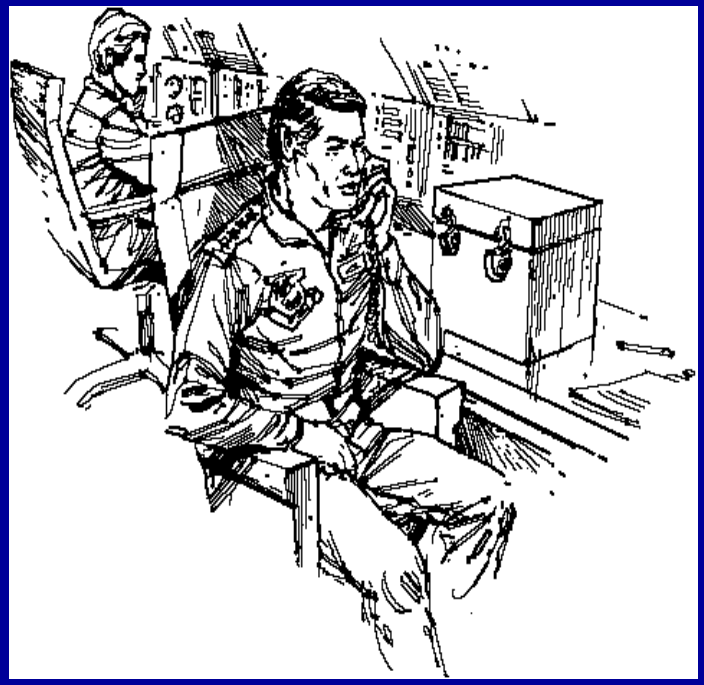
Lockheed Martin
Advanced Technology Laboratories

CYPRIS
An Application Specific Reconfigurable Processor

Michael Stebnisky

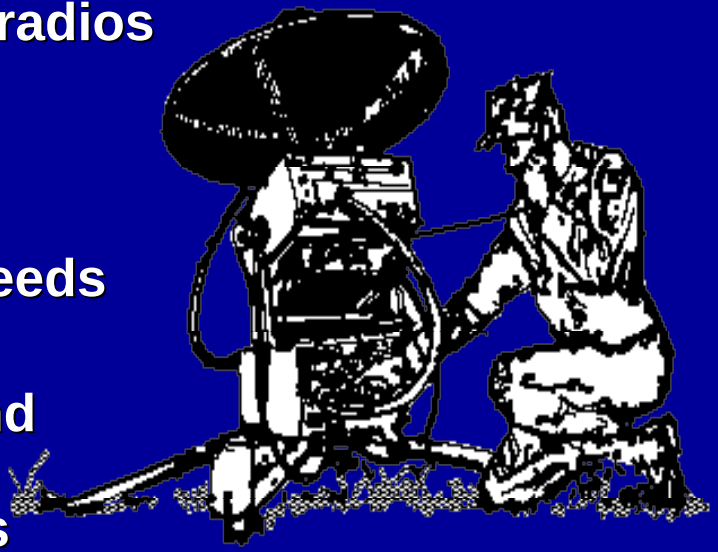
Abstract

CYPRIS (Cryptographic RISC microprocessor) is a high performance, algorithm agile reconfigurable processor specifically designed to address the cryptographic requirements of military software radios and wireless systems. Designed under a NSA contract, CYPRIS was optimized to implement a variety of legacy COMSEC and TRANSEC algorithms while enabling field upgrades to new and emerging INFOSEC algorithms. CYPRIS contains a high performance RISC core, a reconfigurable hardware unit, and a suite of programmable and automatic system check features. Unprogrammed, CYPRIS is an unclassified, non CCI, exportable device; when programmed it assumes the classification of its software. Over 20 core cryptoalgorithms have been developed.



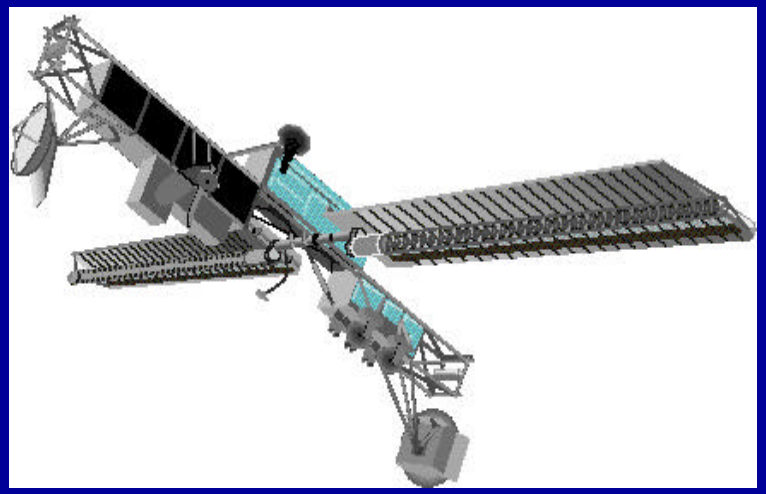
Cryptographic RISC Processor

- **CYPRIS was developed as an Application Specific Reconfigurable Processor:**
  - **Primary application domain: Type 1 Cryptography**
  - **Primary insertion target: Software radios**



- **Objectives:**
  - **Provide flexibility to meet different COMSEC and TRANSEC system needs for both legacy and future devices**
  - **Provide ability to easily, quickly and economically upgrade crypto-algorithm, including field upgrades**
  - **Significantly reduce time needed to satisfy new requirements**
  - **Combine the best domain specific features of hardware and software in a single device**

Design Approach



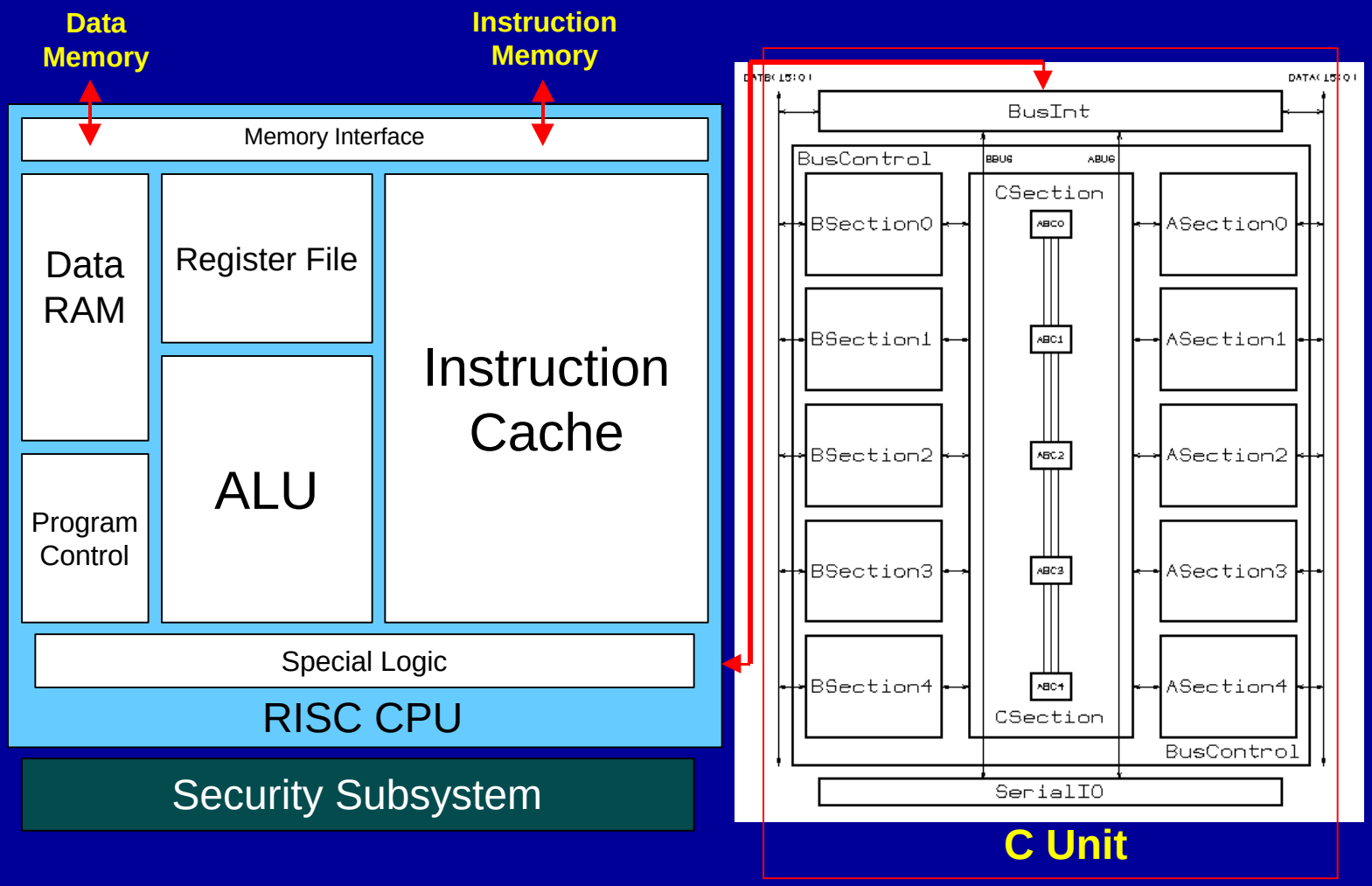
- **Identify a group of cryptoalgorithms representative of a broad range of applications**
- **Identify throughput requirements for each cryptoalgorithm**
- **Identify features and characteristics necessary to ensure a certifiable subsystem design**
- **Develop a general architecture (RISC processor plus “other stuff”) to enable top level simulation**
- **Refine trades between RISC core and reconfigurable hardware**
- **Optimize at RTL, then gate, then transistor level**
- **Trade features versus manufacturable design**
- **Complete 100% full custom VLSI implementation**

Cryptoalgorithm Implementations

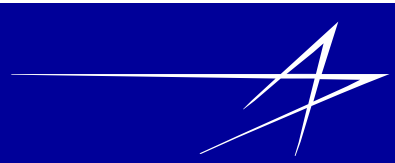
- **Required by original spec**
  - — Bayless
  - — Byteman
  - — Cordoba
  - — Crayon (4 modes)
  - — Keesee
  - — Padstone (2 modes)
  - — Phalanx I
  - — Phalanx II
  - — Saville (3 modes)

- **Added**
  - — DES (ECB and CBC)
  - — Triple DES
  - — Baton
  - — Cardholder
  - — Cardigan
  - — Have Quick
  - — Arcfour

CYPRIS Architecture



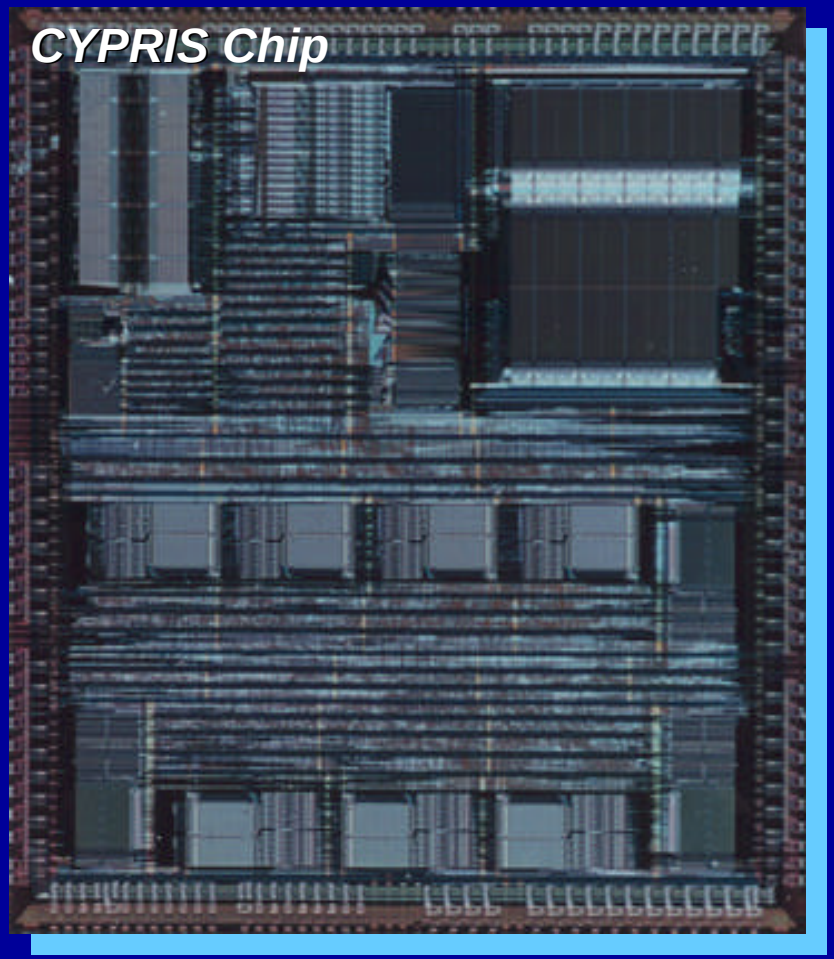
Key Architectural Features



- **Three Independent Units enable unique and optimum trades among throughput, flexibility and security**
- **RISC core**
  - **Enables software coding of processor oriented functions, control and I/O**
  - **Some special instructions and features added versus “typical RISC”**
  - **Some “typical RISC” instructions and features eliminated**
- **Reconfigurable hardware unit (C Unit)**
  - **Enables hardware implementation of functions inefficient in software**
  - **10 large reconfigurable blocks and programmable interconnect structure**
  - **Encrypts at up to 1 bit/clock**
  - **High speed configuration: 38 µsec worst case context switch**
- **System check features**
  - **Six automatic and five programmable checks with Zeroize**

Key Benefits versus COTS Processors and Custom Hardware

- **Up to 100X higher performance than straight processor/software**
- **Completely unclassified, non-CCI when unprogrammed**
- **COMSEC and TRANSEC in one reprogrammable device**
- **Certifiable design**
- **Built-in system integrity features**
- **Full on-chip Zeroize in 75 nsec**
- **Low power (<1.5W @ 50 MHz)**
- **Low cost (including plastic package)**
- **Small weight/volume subsystems**



Example Application: SPEAKEASY

- **For SPEAKEASY, CYPRIS was specified to provide all COMSEC and TRANSEC required for interoperating with the following:**
  - **KGV-10**
  - **KY57**
  - **KG-184**
  - **KG-13**
  - **KYV-5 (ANDVT)**
  - **KGV-11/CTIC/CDH**
  - **KGV-8**
  - **KGV-6**
  - **Baton**
  - **Railman**
  - **Skipjack**
  - **Thornton**
  - **KGR-96/Ricebird**

Results

- **The anticipated benefits of the mixed processor/ reconfigurable hardware architecture were achieved**
  - **— Some cryptoalgorithms were most effectively implemented in software alone**
  - **— Some cryptoalgorithms were most effectively implemented in reconfigurable hardware alone**
  - **— Others are hardware/software mixtures**
- **All requirements have been met or exceeded**

Related Activity

- **Domain expertise in reconfigurable processors and cryptographic applications is being utilized in a new DARPA Adaptive Computing Systems (ACS) development**
- **Lockheed Martin ATL is a subcontractor to Synopsys Inc. in their ACS contract entitled "The Nimble Compiler for Agile Hardware"**
- **The Synopsys team will develop a capability to automatically perform retargetable hardware/software partitioning, parallelization and other optimizations from straight C code input**
- **Lockheed Martin ATL will address the ACS INFOSEC Challenge by developing both classified and unclassified cryptography domain specific test cases, examples, analyses and RC algorithm implementations**

Conclusion

- **CYPRIS is an application specific reconfigurable processor that combines a RISC processor, a reconfigurable hardware unit, and a suite of system check features**
- **Each of these elements is optimized for the application domain: Type 1 Cryptography**
- **The result is a cryptoprocessor which is unmatched in its domain of application**
- **This general architecture, combining a RISC processor with reconfigurable hardware, will be effectively utilized across several application domains**