XELERA

High-Performance Hash Computation Software

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 2.5x higher hash rates than state-of-the-art GPU-based systems. The system also saves electrical power compared to CPU- and GPU-based appliances.

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.

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.

COVERAGE

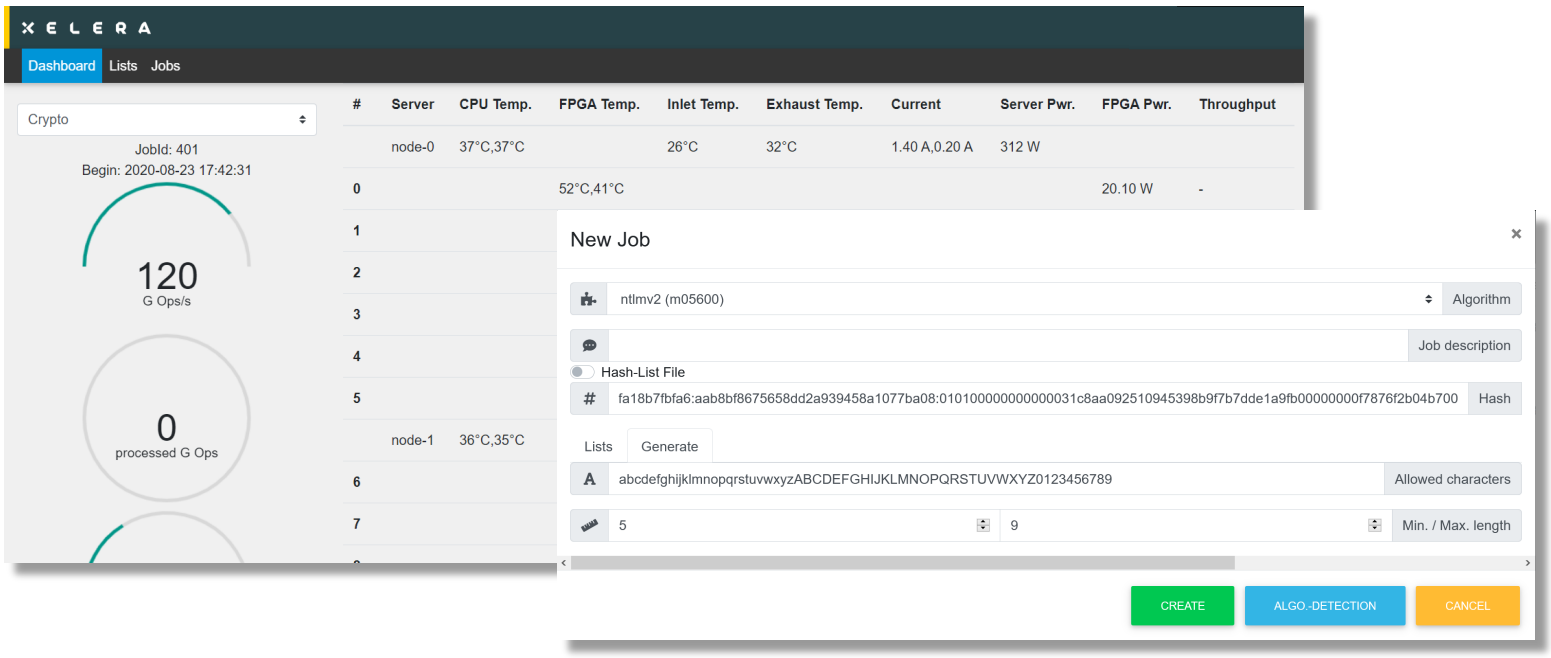
Secra provides highly optimized implementations of dozens of hash formats, such as NetNTLMv1, NetNTLMv2, Unix Crypt MD5, SHA256, or MYSQL hashes. It supports password lists and brute-force modes.

SOLUTION BRIEF

XELERA

ANALYTICS

- Distributed, scalable hash computation
- Up to 2.5x faster than GPU systems
- 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



XELERA TECHNOLOGIES GMBH
RHEINSTR. 40–42
64283 DARMSTADT
GERMANY

FON: +49 6151 162 24 25
CELL: +49 175 268 17 56
MAIL: SALES@XELERA.IO
WEB: WWW.XELERA.IO

MANAGING DIRECTOR:
FELIX WINTERSTEIN
REGISTERGERICHT (LEGAL DOMICILE):
DARMSTADT HRB 97805

IBAN:
DE 17 5085 0150 0000 7709 90
BIC: HELADEF1DAS
UST-ID-NR.: DE318360521

XELERA

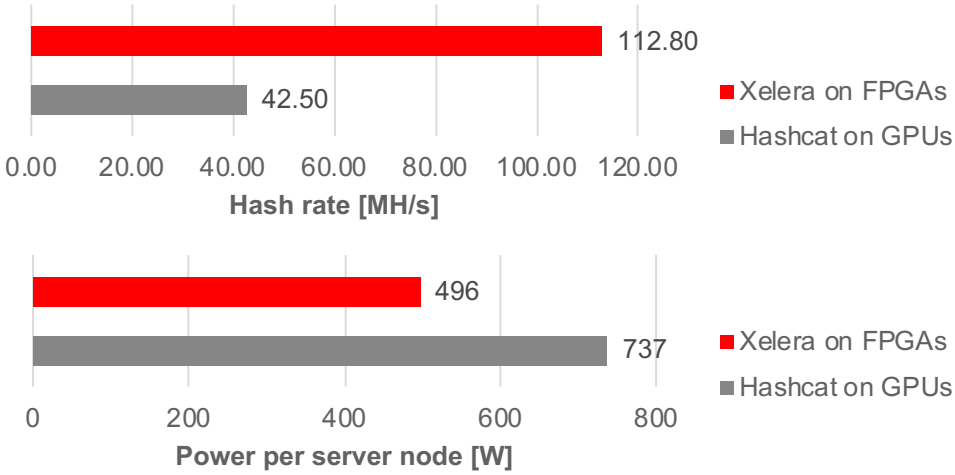
High-Performance Hash Computation Software

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 hash rates and better power efficiency over state-of-the-art GPU-based systems.

Hash format:	Unix Crypt MD5, 1000 rounds
Mode:	Brute-force
Servers:	Dell Poweredge R7525
Test setup 1:	Xelera on Xilinx Alveo U50 FPGAs
Test setup 2:	Hashcat on Nvidia Tesla T4 GPUs



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.

NTHash	SHA2-512	SHA2-256 Crypt
NetNTLMv1	MD4	SHA2-512 Crypt
NetNTLMv2	MD5	DES-crypt
SHA1	Unix Crypt MD5	HMAC-SHA1
SHA2-224	Apache Crypt MD5	HMAC-SHA2-224
SHA2-256	MySQL-4.0	HMAC-SHA2-256
SHA2-384	MySQL-4.1	HMAC-SHA2-384
...	...	...

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

XELERA TECHNOLOGIES GMBH
RHEINSTR. 40–42
64283 DARMSTADT
GERMANY

FON: +49 6151 162 24 25
CELL: +49 175 268 17 56
MAIL: SALES@XELERA.IO
WEB: WWW.XELERA.IO

MANAGING DIRECTOR:
FELIX WINTERSTEIN

REGISTERGERICHT (LEGAL DOMICILE):
DARMSTADT HRB 97805

IBAN:
DE 17 5085 0150 0000 7709 90
BIC: HELADEF1DAS

UST-ID-NR.: DE318360521