No Trade-off Necessary

Security, Performance, Ultra-Low Energy, and Assurance

Dr. Joseph Kiniry
Principal Investigator, Galois

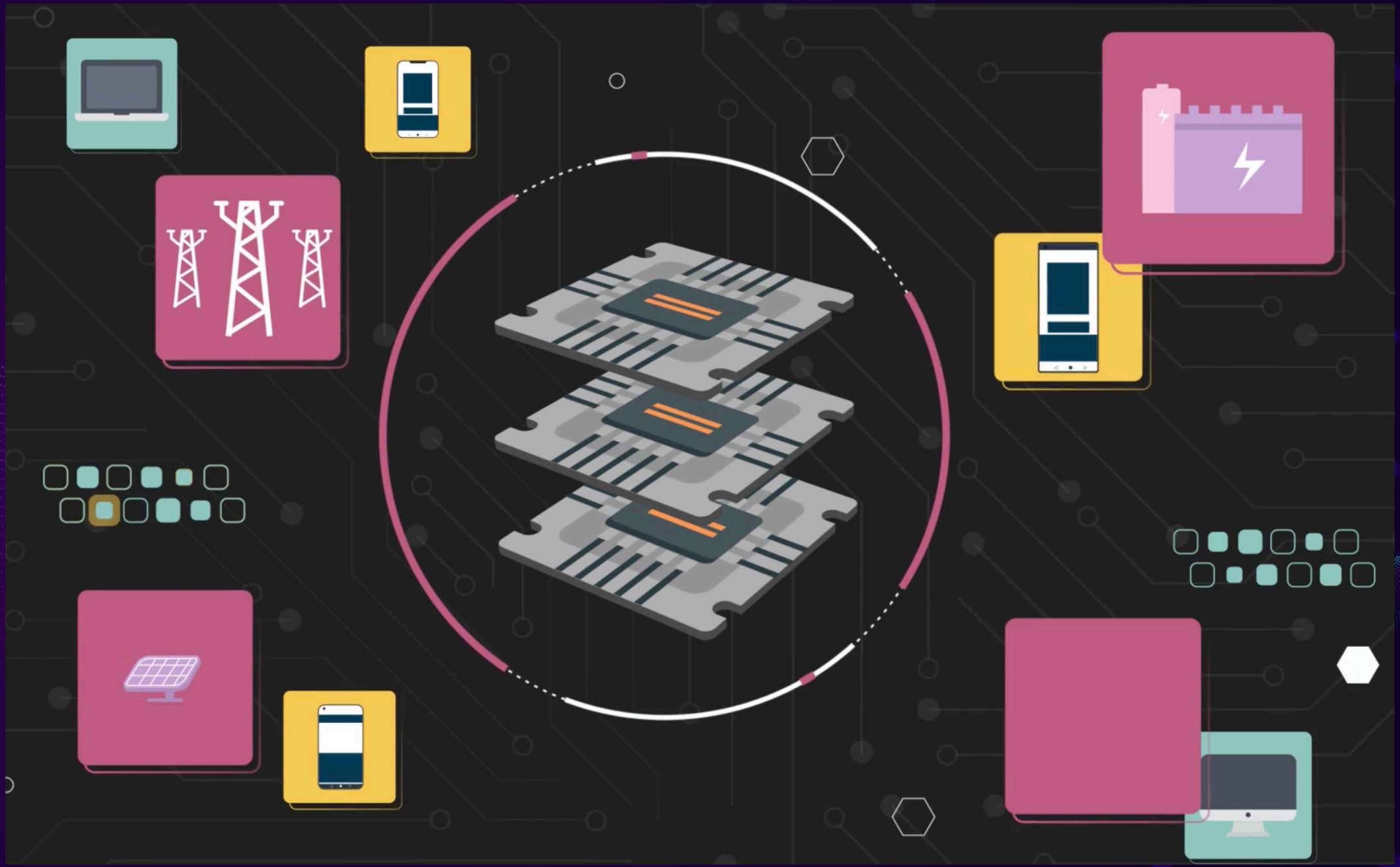
This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Distribution Statement A – Approved for public release. Distribution unlimited.

ASICs Today

- Enormously complex
    - Barely understood by their own creators
    - Tested like software 20 years ago
    - Lack true hardware / software co-design
- Lack security and assurance guarantees
    - "Try Hard" versus formal proof
    - Little hardware / software co-verification
    - Limited side-channel guarantees
- Ubiquitous

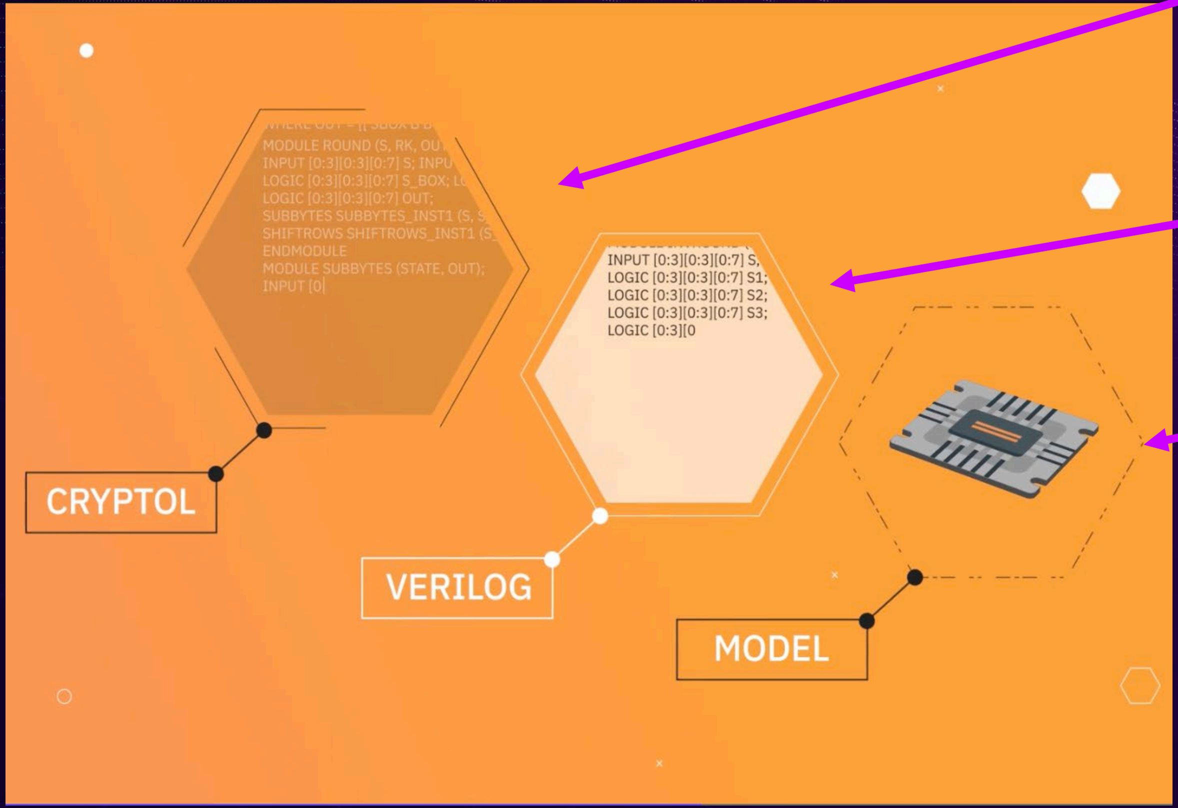


src: Author's own

Rigorous Digital Engineering

Galois's 15-Year-Old Solution

- Model-based Engineering (MBE) using Formal Methods (FM) for **"Correct by Construction"** hardware and software co-design and co-verification



```
MODULE ROUND (S, RK, OU
INPUT [0:3][0:3][0:7] S; INPU
LOGIC [0:3][0:3][0:7] S_BOX; LO
LOGIC [0:3][0:3][0:7] OUT;
SUBBYTES SUBBYTES_INST1 (S, S
SHIFTROWS SHIFTROWS_INST1 (S
ENDMODULE
MODULE SUBBYTES (STATE, OUT);
INPUT [0|
```

```
INPUT [0:3][0:3][0:7] S,
LOGIC [0:3][0:3][0:7] S1;
LOGIC [0:3][0:3][0:7] S2;
LOGIC [0:3][0:3][0:7] S3;
LOGIC [0:3][0
```

Describe product lines with Domain Specific Language

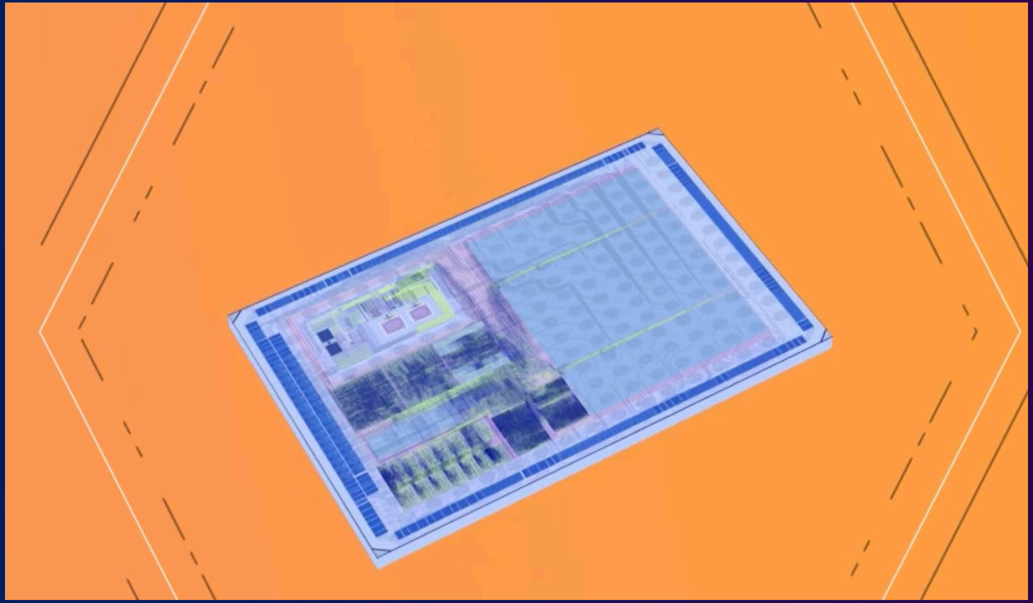
Automatically generate product designs leveraging traditional EDA tools

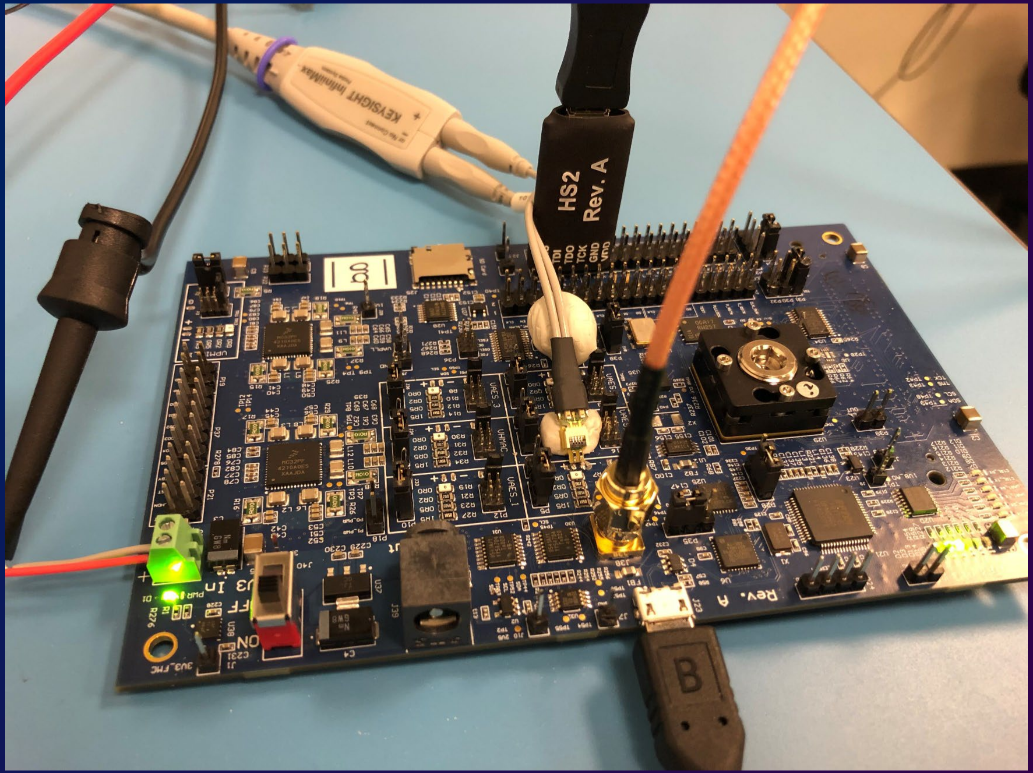
Full product assurance including software, firmware and hardware

src: Author's own

The 21CC ASIC

- Our 21CC project is a Hardware Security Module ASIC created using RDE
  - AES-256, SHA-384, HMAC/SHA-384, RISC-V
  - Designed using a correct-by-construction flow
  - Fabricated on GF12LP
  - Side-channel free
- Ready for certification
  - Project unveiled by co-PI, Dr. Dan Zimmerman, at the ERI Summit 2020
  - Government has possession of the ASIC
  - Assurance case and red teaming results demonstrating correctness and security

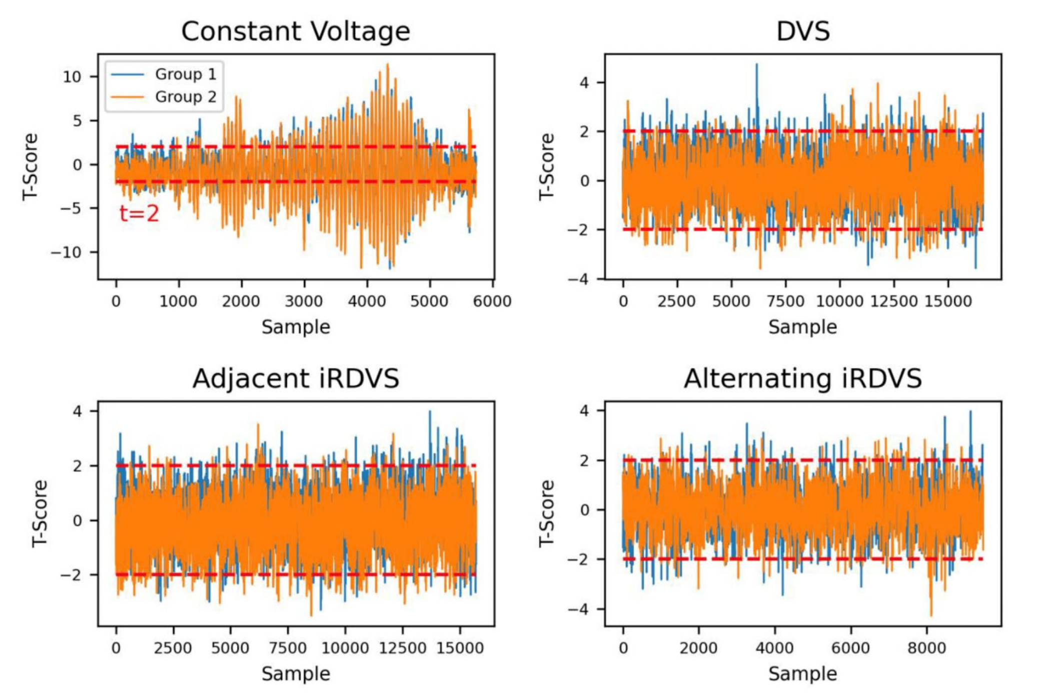




src: Author’s own

Distribution Statement A – Approved for public release. Distribution unlimited.

21CC Details



src: Author's own

C Value	Case	Number of Samples with T-Scores Exceeding C
4.5	Constant	740
4.5	DVS	0
4.5	Adjacent iRDVS	0
4.5	Alternating iRDVS	0
2	Constant	2211
2	DVS	34
2	Adjacent iRDVS	12
2	Alternating iRDVS	4

- **Applied RDE process including** several digital twins
- **Asynchronous Design** permits an optimal balance between power, performance, and energy use.
  - Ultra-low power + High Performance
  - Smooth distribution of power consumption for performance
- **Power Side Channel-Free** using island-based random dynamic voltage scaling (iRDVS)
  - iRDVS automatically adapts voltage in a cryptographically random fashion, across 14 pipelined power islands, while optimizing performance
  - Throughput of 20Gbps @ 22mW, and 12Gbps @ 14mW
  - >> 200K minimum traces for disclosure

Moving from Strength to Strength: Partners and Capabilities

- Galois is now working on RDE for HW with other firms including:
  - **Niobium Microsystems** (our daughter company)
  - **PQSecurity** (post-quantum cryptography IP)
  - **Riscure** (pre- and post-silicon side channel analysis)
- Our capabilities have broadened considerably. We have created new EDA tools for reasoning about:
  - Information Flow
  - Timing Leakage
  - Product Line Discovery
  - Product Generation from Product Lines
  - Improved SV Generation from Cryptol Models
  - Software and Firmware Generation from Cryptol Models
  - Integrated Formal Reasoning spanning systems, software, firmware, and hardware models and code, including reasoning about VHDL, Verilog, SystemVerilog, Bluespec SystemVerilog, and more

Typical RDE Product Line Artifacts

Informal or Semi-Formal Artifacts:

- CONOPS, slides, reports, user's guides, developer's guides, etc.

Formal Models:

- Domain Engineering
- Product Line Engineering
- Requirements engineering
- Systems architecture
  - Static and dynamic structure
  - Behavioral properties
  - Non-behavioral properties, particularly cybersecurity and PPA/SWaP
- Executable models of system, software, firmware, and hardware at several fidelities with known, verified properties
- Digital twins that run in co-simulation
- Integrated assurance case includes:
  - Rigorous runtime verification and formal validation of executable models
  - Rigorous runtime verification and formal validation of SW, FW, and HW
  - Formal verification of critical SW, FW, HW component implementations

Other Recent RDE HW Projects

- **HIPERSPACE (SDA)**
    - Ultra-high performance, formally verified crypto for space deployment
- **HARDENS (NRC)**
    - Fault tolerant, online self test, diverse design, correct-by-construction, sense-compute-control protection system for nuclear power reactors, including a formally assured RISC-V core
- **BASILISC (DARPA MTO)**
    - High-assurance fully homomorphic encryption (FHE) accelerator, which includes the largest multipliers ever formally verified