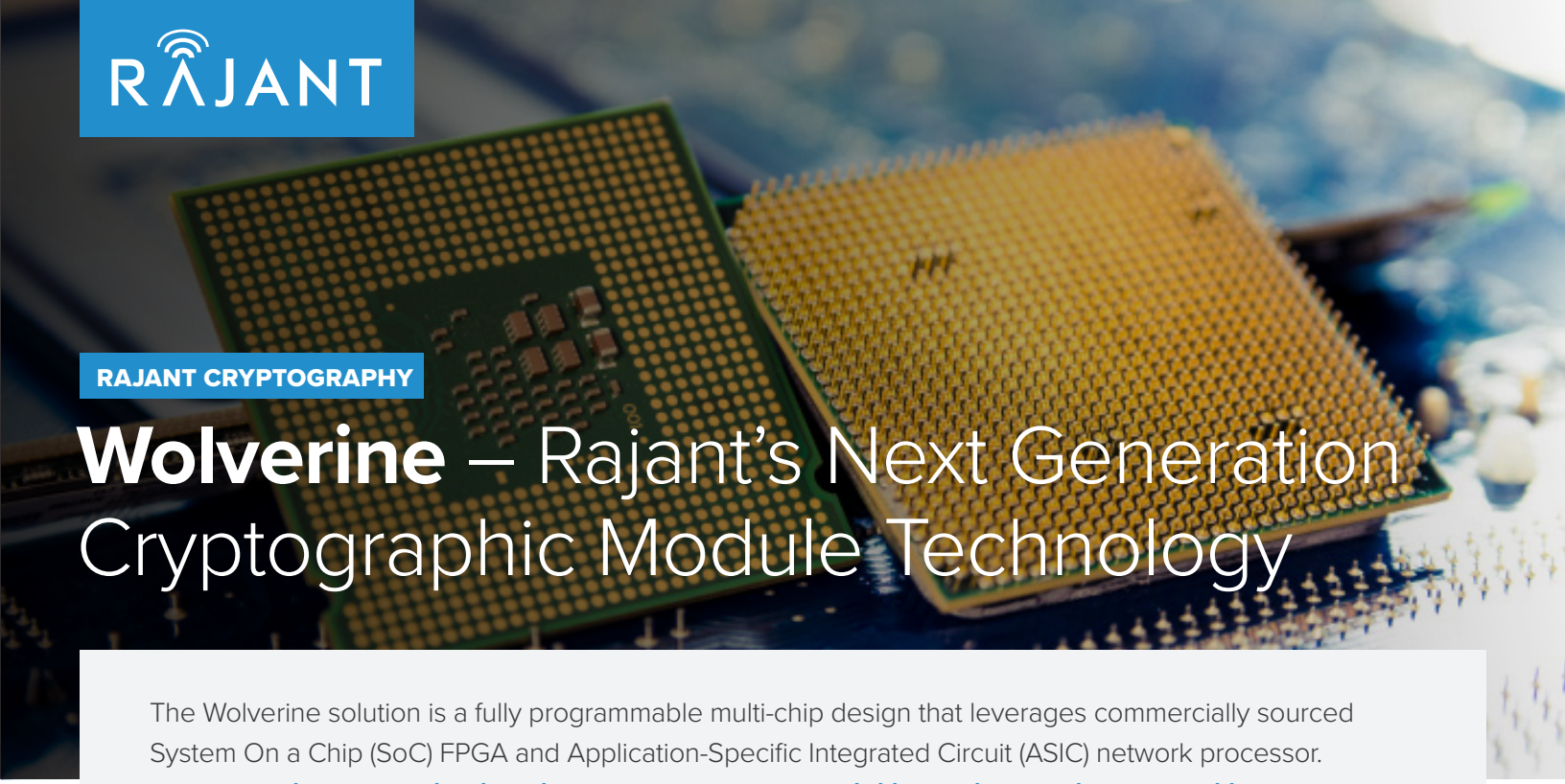
RAJANT



RAJANT CRYPTOGRAPHY

Wolverine – Rajant's Next Generation Cryptographic Module Technology

The Wolverine solution is a fully programmable multi-chip design that leverages commercially sourced System On a Chip (SoC) FPGA and Application-Specific Integrated Circuit (ASIC) network processor. **The Wolverine CM design is built for programmable flexibility, which provides the ability to add new algorithms in the future, while also meeting stringent U.S. Government certification requirements.** Wolverine contains advanced encryption and authentication algorithms using a fail-safe design to provide design flexibility for multiple IoT applications.

Key Technology Features

Planned Certifications

- Suite B Certification
- Crypto High-Value Processing (CHVP) while unkeyed
- FIPS 140-2

Performance

- 100 Mbps Full-Duplex 256 AES-GCM Traffic throughput

Fail-Safe Design

- Red/Black processing separation
- Passive and active tamper protections
- Security monitoring features
- Bypass traffic inspection
- All-flash software code images are serialized with device unique encryption key
- Software execution only occurs in internal memories

Interfaces

- Red side 10/100 MII interface
- Black side 10/100 PHY interface
- DS101: Supports SKL
- Red and black side discrete IOs

Future Proof

- Fully software programmable for future needs
- Footprint compatible FPGA options are available to increase FPGA fabric size

Field Software Upgrade Support

- Accepts only signed and encrypted SW images
- Security partitioning for factory only versus field upgrade level support

Algorithms Currently Implemented

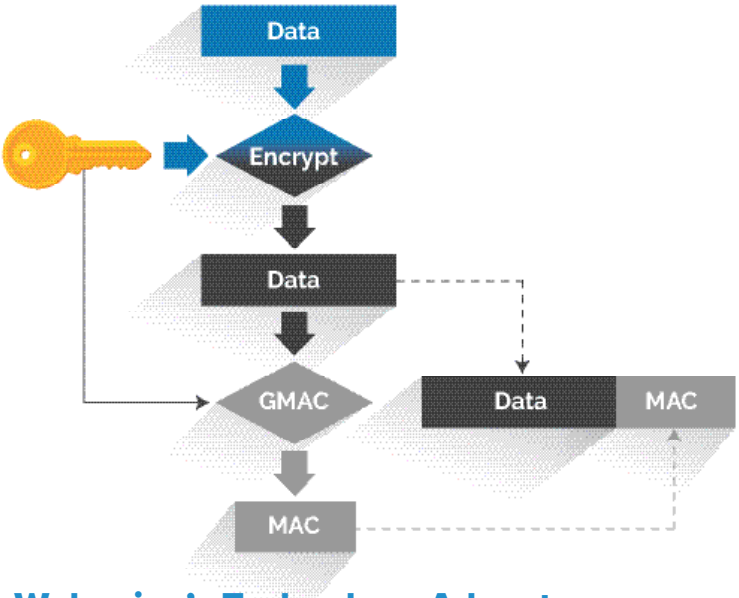
- Red/Black processing separation
- AES 256 GCM/CTR/ECB
- SHA 256/384
- HMAC-SHA384
- ECDSA 256/384
- AEMODN
- A+BMODN
- AES-KEYWRAP
- AES-KEYUNWRAP

Module Size

- 2" x 2.75"

Temperature

- -40°C to 80°C



Wolverine's Technology Advantages

- **Future Proof:** Wolverine is a fully programmable solution in that it can easily be modified to meet a wide range of future crypto processing needs. This includes algorithm agility, I/O flexibility, and Key Management evolution.
- **Scalable Architecture:** Wolverine is a scalable design, such that it can easily be migrated to meet higher performance requirements. It also utilizes industry-standard cells and IOs so that it can be later be migrated to an ASIC design with minimal changes.
- **Secure Boot Trust Anchor with Intellectual Property (IP) Protection:** Wolverine's Secure Boot capability goes beyond what today's security processors provide. It not only governs what trusted software is allowed to run within the system, it also serializes the IP software/firmware modules upon initial load. Serialization is a process where the software/firmware is encrypted with a unique per-Wolverine key (that is created once upon boot) prior to being written and stored in external non-volatile flash memory. This, in turn, results in every Wolverine based solution to have a uniquely encrypted software/FPGA image stored in flash while it is fielded. This is important as it protects all Wolverine fielded solutions from being compromised in the event an adversary is able to invest extensive amounts of time and capital to hack an encrypted image of another common fielded solution. The decryption key the adversary might obtain form one Wolverine unit will be useless on all other Wolverine units due to this unique Secure Boot capability.

  Key/Certificate Store: Wolverine can serve as the root certificate and symmetric key storage element for the system. Its certifiable anti-tamper capabilities will ensure that the most critical aspect of the security architecture (the keys) are inaccessible to an adversary. The certificates and keys managed by Wolverine are those that would be used throughout the technology trust chain hierarchy. This includes keys and authority certificates for firmware/software updates and all encrypted communication links.

  Flexible Key Management: Wolverine's programmability allows for customization of key management protocols, such as EKMS and Tactical Key Management (TKM). Furthermore, Wolverine's cryptographic algorithms enable support for robust Key Rollover and future Over-The-Air-Keying (OTAK) solutions. Key Rollover and OTAK methods are essential for protecting not only classified data but also for protecting the personnel that are responsible for keying the crypto device while fielded. By reducing (or eliminating) the need for a person to manually key the crypto device, it reduces the risk that individual may face in the event the fielded crypto device is in a hazardous environment.
- **High Throughput Data-Path Cryptographic Processing:** Wolverine has a programmable data-path processing core that can be customized to include application-specific interfaces and data packet formats. By optimizing the data-path, the encryption/decryption processing throughput can be optimized while the over-all throughput latency is minimized.
- **Ease of Certification:** Wolverine's architecture has been designed around the concept of Red and Black data separation from the start. This ensures that Red data (most sensitive) cannot inadvertently be leaked across to the Black data side (less sensitive) without being encrypted. In doing so, the logical red/black separation architecture simplifies the software and firmware code modules that will run within Wolverine and will need to be reviewed to meet various certification levels (i.e. FIPS-140 or U.S. Government certification).

Wolverine's Technology Team

Wolverine is made possible by Rajant's Information Assurance (IA) team comprised of Embedded Security Engineers who were part of ITT Defense, which became Exelis and then later Harris. The team includes hardware and software engineers as well as ASIC, FPGA and System engineers. Together, they developed cryptographic solutions primarily for DoD applications. Their custom SoC ASIC solutions are NSA certifi ed for SECRET and TOP SECRET applications.

Tel: 484.595.0233 | **www.rajant.com**

20+ Years OF GAME-CHANGING WIRELESS

RAJANT
MAKING THE COMPLICATED ***SIMPLE***
Continuous, Connectivity, Anywhere