**T5–**

NIST has initiated a standardization process for new KEMs and DSs . this work presents an agile hardware implementation supporting both LMS and XMSS stateful hash-based Signatures . the design offers flexibility in configuring hashcores and accelerators, showing increased hardware utilization efficiency . the implementation targets devices with long lifetimes and limited maintenance capabilities - aligning with NIST recommendations for post-quantum cryptography . a swiss company is developing a swis

**Bart-**

Agile Acceleration of Stateful Hash-based Signatures in Hardware. With the development of large-scale quantum computers, the landscape of asymmetric cryptographic algorithms is changing. NIST has initiated a standardization process for new Key Encapsulation Mechanisms (KEMs) and Digital Signatures (DSs) This work presents an agile hardware implementation supporting both LMS and XMSS statefulHash-Based Signatures, evaluated on the Xilinx Artix-7 FPGA platform. The design offers flexibility in configuring hashcores and accelerators, showing increased hardware utilization efficiency. The implementation targets devices with long lifetimes and limited maintenance capabilities, aligning with NIST recommendations for post-quantum cryptography. It is based on the NIST KEM and Ds standard, developed by the National Institute of Standards and Technology (NIST) in Washington, D.C. and developed by a team of researchers at the University of Illinois at Urbana-Champaign, with funding from the National Security Agency (NSA) and the Department of Homeland Security (DHS). It is currently being trialled on a small number of small-scale, low-power, quantum-computing-capable devices. It will be rolled out in the next few years and will be used to develop a range of quantum computing-related applications. It has been described as a “quantum quantum computer’s operating system.” It is the first of its kind in the world.

**Gemini -To address the threat of quantum computing to asymmetric cryptography, NIST is standardizing new post-quantum algorithms. This work focuses on implementing two stateful hash-based signature schemes, LMS and XMSS, in hardware. The implementation provides flexibility in configuring hash functions and acceleration units, optimizing hardware utilization. It targets devices with extended lifespans and limited maintenance capabilities, as recommended by NIST for post-quantum cryptographic implementations.**

**GPT\_4**

The research paper discusses the development of a hardware implementation designed to support stateful hash-based signatures, specifically focusing on the LMS and XMSS algorithms, in response to the potential threats posed by quantum computing to asymmetric cryptographic algorithms. The National Institute of Standards and Technology (NIST) has initiated a standardization process to establish new Key Encapsulation Mechanisms (KEMs) and Digital Signatures (DSs) that are secure against quantum attacks. The implementation presented in this work is performed on the Xilinx Artix-7 FPGA platform, which is known for its robustness and suitability for cryptographic applications.

The design of the hardware implementation is notably agile, allowing for flexible configuration of hashcores and accelerators. This flexibility leads to improved efficiency in hardware utilization, which is crucial for devices that are expected to have long lifetimes and limited opportunities for maintenance. Such characteristics are essential as they align with the NIST recommendations for post-quantum cryptography, which emphasize the need for cryptographic solutions that can remain secure against evolving quantum technologies.

This work is significant as it addresses the urgent need for cryptographic systems that can withstand the security challenges posed by the advent of quantum computing. By focusing on stateful hash-based signatures and implementing these in a flexible, efficient hardware environment, the research contributes to the foundational technology necessary for securing digital communications in the post-quantum era. The use of the Xilinx Artix-7 FPGA platform underscores the practical applicability of the research, suggesting that these advanced cryptographic mechanisms can be deployed effectively in real-world scenarios where security and efficiency are paramount.

**Gpt-3** The emergence of large-scale quantum computers is reshaping the field of asymmetric cryptographic algorithms, prompting NIST to spearhead the standardization of new Key Encapsulation Mechanisms (KEMs) and Digital Signatures (DSs). This study introduces a versatile hardware implementation that backs both LMS and XMSS stateful Hash-Based Signatures, assessed on the Xilinx Artix-7 FPGA platform. Noteworthy for its adaptability in configuring hashcores and accelerators, the design showcases heightened hardware utilization efficiency. Tailored for devices with enduring lifespans and minimal maintenance requirements, the implementation aligns with NIST's guidelines for post-quantum cryptography.