PQSHIELD

Pioneering Side Channel Resistance for PQC

PQShield enables their customers to de-risk their development process with a comprehensive security strategy, rooted in the expertise of its world-class R&D team. This strategy comprises our dedicated SCA test lab, fully automated and continuous SCA test procedures, PQShield's unique definition of security levels that cater to three different real-world threat models, and a forward-looking certification roadmap for our product portfolio.

PQShield's cutting-edge SCA test lab

- Validates the efficacy of our countermeasures
- Based on TVLA (ISO/IEC 17825) and implementation specific methods
- Follows testing and calibration procedures in ISO/IEC 20085-1/-2
- Validated by industry leader Riscure

Host machine
- USB Connection
- FTDI Connection

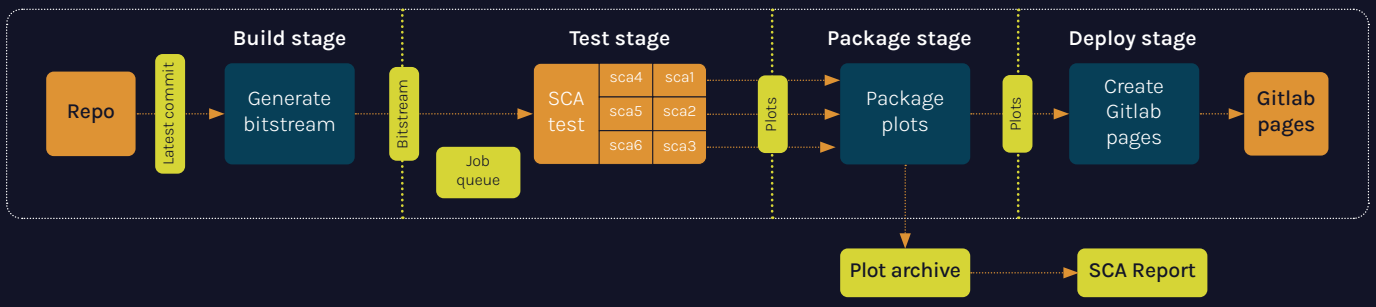
Target
- Chipwhisperer CW305
- Artix 7 FPGA

Oscilloscope

Picoscope 6424E
- 8 bit resolution (can be increased to 12-bit)
- 500 MHz bandwidth
- 4 GS memory

Fully Automated Continuous SCA Testing

- Fully integrated into our IP development cycle (10s of TB/week)
- Daily/Weekly tests



Multi-Level Security Profiles

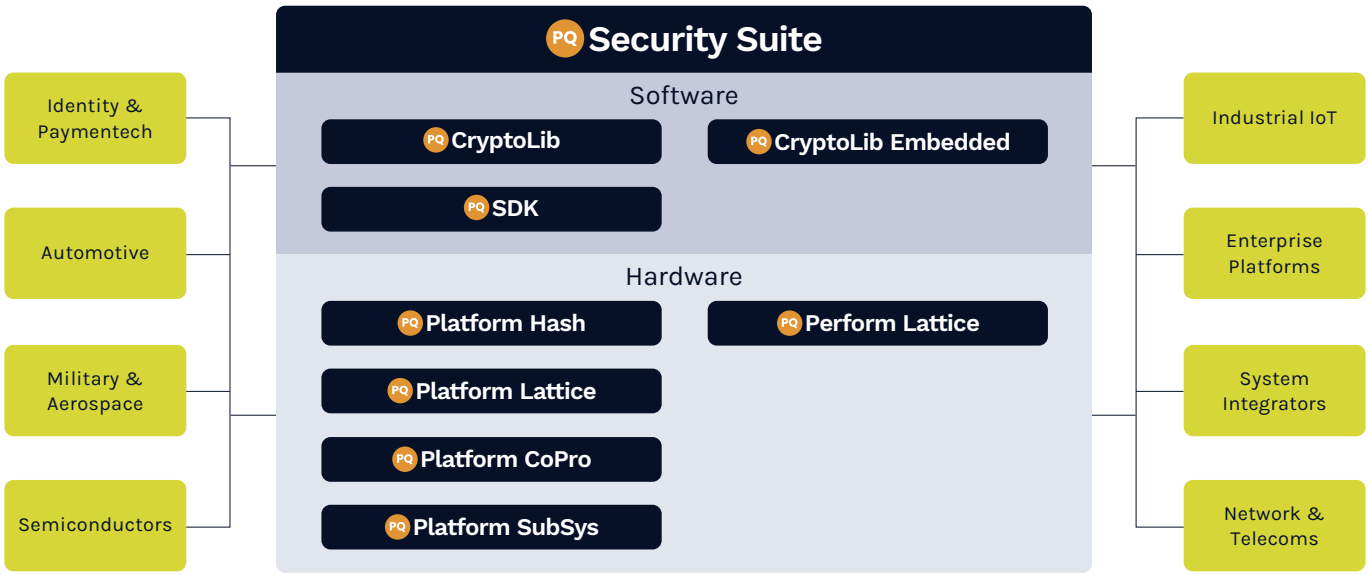
- Different applications require different threat model
- PQShield products are offered in 3 security levels to address all use cases
- 21 papers published on SCA attacks and countermeasures for PQC, all and many more papers are available on our website

Level	Target	FIPS 140-3	Common-Criteria	SESIP	PSA
Cloud grade	Safe against fuzzing Safe against remote attacks*	Level 1	EAL1 AVA_VAN.1	1	1
Commercial grade	Safe against "push button" physical attacks (basic attack potential)	SW: Level 2 HW: Level 3	EAL2 to 3 AVA_VAN.2	2 to 3	2 to 3
Government grade	Safe against expert lab (high attack potential)	SW: Level 2 HW: Level 4	EAL4+ to 7 AVA_VAN.5	4 to 5	NA

*For software libraries, micro-architecturale attacks such as RowHammer, Spectre, Meltdown... may be applicable if the hardware platform is vulnerable to them.

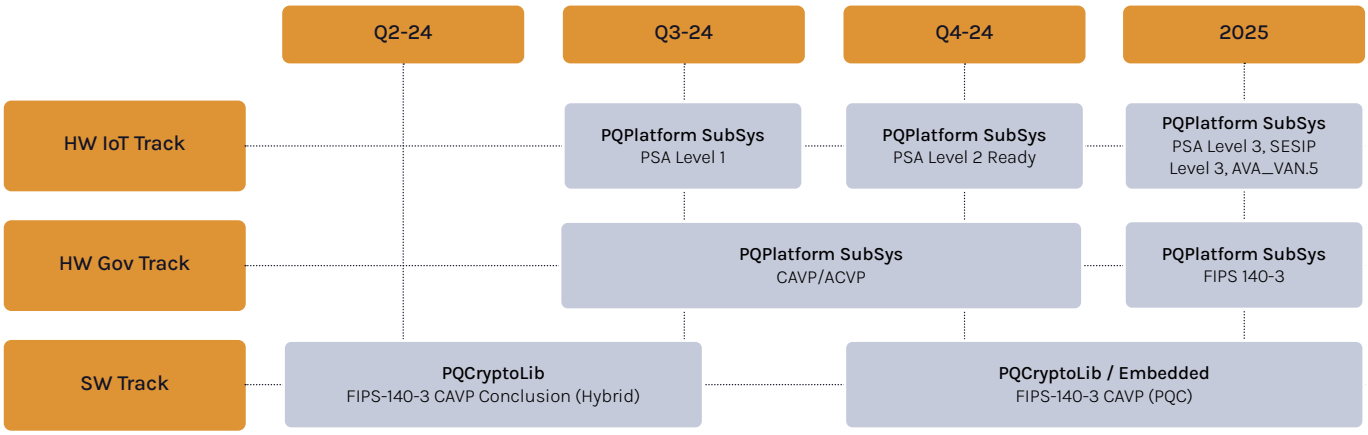
PQShield Security Suite

- Our product portfolio covers a comprehensive range of solutions, from high-performance PQC for data centers, to the high security required for embedded devices
- PQPerform: high-performance IPs
- PQPlatform: compact and high-security IPs
- All PQShield hardware IPs are provided with a software driver



Certification Roadmap

- We target PSA and SESIP level 3 certifications for hardware
- Cryptography library and hardware supports FIPS 140-3



PQ SHIELD

Ready to learn more?
Get in touch: contact@pqshield.com
www.pqshield.com

Products

Publications

Careers