Efficient Lattice-Based Cryptography
Chris Peikert (SRI International) and Jonathan Katz (U Maryland)

Cryptographic schemes based on lattices are simple, parallelizable, and potentially secure against quantum attacks. However, known primitives are too inefficient for practical use, and lack desirable functionality and security properties.

We use hard lattice problems as a foundation for cryptographic schemes. A primary focus is on expanding the set of tools to include important notions such as digital signatures.

For efficiency, we rely on lattices having extra algebraic structure. The resulting schemes can be highly parallelized on today’s microprocessors.

Reducing a noise vector modulo a “long” lattice basis is a one-way operation.

<table>
<thead>
<tr>
<th>Approach and Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New approach</strong></td>
</tr>
<tr>
<td>• Design variety of crypto schemes using lattices</td>
</tr>
<tr>
<td>• Investigate special classes of lattices for efficiency</td>
</tr>
</tbody>
</table>

Technical Description

We construct provably secure cryptographic schemes under worst-case assumptions on standard lattice problems (such as the Shortest Vector Problem). Prior constructions were limited mainly to collision-resistant hashing and (semantically secure) public-key encryption. We show that many other important cryptographic primitives can be realized via simple and “direct” constructions based on lattices.

New Constructions

• Chosen ciphertext-secure encryption
• Direct “hash-and-sign” signature schemes
• Efficient, two-round, composable oblivious transfer (OT)
• Identity-based encryption (IBE)