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

Aron van Baarsen and Marc Stevens

CWI
Centrum Wiskunde & Informatica

November 30, 2021

What are Hidden-Order Groups?

A finite group $\mathbb{G}$ such that:

- It is *hard* to compute (a multiple) of the order $|\mathbb{G}|$.
- *Preferably:* can be sampled without a trusted setup.

RSA Groups

$\mathbb{G} = \mathbb{Z}_N^*$, $N = pq$, with p, q large primes.

- Computing a multiple of the order $\Leftrightarrow$ factoring N.
- Fastest known classical method: GNFS in $L_N[1/3, c]$.
- Requires trusted setup.

IQ Class Groups

$\mathbb{G} = \mathsf{Cl}(\mathcal{O})$ class group of an order $\mathcal{O} \subset \mathbb{Q}(\sqrt{\Delta})$ with $\Delta < 0$.

- Historically less studied compared to RSA groups.
- Fastest known classical method: MPQS in $L_{|\Delta|}[1/2, 1]$.
- *No* trusted setup.

Applications

Verifiable Delay Functions (VDFs) & Time-Lock Cryptography

- Based on the hardness of computing X^{2^T} for $X \xleftarrow{\$} \mathbb{G}$ with less than T *sequential* operations [RSW96, Wes19, Pie19].
- $|\mathbb{G}|$ known* $\implies$ $X^{2^T \bmod |\mathbb{G}|}$ can be computed in cost $\approx \log_2 |\mathbb{G}|$.

Hardness of Computing Roots

- $|\mathbb{G}|$ known* $\wedge$ $\gcd(e, |\mathbb{G}|) = 1$
  $\implies$ $Y := X^d$ is e-th root of $X \in \mathbb{G}$, where $d := e^{-1} \bmod |\mathbb{G}|$.
- Related to hardness of RSA/e-RT, StRSA/StRoot, ARoot.
- Important for: Cryptographic Accumulators [BBF19], Zero-Knowledge Arguments [BFS20, BHR+21], VDF Soundness [Wes19, Pie19, BBF18].

*Hold analogously if only a multiple of $|\mathbb{G}|$ is known

Cyclic vs. Abelian Groups

Let $\mathbb{G}$ a finite abelian group (i.e., $gh = hg$ for all $g, h \in \mathbb{G}$) with $N = |\mathbb{G}|$.

Cyclic

- There exists $g \in \mathbb{G}$ such that $\mathbb{G} = \langle g \rangle$.
- More precisely, there are $\varphi(N)$ such generators.
- Hence a *single* uniformly random element is a generator with probability $\varphi(N)/N$.

Abelian

- There exist $g_1, \ldots, g_n \in \mathbb{G}$ such that $\mathbb{G} = \langle g_1, \ldots, g_n \rangle$.
- Holds for $n := \lceil \log_2 N \rceil$ (but a smaller n is often sufficient).
- $2n$ uniformly random elements generate $\mathbb{G}$ with probability $\geq 1 - 1/N$.

Why *Abelian* Hidden-Order Groups?

RSA Groups

- Picking safe primes $p = 2p' + 1$, $q = 2q' + 1$, the subgroup of quadratic residues in $\mathbb{Z}_N^*$ has order $|\mathcal{QR}_N| = p'q'$ and *cyclic*.
- For $x \xleftarrow{\$} \mathbb{Z}_N^*$, x^2 is a generator with overwhelming probability.
- Requires trusted setup.

IQ Class Groups

- Picking a random fundamental discriminant $\Delta < 0$, $\mathsf{Cl}_{\mathsf{odd}}(\Delta)$ is heuristically cyclic with high probability [CL84].
- But, no efficient way to check if it is cyclic!
- *No* trusted setup.

Motivates the study of (non-cyclic) abelian hidden-order groups.

- Historically, non-cyclic groups have received far less attention in cryptologic research compared to cyclic groups.
- So new methods need to be developed!

Goals/Contributions

- Study and define Abelian Hidden-Order group setting.
  - **AHO-SM:** Standard Model
    - Sample group and *sample n random elements as generators*.
  - **AHO-AGM:** generalization Algebraic Group Model [FKL18]
    - Algebraic relation for every output group element.
    - *Explicit group description and random set of generators in input*.
  - **AHO-SAGM:** generalization Strong Algebraic Group Model [KLX20]
    - Similar to AGM, but using many "algebraic rounds":
      output rounds with only elementary algebraic relations.
    - *Explicit group description and random set of generators in input*.
  - Adapt defs. of cryptographic problems to abelian hidden-order setting.
- Study relations between cryptographic problems in abelian groups of *hidden* order in these three models.

Computational Problems (informally)

(MO)/HO :	Calculate (a multiple of) the group order $\lvert\mathbb{G}\rvert$
LO :	Find a non-trivial $X \in \mathbb{G}$ of low order d
e-RT :	Find e-th root of a random $X \xleftarrow{\$} \mathbb{G}^{(e)}$ $(e > 1)$
StRoot :	Find any non-trivial root $Y^e = X$ of random $X \xleftarrow{\$} \mathbb{G}$
ARoot :	Find prime root $Y^\ell = X$ for chosen non-trivial $X \in \mathbb{G}$, where random prime ℓ is sampled *after* X
T-RSW :	Compute X^{2^T} faster than T squarings for random $X \xleftarrow{\$} \mathbb{G}$
DLog_1 :	Find $e_1, \ldots, e_n \in \mathbb{N}$ such that $g_1^{e_1} g_2^{e_2} \cdots g_n^{e_n} = X$ for random $X, g_1, \ldots, g_n \xleftarrow{\$} \mathbb{G}$
DLog_2 :	Find $d \in \mathbb{N}$ s.t. $X^d = Y$ for random $X \xleftarrow{\$} \mathbb{G}$, $Y \xleftarrow{\$} \langle X \rangle$
CDH_2 :	Compute X^{ab} given X, X^a, X^b for $X \xleftarrow{\$} \mathbb{G}$, $a, b \xleftarrow{\$} \mathcal{U}_{\lvert\langle X\rangle\rvert}$

Overview of Reductions/Contributions

A \ B	DLog_1	DLog_2	CDH_2	HO	MO	T-RSW	StRoot	ARoot	e-RT	LO
DLog_1				[1]	[1]	[1]	[1]	[1]	[1]	[1]
DLog_2				[1]	[1]	[1]	[1]	[1]	[1]	[1]
CDH_2				[1]	[1]	[1]	[1]	[1]	[1]	[1]
HO										
MO				Trivial						
T-RSW				[2]	[2]					
StRoot				[3]	[3]					
ARoot				[4]	[4]					[5]
e-RT	†[6] ‡	†[6] ‡	†[6] ‡	†[6] ‡	†[6] ‡	†[6] ‡	†[6] ‡	†[6] ‡		†[6]
LO										

Figure: Overview of reductions $A \Rightarrow B$ (in SM/AGM/SAGM)

- 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
- [1] = [Sho97], [2] = [KLX20], [3] = [DK02], [4] = [Wes19], [5] = [BBF18], [6] = [BBHM02]

Related Work

- **[DK02]:** Prove hardness of StRoot and e-RT in the GGM.
- **[KLX20]:** Prove that hardness of factoring implies the hardness of the T-RSW problem in RSA groups in the SAGM.
  $\rightsquigarrow$ straightforward generalization to MO $\Rightarrow$ T-RSW in *cyclic* groups.
  (Factoring $\Leftrightarrow$ HO $\Leftrightarrow$ MO in RSA groups.)
- **[RSS20, RS20]:** Prove that delay functions require hidden order groups in the GGM for *cyclic* groups [RSS20], and that generically speeding up repeated squaring in RSA groups is equivalent to factoring in the *generic ring model* (GRM) [RS20].

Computational Models (informally)

- *Standard Model* (SM)

  Adversaries receive group description and have no restriction on what they are allowed to output.

- *Algebraic Group Model* (AGM) – [FKL18]

  Adversaries need to output an algebraic representation for each output group element in terms of input group elements.

- *Strong Algebraic Group Model* (SAGM) – [KLX20]

  Adversaries need to expose the path of computation, in terms of elementary group operations, leading from input group elements to output group elements.

- *Generic Group Model* (GGM) – [Nec94, Sho97]

  Adversaries only have access to random identifiers of group elements, and can only perform group operations by querying an oracle on the identifiers.

Algebraic Group Model (AGM)

Definition ([FKL18]).

An adversary $\mathcal{A}$ is called *algebraic* if for all group elements $X \in \mathbb{G}$ that $\mathcal{A}$ outputs, it outputs a representation $(a_1, \ldots, a_\ell) \in \mathbb{Z}^\ell$ such that $X = \prod_{i=1}^{\ell} g_i^{a_i}$, where $(g_1, \ldots, g_\ell)$ is the list of all group elements that have been given to $\mathcal{A}$ so far.

AGM ([FKL18])

- Introduced for *cyclic* groups of *known* prime order.
- In game G: $\mathcal{A}$ receives $(\mathbb{G}, g, p)$, where $\mathbb{G} = \langle g \rangle$ has prime order p, and $\mathbb{G}$, g, p are *fixed*.

AHO-AGM (This work)

- Generalized to *abelian* groups of arbitrary *unknown* order.
- In game G: $\mathcal{A}$ receives $(\mathbb{G}, (g_1, \ldots, g_n))$, where $\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa$, $(g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G}^n$, and $\mathbb{G} = \langle g_1, \ldots, g_n \rangle$ with overwhelming probability.

Strong Algebraic Group Model (SAGM)

Definition ([KLX20]).

An adversary $\mathcal{A}$ is called *strongly algebraic* if it has one or more output rounds in which, for each element $X \in \mathbb{G}$ that $\mathcal{A}$ outputs, it outputs a representation of one of the following forms:

- $(X, X_1, X_2) \in \mathbb{G}^3$ such that $X = X_1 X_2$.
- $(X, X_1) \in \mathbb{G}^2$ such that $X = X_1^{-1}$.

SAGM ([KLX20])

- Introduced for *cyclic* groups of *unknown* semiprime order.
- In game G: $\mathcal{A}$ receives N, where $N \xleftarrow{\$} \mathsf{GenMod}(1^\kappa)$.

AHO-SAGM (This work)

- Generalized to *abelian* groups of arbitrary *unknown* order.
- In game G: $\mathcal{A}$ receives $(\mathbb{G}, (g_1, \ldots, g_n))$, where $\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa$, $(g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G}^n$, and $\mathbb{G} = \langle g_1, \ldots, g_n \rangle$ with overwhelming probability.

Relations

Let $\mathbb{G} = \langle g_1, \ldots, g_n \rangle$ be a finite abelian group, and let $\mathbf{g} := (g_1, \ldots, g_n)$.

- A vector $\mathbf{e} := (e_1, \ldots, e_n) \in \mathbb{Z}^n$ for which

$$\mathbf{g}^{\mathbf{e}} := g_1^{e_1} g_2^{e_2} \cdots g_n^{e_n} = 1_{\mathbb{G}}$$

  is called a *relation* for $\mathbf{g}$.
- The relations for $\mathbf{g}$ form a lattice in $\mathbb{Z}^n$, called the *relationship lattice*.

Example

A DLog_1 adversary $\mathcal{A}$ naturally gives rise to relations as follows:

- Sample $r_i \xleftarrow{\$} \mathcal{U}_{|\langle g_i \rangle|}$, $i = 1, \ldots, n$, and set $X := g_1^{r_1} \cdots g_n^{r_n}$
- Query $(d_1, \ldots, d_n) \leftarrow \mathcal{A}(\mathbf{g}, X)$

$\rightsquigarrow$ If $\mathcal{A}$ is successful, $(r_1 - d_1, \ldots, r_n - d_n)$ is a relation for $\mathbf{g}$.

From Relations to Order

Let $\mathbb{G} = \langle g_1, \ldots, g_n \rangle$ be a finite abelian group, and let $\mathbf{g} := (g_1, \ldots, g_n)$.

- The *relationship lattice* $L(\mathbf{g})$ is the kernel of the surjective morphism

$$\mathbb{Z}^n \to \mathbb{G}, \quad \mathbf{e} \mapsto \mathbf{g}^{\mathbf{e}}.$$

- Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis for $L(\mathbf{g})$. Then $\mathbb{Z}^n / B\mathbb{Z}^n \cong \mathbb{G}$, and in particular

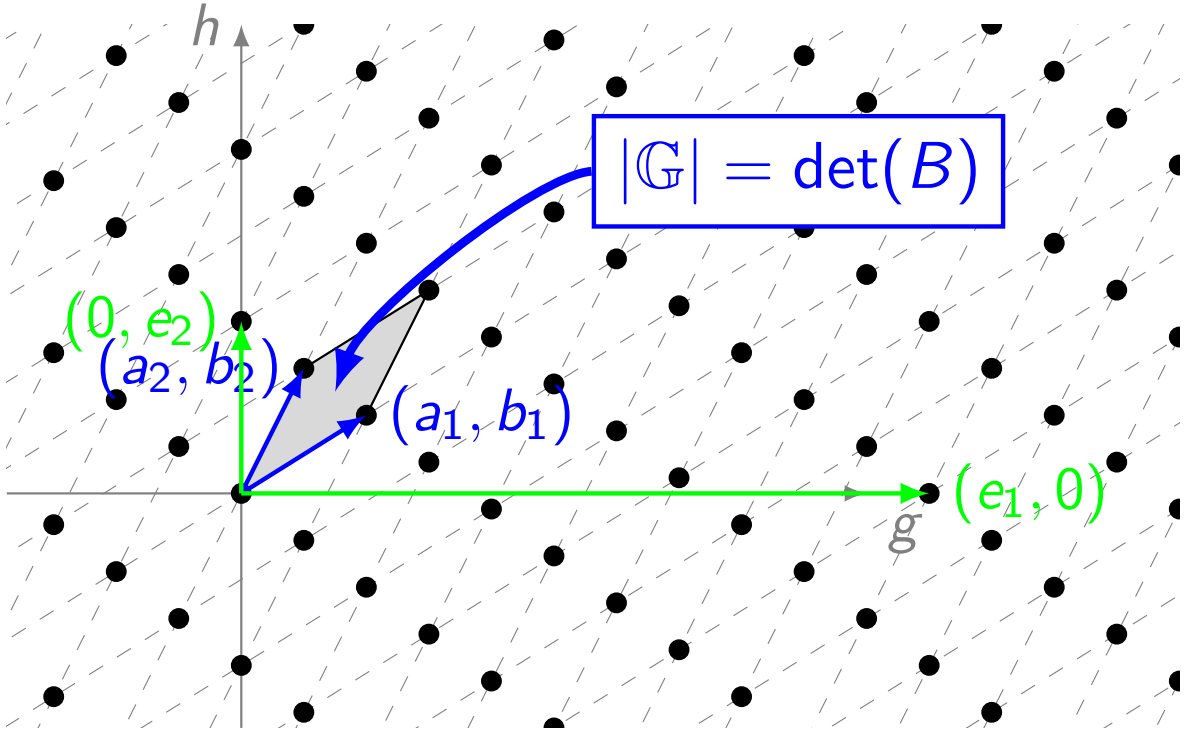
$$|\det(B)| = |\mathbb{Z}^n / B\mathbb{Z}^n| = |\mathbb{G}|.$$

Idea: Obtain relations from an adversary solving a given computational problem $\rightsquigarrow$ a basis for the lattice allows us to compute the group order.

Relationship Lattice

Let $\mathbb{G} = \langle g, h \rangle$ and $B = (a_1, b_1), (a_2, b_2)$ a basis of the relationship lattice:

$$g^a h^b = 1_{\mathbb{G}} \quad \Leftrightarrow \quad (a, b) \in (a_1, b_1)\mathbb{Z} + (a_2, b_2)\mathbb{Z}$$



$\Rightarrow$ Easy to find order of h, g, $\mathbb{G}$ if a basis is known

From Relations to Structure

Let $\mathbb{G} = \langle g_1, \ldots, g_n \rangle$ be a finite abelian group, and let $\mathbf{g} := (g_1, \ldots, g_n)$.

- Let $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis for $L(\mathbf{g})$. Then $\mathbb{Z}^n / B\mathbb{Z}^n \cong \mathbb{G}$.
- The *Smith normal form* of B completely characterizes the structure of $\mathbb{G}$. That is, it provides generators $h_1, \ldots, h_k$ of order $N_1, \ldots, N_k$, respectively, such that $N_1 \mid N_2 \mid \cdots \mid N_k$ and

$$\mathbb{G} = \langle h_1 \rangle \times \langle h_2 \rangle \times \cdots \times \langle h_k \rangle$$

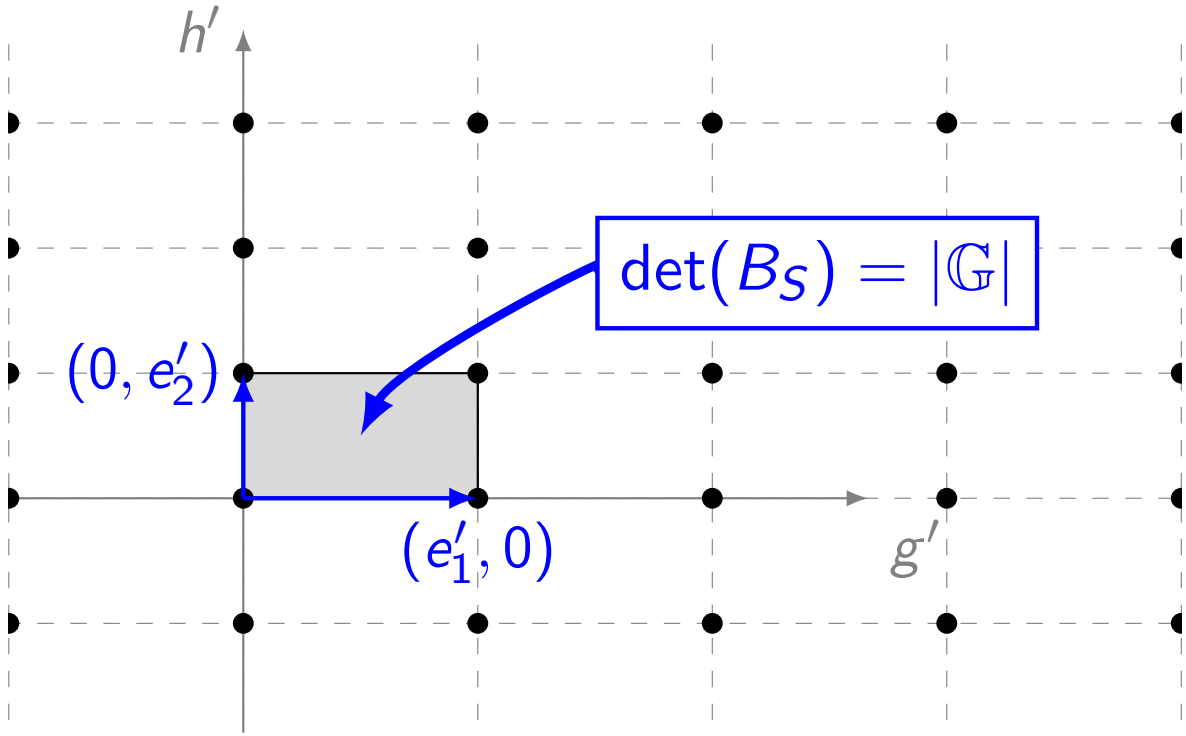
  i.e., the decomposition of $\mathbb{G}$ in terms of its *invariants*.

Relationship Lattice: Smith Normal Form

New 'orthogonal' generators g', h' of $\mathbb{G}$ with relationship lattice

$$B_S = \{(e'_1, 0), (0, e'_2)\} :$$

$$g'^a h'^b = 1_{\mathbb{G}} \quad \Leftrightarrow \quad (a, b) \in (e'_1, 0)\mathbb{Z} + (0, e'_2)\mathbb{Z}$$



Problem: No known efficient way to check if we have found a basis for the *full* lattice!

Computing a Multiple of the Order

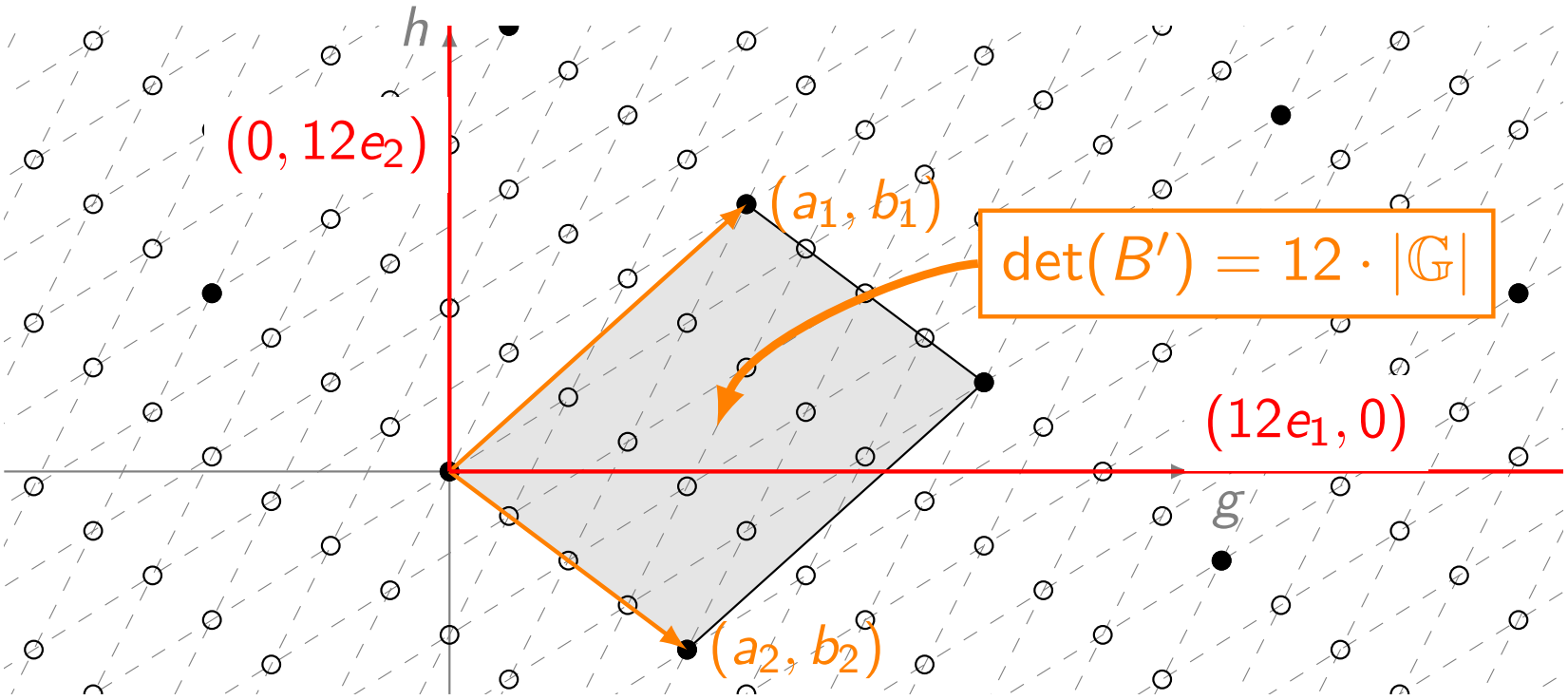
Lemma

Let $\mathbb{G}$ be a finite abelian group, let $\mathbf{g} = (g_1, \ldots, g_n)$ be a system of generators for $\mathbb{G}$, and let $B = (\mathbf{b_1}, \ldots, \mathbf{b_n})$ be a basis for the relationship lattice $L(\mathbf{g})$. Then any linearly independent (over $\mathbb{R}$) system of relations $R = (\mathbf{r}_1, \ldots, \mathbf{r}_n)$ forms a full rank sublattice $R\mathbb{Z}^n \subset L(\mathbf{g})$, and $|\det(R)|$ is an integer multiple of $|\mathbb{G}|$.

Relationship Lattice: Sublattice Basis

Let $\mathbb{G} = \langle g, h \rangle$ and $B' = \{(a_1, b_1), (a_2, b_2)\}$ a sampled sublattice basis:

$$g^a h^b = 1_{\mathbb{G}} \quad \Leftarrow \quad (a, b) \in (a_1, b_1)\mathbb{Z} + (a_2, b_2)\mathbb{Z}$$



$\Rightarrow$ Results in multiple of order of h, g, $\mathbb{G}$

Multiple Order Reduction (overview/sketch)

Goal

Prove that MO $\Rightarrow$ G for a given computational problem G.

Idea

Obtain n linearly independent relations $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathbb{Z}^n$ with respect to a system of generators $(g_1, \ldots, g_n) \in \mathbb{G}^n$ from an adversary $\mathcal{A}$ solving a computational problem G.

$\Longrightarrow$ $\det(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ is a multiple of $|\mathbb{G}|$.

Challenges

1. Extract relation from $\mathcal{A}$ successfully solving an instance of G.
2. Randomize instances of G such that:
   - 2.1. $\mathcal{A}$ succeeds with independent and identical success probability on each instance.
   - 2.2. $\mathcal{A}$ succeeds on n out of N instances with sufficiently large probability.
   - 2.3. n successfully extracted relations will be linearly independent with overwhelming probability.

Notation & Conventions

- All computational games G are defined with respect to a group family $\mathcal{G} = (\mathcal{G}_\kappa)_{\kappa=1}^{\infty}$, for which we assume:
  - A group order upper bound $U(\kappa)$ such that for all κ and all $\mathbb{G} \in \mathcal{G}_\kappa$: $|\mathbb{G}| \leq U(\kappa)$, $\log U(\kappa) \in \mathsf{poly}(\kappa)$, and $1/U(\kappa) \in \mathsf{negl}(\kappa)$.
  - A random group generator count $n(\kappa) \in \mathsf{poly}(\kappa)$ such that

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

- For $A := (\mathbf{a}_1, \ldots, \mathbf{a}_m) \in \mathbb{Z}^{m \times n}$, we denote

$$\mathbf{g}^A = (\mathbf{g}^{\mathbf{a}_1}, \mathbf{g}^{\mathbf{a}_2}, \ldots, \mathbf{g}^{\mathbf{a}_m}).$$

- Denote $[X]_{g_1,\ldots,g_\ell}$ for a representation of X w.r.t. $g_1, \ldots, g_\ell \in \mathbb{G}$. That is, $(a_1, \ldots, a_\ell) := [X]_{g_1,\ldots,g_\ell}$ satisfy $g_1^{a_1} \cdots g_\ell^{a_\ell} = X$.
- From here on we assume κ is fixed and often omitted for brevity.

1. Extracting relations from adversaries

StRoot ($\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa$, $\mathbf{g} := (g_1, \ldots, g_n) \xleftarrow{\$} \mathbb{G}^n$)

- $X \xleftarrow{\$} \mathbb{G}$, $(Y, e) \leftarrow \mathcal{A}(\mathbf{g}, X)$
- $\mathcal{A}$ wins if $e > 1$ and $Y^e = X$

Relation sampler for *algebraic* StRoot adversary $\mathcal{A}$

On input $\mathbb{G} \in \mathcal{G}_\kappa$, $\mathbf{g} \in \mathbb{G}^n$:

- Sample $\mathbf{r} \xleftarrow{\$} (\mathcal{U}_{U^3})^n$ and put $X := \mathbf{g}^{\mathbf{r}}$
- Query $([Y]_{\mathbf{g},X}, e) \leftarrow \mathcal{A}(\mathbf{g}, X)$ and put $(\mathbf{b}, c) := [Y]_{\mathbf{g},X}$
- If $Y^e = X$ and $e > 1$, return $\mathbf{r}(1 - ce) - \mathbf{b}e$
- Else, return $\perp$

Succeeds with probability $p_{\mathbb{G},\mathbf{g}} := \Pr[\mathrm{StRoot}^{\mathcal{A}}_{\mathcal{G}}(\kappa) = 1 \mid \mathbb{G}, \mathbf{g}]$ on a *single* call, but can not say much about repeated calls w.r.t. the same $\mathbb{G}$, $\mathbf{g}$!

Randomized relation sampler for *algebraic* StRoot adversary $\mathcal{A}$

On input $\mathbb{G} \in \mathcal{G}_\kappa$, $\mathbf{g} \in \mathbb{G}^n$:

- Sample $A \leftarrow (\mathcal{U}_{U^2})^{n \times n}$ and $\mathbf{r} \xleftarrow{\$} (\mathcal{U}_{U^3})^n$
- Put $\tilde{\mathbf{g}} := \mathbf{g}^A$ and $X := \mathbf{g}^{\mathbf{r}}$
- Query $([Y]_{\tilde{\mathbf{g}},X}, e) \leftarrow \mathcal{A}(\tilde{\mathbf{g}}, X)$ and put $(\mathbf{b}, c) := [Y]_{\tilde{\mathbf{g}},X}$.
- If $Y^e = X$ and $e > 1$, return $\mathbf{r}(1 - ce) - \mathbf{b}Ae$
- Else, return $\perp$

Let $p'_{\mathbb{G},\mathbf{g}}$ be the success probability of the relation sampler on $\mathbb{G}$, $\mathbf{g}$.

- If $\mathbb{G} = \langle \mathbf{g} \rangle$, then $\tilde{\mathbf{g}}$, X are almost uniformly distributed: $\delta((\tilde{\mathbf{g}}, X), \mathcal{U}_{\mathbb{G}^{n+1}}) \in \mathsf{negl}$ and $p'_{\mathbb{G},\mathbf{g}}$ is negligibly close to

$$p_{\mathbb{G}} := \Pr[\mathsf{StRoot}^{\mathcal{A}}_{\mathcal{G}}(\kappa) = 1 \mid \mathbb{G}].$$

- $\mathbb{G} \neq \langle \mathbf{g} \rangle$ with negligible probability over $\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa$, $\mathbf{g} \xleftarrow{\$} \mathbb{G}^n$.

$\Rightarrow$ If $\mathbb{G} = \langle \mathbf{g} \rangle$ each call has independent identical success probability!

2.2. Number of Calls

Let $p := \mathrm{E}_{\mathbb{G}}[p_{\mathbb{G}}]$ be the average success probability of $\mathcal{A}$ and $N := \lceil Sn/p \rceil$. What is the probability we obtain n relations with respect to $\mathbf{g} \in \mathbb{G}^n$ from N calls to $\mathcal{A}$ on randomized instances from $\mathbb{G}$?

- The number of successful calls has binomial distribution $B(N, p'_{\mathbb{G},\mathbf{g}})$.
- If $\mathbb{G} = \langle \mathbf{g} \rangle$, $B(N, p'_{\mathbb{G},\mathbf{g}})$ has negligible statistical distance to $B(N, p_{\mathbb{G}})$.
- [Lemma 2.6]: Chernoff Bound $\implies$ For $X_{\mathbb{G}} \sim B(N, p_{\mathbb{G}})$:

$$\Pr_{\mathbb{G} \xleftarrow{\$} \mathcal{G}_\kappa}[X_{\mathbb{G}} \geq n] \geq (p/2) \cdot (1 - e^{-n \cdot C_S}),$$

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

$\Rightarrow$ Out of $\lceil Sn/p \rceil$ randomized calls to $\mathcal{A}$ we can successfully extract n relations with probability $\geq (p/2) \cdot (1 - e^{-n \cdot C_S}) - \mathrm{negl}(\kappa)$.

Remains: Prove that n successfully extracted relations are linearly independent with overwhelming probability.

2.3. Distribution of Sampled Relations

Relation samples from algebraic StRoot adversary $\mathcal{A}$:

$$Y^e = X \rightsquigarrow (\tilde{\mathbf{g}}^{\mathbf{b}} X^c)^e = X$$
$$\rightsquigarrow \mathbf{g}^{\mathbf{r}(1-ce)-\mathbf{b}Ae} = 1_{\mathbb{G}}.$$

Coordinate-wise, for $j = 1, \ldots, n$:

$$g_j^{r_j(1-ce)-e\sum_{i=1}^{n} a_{ij} b_i}.$$

Let $r_j = r'_j + r''_j O_j$ with $O_j := |\langle g_j \rangle|$ and $0 \leq r'_j < O_j$:

$$g_j^{r_j(1-ce)-e\sum_{i=1}^{n} a_{ij} b_i} = g_j^{r'_j(1-ce)-e\sum_{i=1}^{n} a_{ij} b_i}.$$

So the output of $\mathcal{A}$ is independent of all r''_j.

Idea: Sampling r_j from a large enough interval, r''_j will randomly shift the relation coefficients along the relationship lattice.

2.3. Distribution of Sampled Relations

Pick a prime $|\mathbb{G}|/2 < p < |\mathbb{G}|$, coprime to $(1 - ce)$, and write:

$$d_j := r_j(1-ce) - e\sum_{i=1}^{n} a_{ij}\, b_i = r''_j \underbrace{(1-ce)O_j}_{\text{coprime to } p} + r'_j \underbrace{(1-ce)}_{*} + \underbrace{e\sum_{i=1}^{n} a_{ij}\, b_i}_{*\text{independent of } r''_j} .$$

Lemma

Sampling $(r_1, \ldots, r_n) \xleftarrow{\$} (\mathcal{U}_{U^3})^n$, the distribution of $(r''_1, \ldots r''_n)$ mod p, conditioned on any value of $(r'_1, \ldots, r'_n) \in [0, O_j)^n$, has negligible statistical distance to the uniform distribution on $\mathbb{Z}_p^n$.

$\implies$ Relation $\mathbf{d} := (d_1, \ldots, d_n)$ such that $\mathbf{d}$ mod p is distributed negligibly close to the uniform distribution on $\mathbb{Z}_p^n$.

2.3. Linear Independence of Sampled Relations

Relations $\mathbf{d}_1, \ldots, \mathbf{d}_n$ are distributed negligibly close to uniform modulo p for a prime $|\mathbb{G}|/2 < p < |\mathbb{G}|$.

$$\begin{aligned} \implies \Pr[\det(\mathbf{d}_1, \ldots, \mathbf{d}_n) \equiv 0 \bmod p] &\leq n/p + \mathsf{negl}(\kappa) \\ &< 2n/|\mathbb{G}| + \mathsf{negl}(\kappa) \\ &=: \mathsf{negl}'(\kappa) \end{aligned}$$

Moreover, $\Pr[\det(\mathbf{d}_1, \ldots, \mathbf{d}_n) = 0] \leq \Pr[\det(\mathbf{d}_1, \ldots, \mathbf{d}_n) \equiv 0 \bmod p]$.

$\implies$ Hence n successfully extracted relations are linearly independent with overwhelming probability!

Multiple Order Reduction (MO $\Rightarrow$ G)

Idea

Obtain n linearly independent relations $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathbb{Z}^n$ with respect to a system of generators $(g_1, \ldots, g_n) \in \mathbb{G}^n$ from an adversary $\mathcal{A}$ solving a computational problem G.

$\Longrightarrow$ $\det(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ is a multiple of $|\mathbb{G}|$.

Challenges

1. Extract relation from $\mathcal{A}$ successfully solving an instance of G. ✓
2. Randomize instances of G such that:
   - 2.1. $\mathcal{A}$ succeeds with independent and identical success probability on each instance. ✓
   - 2.2. $\mathcal{A}$ succeeds on n out of N instances with sufficient probability. ✓
   - 2.3. n successfully extracted relations will be linearly independent with overwhelming probability. ✓

Obtain a multiple of $|\mathbb{G}|$ with probability $\geq p_{\mathcal{A}} \cdot (1 - e^{-n \cdot C_s})/2$ (up to negligible terms) in time $\leq \lceil Sn/p \rceil \cdot T_{\mathcal{A}}$ (up to insignificant terms).

Exact Order Reduction (HO $\Rightarrow$ G)

For *cyclic* groups of *hidden order* we can obtain the *exact* order from SM adversary solving the discrete logarithm problem, i.e.: HO $\Rightarrow$ DLog.

- [Theorem 3.4.]: Given $k \geq 2$ bounded integer shifts $s_1, \ldots, s_k \in \mathbb{Z}$, where $|s_i| \leq n^d$ and $1 \leq d < n$. Then for k independent uniformly random variables $X_1, \ldots, X_k \sim \mathcal{U}_n$:

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

  where $\epsilon_k \leq 0.077$ for $k = 2$, $\epsilon_k \leq 2.9 \cdot 10^{-5}$ for $k \geq 3$ and $\zeta(k)$ is the Riemann zeta function.
- Open question if this reduction generalizes to *abelian* groups.

Note that for computational problems G such that G $\Rightarrow$ MO, we do *not* expect a reduction HO $\Rightarrow$ G to be possible:

- Adversary can solve G by always restricting to a strict sublattice of the relationship lattice.
- However, knowledge of the *full* lattice is required to solve HO.

Recap & Conclusion

Formalized the AHO-SM, AHO-AGM and AHO-SAGM for the study of *abelian* groups of *hidden-order*.

- Adapted definition of cryptographic problems to sample random group from group family and random set of generators.

Studied relations between cryptographic problems in abelian groups of hidden order in these models:

- **AHO-SM:** MO $\Rightarrow \{\mathsf{DLog}_1, \mathsf{DLog}_2\}$,
  no efficient *generic* reductions in the opposite direction.
- **AHO-AGM:** MO $\Leftrightarrow \{e\text{-RT}^{\dagger}, \mathsf{LO}^{\ddagger}, \mathsf{StRoot}, \mathsf{ARoot}\}$,
  MO $\Rightarrow \{\mathsf{CDH}_2\}$, using template for extracting random independent relations from algebraic adversaries.
- **AHO-SAGM:** MO $\Leftrightarrow \{T\text{-RSW}\}$
  Similar to AGM, but using bounded depth algebraic circuit instead of algebraic representation

---

†for $\gcd(e, |\mathbb{G}) = 1$

‡if small prime divisor of $|\mathbb{G}|$ can be guessed with non-negligible probability

Open Questions

Is it possible to reduce HO $\Rightarrow$ $\mathsf{DLog}_1/\mathsf{DLog}_2$ for abelian groups?

- Is there a way to check the obtained relations generate the full lattice?
- Or can we guarantee several independently obtained multiples have greatest common divisor equal to the exact order with high probability?

When is a reduction DLog $\Rightarrow$ CDH possible in the *hidden-order* AGM?

- Possible for *cyclic* groups of *known prime order* in the AGM [FKL18].
- Possible for *cyclic* groups $\mathbb{G}$ of *known order* $|\mathbb{G}|$ in the GGM if all multiple prime factors of $|\mathbb{G}|$ are polynomial in $\log|\mathbb{G}|$ [MW98].
- No *generic* reduction exists when $\mathbb{G}$ is cyclic and $|\mathbb{G}|$ is divisible by p^2 for a large prime p [MW98].

Thank you for your attention!

Full Version: https://eprint.iacr.org/2021/1184

Questions? Feel free to email me at: anvb@cwi.nl

References I


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


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.


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.


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


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.


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


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.


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


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.


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

References II


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


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


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.


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.


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


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


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