Chair of Applied Cryptography

ChaAC

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

FACULTY OF ENGINEERING

Subtractive Sets over Cyclotomic Rings

Limits of Schnorr-like Arguments over Lattices

ia.cr/2021/202

Martin R. Albrecht[1], **Russell W. F. Lai**[2]

[1]Royal Holloway, University of London

[2]Friedrich-Alexander-Universität Erlangen-Nürnberg

Perspective

This work

Subtractive sets $\leftrightarrow$ lattice-based Schnorr-like arguments

Perspective

This work

Subtractive sets $\leftrightarrow$ lattice-based Schnorr-like arguments

Concurrent works on Lattice-based Schnorr-like arguments

- [BCS21] Jonathan Bootle, Alessandro Chiesa, Katerina Sotiraki: Sumcheck Arguments and their Applications, CRYPTO'21
- [ACK21] Thomas Attema, Ronald Cramer, Lisa Kohl: A Compressed Sigma-Protocol Theory for Lattices, CRYPTO'21

Every other lattice talk needs this slide!

Short Integer Solution (SIS) over $\mathcal{R}$

Fix q, β. Given $(\mathbf{A}, \mathbf{y})$, find $\mathbf{x}$ such that

$$\begin{cases} \mathbf{A}\mathbf{x} = \mathbf{y} \bmod q \\ \|\mathbf{x}\| \leq \beta. \end{cases}$$

- $h, k \in \mathbb{N}$: dimensions
- $q \in \mathbb{N}$: modulus
- $\beta \in \mathbb{N}$: norm bound
- $\mathcal{R}$: ring ($+$, $-$ and $\times$ but not always $\div$, e.g. $\mathbb{Z}$)
- $\mathcal{R}_q := \mathcal{R}/q\mathcal{R}$
- $\mathbf{A} \in \mathcal{R}_q^{h \times k}$: matrix
- $\mathbf{x} \in \mathcal{R}^k$: vector
- $\mathbf{y} \in \mathcal{R}_q^h$: vector
- $\|\cdot\|$: infinity norm

Every other lattice talk needs this slide!

Short Integer Solution (SIS) over $\mathcal{R}$

Fix q, β. Given $(\mathbf{A}, \mathbf{y})$, find $\mathbf{x}$ such that

$$\begin{cases} \mathbf{A}\mathbf{x} = \mathbf{y} \bmod q \\ \|\mathbf{x}\| \leq \beta. \end{cases}$$

Motivating Problem

Proving knowledge of SIS witness $\mathbf{x}$.

- $h, k \in \mathbb{N}$: dimensions
- $q \in \mathbb{N}$: modulus
- $\beta \in \mathbb{N}$: norm bound
- $\mathcal{R}$: ring ($+$, $-$ and $\times$ but not always $\div$, e.g. $\mathbb{Z}$)
- $\mathcal{R}_q := \mathcal{R}/q\mathcal{R}$
- $\mathbf{A} \in \mathcal{R}_q^{h \times k}$: matrix
- $\mathbf{x} \in \mathcal{R}^k$: vector
- $\mathbf{y} \in \mathcal{R}_q^h$: vector
- $\|\cdot\|$: infinity norm

Proving Knowledge of SIS

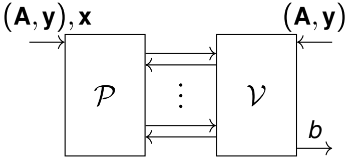
$$R_{s,\beta}((\mathbf{A},\mathbf{y}),\mathbf{x}) := (\mathbf{Ax} = s \cdot \mathbf{y} \bmod q \wedge \|\mathbf{x}\| \leq \beta)$$

where $s \in \mathcal{R}$ is called the "slack" ($s = 1 \implies$ no slack)

Proving Knowledge of SIS

$$R_{s,\beta}\left((\mathbf{A},\mathbf{y}),\mathbf{x}\right) := \left(\mathbf{A}\mathbf{x} = s \cdot \mathbf{y} \bmod q \wedge \|\mathbf{x}\| \leq \beta\right)$$

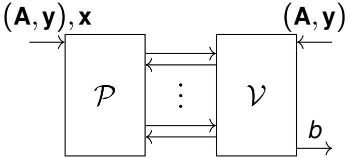
where $s \in \mathcal{R}$ is called the "slack" ($s = 1 \implies$ no slack)



Proving Knowledge of SIS

$$R_{s,\beta}\left((\mathbf{A},\mathbf{y}),\mathbf{x}\right) := \left(\mathbf{A}\mathbf{x} = s\cdot\mathbf{y} \bmod q \wedge \|\mathbf{x}\| \leq \beta\right)$$

where $s \in \mathcal{R}$ is called the “slack” ($s = 1 \implies$ no slack)

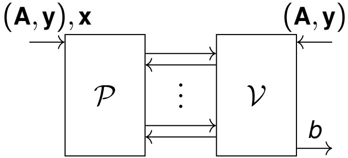


- Completeness for $R_{1,\beta}$: If $R_{1,\beta}\left((\mathbf{A},\mathbf{y}),\mathbf{x}\right) = 1$ then $\mathcal{V}$ accepts $(\mathbf{A},\mathbf{y})$, i.e. $b = 1$.

Proving Knowledge of SIS

$$R_{s,\beta}\left((\mathbf{A},\mathbf{y}),\mathbf{x}\right) := \left(\mathbf{A}\mathbf{x} = s \cdot \mathbf{y} \bmod q \wedge \|\mathbf{x}\| \leq \beta\right)$$

where $s \in \mathcal{R}$ is called the “slack” ($s = 1 \implies$ no slack)



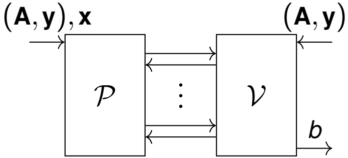
- Completeness for $R_{1,\beta}$: If $R_{1,\beta}\left((\mathbf{A},\mathbf{y}),\mathbf{x}\right) = 1$ then $\mathcal{V}$ accepts $(\mathbf{A},\mathbf{y})$, i.e. $b = 1$.
- κ-Knowledge Soundness for $R_{s,\beta'}$: There exists efficient *knowledge extactor* $\mathcal{E}$ such that

if	$\mathcal{P}$ convinces $\mathcal{V}$ to accept $(\mathbf{A},\mathbf{y})$	with probability $\rho > \kappa$,
then	$\mathcal{E}^{\mathcal{P}}$ extracts $\tilde{\mathbf{x}}$ such that $R_{s,\beta'}\left((\mathbf{A},\mathbf{y}),\tilde{\mathbf{x}}\right) = 1$	with probability $\rho - \kappa$.

Proving Knowledge of SIS

$$R_{s,\beta}\left((\mathbf{A},\mathbf{y}),\mathbf{x}\right) := \left(\mathbf{A}\mathbf{x} = s\cdot\mathbf{y} \bmod q \wedge \|\mathbf{x}\| \leq \beta\right)$$

where $s \in \mathcal{R}$ is called the "slack" ($s = 1 \implies$ no slack)



- Completeness for $R_{1,\beta}$: If $R_{1,\beta}\left((\mathbf{A},\mathbf{y}),\mathbf{x}\right) = 1$ then $\mathcal{V}$ accepts $(\mathbf{A},\mathbf{y})$, i.e. $b = 1$.
- κ-Knowledge Soundness for $R_{s,\beta'}$: There exists efficient *knowledge extactor* $\mathcal{E}$ such that

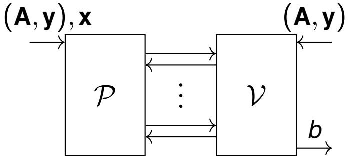
if	$\mathcal{P}$ convinces $\mathcal{V}$ to accept $(\mathbf{A},\mathbf{y})$	with probability $\rho > \kappa$,
then	$\mathcal{E}^{\mathcal{P}}$ extracts $\tilde{\mathbf{x}}$ such that $R_{s,\beta'}\left((\mathbf{A},\mathbf{y}),\tilde{\mathbf{x}}\right) = 1$	with probability $\rho - \kappa$.

- Challenge: Design $\langle\mathcal{P},\mathcal{V}\rangle$ to minimise
  - knowledge error κ
  - "slack" s

Proving Knowledge of SIS

$$R_{s,\beta}((\mathbf{A},\mathbf{y}),\mathbf{x}) := (\mathbf{A}\mathbf{x} = s \cdot \mathbf{y} \bmod q \wedge \|\mathbf{x}\| \leq \beta)$$

where $s \in \mathcal{R}$ is called the "slack" ($s = 1 \implies$ no slack)



- Completeness for $R_{1,\beta}$: If $R_{1,\beta}((\mathbf{A},\mathbf{y}),\mathbf{x}) = 1$ then $\mathcal{V}$ accepts $(\mathbf{A},\mathbf{y})$, i.e. $b = 1$.
- κ-Knowledge Soundness for $R_{s,\beta'}$: There exists efficient *knowledge extactor* $\mathcal{E}$ such that

  if $\mathcal{P}$ convinces $\mathcal{V}$ to accept $(\mathbf{A},\mathbf{y})$ with probability $\rho > \kappa$,
  then $\mathcal{E}^{\mathcal{P}}$ extracts $\tilde{\mathbf{x}}$ such that $R_{s,\beta'}((\mathbf{A},\mathbf{y}),\tilde{\mathbf{x}}) = 1$ with probability $\rho - \kappa$.
- Challenge: Design $\langle \mathcal{P}, \mathcal{V} \rangle$ to minimise
  - knowledge error κ
  - "slack" s
  - "stretch" $\frac{\beta'}{\beta}$

Landscape

Pre-2019

- PCP-based: *// Probabilistically-checkable proofs*
  - ℹ PCP (e.g. for R1CS) + commitments
  - ⊞ logarithmic-size proof, no slack ($s = 1$), no stretch $\beta' = \beta$
  - ⊟ Super-polynomial modulus q
- Stern-like:
- Schnorr-like:

Landscape

Pre-2019

- PCP-based: *// Probabilistically-checkable proofs*
  - ℹ PCP (e.g. for R1CS) + commitments
  - ⊞ logarithmic-size proof, no slack ($s = 1$), no stretch $\beta' = \beta$
  - ⊟ Super-polynomial modulus q
- Stern-like:
  - ℹ combinatorial (cut-and-choose)
  - ⊞ no slack ($s = 1$), no stretch $\beta' = \beta$
  - ⊟ linear-size proof, $\Omega(1)$ knowledge error (need $\Omega(\lambda)$ repetition)
- Schnorr-like:

Landscape

Pre-2019

- PCP-based: *// Probabilistically-checkable proofs*
  - ℹ PCP (e.g. for R1CS) + commitments
  - ⊞ logarithmic-size proof, no slack ($s = 1$), no stretch $\beta' = \beta$
  - ⊟ Super-polynomial modulus q
- Stern-like:
  - ℹ combinatorial (cut-and-choose)
  - ⊞ no slack ($s = 1$), no stretch $\beta' = \beta$
  - ⊟ linear-size proof, $\Omega(1)$ knowledge error (need $\Omega(\lambda)$ repetition)
- Schnorr-like:
  - ℹ algebraic
  - ⊞ $1/\text{poly}(\lambda)$ knowledge error ($O(\lambda/\log\lambda)$ repetition)
  - ⊞ linearity $\implies$ recursive composition (“Bulletproof folding”) $\implies$ logarithmic-size proof
  - ⊟ slack $s \neq 1$, stretch $\beta'/\beta > 1$ (amplified by recursive composition)

Landscape

Post-2019

- Stern+Schnorr:
  - ℹ Schnorr but with extra non-linear constraints
  - ⊞ $1/\text{poly}(\lambda)$ knowledge error, no slack ($s = 1$), no stretch $\beta' = \beta$
  - ⊟ non-linearity $\implies$ not "Bulletproof" compatible

Landscape

Post-2019

- Stern+Schnorr:
  - ℹ Schnorr but with extra non-linear constraints
  - ⊞ $1/\mathrm{poly}(\lambda)$ knowledge error, no slack ($s = 1$), no stretch $\beta' = \beta$
  - ⊟ non-linearity $\Longrightarrow$ not “Bulletproof” compatible

Question

Keep linearity and $1/\mathrm{poly}(\lambda)$ knowledge error of Schnorr, but reduce slack and stretch?

Schnorr-like Protocol 1

Parameters: $\mathcal{C} \subseteq \mathcal{R}$: challenge set, $\gamma \in \mathbb{N}$: norm bound, $\kappa = \frac{1}{|\mathcal{C}|}$: knowledge error

$\mathcal{P}((\mathbf{A}, \mathbf{y}), \mathbf{x})$		$\mathcal{V}(\mathbf{A}, \mathbf{y})$
$\mathbf{u} \leftarrow\$ \mathcal{R}^k$		
$\mathbf{v} := \mathbf{A}\mathbf{u}$	$\xrightarrow{\mathbf{v}}$	
	$\xleftarrow{c}$	$c \leftarrow\$ \mathcal{C}$
$\hat{\mathbf{x}} := \mathbf{u} + c \cdot \mathbf{x}$	$\xrightarrow{\hat{\mathbf{x}}}$	return $\begin{cases} \mathbf{A}\hat{\mathbf{x}} = \mathbf{v} + c \cdot \mathbf{y} \bmod q \\ \|\hat{\mathbf{x}}\| \leq \gamma \end{cases}$

Knowledge Extractor

- Recall verification equation

$$\mathbf{A}\hat{\mathbf{x}} \stackrel{?}{=} \mathbf{v} + c \cdot \mathbf{y} \bmod q$$

Knowledge Extractor

- Recall verification equation

$$\mathbf{A}\hat{\mathbf{x}} \stackrel{?}{=} \mathbf{v} + c \cdot \mathbf{y} \bmod q$$

- Run $\mathcal{P}$ twice on c_0, c_1 to get $\mathbf{v}, \hat{\mathbf{x}}_0, \hat{\mathbf{x}}_1$ such that

$$\mathbf{A}\begin{pmatrix}\hat{\mathbf{x}}_0 & \hat{\mathbf{x}}_1\end{pmatrix} = \begin{pmatrix}\mathbf{v} & \mathbf{y}\end{pmatrix}\begin{pmatrix}1 & 1 \\ c_0 & c_1\end{pmatrix} \bmod q$$

Knowledge Extractor

- Recall verification equation

$$\mathbf{A}\hat{\mathbf{x}} \stackrel{?}{=} \mathbf{v} + c \cdot \mathbf{y} \bmod q$$

- Run $\mathcal{P}$ twice on c_0, c_1 to get $\mathbf{v}, \hat{\mathbf{x}}_0, \hat{\mathbf{x}}_1$ such that

$$\mathbf{A} \begin{pmatrix} \hat{\mathbf{x}}_0 & \hat{\mathbf{x}}_1 \end{pmatrix} = \begin{pmatrix} \mathbf{v} & \mathbf{y} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ c_0 & c_1 \end{pmatrix} \bmod q$$

- **Try** to solve the following dual Vandermonde system for $\mathbf{z}$ over $\mathcal{R}$:

$$\begin{pmatrix} 1 & 1 \\ c_0 & c_1 \end{pmatrix} \mathbf{z} = s \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Knowledge Extractor

- Recall verification equation

$$\mathbf{A}\hat{\mathbf{x}} \stackrel{?}{=} \mathbf{v} + c \cdot \mathbf{y} \bmod q$$

- Run $\mathcal{P}$ twice on c_0, c_1 to get $\mathbf{v}, \hat{\mathbf{x}}_0, \hat{\mathbf{x}}_1$ such that

$$\mathbf{A}\begin{pmatrix}\hat{\mathbf{x}}_0 & \hat{\mathbf{x}}_1\end{pmatrix} = \begin{pmatrix}\mathbf{v} & \mathbf{y}\end{pmatrix}\begin{pmatrix}1 & 1 \\ c_0 & c_1\end{pmatrix} \bmod q$$

- **Try** to solve the following dual Vandermonde system for $\mathbf{z}$ over $\mathcal{R}$:

$$\begin{pmatrix}1 & 1 \\ c_0 & c_1\end{pmatrix}\mathbf{z} = s \cdot \begin{pmatrix}0 \\ 1\end{pmatrix}$$

- Output $\tilde{\mathbf{x}} := \begin{pmatrix}\hat{\mathbf{x}}_0 & \hat{\mathbf{x}}_1\end{pmatrix}\mathbf{z}$ such that

$$\mathbf{A}\tilde{\mathbf{x}} = \mathbf{A}\begin{pmatrix}\hat{\mathbf{x}}_0 & \hat{\mathbf{x}}_1\end{pmatrix}\mathbf{z} = \begin{pmatrix}\mathbf{v} & \mathbf{y}\end{pmatrix}\begin{pmatrix}1 & 1 \\ c_0 & c_1\end{pmatrix}\mathbf{z} = s \cdot \mathbf{y} \bmod q$$

Schnorr-like Protocol 2: Lattice Bulletproof [Bootle et al. @ Crypto'20]

Parameters: $\mathcal{C} \subseteq \mathcal{R}$: challenge set, $\gamma \in \mathbb{N}$: norm bound, $\kappa = \frac{2}{|\mathcal{C}|}$: knowledge error

Structural Assumptions: $\mathbf{A} = (\mathbf{A}_0 \quad \mathbf{A}_1)$, $\mathbf{x} = \begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_1 \end{pmatrix}$, $\mathbf{y} = \mathbf{A}\mathbf{x} = \mathbf{A}_0\mathbf{x}_0 + \mathbf{A}_1\mathbf{x}_1 \mod q$

$\mathcal{P}((\mathbf{A},\mathbf{y}),\mathbf{x})$		$\mathcal{V}(\mathbf{A},\mathbf{y})$
$\mathbf{y}_{01} := \mathbf{A}_0\mathbf{x}_1,\ \mathbf{y}_{10} := \mathbf{A}_1\mathbf{x}_0$	$\xrightarrow{\mathbf{y}_{01},\mathbf{y}_{10}}$	
	$\xleftarrow{c}$	$c \leftarrow\$ \mathcal{C}$
$\hat{\mathbf{x}} := \mathbf{x}_0 + c \cdot \mathbf{x}_1$	$\xrightarrow{\hat{\mathbf{x}}}$	**return** $\begin{cases} (c \cdot \mathbf{A}_0 + \mathbf{A}_1)\hat{\mathbf{x}} = \mathbf{y}_{10} + c \cdot \mathbf{y} + c^2 \cdot \mathbf{y}_{01} \mod q \\ \|\hat{\mathbf{x}}\| \leq \gamma \end{cases}$

Lattice Bulletproof Knowledge Extractor

- Recall verification equation $(c \cdot \mathbf{A}_0 + \mathbf{A}_1)\hat{\mathbf{x}} \stackrel{?}{=} \mathbf{y}_{10} + c \cdot \mathbf{y} + c^2 \cdot \mathbf{y}_{01} \bmod q$

Lattice Bulletproof Knowledge Extractor

- Recall verification equation $(c \cdot \mathbf{A}_0 + \mathbf{A}_1)\hat{\mathbf{x}} \stackrel{?}{=} \mathbf{y}_{10} + c \cdot \mathbf{y} + c^2 \cdot \mathbf{y}_{01} \mod q$
- Run $\mathcal{P}$ 3 times on c_0, c_1, c_2 to get $\mathbf{y}_{01}, \mathbf{y}_{10}, \hat{\mathbf{x}}_0, \hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2$ such that

$$\mathbf{A} \begin{pmatrix} c_0\hat{\mathbf{x}}_0 & c_1\hat{\mathbf{x}}_1 & c_2\hat{\mathbf{x}}_2 \\ \hat{\mathbf{x}}_0 & \hat{\mathbf{x}}_1 & \hat{\mathbf{x}}_2 \end{pmatrix} = \begin{pmatrix} \mathbf{y}_{10} & \mathbf{y} & \mathbf{y}_{01} \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ c_0 & c_1 & c_2 \\ c_0^2 & c_1^2 & c_2^2 \end{pmatrix} \mod q$$

Lattice Bulletproof Knowledge Extractor

- Recall verification equation $(c \cdot \mathbf{A}_0 + \mathbf{A}_1)\hat{\mathbf{x}} \stackrel{?}{=} \mathbf{y}_{10} + c \cdot \mathbf{y} + c^2 \cdot \mathbf{y}_{01} \mod q$
- Run $\mathcal{P}$ 3 times on c_0, c_1, c_2 to get $\mathbf{y}_{01}, \mathbf{y}_{10}, \hat{\mathbf{x}}_0, \hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2$ such that

$$\mathbf{A}\begin{pmatrix} c_0\hat{\mathbf{x}}_0 & c_1\hat{\mathbf{x}}_1 & c_2\hat{\mathbf{x}}_2 \\ \hat{\mathbf{x}}_0 & \hat{\mathbf{x}}_1 & \hat{\mathbf{x}}_2 \end{pmatrix} = \begin{pmatrix} \mathbf{y}_{10} & \mathbf{y} & \mathbf{y}_{01} \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ c_0 & c_1 & c_2 \\ c_0^2 & c_1^2 & c_2^2 \end{pmatrix} \mod q$$

- **Try** to solve the following dual Vandermonde system for $\mathbf{z}$ over $\mathcal{R}$:

$$\begin{pmatrix} 1 & 1 & 1 \\ c_0 & c_1 & c_2 \\ c_0^2 & c_1^2 & c_2^2 \end{pmatrix} \mathbf{z} = s \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

Lattice Bulletproof Knowledge Extractor

- Recall verification equation $(c \cdot \mathbf{A}_0 + \mathbf{A}_1)\hat{\mathbf{x}} \stackrel{?}{=} \mathbf{y}_{10} + c \cdot \mathbf{y} + c^2 \cdot \mathbf{y}_{01} \mod q$
- Run $\mathcal{P}$ 3 times on c_0, c_1, c_2 to get $\mathbf{y}_{01}, \mathbf{y}_{10}, \hat{\mathbf{x}}_0, \hat{\mathbf{x}}_1, \hat{\mathbf{x}}_2$ such that

$$\mathbf{A}\begin{pmatrix} c_0\hat{\mathbf{x}}_0 & c_1\hat{\mathbf{x}}_1 & c_2\hat{\mathbf{x}}_2 \\ \hat{\mathbf{x}}_0 & \hat{\mathbf{x}}_1 & \hat{\mathbf{x}}_2 \end{pmatrix} = \begin{pmatrix} \mathbf{y}_{10} & \mathbf{y} & \mathbf{y}_{01} \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 \\ c_0 & c_1 & c_2 \\ c_0^2 & c_1^2 & c_2^2 \end{pmatrix} \mod q$$

- **Try** to solve the following dual Vandermonde system for $\mathbf{z}$ over $\mathcal{R}$:

$$\begin{pmatrix} 1 & 1 & 1 \\ c_0 & c_1 & c_2 \\ c_0^2 & c_1^2 & c_2^2 \end{pmatrix}\mathbf{z} = s \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

- Output $\tilde{\mathbf{x}} := \begin{pmatrix} c_0\hat{\mathbf{x}}_0 & c_1\hat{\mathbf{x}}_1 & c_2\hat{\mathbf{x}}_2 \\ \hat{\mathbf{x}}_0 & \hat{\mathbf{x}}_1 & \hat{\mathbf{x}}_2 \end{pmatrix}\mathbf{z}$ such that

$$\mathbf{A}\tilde{\mathbf{x}} = \mathbf{A}\begin{pmatrix} c_0\hat{\mathbf{x}}_0 & c_1\hat{\mathbf{x}}_1 & c_2\hat{\mathbf{x}}_2 \\ \hat{\mathbf{x}}_0 & \hat{\mathbf{x}}_1 & \hat{\mathbf{x}}_2 \end{pmatrix}\mathbf{z} = \begin{pmatrix} \mathbf{y}_{10} & \mathbf{y} & \mathbf{y}_{01} \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 \\ c_0 & c_1 & c_2 \\ c_0^2 & c_1^2 & c_2^2 \end{pmatrix}\mathbf{z} = s \cdot \mathbf{y} \mod q$$

(s,t)-Subtractive Sets over $\mathcal{R}$

For what challenges $c_0, \ldots, c_{t-1}$ and slack s is the following dual Vandermonde system solvable over $\mathcal{R}$?

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ c_0 & c_1 & \ldots & c_{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_0^{t-1} & c_1^{t-1} & \ldots & c_{t-1}^{t-1} \end{pmatrix} \mathbf{z} = s \cdot \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{t-1} \end{pmatrix} \quad (\star)$$

(s, t)-Subtractive Sets over $\mathcal{R}$

For what challenges $c_0, \ldots, c_{t-1}$ and slack s is the following dual Vandermonde system solvable over $\mathcal{R}$?

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ c_0 & c_1 & \cdots & c_{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_0^{t-1} & c_1^{t-1} & \cdots & c_{t-1}^{t-1} \end{pmatrix} \mathbf{z} = s \cdot \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{t-1} \end{pmatrix} \quad (\star)$$

Observation. If $\prod_{j \in \mathbb{Z}_t \setminus \{i\}} (c_i - c_j) \mid s$ for all $i \in \mathbb{Z}_t$, then Equation $(\star)$ is solvable over $\mathcal{R}$.

(s,t)-Subtractive Sets over $\mathcal{R}$

For what challenges $c_0, \ldots, c_{t-1}$ and slack s is the following dual Vandermonde system solvable over $\mathcal{R}$?

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ c_0 & c_1 & \ldots & c_{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_0^{t-1} & c_1^{t-1} & \ldots & c_{t-1}^{t-1} \end{pmatrix} \mathbf{z} = s \cdot \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{t-1} \end{pmatrix} \qquad (\ast)$$

Observation. If $\prod_{j \in \mathbb{Z}_t \setminus \{i\}} (c_i - c_j) \mid s$ for all $i \in \mathbb{Z}_t$, then Equation $(\ast)$ is solvable over $\mathcal{R}$.

Definition. A set $\mathcal{C} \subseteq_n \mathcal{R}$ is (s,t)*-subtractive* if for any t-subset $T = \{c_0, \ldots, c_{t-1}\} \subseteq_t \mathcal{C}$ it holds that $\prod_{j \in \mathbb{Z}_t \setminus \{i\}} (c_i - c_j) \mid s$ for all $i \in \mathbb{Z}_t$. If $s = 1$ we say $\mathcal{C}$ is subtractive.

(s, t)-Subtractive Sets over $\mathcal{R}$

Definition. A set $\mathcal{C} \subseteq_n \mathcal{R}$ is (s, t)-*subtractive* if for any t-subset $T = \{c_0, \ldots, c_{t-1}\} \subseteq_t \mathcal{C}$ it holds that $\prod_{j \in \mathbb{Z}_t \setminus \{i\}} (c_i - c_j) \mid s$ for all $i \in \mathbb{Z}_t$. If $s = 1$ we say $\mathcal{C}$ is subtractive.

(s,t)-Subtractive Sets over $\mathcal{R}$

Definition. A set $\mathcal{C} \subseteq_n \mathcal{R}$ is (s,t)-*subtractive* if for any t-subset $T = \{c_0, \ldots, c_{t-1}\} \subseteq_t \mathcal{C}$ it holds that $\prod_{j \in \mathbb{Z}_t \setminus \{i\}} (c_i - c_j) \mid s$ for all $i \in \mathbb{Z}_t$. If $s = 1$ we say $\mathcal{C}$ is subtractive.

A Note about Secret Sharing over $\mathcal{R}$. If $\mathcal{C} \subseteq_n \mathcal{R}$ is (s,t)-subtractive, then for any $T = \{c_0, \ldots, c_{t-1}\} \subseteq_t \mathcal{C}$, the following Vandermonde system is solvable over $\mathcal{R}$:

$$\begin{pmatrix} 1 & c_0 & \cdots & c_0^{t-1} \\ 1 & c_1 & \cdots & c_1^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & c_{t-1}^{t-1} & \cdots & c_{t-1}^{t-1} \end{pmatrix} \mathbf{z} = s \cdot \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{t-1} \end{pmatrix}$$

$\Longrightarrow$ t-out-of-n secret sharing over $\mathcal{R}$.

(s,t)-Subtractive Sets over $\mathcal{R}$

Definition. A set $\mathcal{C} \subseteq_n \mathcal{R}$ is (s,t)*-subtractive* if for any t-subset $T = \{c_0, \ldots, c_{t-1}\} \subseteq_t \mathcal{C}$ it holds that $\prod_{j \in \mathbb{Z}_t \setminus \{i\}} (c_i - c_j) \mid s$ for all $i \in \mathbb{Z}_t$. If $s = 1$ we say $\mathcal{C}$ is subtractive.

Sample Implications.

- $(s,3)$-subtractive set of size $n \implies$ Lattice Bulletproof with slack s and knowledge error $2/n$
- (s,t)-subtractive set of size $n \implies$ Lattice-based t-out-of-n threshold primitives

(s,t)-Subtractive Sets over $\mathcal{R}$

Definition. A set $\mathcal{C} \subseteq_n \mathcal{R}$ is (s,t)-*subtractive* if for any t-subset $T = \{c_0, \ldots, c_{t-1}\} \subseteq_t \mathcal{C}$ it holds that $\prod_{j \in \mathbb{Z}_t \setminus \{i\}} (c_i - c_j) \mid s$ for all $i \in \mathbb{Z}_t$. If $s = 1$ we say $\mathcal{C}$ is subtractive.

Sample Implications.

- $(s,3)$-subtractive set of size $n \implies$ Lattice Bulletproof with slack s and knowledge error $2/n$
- (s,t)-subtractive set of size $n \implies$ Lattice-based t-out-of-n threshold primitives

Challenge. Find large (poly-size) (s,t)-subtractive sets with small slack s over interesting $\mathcal{R}$, e.g. cyclotomic rings $\mathcal{R} = \mathbb{Z}[\zeta_m]$ where ζ_m is a primitive m-th root of unity, $m = \mathrm{poly}(\lambda)$.

Our Results over $\mathcal{R} = \mathbb{Z}[\zeta_m]$

- Power-of-2 cyclotomic rings $m = 2^\ell$:
  - ⊞ Construct family of (s, t)-subtractive sets of size n for a wide range of s, t, n,
    e.g. $(2, 3)$-subtractive set of size $n = m/2 + 1$ ($\implies$ Bulletproof with slack 2)
  - ⊟ Impossibility of family of $(2, t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m + 1$

Our Results over $\mathcal{R} = \mathbb{Z}[\zeta_m]$

- Power-of-2 cyclotomic rings $m = 2^\ell$:
  - ⊞ Construct family of (s, t)-subtractive sets of size n for a wide range of s, t, n, e.g. $(2, 3)$-subtractive set of size $n = m/2 + 1$ ($\implies$ Bulletproof with slack 2)
  - ⊟ Impossibility of family of $(2, t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m + 1$
- Prime-power cyclotomic rings $m = p^\ell$:
  - ⊞ Construct family of subtractive sets of size p ($\implies$ Bulletproof with no slack)
  - ⊟ Impossibility of subtractive set $\mathcal{C}$ of size $|\mathcal{C}| > p$

Our Results over $\mathcal{R} = \mathbb{Z}[\zeta_m]$

- Power-of-2 cyclotomic rings $m = 2^\ell$:
  - ⊞ Construct family of (s, t)-subtractive sets of size n for a wide range of s, t, n,
    e.g. $(2, 3)$-subtractive set of size $n = m/2 + 1$ ($\Longrightarrow$ Bulletproof with slack 2)
  - ⊟ Impossibility of family of $(2, t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m + 1$
- Prime-power cyclotomic rings $m = p^\ell$:
  - ⊞ Construct family of subtractive sets of size p ($\Longrightarrow$ Bulletproof with no slack)
  - ⊟ Impossibility of subtractive set $\mathcal{C}$ of size $|\mathcal{C}| > p$
- Proof system for SIS over $\mathcal{R}$:
  - ⊞ Better lattice Bulletproof ($m = 2^\ell$):

[Bootle et al. @ Crypto'20]			[This work]	
slack	k^3	$\rightarrow$	slack	k
stretch	$k^{3\log m + 4.5}$		stretch	$k^{2\log m + 0.58}$

  - ⊟ Let $\mathcal{R}$ have an ideal $\mathfrak{q}$ with q cosets. For 3-move 1-challenge public-coin proofs with "algebraic" knowledge extractor, knowledge error $\kappa < q^{-1}$ is impossible unless $s \in \mathfrak{q}$.

Our Results over $\mathcal{R} = \mathbb{Z}[\zeta_m]$

- Power-of-2 cyclotomic rings $m = 2^\ell$:
  - ⊞ Construct family of (s,t)-subtractive sets of size n for a wide range of s, t, n,
    e.g. $(2,3)$-subtractive set of size $n = m/2 + 1$ ($\implies$ Bulletproof with slack 2)
  - ⊟ Impossibility of family of $(2,t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m+1$
- Prime-power cyclotomic rings $m = p^\ell$:
  - ⊞ Construct family of subtractive sets of size p ($\implies$ Bulletproof with no slack)
  - ⊟ Impossibility of subtractive set $\mathcal{C}$ of size $|\mathcal{C}| > p$
- Proof system for SIS over $\mathcal{R}$:
  - ⊞ Better lattice Bulletproof ($m = 2^\ell$):

[Bootle et al. @ Crypto'20]		→	[This work]	
slack	k^3	→	slack	k
stretch	$k^{3\log m + 4.5}$		stretch	$k^{2\log m + 0.58}$

  - ⊟ Let $\mathcal{R}$ have an ideal $\mathfrak{q}$ with q cosets. For 3-move 1-challenge public-coin proofs with "algebraic" knowledge extractor, knowledge error $\kappa < q^{-1}$ is impossible unless $s \in \mathfrak{q}$.
- Application to threshold secret sharing over $\mathcal{R}$, e.g. distributed PRF

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

- For $c \in \mathcal{R}$, ideal $\langle c \rangle := c\mathcal{R} = \{c \cdot r : r \in \mathcal{R}\} = \{\text{all } \mathcal{R} \text{ elements divisible by } c\}$.

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

- For $c \in \mathcal{R}$, ideal $\langle c \rangle := c\mathcal{R} = \{c \cdot r : r \in \mathcal{R}\} = \{$all $\mathcal{R}$ elements divisible by $c\}$.

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

- For $c \in \mathcal{R}$, ideal $\langle c \rangle := c\mathcal{R} = \{c \cdot r : r \in \mathcal{R}\} = \{$all $\mathcal{R}$ elements divisible by $c\}$.

Definition. (s,t)-subtractive set $\mathcal{C}$: For any $T \subseteq_t \mathcal{C}$, any $c \in T$, we have $s \in \left\langle \prod_{c' \in T \setminus \{c\}} (c - c') \right\rangle$.

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

- For $c \in \mathcal{R}$, ideal $\langle c \rangle := c\mathcal{R} = \{c \cdot r : r \in \mathcal{R}\} = \{\text{all } \mathcal{R} \text{ elements divisible by } c\}$.

Definition. (s,t)-subtractive set $\mathcal{C}$: For any $T \subseteq_t \mathcal{C}$, any $c \in T$, we have $s \in \langle \prod_{c' \in T \setminus \{c\}} (c - c') \rangle$.

How hard is it to construct large (s,t)-subtractive sets for small s?

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

- For $c \in \mathcal{R}$, ideal $\langle c \rangle := c\mathcal{R} = \{c \cdot r : r \in \mathcal{R}\} = \{$all $\mathcal{R}$ elements divisible by $c\}$.

Definition. (s,t)-subtractive set $\mathcal{C}$: For any $T \subseteq_t \mathcal{C}$, any $c \in T$, we have $s \in \langle \prod_{c' \in T \setminus \{c\}} (c - c') \rangle$.

How hard is it to construct large (s,t)-subtractive sets for small s?

- We want lots of elements to divide the small s.

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

- For $c \in \mathcal{R}$, ideal $\langle c \rangle := c\mathcal{R} = \{c \cdot r : r \in \mathcal{R}\} = \{\text{all } \mathcal{R} \text{ elements divisible by } c\}$.

Definition. (s,t)-subtractive set $\mathcal{C}$: For any $T \subseteq_t \mathcal{C}$, any $c \in T$, we have $s \in \langle \prod_{c' \in T \setminus \{c\}} (c - c') \rangle$.

How hard is it to construct large (s,t)-subtractive sets for small s?

- We want lots of elements to divide the small s.
- If $\mathcal{R} = \mathbb{Z}$, it is difficult:

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

- For $c \in \mathcal{R}$, ideal $\langle c \rangle := c\mathcal{R} = \{c \cdot r : r \in \mathcal{R}\} = \{\text{all } \mathcal{R} \text{ elements divisible by } c\}$.

Definition. (s,t)-subtractive set $\mathcal{C}$: For any $T \subseteq_t \mathcal{C}$, any $c \in T$, we have $s \in \langle \prod_{c' \in T \setminus \{c\}} (c - c') \rangle$.

How hard is it to construct large (s,t)-subtractive sets for small s?

- We want lots of elements to divide the small s.
- If $\mathcal{R} = \mathbb{Z}$, it is difficult:
  - $s = 1$: The only invertible elements in $\mathbb{Z}$ are $-1, 1$.

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

- For $c \in \mathcal{R}$, ideal $\langle c \rangle := c\mathcal{R} = \{c \cdot r : r \in \mathcal{R}\} = \{\text{all } \mathcal{R} \text{ elements divisible by } c\}$.

Definition. (s, t)-subtractive set $\mathcal{C}$: For any $T \subseteq_t \mathcal{C}$, any $c \in T$, we have $s \in \langle \prod_{c' \in T \setminus \{c\}} (c - c') \rangle$.

How hard is it to construct large (s, t)-subtractive sets for small s?

- We want lots of elements to divide the small s.
- If $\mathcal{R} = \mathbb{Z}$, it is difficult:
  - $s = 1$: The only invertible elements in $\mathbb{Z}$ are $-1, 1$.
  - $s = 2$: The only factors of 2 are $-2, -1, 1, 2$.

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

- For $c \in \mathcal{R}$, ideal $\langle c \rangle := c\mathcal{R} = \{c \cdot r : r \in \mathcal{R}\} = \{\text{all } \mathcal{R} \text{ elements divisible by } c\}$.

Definition. (s,t)-subtractive set $\mathcal{C}$: For any $T \subseteq_t \mathcal{C}$, any $c \in T$, we have $s \in \left\langle \prod_{c' \in T \setminus \{c\}} (c - c') \right\rangle$.

How hard is it to construct large (s,t)-subtractive sets for small s?

- We want lots of elements to divide the small s.
- If $\mathcal{R} = \mathbb{Z}$, it is difficult:
  - $s = 1$: The only invertible elements in $\mathbb{Z}$ are $-1, 1$.
  - $s = 2$: The only factors of 2 are $-2, -1, 1, 2$.
- $\mathbb{Z}[\zeta_{2^\ell}]$: $1 - \zeta_{2^\ell}^k$ divides 2 whenever $2^\ell \nmid k$.

Some Math Background and Intuition

Our results critically rely on the presence and absence of *ideals* in $\mathcal{R}$.

- For $c \in \mathcal{R}$, ideal $\langle c \rangle := c\mathcal{R} = \{c \cdot r : r \in \mathcal{R}\} = \{\text{all } \mathcal{R} \text{ elements divisible by } c\}$.

Definition. (s,t)-subtractive set $\mathcal{C}$: For any $T \subseteq_t \mathcal{C}$, any $c \in T$, we have $s \in \left\langle \prod_{c' \in T \setminus \{c\}} (c - c') \right\rangle$.

How hard is it to construct large (s,t)-subtractive sets for small s?

- We want lots of elements to divide the small s.
- If $\mathcal{R} = \mathbb{Z}$, it is difficult:
  - $s = 1$: The only invertible elements in $\mathbb{Z}$ are $-1, 1$.
  - $s = 2$: The only factors of 2 are $-2, -1, 1, 2$.
- $\mathbb{Z}[\zeta_{2^\ell}]$: $1 - \zeta_{2^\ell}^k$ divides 2 whenever $2^\ell \nmid k$.
- $\mathbb{Z}[\zeta_{p^\ell}]$: $\frac{1-\zeta_{p^\ell}^k}{1-\zeta_{p^\ell}}$ is invertible whenever $\gcd(p,k) = 1$.

Prime-Power Cyclotomic Rings $\mathbb{Z}[\zeta_{p^\ell}]$

Theorem. The set $\mathcal{C}$ is subtractive and $|\mathcal{C}| = p$.

$$\mathcal{C} = \{\mu_0, \mu_1, \ldots, \mu_{p-1}\} \qquad \mu_k = \frac{1-\zeta^k}{1-\zeta}$$

Prime-Power Cyclotomic Rings $\mathbb{Z}[\zeta_{p^\ell}]$

Theorem. The set $\mathcal{C}$ is subtractive and $|\mathcal{C}| = p$.

$$\mathcal{C} = \{\mu_0, \mu_1, \ldots, \mu_{p-1}\} \qquad \mu_k = \frac{1-\zeta^k}{1-\zeta}$$

Proof.

- $\mu_k = \frac{1-\zeta^k}{1-\zeta}$ is invertible over $\mathcal{R}$ whenever $\gcd(p,k) = 1$.

Prime-Power Cyclotomic Rings $\mathbb{Z}[\zeta_{p^\ell}]$

Theorem. The set $\mathcal{C}$ is subtractive and $|\mathcal{C}| = p$.

$$\mathcal{C} = \{\mu_0, \mu_1, \ldots, \mu_{p-1}\} \qquad \mu_k = \frac{1-\zeta^k}{1-\zeta}$$

Proof.

- $\mu_k = \frac{1-\zeta^k}{1-\zeta}$ is invertible over $\mathcal{R}$ whenever $\gcd(p,k) = 1$.
- For $i < j < p$ we have

$$\mu_j - \mu_i = \frac{1-\zeta^j}{1-\zeta} - \frac{1-\zeta^i}{1-\zeta} = \frac{\zeta^i - \zeta^j}{1-\zeta} = \zeta^i \cdot \frac{1-\zeta^{j-i}}{1-\zeta} = \zeta^i \cdot \mu_{j-i}$$

which is invertible over $\mathcal{R}$.

Prime-Power Cyclotomic Rings $\mathbb{Z}[\zeta_{p^\ell}]$

Theorem. There is no subtractive set $\mathcal{C}$ of size $|\mathcal{C}| > p$.

Prime-Power Cyclotomic Rings $\mathbb{Z}[\zeta_{p^\ell}]$

Theorem. There is no subtractive set $\mathcal{C}$ of size $|\mathcal{C}| > p$.

Proof.

- The ideal $\mathcal{I} = \langle 1 - \zeta \rangle$ has p cosets and $1 \notin \mathcal{I}$.

Prime-Power Cyclotomic Rings $\mathbb{Z}[\zeta_{p^\ell}]$

Theorem. There is no subtractive set $\mathcal{C}$ of size $|\mathcal{C}| > p$.

Proof.

- The ideal $\mathcal{I} = \langle 1 - \zeta \rangle$ has p cosets and $1 \notin \mathcal{I}$.
- Let $\mathcal{C}$ be a subtractive set of size $|\mathcal{C}| > p$.

Prime-Power Cyclotomic Rings $\mathbb{Z}[\zeta_{p^\ell}]$

Theorem. There is no subtractive set $\mathcal{C}$ of size $|\mathcal{C}| > p$.

Proof.

- The ideal $\mathcal{I} = \langle 1 - \zeta \rangle$ has p cosets and $1 \notin \mathcal{I}$.
- Let $\mathcal{C}$ be a subtractive set of size $|\mathcal{C}| > p$.
- Pigeonhole principle $\implies$ There exist $c_0, c_1 \in \mathcal{C}$ such that $c_0 - c_1 \in \mathcal{I}$.

Prime-Power Cyclotomic Rings $\mathbb{Z}[\zeta_{p^\ell}]$

Theorem. There is no subtractive set $\mathcal{C}$ of size $|\mathcal{C}| > p$.

Proof.

- The ideal $\mathcal{I} = \langle 1 - \zeta \rangle$ has p cosets and $1 \notin \mathcal{I}$.
- Let $\mathcal{C}$ be a subtractive set of size $|\mathcal{C}| > p$.
- Pigeonhole principle $\implies$ There exist $c_0, c_1 \in \mathcal{C}$ such that $c_0 - c_1 \in \mathcal{I}$.
- $\mathcal{C}$ is subtractive $\implies$ $c_0 - c_1$ is invertible $\implies$ $1 \in \mathcal{I}$, a contradiction.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. For $0 \leq i \leq \ell$, $s \in \langle 1-\zeta \rangle^{\lceil \log t \rceil 2^{i-1}}$, the set $\mathcal{C}$ is (s,t)-subtractive and $|\mathcal{C}| = 2^i + 1$.

$$\mathcal{C} = \left\{ 0, 1, \zeta, \zeta^2, \ldots, \zeta^{2^i - 1} \right\}$$

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. The set $\mathcal{C}$ is $(2,3)$-subtractive and $|\mathcal{C}| = \varphi(m) + 1 = m/2 + 1$.

$$\mathcal{C} = \left\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(m)-1}\right\}$$

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. The set $\mathcal{C}$ is $(2,3)$-subtractive and $|\mathcal{C}| = \varphi(m) + 1 = m/2 + 1$.

$$\mathcal{C} = \left\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(m)-1}\right\}$$

Proof.

1. Ignore the 0. It's for free.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. The set $\mathcal{C}$ is $(2,3)$-subtractive and $|\mathcal{C}| = \varphi(m) + 1 = m/2 + 1$.

$$\mathcal{C} = \left\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(m)-1}\right\}$$

Proof.

1. Ignore the 0. It's for free.
2. WLOG, let $T = \{\zeta^a, \zeta^b, \zeta^c\} \subseteq \mathcal{C}$ with $0 \leq a < b < c < \varphi(m)$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. The set $\mathcal{C}$ is $(2,3)$-subtractive and $|\mathcal{C}| = \varphi(m) + 1 = m/2 + 1$.

$$\mathcal{C} = \left\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(m)-1}\right\}$$

Proof.

1. Ignore the 0. It's for free.
2. WLOG, let $T = \{\zeta^a, \zeta^b, \zeta^c\} \subseteq \mathcal{C}$ with $0 \leq a < b < c < \varphi(m)$.
3. We want to show that $2 \in \langle(\zeta^a - \zeta^b)(\zeta^a - \zeta^c)\rangle := \mathcal{I}$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. The set $\mathcal{C}$ is $(2,3)$-subtractive and $|\mathcal{C}| = \varphi(m) + 1 = m/2 + 1$.

$$\mathcal{C} = \left\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(m)-1}\right\}$$

Proof.

1. Ignore the 0. It's for free.
2. WLOG, let $T = \{\zeta^a, \zeta^b, \zeta^c\} \subseteq \mathcal{C}$ with $0 \leq a < b < c < \varphi(m)$.
3. We want to show that $2 \in \langle(\zeta^a - \zeta^b)(\zeta^a - \zeta^c)\rangle := \mathcal{I}$.
4. ζ^a is invertible $\implies \mathcal{I} = \langle(1 - \zeta^{b-a})(1 - \zeta^{c-a})\rangle$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. The set $\mathcal{C}$ is $(2,3)$-subtractive and $|\mathcal{C}| = \varphi(m) + 1 = m/2 + 1$.

$$\mathcal{C} = \left\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(m)-1}\right\}$$

Proof.

1. Ignore the 0. It's for free.
2. WLOG, let $T = \{\zeta^a, \zeta^b, \zeta^c\} \subseteq \mathcal{C}$ with $0 \leq a < b < c < \varphi(m)$.
3. We want to show that $2 \in \langle (\zeta^a - \zeta^b)(\zeta^a - \zeta^c) \rangle := \mathcal{I}$.
4. ζ^a is invertible $\implies \mathcal{I} = \langle (1 - \zeta^{b-a})(1 - \zeta^{c-a}) \rangle$.
5. Routine calculation $\implies \mathcal{I} = \langle 1 - \zeta \rangle^{\mathrm{Ev}(b-a) + \mathrm{Ev}(c-a)}$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. The set $\mathcal{C}$ is $(2,3)$-subtractive and $|\mathcal{C}| = \varphi(m) + 1 = m/2 + 1$.

$$\mathcal{C} = \left\{0, 1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(m)-1}\right\}$$

Proof.

1. Ignore the 0. It's for free.
2. WLOG, let $T = \{\zeta^a, \zeta^b, \zeta^c\} \subseteq \mathcal{C}$ with $0 \leq a < b < c < \varphi(m)$.
3. We want to show that $2 \in \langle (\zeta^a - \zeta^b)(\zeta^a - \zeta^c) \rangle := \mathcal{I}$.
4. ζ^a is invertible $\implies \mathcal{I} = \langle (1 - \zeta^{b-a})(1 - \zeta^{c-a}) \rangle$.
5. Routine calculation $\implies \mathcal{I} = \langle 1 - \zeta \rangle^{\mathrm{Ev}(b-a) + \mathrm{Ev}(c-a)}$.
6. $\mathrm{Ev}(b-a) + \mathrm{Ev}(c-a) \leq \varphi(m) \implies 2 \in \langle 1 - \zeta \rangle^{\varphi(m)} \subseteq \mathcal{I}$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. There is no family of $(2, t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m + 1$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. There is no family of $(2, t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m + 1$.

Proof.

- It suffices to find m such that $|\mathcal{C}_m| \leq m + 1$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. There is no family of $(2,t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m+1$.

Proof.

- It suffices to find m such that $|\mathcal{C}_m| \leq m+1$.
- Let $m = 2^\ell \geq 4$, $m+1$ prime (Fermat prime), e.g. $m+1 = 5, 17, 257, 65537$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. There is no family of $(2,t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m+1$.

Proof.

- It suffices to find m such that $|\mathcal{C}_m| \leq m+1$.
- Let $m = 2^\ell \geq 4$, $m+1$ prime (Fermat prime), e.g. $m+1 = 5, 17, 257, 65537$.
- Any factor $\mathcal{I}$ of $\langle m+1 \rangle$ has $m+1$ cosets and $2 \notin \mathcal{I}$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. There is no family of $(2,t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m+1$.

Proof.

- It suffices to find m such that $|\mathcal{C}_m| \leq m+1$.
- Let $m = 2^\ell \geq 4$, $m+1$ prime (Fermat prime), e.g. $m+1 = 5, 17, 257, 65537$.
- Any factor $\mathcal{I}$ of $\langle m+1 \rangle$ has $m+1$ cosets and $2 \notin \mathcal{I}$.
- Let $\mathcal{C}$ be $(2,t)$-subtractive and $|\mathcal{C}| > m+1$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. There is no family of $(2,t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m+1$.

Proof.

- It suffices to find m such that $|\mathcal{C}_m| \leq m+1$.
- Let $m = 2^\ell \geq 4$, $m+1$ prime (Fermat prime), e.g. $m+1 = 5, 17, 257, 65537$.
- Any factor $\mathcal{I}$ of $\langle m+1 \rangle$ has $m+1$ cosets and $2 \notin \mathcal{I}$.
- Let $\mathcal{C}$ be $(2,t)$-subtractive and $|\mathcal{C}| > m+1$.
- Pigeonhole principle $\implies$ There exist $c_0, c_1 \in \mathcal{C}$ such that $c_0 - c_1 \in \mathcal{I}$.

Power-of-2 Cyclotomic Rings $\mathbb{Z}[\zeta_{2^\ell}]$

Theorem. There is no family of $(2,t)$-subtractive sets $\{\mathcal{C}_m\}_m$ of size $|\mathcal{C}_m| > m+1$.

Proof.

- It suffices to find m such that $|\mathcal{C}_m| \leq m+1$.
- Let $m = 2^\ell \geq 4$, $m+1$ prime (Fermat prime), e.g. $m+1 = 5, 17, 257, 65537$.
- Any factor $\mathcal{I}$ of $\langle m+1 \rangle$ has $m+1$ cosets and $2 \notin \mathcal{I}$.
- Let $\mathcal{C}$ be $(2,t)$-subtractive and $|\mathcal{C}| > m+1$.
- Pigeonhole principle $\implies$ There exist $c_0, c_1 \in \mathcal{C}$ such that $c_0 - c_1 \in \mathcal{I}$.
- $\mathcal{C}$ is $(2,t)$-subtractive $\implies$ $(c_0 - c_1) \mid 2 \implies 2 \in \mathcal{I}$, a contradiction.

Conclusion

- Formalisation of (s, t)-subtractive sets
- Applications to Schnorr-like arguments and threshold secret sharing
- Construction of poly(λ)-size (s, t)-subtractive sets with (almost) matching impossibility results
- Improved lattice Bulletproof instantiation
- Impossibility of better knowledge error assuming algebraic extractors

Paper	`ia.cr/2021/202`
Blog Post	`russell-lai.hk/2021/07/15/subtractive-sets-over-cyclotomic-rings/`

Russell W. F. Lai
Friedrich-Alexander-Universität Erlangen-Nürnberg
russell.lai@cs.fau.de
russell-lai.hk