output a non-trivial X_i to succeed. For each $i = 1, \ldots, n$, pick such a $k \in \{1, \ldots, n\}$, and denote it by k_i. Put $\delta_{ik} := b_{ik}(1 - d_i\ell_i) - c_{ik}\ell_i$, expand and split the relation coefficients as

$$\hat{r}_{ij} + \hat{d}_{ij} \quad \text{with} \quad \hat{r}_{ij} := a''_{ik_ij}\delta_{ik_i} O_j, \quad \hat{d}_{ij} := a'_{ik_ij}\delta_{ik_i} + \sum_{k \neq k_i} a_{ikj}\delta_{ik}.$$

As before, our goal is to show that the $\hat{r}_{ij}$ are distributed negligibly close to uniform modulo some prime p given arbitrary values of the shifts $\hat{d}_{ij}$. We first claim that the δ_{ik_i} can only be zero with negligible probability, so that we can pick the prime p coprime to δ_{ik_i} for all $i = 1, \ldots, n$, just as in the proof of Theorem 7.1. Then it suffices to show that the distribution of $(a''_{ik_ij} \bmod p)_{i,j=1}^n$, conditioned on arbitrary values of the $(a'_{ik_ij})_{i,j=1}^n \in \prod_{i,j=1}^n [0, O_j)$, has negligible statistical distance to $(\mathcal{U}_p)^{n^2}$. The latter follows completely analogous as in the proof of Theorem 6.5. So it remains to show the first claim.

Recall that $\delta_{ik_i} = b_{ik_i}(1 - d_i\ell_i) - c_{ik_i}\ell_i$ with $b_{ik_i} \neq 0$. If $c_{ik_i} = 0$, then $\delta_{ik_i} = b_{ik_i}(1 - d_i\ell_i) \neq 0$ since $\ell_i > 1$. If $c_{ik_i} \neq 0$ and $\delta_{ik_i} = 0$, this implies that ℓ_i divides b_{ik_i}, which can only happen with negligible probability since b_{ik_i} is chosen before ℓ_i is picked uniformly from a superpolynomially large set of primes.

Ultimately we can conclude analogous to Theorem 7.1 that Lemma 5.4(iii) is satisfied, which concludes our proof. □

Boneh, Bünz and Fisch [6] previously established the standard model reduction $\mathsf{ARoot} \xrightarrow[\text{SM}]{} \mathsf{LO}$. (That is, given an element $X \in \mathbb{G}$ whose order divides d, one can compute an ℓ-th root as $Y = X^e$ where $e\ell \equiv 1 \bmod d$.) We note that this reduction is generic, and thus $\mathsf{ARoot} \xrightarrow[\text{AHO-AGM}]{} \mathsf{LO}$ as well. Composing this reduction with Theorem 7.2, we obtain the following corollary.

$\mathsf{Rel}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$	$\mathsf{Samp}(\mathbb{G})$
$(\tilde{\boldsymbol{g}}_i, X_i, A_i, B_i) \leftarrow \mathsf{Samp}(\mathbb{G})$	$H_i \xleftarrow{\$} (\mathcal{U}_{U^2})^{n^2}$
$[Y_i]_{(\tilde{\boldsymbol{g}}_i, X_i, A_i, B_i)} \leftarrow \mathcal{A}(\tilde{\boldsymbol{g}}_i, X_i, A_i, B_i)$	$(\boldsymbol{r}_i, a_i, b_i) \xleftarrow{\$} (\mathcal{U}_{U^3})^{n+2}$
$(\boldsymbol{c}_i, d_i, e_i, f_i) := [Y_i]_{(\tilde{\boldsymbol{g}}_i, X_i, A_i, B_i)}$	**return** $(\boldsymbol{g}^{H_i}, \boldsymbol{g}^{\boldsymbol{r}_i}, \boldsymbol{g}^{\boldsymbol{r}_i a_i}, \boldsymbol{g}^{\boldsymbol{r}_i b_i})$
return $\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$	

$\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$
if $Y_i = X_i^{a_i b_i}$ **then**
return $\boldsymbol{r}_i(d_i + a_i e_i + b_i f_i - a_i b_i) + H_i \boldsymbol{c}_i$
else return $\perp$

Fig. 3. The MO relation sampler $\mathsf{Rel}(\mathbb{G}, \boldsymbol{g}, \mathcal{A})$ given CDH_2 adversary $\mathcal{A}$.

Corollary 7.3.

$$\mathsf{MO} \xrightarrow[\text{AHO-AGM}]{(1-e^{-n \cdot C_S})/2,\, \lceil Sn/p \rceil} \mathsf{LO}, \quad \textit{for } S \geq 4,$$

where $p := \mathsf{Adv}^{\mathsf{LO}}_{\mathcal{G}, \mathcal{A}}(\kappa)$ *and* C_S *is defined as in Lemma 2.6.*

Theorem 7.4.

$$\mathsf{MO} \xrightarrow[\text{AHO-AGM}]{(1-e^{-n \cdot C_S})/2,\, \lceil Sn/p \rceil} e\text{-}\mathsf{RT}, \quad \textit{for } S \geq 4,$$

where $p := \mathsf{Adv}^{e\text{-}\mathsf{RT}}_{\mathcal{G}, \mathcal{A}}(\kappa)$ *and* C_S *is defined as in Lemma 2.6.*

Proof. Given an *algebraic* e-RT adversary $\mathcal{A}$ for some fixed $e \in \mathbb{Z}_{>1}$, we use the template from Lemma 5.4 to construct an MO adversary $\mathcal{B}^{\mathcal{A}}$, which takes input $(\mathbb{G}, \boldsymbol{g})$ with $\mathbb{G} \in \mathcal{G}_\kappa$ and $\boldsymbol{g} \in \mathbb{G}^n$. We define a relation sampler $\mathsf{Rel}^{\mathcal{A}}$ as follows, where we assume that a state is maintained in which all internal variables are stored and which is passed between the subroutines.

It is straightforward to check that $\boldsymbol{r}_i(e - c_i e^2) - A_i \boldsymbol{b}_i e$ do indeed form relations with respect to $\boldsymbol{g}$; hence Lemma 5.4(i) is satisfied. Again, completely analogous to Theorem 6.5, conditions (ii) and (iv) of Lemma 5.4 are satisfied.

$\mathsf{Rel}^{\mathcal{A}}(\mathbb{G}, \boldsymbol{g})$	$\mathsf{Samp}(\mathbb{G})$	$\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$
$(\tilde{\boldsymbol{g}}_i, X_i) \leftarrow \mathsf{Samp}(\mathbb{G})$	$A_i \xleftarrow{\$} (\mathcal{U}_{U^2})^{n^2}$	**if** $Y_i^{e_i} = X_i$ **then**
$[Y_i]_{(\tilde{\boldsymbol{g}}_i, X_i)} \leftarrow \mathcal{A}(\tilde{\boldsymbol{g}}_i, X_i)$	$\boldsymbol{r}_i \xleftarrow{\$} (\mathcal{U}_{U^3})^n$	**return** $\boldsymbol{r}_i(e - c_i e^2) - A_i \boldsymbol{b}_i e$
$(\boldsymbol{b}_i, c_i) := [Y_i]_{(\tilde{\boldsymbol{g}}_i, X_i)}$	**return** $(\boldsymbol{g}^{A_i}, \boldsymbol{g}^{\boldsymbol{r}_i e})$	**else return** $\perp$
return $\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$		

We can show almost completely analogous to the proof of Theorem 7.1 that condition Lemma 5.4(iii) is satisfied, with the only difference being that we now pick the prime p coprime to $e - c_i e^2$ for $i = 1, \ldots, n$ (where we again assume without loss of generality that $\mathcal{A}$ succeeds on the instances $i = 1, \ldots, n$). Note that $e - c_i e^2$ is nonzero since $e > 1$. □

Theorem 7.5.

$$\mathsf{MO} \xrightarrow[\text{AHO-AGM}]{(1-e^{-n \cdot C_S})/2,\, \lceil Sn/p \rceil} \mathsf{CDH}_2, \quad \textit{for } S \geq 4,$$

where $p := \mathsf{Adv}^{\mathsf{CDH}_2}_{\mathcal{G}, \mathcal{A}}(\kappa)$ *and* C_S *is defined as in Lemma 2.6.*

Proof. Given an *algebraic* CDH_2 adversary $\mathcal{A}$, we construct an MO adversary $\mathcal{B}^{\mathcal{A}}$, which takes input $(\mathbb{G}, \boldsymbol{g})$ with $\mathbb{G} \in \mathcal{G}_\kappa$ and $\boldsymbol{g} \in \mathbb{G}^n$, using the template from Lemma 5.4. We define a relation sampler $\mathsf{Rel}^{\mathcal{A}}$ as shown in Figure 3, where we assume that a state is maintained in which all internal variables are stored and which is passed between the subroutines. It is again straightforward to

check that $\boldsymbol{r}_i(d_i + a_i e_i + b_i f_i - a_i b_i) + H_i \boldsymbol{c}_i$ do indeed form relations with respect to $\boldsymbol{g}$; hence Lemma 5.4(i) is satisfied. Conditions (ii) and (iv) of Lemma 5.4 hold up analogous to Theorem 6.5.

To show that Lemma 5.4(iii) is satisfied, we again follow a similar approach to Theorem 6.5, only with a few more subtleties. Without loss of generality, we assume that $\mathcal{A}$ succeeds on instances $i = 1, \ldots, n$. Write $H_i = (\boldsymbol{h}_{i1}, \ldots, \boldsymbol{h}_{in})$ and $r_{ij} = r'_{ij} + r''_{ij} O_j$ with $0 \leq r'_{ij} < O_j$, put $\delta_i := d_i + a_i e_i + b_i f_i - a_i b_i$, and split the relation coefficients as $\hat{r}_{ij} + \hat{d}_{ij}$ with $\hat{r}_{ij} := r''_{ij} \delta_i O_j$, $\hat{d}_{ij} := r'_{ij} \delta_i + \sum_{k=1}^{n} h_{ikj} c_{ik}$. Similar to the proof of Theorem 7.2, we want to pick our prime p coprime to δ_i for all $i = 1, \ldots, n$. We claim that δ_i can only be zero with all but negligible probability, and show this using a similar argument as for that the determinant of the relationship matrix can only be zero with all but negligible probability.

Write $a_i = a'_i + a''_i |\langle X_i \rangle|$ and $b_i = b'_i + b''_i |\langle X_i \rangle|$ with $0 \leq a'_i, b'_i \leq |\langle X_i \rangle|$. Pick a prime $|\mathbb{G}|/2 < p' < |\mathbb{G}|$ so that it is coprime to $|\langle X_i \rangle|$ for each $i = 1, \ldots, n$. Completely analogous to the proof of Theorem 6.5, the distribution of $(a''_i \bmod p', b''_i \bmod p')_{i=1}^n$, conditioned on arbitrary values of $(a'_i, b'_i) \in \prod_{i=1}^n [0, |\langle X_i \rangle|)^2$, has negligible statistical distance to $(\mathcal{U}_{p'})^{2n}$. Moreover, it is independent from d_i, e_i and f_i since a''_i and b''_i are completely hidden from the point of view of the adversary. By Lemma 5.2, the probability that $(z_{1i}, z_{2i})_{i=1}^n \xleftarrow{\$} (\mathcal{U}_{p'})^{2n}$ are a zero modulo p' of the polynomial $F(Z_{11}, \ldots, Z_{1n}, Z_{21}, \ldots, Z_{2n})$, defined as

$$\prod_{i=1}^{n} d_i + (a'_i + Z_{1i} |\langle X_i \rangle|)\, e_i + (b'_i + Z_{2i} |\langle X_i \rangle|)\, f_i - (a'_i + Z_{1i} |\langle X_i \rangle|)\, (b'_i + Z_{2i} |\langle X_i \rangle|)\,,$$

is at most $2n/p'$ (note that F reduces to a nonzero polynomial of degree $2n$ over $\mathbb{F}_{p'}$), which is negligible. It follows that any of the δ_i can only be zero with negligible probability since $F(a''_1, \ldots, a''_n, b''_1, \ldots, b''_n) = \prod_{i=1}^n \delta_i$.

Now analogous to the proof of Theorem 7.2, we can conclude that Lemma 5.4(iii) is satisfied. □

8 Security Reductions in the AHO-SAGM

In this section we will show, using similar arguments as before, that it is possible to reduce the multiple order problem MO to the T-repeated squaring problem T-RSW in the AHO-SAGM. Our result can be seen as a generalization of that of [17, Theorem 2] from the family of *cyclic* RSA groups to *all finite abelian groups*. The proof in the abelian case is more complex due to the additional complications that arise from having to run the T-RSW adversary multiple times in order to extract several group relations, which have to be shown to be independent enough. Furthermore, our security definition of T-RSW in AHO-SAGM is weaker by giving the adversary $\mathcal{A}_1$ more power: (1) in contrast to [17], $\mathcal{A}_1$ itself may be standard model and does not have to be strongly algebraic; (2) in contrast to [17], $\mathcal{A}_1$ is given $\mathbf{g}$ (i.e., the same generators $\mathbf{g}$ as the strongly algebraic online algorithm $\mathcal{A}_2$ output by $\mathcal{A}_1$).

We have already seen the reduction in the opposite direction T-RSW $\Rightarrow$ MO; hence this shows the T-repeated squaring and the multiple order game are (asymptotically) equivalent in the AHO-SAGM. Before we show this reduction, we first prove a useful lemma bounding the size of the representation coefficients of the output elements of strongly algebraic algorithms.

Lemma 8.1. *Let $\mathbb{G}$ be a finite abelian group and let $\boldsymbol{g} = (g_1, \ldots, g_n)$ be a tuple of elements of $\mathbb{G}$. Let $\mathcal{A}$ be any* strongly algebraic *algorithm running in at most t rounds on input $\boldsymbol{g}$ and $X = \boldsymbol{g}^{\boldsymbol{r}} = g_1^{r_1} \cdots g_n^{r_n}$ for $\boldsymbol{r} = (r_1, \ldots, r_n) \in \mathbb{Z}_{\geq 1}^n$ (i.e. $\mathsf{ATime}(\mathcal{A}(\boldsymbol{g}, X)) \leq t$). Let Y be any output of $\mathcal{A}$ and let $(Y_s, Y_{s,1}, Y_{s,2})$ or $(Y_s, Y_{s,1})$ be the corresponding tuples for each element Y_s being output at round $1 \leq s \leq t$. (Note that $\mathcal{A}$ is in fact allowed to output arbitrary many tuples in each round, but we can always pick a path of sequential computation leading to Y.) Then the following two statements hold.*

1. *The generalized discrete logarithm $\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y)$ of Y with respect to $\boldsymbol{g}$ and $\mathcal{A}$, can be recursively computed as follows:*
   - $\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, g_i) = \mathbf{1}_i$ *(the vector with a 1 on the i-th place and 0 on all others) for $1 \leq i \leq n$,* $\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, X) = \boldsymbol{r}$*;*

– *For $s = 1, \ldots, t$, let*

$$\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y_s) = \begin{cases} \mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y_{s,1}) + \mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y_{s,2}) & \text{if } Y_s = Y_{s,1}Y_{s,2} \\ -\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y_{s,1}) & \text{if } Y_s = Y_{s,1}^{-1} \end{cases}$$

2. *The generalized discrete logarithm $\boldsymbol{d} = (d_1, \ldots, d_n) := \mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y)$ satisfies $|d_i| \leq 2^t\, r_i$ for all $1 \leq i \leq n$.*

Proof. The first statement is clear. For the second statement we note that if $t = 1$, the only elements $\mathcal{A}$ can output are

$$g_i = \boldsymbol{g}^{\mathbf{1}_i}, \quad g_i^2 = \boldsymbol{g}^{2\cdot\mathbf{1}_i}, \quad g_i g_j = \boldsymbol{g}^{\mathbf{1}_i+\mathbf{1}_j}, \quad g_i^{-1} = \boldsymbol{g}^{-\mathbf{1}_i},$$
$$X = \boldsymbol{g}^{\boldsymbol{r}}, \quad g_i X = \boldsymbol{g}^{\boldsymbol{r}+\mathbf{1}_i}, \quad X^2 = \boldsymbol{g}^{2\boldsymbol{r}}, \quad X^{-1} = \boldsymbol{g}^{-\boldsymbol{r}}$$

for $1 \leq i \neq j \leq n$; hence the statement holds for $t = 1$. We proceed to prove the statement by induction. Suppose that the lemma holds for $t-1$. Now suppose that $\mathcal{A}$ outputs (Y, Y_1, Y_2) in round t. Then Y_1 and Y_2 are either equal to one of the g_i ($1 \leq i \leq n$), $X = \boldsymbol{g}^{\boldsymbol{r}}$, or one of the outputs of $\mathcal{A}$ in rounds $1, \ldots, t-1$. Hence we see that for $1 \leq i \leq n$

$$\begin{aligned} |\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y)_i| &= |\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y_1)_i + \mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y_2)_i| \\ &\leq |\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y_1)_i| + |\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y_2)_i| \leq 2^{t-1} r_i + 2^{t-1} r_i = 2^t\, r_i. \end{aligned}$$

Similarly, if $\mathcal{A}$ outputs (Y, Y_1) in round t, then for $1 \leq i \leq n$ we have that $|\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y)_i| = |\mathsf{DLog}_{\mathcal{A}}(\boldsymbol{g}, Y_1)_i| \leq 2^{t-1} r_i$, which completes the proof of the second statement. □

Theorem 8.2.

$$\mathsf{MO} \xrightarrow[\text{AHO-SAGM}]{(1-e^{-n\cdot C_S})/2,\, \lceil Sn/p \rceil} T\text{-}\mathsf{RSW}, \quad \text{for } S \geq 4,$$

where $p := \mathsf{Adv}^{T\text{-}\mathsf{RSW}}_{\mathcal{G},\mathcal{A}}(\kappa)$ and C_S is defined as in Lemma 2.6.

Proof. Let $\mathcal{A}_1$ be an adversary which runs in the *standard model* in the preprocessing phase and produces $\mathcal{A}_2 \leftarrow \mathcal{A}_1(\mathbb{G}, \mathbf{g})$ which runs as a *strongly algebraic* algorithm in the online phase. We use the template from Lemma 5.4 to construct an adversary $\mathcal{B}^{\mathcal{A}_1}$, which takes input $(\mathbb{G}, \boldsymbol{g})$ with $\mathbb{G} \in \mathcal{G}_\kappa$ and $\boldsymbol{g} \in \mathbb{G}^n$. We define a relation sampler $\mathsf{Rel}^{\mathcal{A}_1}$ as follows, where we assume that a state is maintained in which all internal variables are stored and which is passed between the subroutines, and use the shorthand $t_i := \mathsf{ATime}(\mathcal{A}_2(\tilde{\boldsymbol{g}}_i, X_i))$.

$\mathsf{Rel}^{\mathcal{A}_1}(\mathbb{G}, \boldsymbol{g})$	$\mathsf{Samp}(\mathbb{G})$	$\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$
$(\tilde{\boldsymbol{g}}_i, X_i) \leftarrow \mathsf{Samp}(\mathbb{G})$	$A_i \xleftarrow{\$} (\mathcal{U}_{U^3})^{n^2}$	**if** $\left(Y_i = X_i^{2^T} \wedge t_i < T\right)$ **then**
$\mathcal{A}_2 \leftarrow \mathcal{A}_1(\mathbb{G}, \tilde{\boldsymbol{g}}_i)$	$\boldsymbol{r}_i \xleftarrow{\$} (\mathcal{U}_{U^3})^n$	$\quad \boldsymbol{d}_i \leftarrow \mathsf{DLog}_{\mathcal{A}_2}(\tilde{\boldsymbol{g}}_i, Y_i)$
$(Y_i, ([Y_{i,s}])_{s=1}^{t_i}) \leftarrow \mathcal{A}_2(\tilde{\boldsymbol{g}}_i, X_i)$	**return** $(\boldsymbol{g}^{A_i}, \boldsymbol{g}^{A_i \boldsymbol{r}_i})$	$\quad$ **return** $2^T A_i \boldsymbol{r}_i - A_i \boldsymbol{d}_i$
return $\mathsf{Ext}(\mathbb{G}, \boldsymbol{g}, \text{state})$		**else return** $\perp$

It is straightforward to check that $2^T A_i \boldsymbol{r}_i - A_i \boldsymbol{d}_i$ do indeed form relations with respect to $\boldsymbol{g}$; hence Lemma 5.4(i) is satisfied. Conditions (ii) and (iv) of Lemma 5.4 again hold up completely analogous to Theorem 6.5.

We once more show similar to the proof of Theorem 6.5 that Lemma 5.4(iii) is satisfied. Without loss of generality, we assume that $\mathcal{A}$ succeeds on instances $i = 1, \ldots, n$. Write $A_i = (\boldsymbol{a}_{i1}, \ldots, \boldsymbol{a}_{in})$ and $a_{ikj} = a'_{ikj} + a''_{ikj} O_j$ with $0 \leq a'_{ikj} < O_j$, and expand the relationship coefficients as

$$\sum_{k=1}^{n} a''_{ikj}(2^T r_{ik} - d_{ik}) O_j + \sum_{k=1}^{n} a'_{ikj}(2^T r_{ik} - d_{ik}).$$

Then by Lemma 8.1 and the fact that $\mathcal{A}_2$ runs in $t_i < T$ rounds on input $(\tilde{\boldsymbol{g}}_i, X_i)$, we see that $|d_{ik}| < 2^T r_{ik}$ and thus that $\delta_{ik} := 2^T r_{ik} - d_{ik} \neq 0$ for all $i = 1, \ldots, n$ and $k = 1, \ldots, n$. Now we can pick an arbitrary $k_i \in \{1, \ldots, n\}$ for each $i = 1, \ldots, n$ (e.g. $k_i = 1$ for all $i = 1, \ldots, n$ suffices),

and split the coefficients as $\hat{r}_{ij} + \hat{d}_{ij}$ with $\hat{r}_{ij} := a''_{ik_ij}\delta_{ik_i}O_j$, $\hat{d}_{ij} := a'_{ik_ij}\delta_{ik_i} + \sum_{k \neq k_i} a_{ikj}\delta_{ik}$. Then, similar to the proof of Theorem 7.2, we can pick our prime p coprime to δ_{ik_i} for all $i = 1, \ldots, n$. Analogously to the proof of Theorem 6.5 it follows that the distribution of $(a''_{ik_ij} \mod p)_{i,j=1}^n$, conditioned on arbitrary values of $(a'_{ik_ij})_{i,j=1}^n \in \prod_{i,j=1}^n [0, O_j)$, has negligible statistical distance to $(\mathcal{U}_p)^{n^2}$. Hence we conclude as in the proof of Theorem 6.5 that $(\hat{r}_{ij} - \hat{d}_{ij} \mod p)_{i,j=1}^n$ has negligible statistical distance to $(\mathcal{U}_p)^{n^2}$ and thus that Lemma 5.4(iii) is satisfied. □

References

[1] M. Aigner and G.M. Ziegler, *Proofs from the book*, vol. 274, Springer, 2010.

[2] Ingrid Biehl, Johannes Buchmann, Safuat Hamdy, and Andreas Meyer, *A signature scheme based on the intractability of computing roots*, Des. Codes Cryptogr. **25** (2002), no. 3, 223–236.

[3] Alexander R. Block, Justin Holmgren, Alon Rosen, Ron D. Rothblum, and Pratik Soni, *Time- and space-efficient arguments from groups of unknown order*, CRYPTO (4), LNCS, vol. 12828, Springer, 2021, pp. 123–152.

[4] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch, *Verifiable delay functions*, CRYPTO (1), LNCS, vol. 10991, Springer, 2018, pp. 757–788.

[5] Dan Boneh, Benedikt Bünz, and Ben Fisch, *Batching techniques for accumulators with applications to iops and stateless blockchains*, CRYPTO (1), LNCS, vol. 11692, Springer, 2019, pp. 561–586.

[6] Dan Boneh, Benedikt Bünz, and Ben Fisch, *A survey of two verifiable delay functions*, Cryptology ePrint Archive, Report 2018/712, 2018.

[7] Johannes Buchmann and Arthur Schmidt, *Computing the structure of a finite abelian group*, Math. Comput. **74** (2005), no. 252, 2017–2026.

[8] Johannes Buchmann and Ulrich Vollmer, *Binary quadratic forms - an algorithmic approach*, Algorithms and computation in mathematics, vol. 20, Springer, 2007.

[9] Johannes Buchmann and Hugh C. Williams, *A key-exchange system based on imaginary quadratic fields*, J. Cryptol. **1** (1988), no. 2, 107–118.

[10] Benedikt Bünz, Ben Fisch, and Alan Szepieniec, *Transparent snarks from DARK compilers*, EUROCRYPT (1), LNCS, vol. 12105, Springer, 2020, pp. 677–706.

[11] H. Cohen and H.W. Lenstra, *Heuristics on class groups of number fields*, Number Theory Noordwijkerhout 1983, Springer, 1984, pp. 33–62.

[12] Ivan Damgård and Eiichiro Fujisaki, *A statistically-hiding integer commitment scheme based on groups with hidden order*, ASIACRYPT, LNCS, vol. 2501, Springer, 2002, pp. 125–142.

[13] Ivan Damgård and Maciej Koprowski, *Generic lower bounds for root extraction and signature schemes in general groups*, EUROCRYPT, LNCS, vol. 2332, Springer, 2002, pp. 256–271.

[14] P Dusart, *Autour de la fonction qui compte le nombre de nombres premiers*, Ph.D. thesis, Université de Limoges, 1998.

[15] Naomi Ephraim, Cody Freitag, Ilan Komargodski, and Rafael Pass, *Continuous verifiable delay functions*, EUROCRYPT (3), LNCS, vol. 12107, Springer, 2020, pp. 125–154.

[16] Georg Fuchsbauer, Eike Kiltz, and Julian Loss, *The algebraic group model and its applications*, CRYPTO (2), LNCS, vol. 10992, Springer, 2018, pp. 33–62.

[17] Jonathan Katz, Julian Loss, and Jiayu Xu, *On the security of time-lock puzzles and timed commitments*, TCC (3), Lecture Notes in Computer Science, vol. 12552, Springer, 2020, pp. 390–413.

[18] Esteban Landerreche, Marc Stevens, and Christian Schaffner, *Non-interactive cryptographic timestamping based on verifiable delay functions*, Financial Cryptography, LNCS, vol. 12059, Springer, 2020, pp. 541–558.

[19] S.C. Lindhurst, *Computing roots in finite fields and groups, with a jaunt through sums of digits*, Ph.D. thesis, Citeseer, 1997.

[20] Ueli M. Maurer and Stefan Wolf, *Lower bounds on generic algorithms in groups*, EUROCRYPT, LNCS, vol. 1403, Springer, 1998, pp. 72–84.

[21] V.I. Nechaev, *Complexity of a determinate algorithm for the discrete logarithm*, Mathematical Notes **55** (1994), no. 2, 165–172.

[22] Krzysztof Pietrzak, *Simple verifiable delay functions*, ITCS, LIPIcs, vol. 124, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, pp. 60:1–60:15.

[23] Michael O. Rabin, *Digitalized signatures and public-key functions as intractable as factorization*, Tech. report, Massachusetts Institute of Technology Cambridge Lab for Computer Science, 1979.

[24] Michael O. Rabin, *Transaction protection by beacons*, J. Comput. Syst. Sci. **27** (1983), no. 2, 256–267.

[25] R.L. Rivest, A. Shamir, and D.A Wagner, *Time-lock puzzles and timed-release crypto*, Tech. report, Massachusetts Institute of Technology, 1996.

[26] Lior Rotem and Gil Segev, *Generically speeding-up repeated squaring is equivalent to factoring: Sharp thresholds for all generic-ring delay functions*, CRYPTO (3), LNCS, vol. 12172, Springer, 2020, pp. 481–509.

[27] Lior Rotem, Gil Segev, and Ido Shahaf, *Generic-group delay functions require hidden-order groups*, EUROCRYPT (3), LNCS, vol. 12107, Springer, 2020, pp. 155–180.

[28] Jacob T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. ACM **27** (1980), no. 4, 701–717.

[29] Victor Shoup, *Lower bounds for discrete logarithms and related problems*, EUROCRYPT, LNCS, vol. 1233, Springer, 1997, pp. 256–266.

[30] Benjamin Wesolowski, *Efficient verifiable delay functions*, EUROCRYPT (3), LNCS, vol. 11478, Springer, 2019, pp. 379–407.

[31] Richard Zippel, *Probabilistic algorithms for sparse polynomials*, EUROSAM, LNCS, vol. 72, Springer, 1979, pp. 216–226.

A Proofs

Lemma 2.5. *Let $\mathcal{U}_M$ be the uniform distribution on the set $[0, M)$ and let $\mathcal{D}_i$ be probability distributions over the same set for $i = 1, \ldots, \ell$. Assume that there exists a constant $0 < \delta \leq 1/M\ell$ such that for all instances $x \in [0, M)$*

$$\left| \Pr_{X \sim \mathcal{D}_i}[X = x] - \Pr_{Y \sim \mathcal{U}_M}[Y = x] \right| \leq \delta.$$

Then the statistical distance Δ between the cartesian products $\prod_{i=1}^{\ell} \mathcal{D}_i$ and $\prod_{i=1}^{\ell} \mathcal{U}_M$ can be upper bounded as

$$\Delta := \delta\left(\prod_{i=1}^{\ell} \mathcal{D}_i, \prod_{i=1}^{\ell} \mathcal{U}_M\right) \leq \frac{1}{2}\left(\delta\ell M + (\delta\ell M)^2\right).$$

Proof. First note that $\Pr_{Y \sim \mathcal{U}_M}[Y = x] = 1/M$ independent of $x \in [0, M)$. Denote

$$\delta_{i,x} := \Pr_{X \sim \mathcal{D}_i}[X = x] - 1/M.$$

By assumption, $|\delta_{i,x}| \leq \delta$ for all $x \in [0, M)$. Hence we can write

$$\begin{aligned}\Delta &= \frac{1}{2} \sum_{x_1, \ldots, x_\ell = 0}^{M-1} \left| \prod_{i=1}^{\ell} (1/M + \delta_{i,x_i}) - 1/M^\ell \right| \\ &\leq \frac{1}{2} \cdot M^\ell \cdot \max\{1/M^\ell - (1/M - \delta)^\ell,\, (1/M + \delta)^\ell - 1/M^\ell\}.\end{aligned}$$

Here

$$1/M^\ell - (1/M - \delta)^\ell \leq 1/M^\ell - (1 - \delta M\ell)/M^\ell = \delta M\ell/M^\ell,$$

where we used that $(1 - x)^\ell \geq 1 - \ell x$ for $x \leq 1$. Moreover

$$\begin{aligned}(1/M + \delta)^\ell - 1/M^\ell &\leq \left(1 + \delta M\ell + (\delta M\ell)^2\right)/M^\ell - 1/M^\ell \\ &= \left(\delta M\ell + (\delta M\ell)^2\right)/M^\ell,\end{aligned}$$

where we used that $1 + x \leq e^x \leq 1 + x + x^2$ for $x < 1.79$. Hence we can conclude that the statistical distance is bounded as

$$\Delta \leq \frac{1}{2}\left(\delta\ell M + (\delta\ell M)^2\right).$$

□

Lemma 2.6. *Let $\mathcal{X} = \{X_i\}_{i \in I}$ be a probability distribution ensemble, where $X_i \sim B(N, p_i)$ follows the binomial distribution with N samples with probability p_i. Let the set $\mathcal{X}$ itself be endowed with the uniform distribution. Given $n \geq 1$, $S \geq 4$ and the average probability $p = \mathrm{E}[p_i]$, if $N = \lceil Sn/p \rceil$ then*

$$\Pr_{X \in \mathcal{X}}[X \geq n] \geq (p/2) \cdot (1 - e^{-n \cdot C_S})$$

where $C_S := (S - 3)/2 + 1/S - \log(S/2)$. Note that $C_S \geq 1$ for $S \geq 8$.

Proof. We consider the subsets

$$\mathcal{X}_1 := \{X_i \in \mathcal{X} \,|\, p_i \leq p/2\}, \quad \mathcal{X}_2 := \{X_i \in \mathcal{X} \,|\, p_i > p/2\},$$

and want to lower bound the size of $\mathcal{X}_2$. Note that $\mathcal{X}_2$ is smallest when $p_i = p/2$ for all $X_i \in \mathcal{X}_1$ and $p_i = 1$ for all $X_i \in \mathcal{X}_2$. This leads to the system of equations

$$(|\mathcal{X}_1 + \mathcal{X}_2|)/|\mathcal{X}| = 1, \quad (|\mathcal{X}_1| \cdot p/2 + |\mathcal{X}_2|)/|\mathcal{X}| = p,$$

with solutions

$$|\mathcal{X}_1|/|\mathcal{X}| = (2 - 2p)/(2 - p), \quad |\mathcal{X}_2|/|\mathcal{X}| = p/(2 - p) \geq p/2.$$

Hence uniformly picking $X \xleftarrow{\$} \mathcal{X}$, then X lands in $\mathcal{X}_2$ with probability $\geq p/2$.

We will continue to lower bound $\Pr[X_i \geq n]$ for each $X_i \in \mathcal{X}_2$, thus $p_i > p/2$. Note that it is sufficient to upper bound $\Pr[X_i \leq n]$. By Chernoff's bound, we have

$$\Pr[X_i \leq n] \leq e^{(-N \cdot \mathrm{D}(n/N \| p_i))},$$

where $\mathrm{D}(a \parallel b) := a \log(a/b) + (1-a) \log\left((1-a)/(1-b)\right)$ (for $a, b \in [0,1]$) is the relative entropy. Note that $\mathrm{D}(a \parallel b)$ is monotonically decreasing in a and monotonically increasing in b for $0 < a \leq b < 1$. Indeed, the partial derivatives are given by

$$\frac{\partial}{\partial a} \mathrm{D}(a \parallel b) = \log\left(\frac{a}{b}\right) - \log\left(\frac{a-1}{b-1}\right), \quad \frac{\partial}{\partial b} \mathrm{D}(a \parallel b) = \frac{b-a}{b(1-b)},$$

which are ≤ 0 and ≥ 0 for $0 < a \leq b < 1$, respectively. Since $\lceil Sn/p \rceil \geq Sn/p$ and $p_i > p/2 > p/S$, we deduce from these two monotonicity properties that

$$\Pr[X_i \leq n] \leq \exp\left(-Sn/p \cdot \mathrm{D}\left(p/S \parallel p/2\right)\right),$$

where we note that the inequality also holds at the pole $p_i = 1$. We therefore continue to lower bound the relative entropy

$$\begin{aligned}
\mathrm{D}\left(\frac{p}{S} \parallel \frac{p}{2}\right) &= \frac{p}{S} \log\left(\frac{2}{S}\right) + \left(1 - \frac{p}{S}\right) \log\left(\frac{1 - p/S}{1 - p/2}\right) \\
&\geq \frac{p}{S} \log\left(\frac{2}{S}\right) + \left(1 - \frac{p}{S}\right) \left(\frac{2}{S} - 1\right) \log\left(1 - \frac{p}{2}\right) \\
&\geq \frac{p}{S} \log\left(\frac{2}{S}\right) + \left(1 - \frac{p}{S}\right) \left(1 - \frac{2}{S}\right) \frac{p}{2},
\end{aligned}$$

where from the first to the second line we use that $1 - p/S \geq (1 - p/2)^{2/S}$ and from the second to the third line that $-\log(1 - p/2) \geq p/2$. Hence

$$\begin{aligned}
\Pr[X_i \leq n] &\leq \exp\left(-n \left(\log\left(\frac{2}{S}\right) + (S - p)\left(1 - \frac{2}{S}\right)\frac{1}{2}\right)\right) \\
&\leq \exp\left(-n \left(\log\left(\frac{2}{S}\right) + \frac{S}{2} + \frac{1}{S} - \frac{3}{2}\right)\right),
\end{aligned}$$

where we used that $p < 1$. Hence ultimately we can conclude that

$$\Pr_{X \in \mathcal{X}}[X \geq n] \geq (p/2) \cdot \left(1 - \exp\left(-n \left(\log\left(\frac{2}{S}\right) + \frac{S}{2} + \frac{1}{S} - \frac{3}{2}\right)\right)\right)$$

□

Theorem 3.4. *Let $k \geq 2$, $n \geq 2^{23}$, and $1 \leq d < n$ be positive integers, and let $s_1, \ldots, s_k$ be arbitrary integers with $|s_i| \leq n^d$. Let $X_1, \ldots, X_k$ be random variables with distribution $\mathcal{U}_n$, then:*

$$\Pr[\gcd(s_1 + X_1, \ldots, s_k + X_k) = 1] \geq (1 - (d/n)^{k-1}) \cdot (1 - \epsilon) \cdot 1/\zeta(k),$$

where $\zeta(k)$ is the Riemann zeta function, $\epsilon \leq .077$ for $k = 2$ and $\epsilon \leq 2.9 \cdot 10^{-5}$ for $k \geq 3$. When $d \leq n/10$, this probability is at least .505 for $k \geq 2$, at least .92 for $k \geq 4$, and at least .99 for $k \geq 7$.

Proof. A prime p divides the joint GCD if and only if p divides $s_i + X_i$ for all $1 \leq i \leq k$. For the joint GCD to equal one, this must not hold for all primes, hence it follows that:

$$\Pr[\gcd(s_1 + X_1, \ldots, s_k + X_k) = 1] = \prod_{\text{Prime } p} \Pr[(X_i)_{i=1}^k \not\equiv (-s_i)_{i=1}^k \bmod p] = P_1 \cdot P_2 \cdot P_3.$$

Here P_1, P_2, P_3 are the following sub products based on the size of p, which we will lower bound separately:

$$P_1 = \prod_{\substack{\text{Prime } p \\ 2 \le p \le \sqrt{n}}} \Pr[(X_i)_{i=1}^k \not\equiv (-s_i)_{i=1}^k \bmod p]$$
$$P_2 = \prod_{\substack{\text{Prime } p \\ \sqrt{n} < p \le n}} \Pr[(X_i)_{i=1}^k \not\equiv (-s_i)_{i=1}^k \bmod p]$$
$$P_3 = \prod_{\substack{\text{Prime } p \\ n < p}} \Pr[(X_i)_{i=1}^k \not\equiv (-s_i)_{i=1}^k \bmod p]$$

Below we will prove that $P_1 \ge 1/\zeta(k) \cdot (1 - 10^{-6})$, $P_3 \ge (1 - (d/n)^{k-1})$ and

$$P_2 \ge \begin{cases} (1 - 0.076) & \text{for } k = 2 \\ (1 - 2.8 \cdot 10^{-5}) & \text{for } k \ge 3 \end{cases}$$

Multiplying these bounds proves the theorem. Note that in this proof we will directly use several numerical bounds without going into too much detail, these should be easy to verify though.

Note that using Lemma 2.3, we can bound each factor for all primes $p \le n$ as:

$$\Pr[(X_i)_{i=1}^k \not\equiv (-s_i)_{i=1}^k \bmod p] \ge 1 - (1/p + 1/n)^k.$$

For primes $p > n$, there is at most one value $1 \le x_i \le n$ such that $p|(s_i + x_i)$ for each $1 \le i \le k$. Thus the probability all $s_i + X_i$ result in a multiple of p is upper bounded by $(1/n)^k$ (and 0 if there is no possible multiple of p for at least one $1 \le i \le k$), hence:

$$\Pr[(X_i)_{i=1}^k \not\equiv (-s_i)_{i=1}^k \bmod p] \ge 1 - n^{-k}.$$

Product P_1. We first consider the product P_1 over primes $p \le \sqrt{n}$. Let $\psi(p) = p'$ where p' is the largest prime $p' < p$, then for $5 \le p \le \sqrt{n}$, one can further lower bound each factor as:

$$1 - (1/p + 1/n)^k \ge 1 - (p-2)^{-k} \ge 1 - \psi(p)^{-k}.$$

Considering the product for all primes $B < p \le \sqrt{n}$, where we choose a prime $B = 2879 < \sqrt{2^{23}}$, one can find:

$$\begin{aligned} \prod_{\substack{\text{Prime } p \\ B < p \le \sqrt{n}}} (1 - (1/p + 1/n)^k) &\ge \prod_{\substack{\text{Prime } p \\ B < p \le \sqrt{n}}} (1 - \psi(p)^{-k}) \\ &\ge \prod_{\substack{\text{Prime } p \\ B-2 < p}} (1 - p^{-k}) \\ &= \frac{1/\zeta(k)}{\prod_{\substack{\text{Prime } p \\ p \le B-2}} (1 - p^{-k})} \end{aligned}$$

Where in the last step we use Euler's Product Formula $1/\zeta(k) = \prod_{\text{Prime } p}(1 - p^{-k})$. This can be multiplied with the product over all primes $p \le B$ which results in $1/\zeta(k) \cdot (1 - \epsilon)$:

$$\begin{aligned} P_1 &\ge 1/\zeta(k) \cdot \frac{\prod_{\substack{\text{Prime} \\ p \le B}} (1 - (1/p + 1/n)^k)}{\prod_{\substack{\text{Prime} \\ p \le B}} (1 - p^{-k})} \cdot (1 - B^{-k}) \\ &\ge 1/\zeta(k) \cdot (1 - 10^{-6}) \end{aligned}$$

In the last step we evaluate that $\epsilon \le 10^{-6}$ for the chosen B and for all $n \ge 2^{23}$ and $k \ge 2$. In principle ϵ can be made arbitrary small for large enough n, k and B, however this constant is sufficient for most purposes.

Product P_2. For primes $\sqrt{n} < p \leq n$, we can lower bound each factor as:

$$1 - (1/p + 1/n)^k \geq 1 - (1/\sqrt{n} + 1/n)^k = 1 - (\sqrt{n}+1/n)^k .$$

As $\{\#\text{Prime } \sqrt{n} < p \leq n\} \leq \{\#\text{Prime } p \leq n\} \leq 1.256 \cdot n/\ln(n)$, the product over these primes can be lower bounded as:

$$\begin{aligned} P_2 &\geq (1 - (\sqrt{n}+1/n)^k)^{1.256n/\ln(n)} \\ &= e^{\ln(1-(\sqrt{n}+1/n)^k) \cdot 1.256n/\ln(n)} \\ &\geq e^{-1.001 \cdot (\sqrt{n}+1/n)^k \cdot 1.256n/\ln(n)} \end{aligned}$$

Where in the last step we use the inequality $\ln(1-x) \geq -1.001x$ that holds for $0 < x < 0.00199$, which is allowed since $(\sqrt{n}+1/n)^k < 0.00199$ for $k \geq 2$ and $n \geq 2^{23}$. We now distinguish on values of k:

- When $k = 2$, the exponent can be rewritten as

  $$-1.257256/\ln(n) - 2.514512/(\sqrt{n}\ln(n)) - 1.257256/(n\ln(n))$$

  For all $n \geq 2^{23}$, we find that this is greater than $-1.259/\ln(n)$, which results in an overall lower bound:

  $$P_2 \geq e^{-1.259/\ln(n)} \geq (1 - 0.076)$$

- Similarly when $k \geq 3$ we can find that for all $n \geq 2^{23}$:

  $$P_2 \geq e^{-1.001 \cdot (\sqrt{n}+1/n)^3 \cdot 1.256n/\ln(n)} \geq e^{-1.259/\sqrt{n}\ln(n)} \geq (1 - 2.8 \cdot 10^{-5})$$

Product P_3. The remaining case to be handled are all primes $p > n$. When we would allow arbitrarily large shifts $s_1, \ldots, s_k$, we cannot prove a lower bound on the probability. In fact, one can always algorithmically generate shifts where the probability that the GCD equals 1 becomes zero:

1. Compute the first n^k primes and arbitrary label these as $p_{(x_j)_{j=1}^k}$ where $(x_j)_{j=1}^k \in \{0, \ldots, n-1\}^k$.
2. For $i = 1, \ldots, k$ use the Chinese Remainder Theorem to solve s_i given the n^k modular equations $s_i \equiv -x_i \bmod p_{(x_j)_{j=1}^k}$ for all possible values $(x_j)_{j=1}^k \in \{0, \ldots, n-1\}^k$.

One can verify that then for all possible values $(x_j)_{j=1}^k \in \{0, \ldots, n-1\}^k$ that the prime $p_{(x_j)_{j=1}^k}$ divides $s_j + x_j$ for $j = 1, \ldots, k$, hence $\gcd(s_1 + x_1, \ldots, s_k + x_k) \neq 1$. For instance, a counter-example for $k = 2$, $n = 5$ are the shifts $s_1 = 97933934092855859$ and $s_2 = 205204317512618213$ for which $\forall x_1, x_2 \in \{1, 2, 3, 4, 5\} : \gcd(s_1 + x_1, s_2 + x_2) \neq 1$.

In this case we will not lower bound each factor of the product, but lower bound the probability that there does not exist a prime $p > n$ that divides $\gcd(s_1 + X_1, \ldots, s_k + X_k)$. For all possible values x_1 the random variable X_1 can take, let $p_1, \ldots, p_m$ be the list of prime divisors p of $s_1 + x_1$ for which $p > n$. As $s_1 + x_1 < n^d + n$, there can be at most d such large prime divisors, thus $m \leq d$. For each p_j and each $2 \leq i \leq k$, there is at most one value x_i for X_i such that $p_j | (s_i + x_i)$, thence

$$\forall 2 \leq i \leq k \ : \ \Pr[\gcd(p_1 \cdots p_m, s_i + X_i) \neq 1] \ \leq \ d/n.$$

It follows that for the given value x_1 of X_1 the probability that no large prime divisor $p > n$ of $s_1 + x_1$ also divides all $s_i + X_i$ for $2 \leq i \leq k$ is:

$$\Pr[\gcd(p_1 \cdots p_m, s_2 + X_2, \ldots, s_k + X_k) = 1] \ \geq \ 1 - (d/n)^{k-1}.$$

Since this lower-bound holds for all possible values x_1 and all large prime divisors $p > n$ of $s_1 + x_1$, we have established that it lower bounds the product over the region $p > n$:

$$P_3 \ \geq \ 1 - (d/n)^{k-1}.$$

□

Lemma 4.7. *Let $\mathbb{G}$ be a finite abelian group and let $g_1, \ldots, g_n \in \mathbb{G}$ be a system of generators. Put $O_i := |\langle g_i \rangle|$ for $i = 1, \ldots, n$. If we sample $(r_i)_{i=1}^n \xleftarrow{\$} \prod_{i=1}^n \mathcal{U}_{O_i}$ and set $X := g_1^{r_1} \cdots g_n^{r_n}$, then X is uniformly distributed in $\mathbb{G}$.*

Proof. By the fundamental theorem of finite abelian groups we can write $\mathbb{G} \cong \bigoplus_{k=1}^t (\mathbb{Z}/q_k\mathbb{Z})$, where $q_1, \ldots, q_t$ are powers of not necessarily distinct prime numbers. Let $\tilde{g}_1, \ldots, \tilde{g}_t$ be the system of generators of $\mathbb{G}$ corresponding to the generators of the respective cyclic components under the aforementioned isomorphism. Every $X \in \mathbb{G}$ can be uniquely represented as

$$X = \tilde{g}_1^{a_1} \cdots \tilde{g}_t^{a_t}, \quad 0 \le a_i < q_i \quad \text{for } i = 1, \ldots, t,$$

and thus one can uniformly sample elements in $\mathbb{G}$ by sampling $(a_i)_{i=1}^t \xleftarrow{\$} \prod_{i=1}^t \mathcal{U}_{q_i}$. In particular, we can represent our original generators as

$$g_i = \tilde{g}_1^{b_{1i}} \cdots \tilde{g}_t^{b_{ti}}, \quad i = 1, \ldots, n. \tag{7}$$

Since $g_1, \ldots, g_n$ generate $\mathbb{G}$, we can also express $\tilde{g}_1, \ldots, \tilde{g}_t$ as

$$\tilde{g}_i = g_1^{c_{1i}} \cdots g_n^{c_{ni}}, \quad i = 1, \ldots, t. \tag{8}$$

Now sample $(r_i)_{i=1}^n \xleftarrow{\$} \prod_{i=1}^n \mathcal{U}_{O_i}$ and $(a_i)_{i=1}^t \xleftarrow{\$} \prod_{i=1}^t \mathcal{U}_{q_i}$, and set

$$X := g_1^{r_1} \cdots g_n^{r_n}, \quad Y := \tilde{g}_1^{a_1} \cdots \tilde{g}_t^{a_t}, \quad Z := XY.$$

Then we can write

$$Z = g_1^{r_1 + \sum_{j=1}^t c_{1j} a_j} \cdots g_n^{r_n + \sum_{j=1}^t c_{nj} a_j},$$

from which we can deduce that Z is distributed identical to X since the coefficients $r_i + \sum_{j=1}^t c_{ij} a_j$ are distributed uniformly modulo O_i for $i = 1, \ldots, n$ by Lemma 2.1. Similarly, we can write

$$Z = \tilde{g}_1^{a_1 + \sum_{j=1}^n b_{1j} r_j} \cdots \tilde{g}_t^{a_t + \sum_{j=1}^n b_{tj} r_j},$$

from which we can deduce that Z is distributed identical to Y since the coefficients $a_i + \sum_{j=1}^n b_{ij} r_j$ are distributed uniformly modulo q_i for $i = 1, \ldots, t$ by Lemma 2.1. Hence we can conclude that Z is distributed uniformly in $\mathbb{G}$ since Y is distributed uniformly in $\mathbb{G}$, from which we can conclude that X is distributed uniformly in $\mathbb{G}$. □

Lemma 4.8. *Let $\mathbb{G}$ be a finite abelian group, let $g_1, \ldots, g_n \in \mathbb{G}$ be a system of generators, and let ℓ, v be positive integers. If we sample $(r_{ij})_{i,j=1}^{\ell,n} \xleftarrow{\$} (\mathcal{U}_{U^v})^{\ell n}$ and set $X_i := g_1^{r_{i1}} \cdots g_n^{r_{in}}$ for $i = 1, \ldots, \ell$. Then the statistical distance between the distribution of $(X_i)_{i=1}^\ell$ and the uniform distribution $\mathcal{U}_{\mathbb{G}^\ell}$ is upper bounded by*

$$\frac{\ell n}{2U^{v-1}} + \frac{\ell^2 n^2}{2U^{2v-2}}. \tag{9}$$

Proof. By Lemma 4.7, it suffices to show that the statistical distance between the distribution of $(r_{ij} \bmod O_j)_{i,j=1}^{\ell,n}$ and $\prod_{i,j=1}^{\ell,n} \mathcal{U}_{O_j}$ is upper bounded by the desired quantity (9).

First note that for $\boldsymbol{x}_i = (x_{i1}, \ldots, x_{in}) \in \prod_{j=1}^n [0, O_j)$, by Lemma 2.3, we have

$$1/O_j - 1/U^v \le \Pr[r_{ij} \equiv x_{ij} \bmod O_j] \le 1/O_j + 1/U^v$$

for each $j = 1, \ldots, n$ and $i = 1, \ldots, \ell$. Similar to the proof of Lemma 2.5, the statistical distance Δ between $\prod_{i,j=1}^{\ell,n} \mathcal{R}_{U^v, O_j}$ and $\prod_{i,j=1}^{\ell,n} \mathcal{U}_{O_j}$ satisfies

$$\begin{aligned}
\Delta &= \frac{1}{2} \sum_{\boldsymbol{x} \in \prod_{i,j=1}^{\ell,n} [0, O_j)} \left| \prod_{i,j=1}^{\ell,n} \Pr[r_{ij} \equiv x_{ij} \bmod O_j] - \prod_{i,j=1}^{\ell,n} \frac{1}{O_j} \right| \\
&\le \frac{1}{2} \cdot \max \left\{ \prod_{j=1}^n \left(1 + \frac{O_j}{U^v}\right)^\ell - 1,\ 1 - \prod_{j=1}^n \left(1 - \frac{O_j}{U^v}\right)^\ell \right\},
\end{aligned}$$

where

$$\prod_{j=1}^{n}\left(1+\frac{O_j}{U^v}\right)^{\ell}-1\leq\left(1+\frac{1}{U^{v-1}}\right)^{\ell n}-1\leq\frac{\ell n}{U^{v-1}}+\frac{\ell^2 n^2}{U^{2v-2}},$$

and

$$1-\prod_{j=1}^{n}\left(1-\frac{O_j}{U^v}\right)^{\ell}\leq 1-\left(1-\frac{1}{U^{v-1}}\right)^{\ell n}\leq\frac{\ell n}{U^{v-1}}.$$

So the statistical distance between the distribution sampling $(X_i)_{i=1}^{\ell}$ in the way described in the Lemma and the uniform distribution on $\mathbb{G}^{\ell}$ is indeed upper bounded by expression (9). $\square$