PRODUCT BRIEF

CETHERA CTHR-01 beta

Quantum-Inspired PCIe Security Accelerator

Executive Overview

The CTHR-01 beta represents a revolutionary advancement in enterprise cryptographic hardware, designed to address the growing demands of an increasingly complex cybersecurity landscape. As organizations worldwide grapple with escalating cyber threats and the looming quantum computing revolution, traditional cryptographic solutions have proven inadequate for protecting sensitive data in modern enterprise environments, and even ordinary desktop PCs. The CTHR-01 beta PCIe security accelerator emerges as a groundbreaking solution that combines quantum-inspired cryptography with high-performance hardware acceleration, delivering unprecedented security capabilities directly within enterprise data center infrastructure. Built on the robust AMD Xilinx UltraScale+ XCU50 FPGA platform, this innovative security accelerator transforms how organizations approach data protection by eliminating the fundamental vulnerabilities inherent in conventional cryptographic systems. Unlike traditional hardware security modules that rely on static encryption algorithms and predictable key schedules, the CTHR-01 beta introduces a paradigm shift toward dynamic, evolving cryptographic protection that adapts in real-time to emerging threats.

The Critical Problems CTHR-01 Beta Solves

1. Limitations of traditional cryptographic systems. Modern enterprises face mounting challenges with conventional encryption approaches that have remained largely unchanged for decades. Classical cryptographic systems suffer from fundamental security limitations, including fixed algorithms that make them relatively easy for adversaries to break and inadequate key management processes that create significant vulnerabilities. The absence of forward secrecy in many traditional ciphers means that if an adversary obtains encryption keys at any point, they can decrypt all past and future messages encrypted with those keys. Traditional encryption solutions also struggle with scalability issues, proving inadequate for encrypting large amounts of data efficiently while maintaining security standards. The computational overhead of software-based encryption creates performance bottlenecks that can slow down enterprise operations, forcing organizations to choose between security and operational efficiency. Furthermore, legacy cryptographic systems lack the adaptability to respond to changing security requirements and emerging threat vectors.

2. Enterprise cryptographic requirements and compliance challenges. Enterprise organizations face increasingly complex regulatory requirements that demand robust encryption capabilities across multiple compliance frameworks. Organizations must ensure compliance with Advanced Encryption Standard requirements of 128-bits or higher for protecting sensitive information. Data centers require encryption systems that can operate transparently without breaking basic operations such as snapshotting or cloning data volumes. The challenge of enterprise key management has become one of the most difficult problems in practical cryptography, as organizations struggle to keep cryptographic keys protected yet always available for use. Improper key management can lead to key leakage, where attackers obtain keys and recover sensitive messages from encrypted data. Traditional key management approaches create dependencies on manual processes and individual key custodians, introducing human error vulnerabilities and resource-intensive maintenance requirements.

3. Hardware security vulnerabilities and performance limitations. Existing hardware security solutions, including traditional HSMs and TPMs, face significant limitations in addressing modern enterprise needs. These systems typically provide limited throughput capabilities that cannot keep pace with the demands of high-performance computing environments and real-time data processing

requirements. Hardware vulnerabilities such as Rowhammer attacks, Meltdown exploits, and various side-channel attacks continue to expose sensitive cryptographic operations to sophisticated adversaries. The PCIe accelerator market has recognized these limitations, driving growth toward solutions that can provide both enhanced security and improved performance. Traditional cryptographic hardware often lacks the flexibility to adapt to new algorithms or changing security requirements without complete hardware replacement. This creates significant operational and financial challenges for enterprises seeking to maintain current security standards while preparing for future threats.

Product Overview and Core Purpose

1. Revolutionary quantum-inspired architecture. The CTHR-01 beta fundamentally reimagines cryptographic protection through its proprietary Quantum Entanglement-Based Cryptographic Protocol (QE-BCP), which delivers security capabilities that were previously considered theoretical. This innovative approach leverages quantum mechanical principles to create continuously evolving cryptographic states that eliminate the predictability and vulnerabilities associated with traditional encryption methods. The system generates non-repeating entropy patterns that adapt to environmental conditions and threat landscapes, ensuring that each cryptographic operation produces unique, unrepeatable security characteristics. Unlike conventional cryptographic systems that rely on mathematical complexity for security, the CTHR-01 beta harnesses the physics of quantum mechanics to provide security guarantees that are fundamentally different from classical approaches. The quantum-inspired design creates cryptographic keys that never repeat and continuously evolve, eliminating the static key vulnerabilities that plague traditional systems. This approach addresses the critical challenge of preparing for post-quantum cryptographic requirements while providing immediate security benefits in current threat environments.

2. Zero plaintext exposure and homomorphic capabilities. A core innovation of the CTHR-01 beta is its ability to ensure zero plaintext exposure throughout the entire cryptographic process, eliminating the risk of data leakage even under sophisticated attack scenarios. The system maintains encrypted data boundaries at the hardware level, ensuring that sensitive information never exists in readable form outside the secure cryptographic environment. This capability addresses one of the most significant vulnerabilities in traditional systems, where plaintext data might be temporarily exposed during processing operations. The integration of homomorphic encryption capabilities enables computation directly on encrypted data without requiring decryption, representing a significant advancement over traditional cryptographic solutions. This functionality allows organizations to perform complex analytics, machine learning operations, and database queries on encrypted datasets while maintaining complete data confidentiality. Such capabilities are particularly valuable for cloud computing environments and collaborative data processing scenarios where data privacy must be maintained throughout the computational process.

3. Hardware-accelerated performance and efficiency. The CTHR-01 beta addresses the performance limitations of software-based encryption by providing dedicated hardware acceleration that offloads cryptographic operations from host CPUs. This approach eliminates the computational bottlenecks typically associated with encryption processes, allowing organizations to implement comprehensive data protection without sacrificing operational performance. The hardware acceleration capabilities enable real-time cryptographic operations that can keep pace with high-throughput enterprise applications and data center workloads. The PCIe interface provides seamless integration with existing server architectures, offering scalable connectivity and high bandwidth for faster data transfers between server components. The accelerator's design leverages the power and versatility of PCIe technology to deliver enterprise-grade performance while maintaining compatibility with diverse server platforms and operating systems. This integration approach ensures that organizations can deploy advanced cryptographic capabilities without requiring fundamental changes to their existing infrastructure.

Target Customers and Use Cases

1. Personal computer users. PC users can leverage the CTHR-01 beta to transform their desktop and workstation systems into highly secure computing platforms capable of protecting sensitive personal and professional data. The accelerator integrates seamlessly into standard desktop PCs through the PCIe interface, providing consumer-grade systems with enterprise-level cryptographic capabilities previously unavailable to individual users. Personal computer applications benefit from the hardware's ability to encrypt local storage, secure communications, and protect sensitive documents without impacting system performance. The quantum-inspired security features provide PC users with long-term protection against evolving cyber threats, including future quantum computing attacks that could compromise traditional encryption methods. Home office workers and remote professionals can utilize the accelerator to create secure work environments that meet enterprise security standards while operating from personal computing systems. Gaming enthusiasts and content creators can protect intellectual property and personal data while maintaining the high-performance computing capabilities required for demanding applications.

2. Enterprise server environments. Enterprise servers represent the primary deployment environment for the CTHR-01 beta, where the accelerator transforms standard server hardware into quantum-ready cryptographic platforms. The PCIe form factor enables easy integration into existing server chassis across multiple rack units without requiring specialized hardware modifications. Enterprise servers equipped with the CTHR-01 beta can handle massive cryptographic workloads while maintaining optimal performance for core business applications. Database servers benefit significantly from the accelerator's transparent encryption capabilities, which protect sensitive data at rest and in transit without impacting database performance or functionality. Web servers and application servers can implement advanced encryption features that secure user communications and protect sensitive business data processing. Email servers and collaboration platforms can leverage the homomorphic encryption capabilities to perform secure communications and data analysis while maintaining complete privacy protection. File servers and network-attached storage systems can provide enterprise-wide data protection through hardware-accelerated encryption that operates transparently to end users. Backup and archive servers can implement long-term data protection strategies that remain secure against future cryptographic threats. Virtual server environments can deploy the accelerator across multiple virtual machines, providing consistent security policies and centralized cryptographic key management.

Installation and Deployment Process

1. PC installation and setup. Installing the CTHR-01 beta in personal computer systems follows standard PCIe card installation procedures while incorporating specific requirements for advanced cryptographic hardware. The installation process begins with system shutdown and power disconnection to ensure safe handling of sensitive electronic components. Users must verify that their PC's power supply can accommodate the accelerator's power requirements and that adequate cooling is available within the computer case. The physical installation involves identifying an appropriate PCIe slot on the motherboard, ensuring proper alignment and secure seating of the accelerator card. Cable connections for power delivery must be completed according to the installation documentation. Post-installation verification includes confirming proper hardware recognition and basic functionality testing. Software configuration for PC users includes driver installation and initial setup of cryptographic policies according to personal security requirements. The accelerator includes user-friendly configuration tools that enable non-technical users to establish encryption settings and security preferences. Integration with existing PC applications occurs through standardized interfaces that maintain compatibility with popular software packages.

2. Enterprise server integration. Enterprise server deployment involves comprehensive planning and coordination to ensure optimal integration with existing data center infrastructure. IT administrators must assess server configurations, rack space requirements, and cooling capabilities to accommodate the accelerator's specifications. Network infrastructure evaluation ensures proper integration with existing server networking and storage systems. The installation process for enterprise servers follows established data center procedures for hardware installation and configuration. Multiple accelerators can

be deployed across server farms with centralized management and monitoring capabilities. Integration with existing server management systems provides comprehensive visibility into accelerator performance and security status. Enterprise deployment includes integration with existing security policies, compliance frameworks, and audit systems. The accelerator's management interface provides centralized control over cryptographic operations across multiple servers and deployment locations. Comprehensive monitoring and alerting systems enable proactive management of cryptographic operations and security events.

Customer Experience and Operational Usage

1. PC user experience. PC users experience the CTHR-01 beta as a transparent enhancement to their computing environment that provides advanced security capabilities without impacting daily operations. The accelerator operates seamlessly in the background, automatically encrypting files, securing communications, and protecting sensitive data according to user preferences. Desktop applications continue to function normally while benefiting from hardware-accelerated encryption that operates faster than traditional software-based solutions. Users interact with the accelerator through intuitive management software that provides easy access to security settings, encryption preferences, and performance monitoring. The system automatically handles key management, security updates, and maintenance tasks without requiring user intervention. Performance monitoring tools enable users to track the accelerator's impact on system performance and adjust settings according to their specific requirements.

2. Enterprise server operations. Enterprise server environments benefit from the CTHR-01 beta's autonomous operation capabilities that require minimal ongoing intervention once properly configured. System administrators manage the accelerator through comprehensive management interfaces that provide visibility into cryptographic operations, performance metrics, and security status across multiple servers. The system generates detailed audit logs for compliance reporting and security analysis. Integration with existing enterprise monitoring systems enables inclusion in current infrastructure management workflows and alerting mechanisms. Performance optimization features allow administrators to adjust operational parameters based on changing workload requirements. Regular maintenance tasks are minimized through automated health monitoring and self-managing capabilities.

Market Positioning and Strategic Advantages

1. Technology leadership and innovation. The CTHR-01 beta establishes a new category of PCIe security accelerators that combine quantum-inspired cryptography with high-performance hardware acceleration. The accelerator's technological advancement over traditional cryptographic hardware creates significant competitive advantages in both performance and security capabilities. The integration of multiple advanced features in a single PCIe form factor represents a unique market position that addresses diverse enterprise requirements.

2. Scalability and future-proofing. The accelerator's modular architecture enables deployment across diverse computing environments from individual PCs to large-scale data centers. The quantum-inspired security features provide long-term protection against emerging threats, including future quantum computing attacks. The system's adaptability and upgrade capabilities ensure continued relevance as cryptographic requirements evolve and new threats emerge. The CTHR-01 beta represents a strategic investment in next-generation security technology that prepares organizations for future challenges while providing immediate operational benefits. The combination of advanced security features, high performance, and seamless integration creates compelling value propositions for both individual users and enterprise organizations seeking to enhance their cryptographic capabilities.