A Compact Signature Scheme Based on Ideal Lattices

Keita Xagawa/Keisuke Tanaka (Tokyo Tech)
Results

- Gentry, Peikert, Vaikuntanathan (2008)
  - Signature Scheme
  - Based on Lattices
  - Large vk

- Ours
  - Signature Scheme
  - ... on Ideal Lattices
  - Small vk
A Compact Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech)

Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai’s algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours
Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai’s algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours
Signature scheme

A Compact Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech)

AAAC 2008
Signature scheme

A Compact Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech)

AAAC 2008
A threat to digital signatures

- RSA Signature
- ElGamal Signature
- ...

Quantum

Efficiently Forgeable
Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai’s algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours
Lattices

\[ L = \{ \sum_i \alpha_i b_i : \alpha_i \in \mathbb{Z} \} \]
Shortest Vector Problem (SVP\(\gamma\))

Input: \(L\)
Output: \(v\)
Importance of lattice problems

Quantum

(Seems) hard

SVPγ

L

b₁

b₂

v

L

o
Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai’s algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours
The GPV signature scheme [GPV08]

- Gentry
- Peikert
- vaikuntanathan

- Sig. scheme based on lattice
GPV sig. →

- CRHFs with trapdoors
GPV sig.←

- CRHFs with trapdoors

15
GPV sig. – Overview

1. \( H(m) \)
2. \( \sigma \leftarrow h^{-1}(H(m)) \)

1. \( h(\sigma) = H(m) ? \)

A Compact Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech)
GPV sig. – Security

\[ \exists \text{s.t.} \]

\[ \exists m^*, \sigma^* \]

\[ \sigma^* \]

\[ \text{accept} \]

\[ \exists \]

Solving any instance of SVP\(\gamma\)
GPV Sig. →

- CRHFs with trapdoors
Lattice-based CRHFs $[A_96, \ldots]$
Lattice-based CRHFs \([A_96, \ldots]\)

\[ h_{vk} : \{ e \in \mathbb{Z}^m : ||e|| \leq t \} \rightarrow \mathbb{Z}_q^n \]

\[ h_{vk}(e) = n \text{ mat. } A \quad e = u \]
Trapdoor \([\text{A}99, \text{GPV}08]\)

- Compose **A** and **S**

\[
\text{m} = \text{mat. } \mathbf{A} \text{ sk } \text{mat. } \mathbf{S} = \text{mat. } \mathbf{o}
\]
Problem in GPV sig.

\[ m = O(n \log n) \]

\[ |A| = \tilde{O}(n^2) \]

\[ m = O(n \log n) \]

\[ |S| = \tilde{O}(n^2) \]
Our goal

\[ m = O(n \log n) \]

\[ |A| = \tilde{O}(n) \]

\[ |S| = \tilde{O}(n) \]

Small

A Compact Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech)
Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai’s algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours
Main Idea

Gentry, Peikert, Vaikuntanathan (2008)

- Hash functions
  - Lattice-based
- Trapdoor
  - Ajtai’s algorithm

Ours

- Hash functions
  - Ideal-lattice-based
- Trapdoor
  - Our algorithm
A Compact Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech)

Ideal-lattice-based CRHFs \([\text{LMo6}]\)

\[ h_{vk}(e) = \text{mat. } A \]

\[ e \xrightarrow{\text{mat. } A} u \]

Lyubashevsky
Micciancio
Ideal-lattice-based CRHFs \cite{LM06} 

\[ m' = O(\log n) \]

\[ \text{mat. } A \]
Ideal-lattice-based CRHFs [LMo6]
Ideal-lattice-based CRHFs \([\text{LMO06}]\)
Trapdoors

Ajtai

Ours

A Comapct Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech) AAAC 2008
Our algorithm

- Compose $A$ and $S$

$\text{mat. } A \times \text{sk} \rightarrow \text{mat. } S \rightarrow \text{mat. } o$
Our algorithm

A Compact Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech)
Our algorithm

\[ a_1, a_2, \ldots, a_n \quad a_1, -a_n, \ldots, -a_2, \ldots, a_1 \]

\[ m', \quad \ldots \quad m' \]

\[ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \]
Our algorithm

vk
mat. $A'$

m'

... ...

sk
mat. $S'$

m'

... ...

... ...

m'

... ...

m'
Our algorithm

\begin{align*}
vk & \text{ mat. } A' \\
\text{mat. } A' & \text{ mat. } S' \\
m' & \text{ sk} \\
\end{align*}
Our algorithm

\[ \text{vk mat. } A' \]

\[ \text{sk mat. } S' \]

\[ m' \]

\[ \ldots \]

\[ \ldots \]

\[ \ldots \]

A Compact Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech)

AAAC 2008
Our algorithm

\[ \begin{align*}
\text{vk} & \quad \text{mat. } A' \\
\text{sk} & \quad \text{mat. } S' \\
\text{mat. } A' & \quad m' \\
\text{mat. } S' & \quad m' \\
m' & \quad m'
\end{align*} \]
Our algorithm

A Compact Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech)

\[ \text{vk} \] mat. \( A' \)

\[ \text{sk} \] mat. \( S' \)

\[ m' \]

\[ m' \]

\[ \ldots \]

\[ \ldots \]

\[ \ldots \]

\[ \ldots \]
Results

\[ |A'| = \tilde{O}(n) \]

\[ |S'| = \tilde{O}(n) \]
Agenda

- Signature schemes
- Lattice problems
- The GPV signature scheme
  - Lattice-based hash functions
  - Ajtai’s algorithm
- Our scheme
  - Ideal-lattice-based hash functions
  - Our algorithm
- Comparison GPV and ours
## Comparison

<table>
<thead>
<tr>
<th>Gentry, Peikert, Vaikuntanathan (2008)</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Signature Scheme</td>
<td>□ Signature Scheme</td>
</tr>
<tr>
<td>□ Based on <strong>Lattices</strong></td>
<td>□ ... on <strong>Ideal Lattices</strong></td>
</tr>
<tr>
<td>□ Large vk and sk. (\tilde{O}(n^2))</td>
<td>□ Small vk and sk. (\tilde{O}(n))</td>
</tr>
<tr>
<td>(n=256, \</td>
<td>vk</td>
</tr>
</tbody>
</table>

A Compact Signature Scheme Based on Ideal Lattices
Keita Xagawa/Keisuke Tanaka (Tokyo Tech)

AAAC 2008
References

- [GPV08]: Gentry, Peikert, and Vaikuntanathan (STOC ‘08)
  Trapdoors for Hard Lattices and New Cryptographic Constructions
- [A96]: Ajtai (STOC ‘96)
  Generating Hard Instances of Lattice Problems
- [A99]: Ajtai (ICALP ‘99)
  Generating Hard Instances of the Short Basis Problem
- [LMo6]: Lyubashevsky and Micciancio (ICALP ‘06)
  Generalized Compact Knapsacks are Collision Resistant