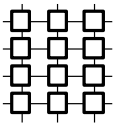
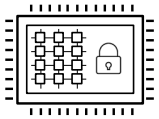
Programmable Fabric and Cryptographic Algorithms

FPGAs are widely used in aerospace and defense applications, often as a vehicle for deploying secure enclaves and anti-tamper cryptographic accelerators such as SHA and AES . FPGAs are highly flexible; they allow their functionality to be changed through the device life. This 'future-proofing' is beneficial to many "long-in-market" applications like Defense, Aerospace, Automotive, and Telecommunications. However, the security of the system can be put at risk through hacking communication between other hard logic chips and the discrete FPGA containing the cryptographic algorithms within deployed systems.



Hard logic chip functionality is determined by design. This means that cryptographic algorithms running on the chip cannot change over the life of the chip; upgrades and new standards cannot be deployed without a new chip design, which often costs millions of dollars.

A solution to this is to embed FPGA logic within the main processor of the system thru the use of eFPGA technology. Like discrete FPGA chips, eFPGAs are reconfigurable. Unlike discrete FPGAs, eFPGA are part of an SoC design, occupying the same silicon. While the standard logic of the SoC remains determined by design, the eFPGA portion of the chip is reconfigurable, allowing future updates to crypto functionality and providing a much more secure implementation of cryptographic algorithms. eFPGAs offer a higher security, lower cost, and smaller size alternative to the deployment of discrete FPGAs, while maintaining the flexibility and future proofing.



The Menta Solution

In today's global multi-player design-chain, preserving IP/trade secrets is more critical and challenging than ever. With Menta eFPGA, you can wait to deliver your most proprietary technology to end-customers as a field-upgrade, minimizing any opportunity for competitors to reverse engineer your product.

Menta offers high quality eFPFAs. It is essential that any IP, whether flexible or not, must never put the remainder of the SoC at risk. For this reason, Menta designed its eFPGA so that it can be verified at various levels: using formal verification for mapped applications, system simulation with SDF timing information, and even gate-level simulation post place-and-route. Bitstream loading can be simulated and verified as well. We call it Trusted eFPGA.

Menta delivers IPs architectures that are unique to a specific customer and unknown by the general public (for instance, no datasheets are available on the web) – further improving security. As such, this offers the trust required by defense, automotive and telecommunication chip makers. In addition, Menta 100% standard cells IPs are fully verifiable within customer EDA environment.

The Rambus Solution

From chip-to-cloud-to-crowd, Rambus secure silicon IP helps protect the world's most valuable resource: data. Securing electronic systems at their hardware foundation, our embedded security solutions span areas including root of trust, tamper resistance, secure protocols, content protection and trusted provisioning.

Rambus offers hardware roots of trust, available in both fixed function and programmable architectures. These roots of trust are complimented by a series of standard and side channel attack anti-tamper cryptographic cores. When data needs to be secured while it is motion, Rambus offers complete inline Protocol Engines that seamlessly integrate with your network interface and look-aside engines. Additionally, Rambus offers a combined hardware and software device provisioning and cloud key management services, which allows device makers to establish device authenticity early in the manufacturing process, the foundation of a secure supply chain.

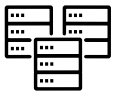
The Combined Solution

A combined solution may consist of Rambus Root of Trust or cryptographic cores ported and optimized into a Menta eFPGA, located on a customer SoC. This enables a series of use cases, including:

- **Encrypting images** loaded into the eFPGA, ensuring integrability
- **Secure boot,** verifying images before loading on all cores
- **Key management and key integrability**

The combined solution would target:

- **Defense and Aerospace**
  - Computing platforms and boards — security coprocessor and configurable fabric
  - Sat COMM platforms and RF boards — embedded security functions and programmable FPGA instances
- **Data Center and AI**
  - Acceleration cards —protecting the acceleration data with Root of trust capabilities
- **Automotive**
  - Autonomous driving platforms
  - Entertainment/Navigation modules



About Menta

Menta is a privately held company based in Sophia-Antipolis, France. For ASIC and SoCs designers who need fast, right-the-first time design and fast time to volume, Menta is the proven eFPGA pioneer whose design-adaptive standard cells-based architecture and state-of-the-art tool set provides the highest degree of design customization, best-in-class testability and fastest time-to-volume for SoC design targeting any production node at any foundry.

http://www.menta-efpga.com

About Rambus

Rambus is a premier silicon IP and chip provider that makes data faster and safer. Throughout our 30-year history, Rambus has led the industry with innovations and IP solutions that solve the fundamental challenges faced by leading-edge computing systems. Leveraging our semiconductor expertise, Rambus solutions speed performance, expand capacity and improve security. From data center and edge to artificial intelligence and automotive, our interface and security IP, and memory interface chips enable SoC and system designers to deliver their vision of the future

https://www.rambus.com/security