Post-Quantum Cryptography

Jeffrey Young

Outline

• Overview of Quantum Computing
• Current Algorithms
• Barriers to Adoption
Definition

• Cryptographic algorithms *thought* to be secure against attacks by a quantum computer

• Pre-quantum algorithms rely on:
  • Integer factorization
  • Discrete Log
  • Elliptic curve discrete log

Quantum Computing

• 2,000 qubits* using quantum annealing
• No evidence that this method is faster than traditional computers [2]

• 50 qubits (IBM)
  • Quantum supremacy
Current Algorithms

- Some crypto systems known to be resistant to both classical and quantum computers
  - Hash-based
  - Code-based
  - Lattice-based
  - Multivariate-quadratic-equations
  - Secret-key (ex. AES)

Shor’s Algorithm

- Relies on the superposition of states enabled by quantum computers
  - Quantum Fourier Transform
- $O((\log N)^2 (\log \log N) (\log \log \log N))$ runtime
- Largest number factored is 21 (10 qubits)
- Would require 4,000-10,000 qubits to run on 2048 bit RSA [1]
Grover’s Algorithm

- Finds with high probability the unique input to a black box function that produces a particular output value with $O(\sqrt{N})$ evaluations
- Classical computer would take $O(N)$ evaluations
- Provides quadratic speedup, not exponential like other quantum algorithms
- Conventional advice – double key size for any symmetric key scheme in quantum setting

McEliece’s Hidden-Goppa-code Encryption

- Invented in 1978 and thought to be secure against classical and quantum attacks
- $2^{(0.5+o(1))n/\lg n}$ operations needed to break codes of length $n$
- Why aren’t we using this instead of RSA?
  - Key size
  - For real world security need keys ~1 million bits in length
Code Based Public Key Encryption

- Let $b$ be a power of 2
- $n = 4b \log b; d = \lfloor \log n \rfloor; t = \lfloor 0.5n/d \rfloor$
- Public key is $dt \times n$ matrix $K$ with coefficients in GF(2)
- Can encrypt $n$-bit strings with exactly $t$ bits set to 1 ("weight-$t$")
- $c \leftarrow Km$, a $dt$ bit ciphertext
Syndrome Decoding

• Separating $m$ from $K$ is known as syndrome decoding

• This is proven to be NP-hard

Decryption

• $K$ is generated with a secret structure (hidden Goppa code)
• $\alpha_1, \alpha_2, \alpha_3 \ldots$ are distinct elements of $GF(2^d)$, $g$ is a degree-$t$ irreducible polynomial in $GF(2^d)$

\[ H = \begin{pmatrix} \frac{1}{g(\alpha_1)} & \cdots & \frac{1}{g(\alpha_n)} \\ \frac{\alpha_1}{g(\alpha_1)} & \cdots & \frac{\alpha_n}{g(\alpha_n)} \\ \vdots & \ddots & \vdots \\ \frac{\alpha_1^{t-1}}{g(\alpha_1)} & \cdots & \frac{\alpha_n^{t-1}}{g(\alpha_n)} \end{pmatrix} \]

• Generate invertible $dt \times dt$ matrix $S$
• Generate $n \times n$ permutation matrix $P$
• $K = SHP$
Decryption

- Given ciphertext $Km = SHPm$
  1. Multiply by $S^{-1}$ to obtain $HPm$
  2. Syndrome decode $H$ to obtain $Pm$
  3. Multiply by $P^{-1}$ to obtain $m$

- Limitation: Requires long key size (~1 MB) [3]

Barriers to Adoption

- Improve efficiency
- Build confidence
- Improve Usability
Efficiency

- Classical elliptic curve systems with $b$ bit signatures and $b$ bit keys appear to provide $b$ bits of security

- No current quantum cryptosystem has $b$ bit signatures and $b$ bit keys combined with polynomial time signing and polynomial time verification

- Some (probably NSA) don’t care

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Type</th>
<th>Public Key</th>
<th>Private Key</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTRU Encrypt</td>
<td>Lattice</td>
<td>6130 B</td>
<td>6743 B</td>
<td></td>
</tr>
<tr>
<td>Streamlined NTRU</td>
<td>Lattice</td>
<td>1232 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prime</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rainbow</td>
<td>Multivariate</td>
<td>124 KB</td>
<td>95 KB</td>
<td></td>
</tr>
<tr>
<td>SPHINCS</td>
<td>Hash Signature</td>
<td>1 KB</td>
<td>1 KB</td>
<td>41 KB</td>
</tr>
<tr>
<td>BLISS-II</td>
<td>Lattice</td>
<td>7 KB</td>
<td>2 KB</td>
<td>5 KB</td>
</tr>
<tr>
<td>GLP-Variant Glyph</td>
<td>Ring-LWE</td>
<td>2 KB</td>
<td>0.4 KB</td>
<td>1.8 KB</td>
</tr>
<tr>
<td>Rainbow</td>
<td>Code-based</td>
<td>1 MB</td>
<td>11.5 KB</td>
<td></td>
</tr>
<tr>
<td>New Hope</td>
<td>Code-based</td>
<td>1 MB</td>
<td>11.5 KB</td>
<td></td>
</tr>
<tr>
<td>Goppa-based McEliece</td>
<td>Code-based</td>
<td>1 MB</td>
<td>11.5 KB</td>
<td></td>
</tr>
<tr>
<td>Random Linear Code</td>
<td>RLCE</td>
<td>115 KB</td>
<td>3 KB</td>
<td></td>
</tr>
<tr>
<td>based encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIDH</td>
<td>Isogeny</td>
<td>751 B</td>
<td>48 B</td>
<td></td>
</tr>
<tr>
<td>SIDH (compressed</td>
<td>Isogeny</td>
<td>564 B</td>
<td>48 B</td>
<td></td>
</tr>
<tr>
<td>keys)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3072-bit Discrete</td>
<td>not PQC</td>
<td>384 B</td>
<td>32 B</td>
<td></td>
</tr>
<tr>
<td>Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>256-bit Elliptic</td>
<td>not PQC</td>
<td>32 B</td>
<td>32 B</td>
<td></td>
</tr>
<tr>
<td>Curve</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Confidence

• Part of RSA’s widespread adoption comes from it’s longevity

• Cryptanalysts need time to search for attacks on the systems

• The must, in turn, become familiar with post quantum cryptography algorithms and analysis techniques

• “Nobody has figured out an attack so we conjecture that no attack exists.”

Usability

• Requires clear definitions and standardization

• Software, and perhaps hardware, implementations
  • Intel has dedicated instructions for AES on modern CPUs

• Implementations must avoid timing and other side-channel leaks
Comparison to Quantum Cryptography

- PCQ covers a wide range of secure communication topics, CQ handles only a single task
- QC is proven secure from generally accepted laws of quantum mechanics
- PCQ includes systems both proven and conjectured to be true
- PCQ can be done on today’s hardware

Conclusion

- While quantum computing may be years from fruition, we need to start thinking about these problems today
- Secure algorithms thought to exist, but need more vetting
- Serious practical barriers
References

