Analyzing Lattice-Based Threshold Signature Schemes for Securing Message Authentication in Preparation for Y2Q

Cruz, Tiffany (School: Mililani High School)

This investigation evaluates lattice-based threshold signature schemes against HMAC (hash-based message authentication code) to secure message authentication in preparation for Y2Q, which is the day when quantum computing will be able to break standard encryption protocols. Post-quantum encryption is critical for general usage since standard encryption methods are susceptible to quantum attacks. Lattice-based TSS potentially offers a good alternative due to the difficulty of lattice math problems, which increases the entropy in the key, thereby making it more resistant to quantum attacks. The experiment begins by creating a message to be encrypted by HMAC and lattice-based TSS. Once this is done, the system load and entropy are recorded. The results show that HMAC was faster and used less memory compared to lattice, while lattice had 4097.585 bits of entropy in comparison to HMAC's 256 bits. Given the low compilation times and memory usage (response times under one second with a maximum memory usage of 160 KB), lattice is more efficient and quantum-resistant than HMAC, providing significantly enhanced security for message authentication, despite being computationally heavier. This can be used in the future to protect MACs against Y2Q day since message authentication code plays a highly important role in our internet society, allowing ourselves and others to be authenticated and secure. Without secure and protected message authentication code, we have no security across the internet.

Awards Won: