Recovering Short Generators of Principal Ideals: Extensions and Open Problems

Chris Peikert

University of Michigan and Georgia Tech

2 September 2015
Math of Crypto @ UC Irvine
Where We Left Off

Short Generator of a Principal Ideal Problem (SG-PIP)

- Given a \( \mathbb{Z} \)-basis of a principal ideal \( \mathcal{I} = \langle g \rangle \subseteq R \) where \( g \) is “rather short,” find \( g \) (up to trivial symmetries).
Where We Left Off

Short Generator of a Principal Ideal Problem (SG-PIP)

- Given a \( \mathbb{Z} \)-basis of a principal ideal \( \mathcal{I} = \langle g \rangle \subseteq R \) where \( g \) is “rather short,” find \( g \) (up to trivial symmetries).

Theorem

In prime-power cyclotomic rings \( R \) of degree \( n \), SG-PIP is solvable in classical subexponential \( 2^{n^{2/3}} \) and quantum polynomial time.
Short Generator of a Principal Ideal Problem (SG-PIP)

- Given a \( \mathbb{Z} \)-basis of a principal ideal \( I = \langle g \rangle \subseteq R \) where \( g \) is “rather short,” find \( g \) (up to trivial symmetries).

Theorem

In prime-power cyclotomic rings \( R \) of degree \( n \), SG-PIP is solvable in classical subexponential \( 2^{n^{2/3}} \) and quantum polynomial time.

Algorithm: SG-PIP = SG-G \( \circ \) G-PIP

1. Find some generator, given a principal ideal (G-PIP)
2. Find the promised short generator, given an arbitrary generator (SG-G)
What Does This Mean for Ring-Based Crypto?

- A few works [SV'10, GGH'13, LSS'14, CGS'14] are classically weakened, and quantumly broken.

  \[\text{these works} \leq \text{SG-PI-SVP} \leq \text{SG-PIP}\]
What Does This Mean for Ring-Based Crypto?

- A few works [SV’10, GGH’13, LSS’14, CGS’14] are classically weakened, and quantumly broken.

  these works \(\leq\) SG-PI-SVP \(\leq\) SG-PIP

- Most ring-based crypto is so far unaffected, because its security is lower-bounded by harder/more general problems:

  SG-PI-SVP \(\leq\) PI-SVP \(\leq\) I-SVP \(\leq\) Ring-SIS/LWE \(\leq\) most crypto

  NTRU also lies somewhere above SG-PI-SVP.
What Does This Mean for Ring-Based Crypto?

- A few works [SV’10, GGH’13, LSS’14, CGS’14] are classically weakened, and quantumly broken.
  
  \[
  \text{these works} \leq \text{SG-PI-SVP} \leq \text{SG-PIP}
  \]

- Most ring-based crypto is so far unaffected, because its security is lower-bounded by harder/more general problems:
  
  \[
  \text{SG-PI-SVP} \leq \text{PI-SVP} \leq \text{I-SVP} \leq \text{Ring-SIS/LWE} \leq \text{most crypto}
  \]

NTRU also lies somewhere above SG-PI-SVP.

- Attack crucially relies on existence of an “unusually short” generator.
Agenda

Animating question: **How far can we push these attack techniques?**

1. Rarity of principal ideals having short generators.
2. Extend SG-PIP attack to non-cyclotomic number fields?
3. Use SG-PIP to attack NTRU? Ring-LWE?
### Rarity of Principal Ideals with Short Generators

#### Facts

1. Less than a $n^{-\Omega(n)}$ fraction of principal ideals $\mathcal{I}$ have a generator $g$ s.t. $\|g\| \leq \lambda_1(\mathcal{I}) \cdot \text{poly}(n)$.

2. A “typical” principal ideal’s shortest generator $g$ has norm $\|g\| \geq \lambda_1(\mathcal{I}) \cdot 2\sqrt{n}$.

So the SG-PIP attack usually approximates PI-SVP quite poorly.
Rarity of Principal Ideals with Short Generators

Facts

1. Less than a $n^{-\Omega(n)}$ fraction of principal ideals $\mathcal{I}$ have a generator $g$ s.t. $\|g\| \leq \lambda_1(\mathcal{I}) \cdot \text{poly}(n)$.

2. A “typical” principal ideal’s shortest generator $g$ has norm $\|g\| \geq \lambda_1(\mathcal{I}) \cdot 2\sqrt{n}$.

So the SG-PIP attack usually approximates PI-SVP quite poorly.

▶ For simplicity, normalize s.t. $N(\mathcal{I}) = 1$, so $\sqrt{n} \leq \lambda_1(\mathcal{I}) \leq n$. 
Rarity of Principal Ideals with Short Generators

Facts

1. Less than a $n^{-\Omega(n)}$ fraction of principal ideals $\mathcal{I}$ have a generator $g$ s.t.
   $$\|g\| \leq \lambda_1(\mathcal{I}) \cdot \text{poly}(n).$$

2. A “typical” principal ideal’s shortest generator $g$ has norm
   $$\|g\| \geq \lambda_1(\mathcal{I}) \cdot 2\sqrt{n}.$$ 

So the SG-PIP attack usually approximates PI-SVP quite poorly.

- For simplicity, normalize s.t. $N(\mathcal{I}) = 1$, so $\sqrt{n} \leq \lambda_1(\mathcal{I}) \leq n$.
- Let $G = \{\text{generators of } \mathcal{I}\} = g \cdot R^*$. Then $\Log(G) = \Log(g) + \Log(R^*)$ is a coset of the log-unit lattice.
Rarity of Principal Ideals with Short Generators

Facts

1. Less than a $n^{-\Omega(n)}$ fraction of principal ideals $\mathcal{I}$ have a generator $g$ s.t.
   \[ \|g\| \leq \lambda_1(\mathcal{I}) \cdot \text{poly}(n). \]

2. A “typical” principal ideal’s shortest generator $g$ has norm
   \[ \|g\| \geq \lambda_1(\mathcal{I}) \cdot 2\sqrt{n}. \]

So the SG-PIP attack usually approximates PI-SVP quite poorly.

- For simplicity, normalize s.t. $N(\mathcal{I}) = 1$, so $\sqrt{n} \leq \lambda_1(\mathcal{I}) \leq n$.
- Let $G = \{\text{generators of } \mathcal{I}\} = g \cdot R^*$. Then $\text{Log}(G) = \text{Log}(g) + \text{Log}(R^*)$ is a coset of the log-unit lattice.
- To have $\|g\| \leq \text{poly}(n)$, we need every
  \[ \log|\sigma_i(g)| \leq O(\log n) \implies \|\text{Log}(g)\|_1 \leq r = O(n \log n). \]
Rarity of Principal Ideals with Short Generators

Facts

1. Less than a $n^{-\Omega(n)}$ fraction of principal ideals $\mathcal{I}$ have a generator $g$ s.t.
   \[ \|g\| \leq \lambda_1(\mathcal{I}) \cdot \text{poly}(n). \]

2. A “typical” principal ideal’s shortest generator $g$ has norm
   \[ \|g\| \geq \lambda_1(\mathcal{I}) \cdot 2\sqrt{n}. \]

So the SG-PIP attack usually approximates PI-SVP quite poorly.

> For simplicity, normalize s.t. $N(\mathcal{I}) = 1$, so $\sqrt{n} \leq \lambda_1(\mathcal{I}) \leq n$.

> Let $G = \{\text{generators of } \mathcal{I}\} = g \cdot R^*$. Then $\log(G) = \log(g) + \log(R^*)$ is a coset of the log-unit lattice.

> To have $\|g\| \leq \text{poly}(n)$, we need every
   \[ \log|\sigma_i(g)| \leq O(\log n) \implies \|\log(g)\|_1 \leq r = O(n \log n). \]

> Volume of such $g$ is $\frac{2^n}{n!} \cdot r^n = O(\log n)^n$.

Volume of log-unit lattice (regulator) is $\Theta(\sqrt{n})^n$. 
SG-PIP Beyond Cyclotomies

- To recover the short generator from any generator of $\mathcal{I} \subseteq R$, it suffices to have a “good” basis of (a dense enough sublattice of) $\Log R^*$. 

- Can we get such a basis for other number rings?

- In general, can preprocess $R$ in $2^{\text{rank}(\Log R^*)}$ time. Then can quickly solve many instances of SG-PIP in $R$.

- In particular cases, we can do much better. E.g., multiquadratic $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_k})$ for appropriate $d_i$. Facts:

  - unit rank $= 2^k - 1 =$ number of quadratic subfields $\mathbb{Q}(\sqrt{d_I})$, $I \subseteq [k] \setminus \emptyset$.
  - fund units of the $\mathbb{Q}(\sqrt{d_I})$ generate a finite-index subgroup of $O_K^*$. (See, e.g., Keith Conrad’s ‘blurb’ on Dirichlet’s unit theorem for proofs.)
  - How “good” are these units? How small is their finite index?

- Other number rings? E.g., $\mathbb{Z}[x]/(x^p - x - 1)$ has many easy units: $x$, $\Phi_d(x)$ for $d | (p - 1)$, . . . 

- 6 / 7
SG-PIP Beyond Cyclotomics

To recover the short generator from any generator of $\mathcal{I} \subseteq R$, it suffices to have a “good” basis of (a dense enough sublattice of) $\text{Log } R^*$. (For cyclotomics: standard basis of the cyclotomic units.)

Can we get such a basis for other number rings?

In general, can preprocess $R$ in $2^{\text{rank}(\text{Log } R^*)}$ time. Then can quickly solve many instances of SG-PIP in $R$. In particular cases, we can do much better. E.g., multiquadratic $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_k})$ for appropriate $d_i$. Facts:

- Unit rank $= 2^k - 1 = \text{number of quadratic subfields } \mathbb{Q}(\sqrt{d_i})$, $I \subseteq \mathbb{Q}[k] \setminus \emptyset$.
- Fund units of the $\mathbb{Q}(\sqrt{d_i})$ generate a finite-index subgroup of $O_K^*$. (See, e.g., Keith Conrad’s ‘blurb’ on Dirichlet’s unit theorem for proofs.)
- How “good” are these units? How small is their finite index?

Other number rings? E.g., $\mathbb{Z}[x]/(x^p - x - 1)$ has many easy units: $x, \Phi_d(x)$ for $d | (p - 1), \ldots$
SG-PIP Beyond Cyclotomics

To recover the short generator from any generator of $I \subseteq \mathbb{R}$, it suffices to have a “good” basis of (a dense enough sublattice of) $\text{Log} \, R^*$. (For cyclotomics: standard basis of the cyclotomic units.)

Can we get such a basis for other number rings?

In general, can preprocess $R$ in $2$-rank $(\text{Log} \, R^*)$ time. Then can quickly solve many instances of SG-PIP in $R$.

In particular cases, we can do much better. E.g., multiquadratic $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_k})$ for appropriate $d_i$. Facts:

- unit rank $= 2^k - 1 = \text{number of quadratic subfields } \mathbb{Q}(\sqrt{d_I})$, $I \subseteq \mathbb{Z}^k, \emptyset$.
- fund units of the $\mathbb{Q}(\sqrt{d_I})$ generate a finite-index subgroup of $O^*_K$.

(See, e.g., Keith Conrad's 'blurb' on Dirichlet's unit theorem for proofs.)

How “good” are these units? How small is their finite index?

Other number rings? E.g., $\mathbb{Z}[(x)/(x^p - x - 1)]$ has many easy units: $x, \Phi_d(x)$ for $d | (p - 1)$, . . .
SG-PIP Beyond Cyclotomics

To recover the short generator from any generator of $\mathcal{I} \subseteq R$, it suffices to have a “good” basis of (a dense enough sublattice of) $\text{Log } R^*$. (For cyclotomics: standard basis of the cyclotomic units.)

Can we get such a basis for other number rings?

In general, can preprocess $R$ in $2^{\text{rank}(\text{Log } R^*)}$ time. Then can quickly solve many instances of SG-PIP in $R$. 

In particular cases, we can do much better. E.g., multiquadratic $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_k})$ for appropriate $d_i$. Facts:

\begin{itemize}
  \item unit rank $= 2^k - 1 = \text{number of quadratic subfields } \mathbb{Q}(\sqrt{d_I}), I \subseteq [k] \setminus \emptyset$.
  \item fund units of the $\mathbb{Q}(\sqrt{d_I})$ generate a finite-index subgroup of $\mathcal{O}^*_K$.
  \item See, e.g., Keith Conrad’s ‘blurb’ on Dirichlet’s unit theorem for proofs.
\end{itemize}

How “good” are these units? How small is their finite index?

Other number rings? E.g., $\mathbb{Z}[x]/(x^p - x - 1)$ has many easy units: $x, \Phi_d(x)$ for $d | (p - 1)$, . . .
SG-PIP Beyond Cyclotomics

- To recover the short generator from any generator of $\mathcal{I} \subseteq R$, it suffices to have a "good" basis of (a dense enough sublattice of) $\log R^*$. (For cyclotomics: standard basis of the cyclotomic units.)

- **Can we get such a basis for other number rings?**

- In general, can preprocess $R$ in $2^{\text{rank}(\log R^*)}$ time. Then can quickly solve many instances of SG-PIP in $R$.

- In particular cases, we can do much better.

  E.g., multiquadratic $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_k})$ for appropriate $d_i$. Facts:
SG-PIP Beyond Cyclotomics

- To recover the short generator from any generator of \( \mathcal{I} \subseteq R \), it suffices to have a “good” basis of (a dense enough sublattice of) \( \text{Log } R^* \).
  (For cyclotomics: standard basis of the cyclotomic units.)

- Can we get such a basis for other number rings?

- In general, can preprocess \( R \) in \( 2^{\text{rank}(\text{Log } R^*)} \) time.
  Then can quickly solve many instances of SG-PIP in \( R \).

- In particular cases, we can do much better.
  E.g., multiquadratic \( K = \mathbb{Q}(\sqrt{d_1},\ldots,\sqrt{d_k}) \) for appropriate \( d_i \). Facts:
    - unit rank = \( 2^k - 1 \) = number of quadratic subfields \( \mathbb{Q}(\sqrt{d_I}), \ I \subseteq [k] \setminus \emptyset \).
SG-PIP Beyond Cyclotomics

▶ To recover the short generator from any generator of $\mathcal{I} \subseteq R$, it suffices to have a “good” basis of (a dense enough sublattice of) $\text{Log} \ R^*$. (For cyclotomics: standard basis of the cyclotomic units.)

▶ Can we get such a basis for other number rings?

▶ In general, can preprocess $R$ in $2^{\text{rank}(\text{Log} \ R^*)}$ time. Then can quickly solve many instances of SG-PIP in $R$.

▶ In particular cases, we can do much better.

E.g., multiquadratic $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_k})$ for appropriate $d_i$. Facts:
- unit rank $= 2^k - 1 =$ number of quadratic subfields $\mathbb{Q}(\sqrt{d_I})$, $I \subseteq [k] \setminus \emptyset$.
- fund units of the $\mathbb{Q}(\sqrt{d_I})$ generate a finite-index subgroup of $O_K^*$. (See, e.g., Keith Conrad’s ‘blurb’ on Dirichlet’s unit theorem for proofs.)
SG-PIP Beyond Cyclotomics

▶ To recover the short generator from any generator of \( \mathcal{I} \subseteq R \), it suffices to have a “good” basis of (a dense enough sublattice of) \( \text{Log} \ R^* \).
(For cyclotomics: standard basis of the cyclotomic units.)

▶ Can we get such a basis for other number rings?

▶ In general, can preprocess \( R \) in \( 2^{\text{rank}(\text{Log} \ R^*)} \) time.
Then can quickly solve many instances of SG-PIP in \( R \).

▶ In particular cases, we can do much better.
E.g., multiquadratic \( K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_k}) \) for appropriate \( d_i \). Facts:
  * unit rank \( = 2^k - 1 = \) number of quadratic subfields \( \mathbb{Q}(\sqrt{d_I}), I \subseteq [k] \setminus \emptyset \).
  * fund units of the \( \mathbb{Q}(\sqrt{d_I}) \) generate a finite-index subgroup of \( \mathcal{O}_K^* \).
(See, e.g., Keith Conrad’s ‘blurb’ on Dirichlet’s unit theorem for proofs.)
  * How “good” are these units? How small is their finite index?
SG-PIP Beyond Cyclotomics

- To recover the short generator from any generator of \( \mathcal{I} \subseteq R \), it suffices to have a “good” basis of (a dense enough sublattice of) \( \Log R^* \).
  (For cyclotomics: standard basis of the cyclotomic units.)

- Can we get such a basis for other number rings?

- In general, can preprocess \( R \) in \( 2^{\text{rank}(\Log R^*)} \) time. Then can quickly solve many instances of SG-PIP in \( R \).

- In particular cases, we can do much better.
  E.g., multiquadratic \( K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_k}) \) for appropriate \( d_i \). Facts:
  - unit rank \( = 2^k - 1 = \) number of quadratic subfields \( \mathbb{Q}(\sqrt{d_I}), I \subseteq [k] \setminus \emptyset \).
  - fund units of the \( \mathbb{Q}(\sqrt{d_I}) \) generate a finite-index subgroup of \( \mathcal{O}_K^* \).
    (See, e.g., Keith Conrad’s ‘blurb’ on Dirichlet’s unit theorem for proofs.)
  - How “good” are these units? How small is their finite index?

- Other number rings? E.g., \( \mathbb{Z}[x]/(x^p - x - 1) \) has many easy units: \( x, \Phi_d(x) \) for \( d | (p - 1) \), \ldots
WARNING: No theorems beyond this point!