

# Xelera Secra

## INTRODUCTION

Password auditing and pentesting are crucial techniques to strengthen the security of enterprise IT systems. These techniques require the computation of very large numbers of password hashes, taking days or weeks to complete. **Xelera Secra** – a high-performance hash computation software – leverages the compute capacity of COTS datacenter-grade FPGA accelerators to perform hash computations at unprecedented rates.

## PERFORMANCE

**Secra** uses modern, commercial-off-the-shelf (COTS) FPGAs to provide up to 75% better performance-per-Watt than GPU-based systems. The system saves electrical power compared to CPU- and GPU-based appliances.

## DEPLOYMENT

COTS servers with FPGA accelerators or cloud instances (SAAS mode) are turned into hash computation clusters. These are operated via a web-based dashboard or through an API for 20+ programming languages.

## SCALABILITY

Hash computation jobs are distributed automatically and transparently over dozens to hundreds of server nodes and accelerator cards. The compute performance scales linearly, allowing users to operate clusters at any scale.

## COVERAGE

**Secra** provides highly optimized implementations of dozens of hash formats, such as NetNTLMv1, NetNTLMv2, Unix Crypt MD5, SHA256, or MYSQL hashes. It supports password lists and brute-force modes.

# SOLUTION BRIEF

XELERA

# ANALYTICS

- Distributed, scalable hash computation
- Up to 75% better performance per Watt than GPU-based
- Built for COTS server and FPGA hardware, or cloud instances
- Web-based dashboard or scriptable via rich API
- Dozens of hash functions and authentication methods

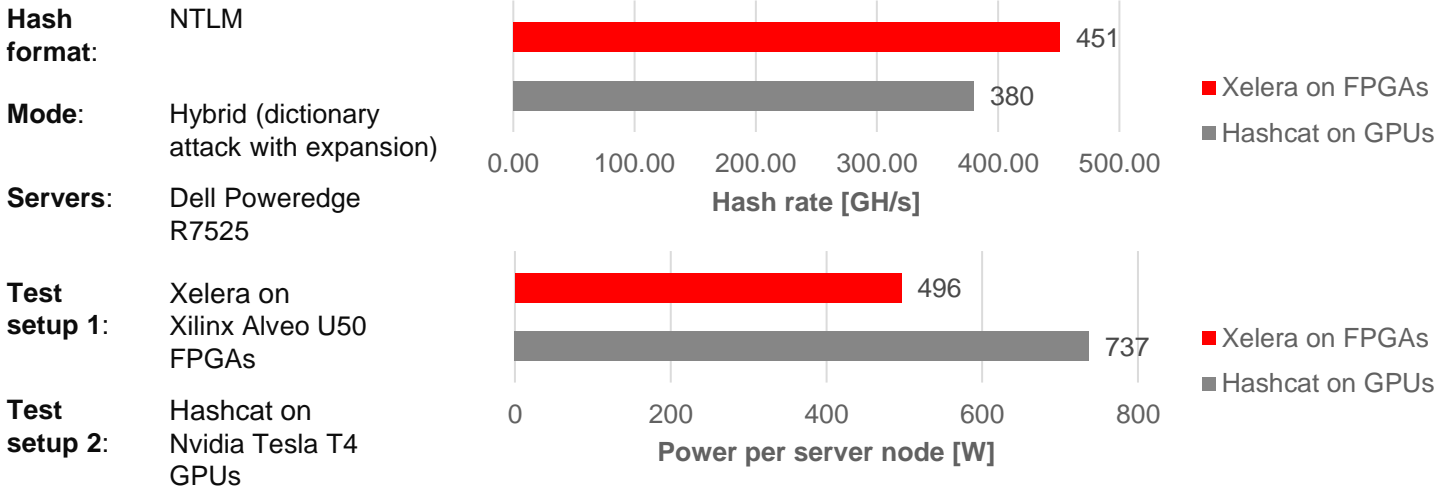
#	Server	CPU Temp.	FPGA Temp.	Inlet Temp.	Exhaust Temp.	Current	Server Pwr.	FPGA Pwr.	Throughput
	node-0	37°C,37°C		26°C	32°C	1.40 A,0.20 A	312 W		
0			52°C,41°C					20.10 W	-
1									
2									
3									
4									
5									
	node-1	36°C,35°C							
6									
7									

## High-Performance Hash Computation Software

# Xelera Secra

## BENCHMARK

**Xelera Secra** runs on commercial-off-the-shelf hardware. It releases the potential of the most recent datacenter-grade FPGA accelerators, such as Xilinx Alveo, to perform hash computations at an unprecedented speed. The software offloads all computationally demanding tasks of the processing chain to energy-efficient FPGA accelerators. This provides better performance per power consumption ratios than GPU-based systems.



## SUPPORTED FORMATS

**Secra** supports standard cryptographic hash algorithms, ciphers, as well as authentication methods of operating systems, network protocols and database systems. Brute-force and password list modes are supported. The software provides full hardware acceleration for all formats. The hash computations are offloaded to highly parallel processing pipelines on commercial-off-the-shelf datacenter-grade FPGA accelerators alongside the functions for text generation and the search for matches in a hash list.

NTLM	MD4	DES-crypt
NetNTLM v1	MD5	HMAC-SHA1
NetNTLM v2	Unix Crypt MD5	HMAC-SHA2-224
SHA1	Apache Crypt MD5	HMAC-SHA2-256
SHA2-224	MySQL-4.0	HMAC-SHA2-512
SHA2-256	MySQL-4.1	Bitcoin Core
SHA2-384	SHA2-256 Crypt	Blockchain
SHA2-512	SHA2-512 Crypt	Blockchain v0
...	...	...

## PASSWORD AUDITING APPLICATIONS

Password auditing scans IT systems in order to assess the strength of password. High-performance password hash computations are a central part of password auditing systems. **Xelera Secra** integrates into auditing workflows through the dashboard or the API for 20+ programming languages.

## PENTESTING APPLICATIONS

Pentesting simulates an attack in order to harden the security of IT systems. A cryptographic analysis with high-performance password hash computations is a frequently used technique in pentesting applications. The software integrates seamlessly into pentesting workflows through the dashboard or the API.

## TAKE THE NEXT STEP

Further information and licensing: [sales@xelera.io](mailto:sales@xelera.io)

© Xelera Technologies GmbH, 04 May 2021