TRUSTED® COMPUTING GROUP

# Lightweight Trusted Computing

NIST Lightweight Cryptography Workshop

November 2019

Tom Broström

Research Technical Director

Cyber Pack Ventures, Inc.

# Imagine…

- 2025
- 8B Humans
- 75B Connected Things

# In the News

NETWORKWORLD FROM IDG INSIDER Sign In | Register

INSIDER

**Microsoft finds Russia-backed attacks that exploit IoT devices**

Microsoft says default passwords, unpatched devices, poor inventory of IoT gear led to exploits against companies by Russia's STRONTIUM hacking group.

Forbes Billionaires Innovation Leadership Money Business Small Business

**Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims**

ZDNet CLOUD AI INNOVATION SECURITY MORE NEWSLETTERS ALL WRITERS

**Five nightmarish attacks that show the risks of IoT security**

The Internet of Things is not going away -- and neither are the attacks that exploit device vulnerabilities. Here are five incidents that illustrate ... prevent breaches.

TechRepublic.

**Kaspersky honeypots find 105 million attacks on IoT devices in first half of 2019**

BANK INFO SECURITY

DDoS Protection , Fraud Management & Cybercrime , Governance

**Massive Botnet Attack Used More Than 400,000 IoT Devices**

Researchers at Imperva Say Incident Mimicked Mirai-Style DDoS Attack

FORTINET

BUSINESS & TECHNOLOGY

**IoT Exploit Activity has Quadrupled - Are You Prepared?**

TRUSTED COMPUTING GROUP

# IoT Markets

## Smart vehicles

### Smart cars
- ADAS / autonom. driving
- Connected car
- Car security
- (H)EV

### Commercial, agriculture & construction vehicles
incl. Trucks & Busses
- ADAS / autonom. driving
- Secured connectivity
- (H)EV

### Other forms of transport
- Commercial aircraft
- Connected trains
- Ships (ferry & container)
- Light electric vehicles

## Smart city & energy

### Energy & infrastructure
- Generation (renewables)
- Advanced transmission & distribution / storage
- Utilities (water), traffic (electr. toll collection), outdoors, government
- Environmental sensors

### Building automation
- Automation
- Access control
- Air conditioning
- Elevators/escalators

### Professional lighting
- Building lighting
- Street lighting
- etc.

## Smart industry & business

### Factory automation
- Industrial automation
  - Motor & motion controller
  - Power quality
  - Power tools
- Industrial robotics

### Medical equipment
- Health sensors Diagnostics
- Rehabilitation systems

### Other businesses
- e. g. Banking & securities, education, mining, retail and wholesale, transportation and logistics

## Smart home & consumer devices

### Smart home
- Home automation incl. home appliances
- Home energy management
- Home security & safety
- Lighting

### Smartphones, tablets & PCs

### Consumer Electronics & wearables
- Media players, smart glasses, smart watches
- Well-being (health & fitness, assisted living
- Gaming

## ICT

### Communication Networks

### Data Center / Server Farms

Source: Infineon Technologies | graphics are courtesy of Infineon

TRUSTED® COMPUTING GROUP

# IoT Defenses

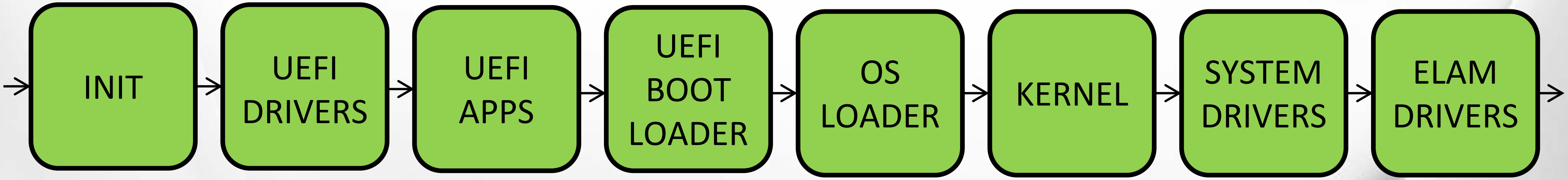

Source: Infineon Technologies | graphics are courtesy of Infineon

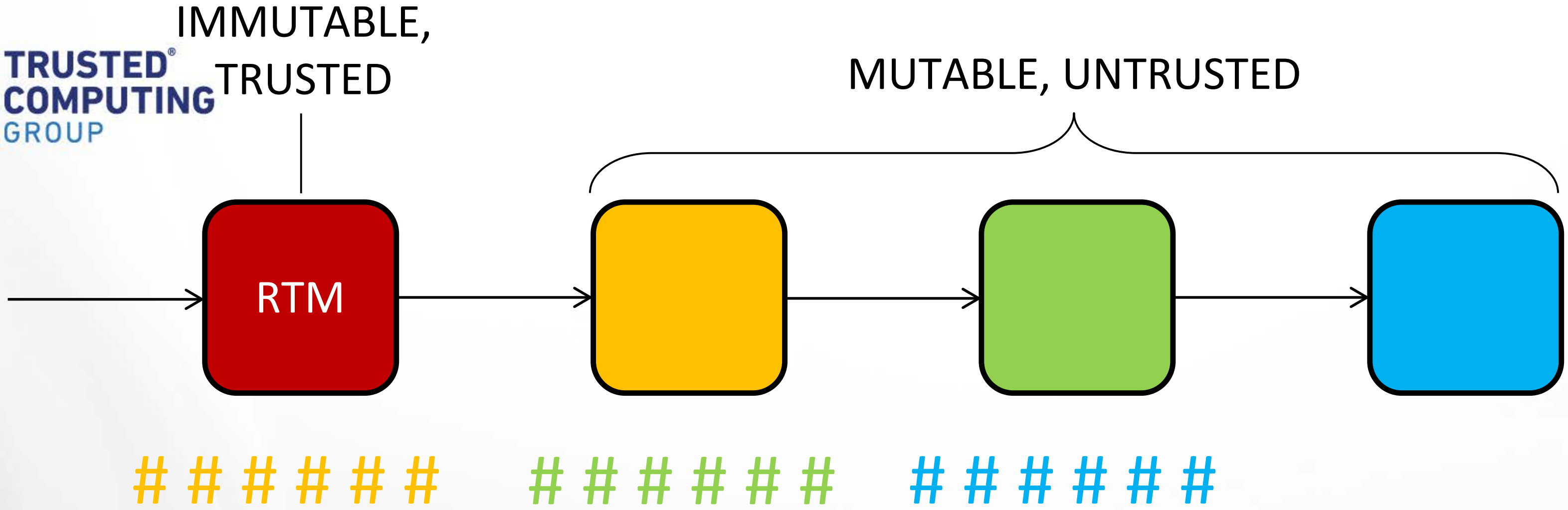
# Verified vs. Measured Boot

- Both compute a measurement
- Both verify measurement against known good

| | VERIFICATION PERFORMED | | | |
|---|---|---|---|---|
| | WHEN | WHERE | WITH | MEASUREMENTS |
| VERIFIED BOOT | Before executed | Booting device | Decrypted copy from signature | Discarded |
| MEASURED BOOT | After booted | Measurement Assessment Authority | Golden measurements | Retained in Event Log |

# Boot Process



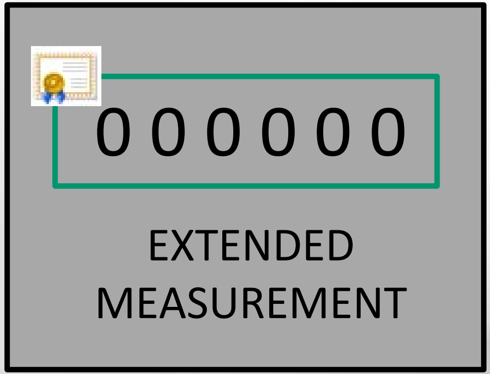



1. LOAD

2. MEASURE

3. EXTEND

4. EXECUTE





**T**RUSTED
**P**LATFORM
**M**ODULE

ROOTS OF TRUST:
- STORAGE
- REPORTING

# Enter the TCG

- Global non-profit consortium
- Creates open technical specifications
- Building block trust and security technologies
  - Endpoint devices: servers to IoT
  - Storage devices
  - Networking elements & protocols

# Board of Directors

Contributor Advisors:

46 Contributor
17 Adopter

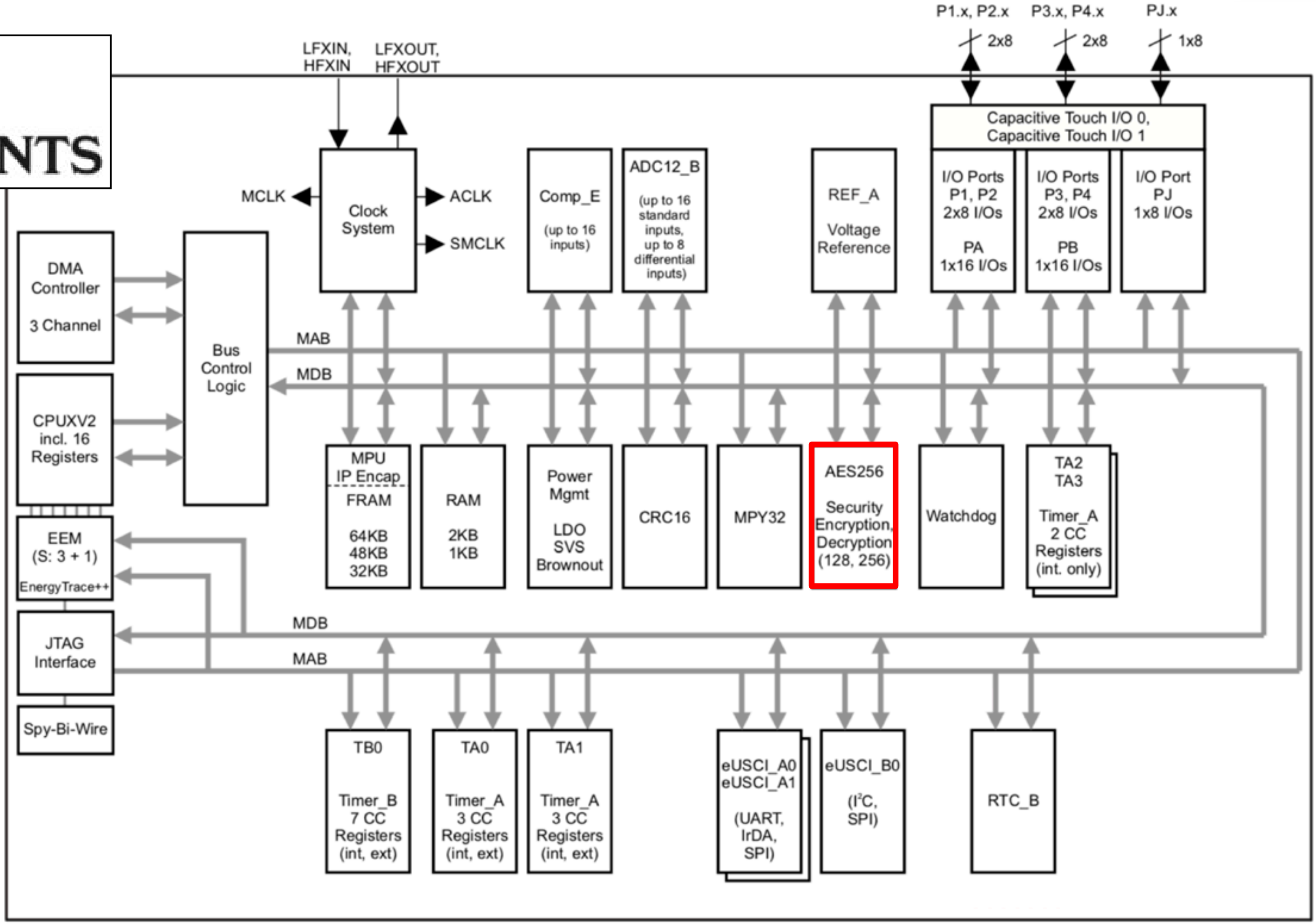
# Trusted Platform Module


- Capabilities
  - Roots of Trust for Storage & Reporting
  - Shielded Storage
  - Algorithm Agility
- Use Cases
  - Non-spoofable device identification
  - Non-spoofable device health attestation
  - Secure generation & storage of keys
  - NVRAM for Certificate Storage, etc.

# IoT Problem

- Connected Things, 75B by 2025
  - No TPM
    - no RTS/RTR
    - Nothing to protect M&A resources
  - No Asymmetric Crypto
- Solution:
  - Integrate minimal RTS/RTR in microcontroller
  - Symmetric attestation

# MSP430




http://www.ti.com/lit/ds/slas704f/slas704f.pdf

# Embedded Systems Working Group
# MARS Subgroup

Measurement and Attestation RootS

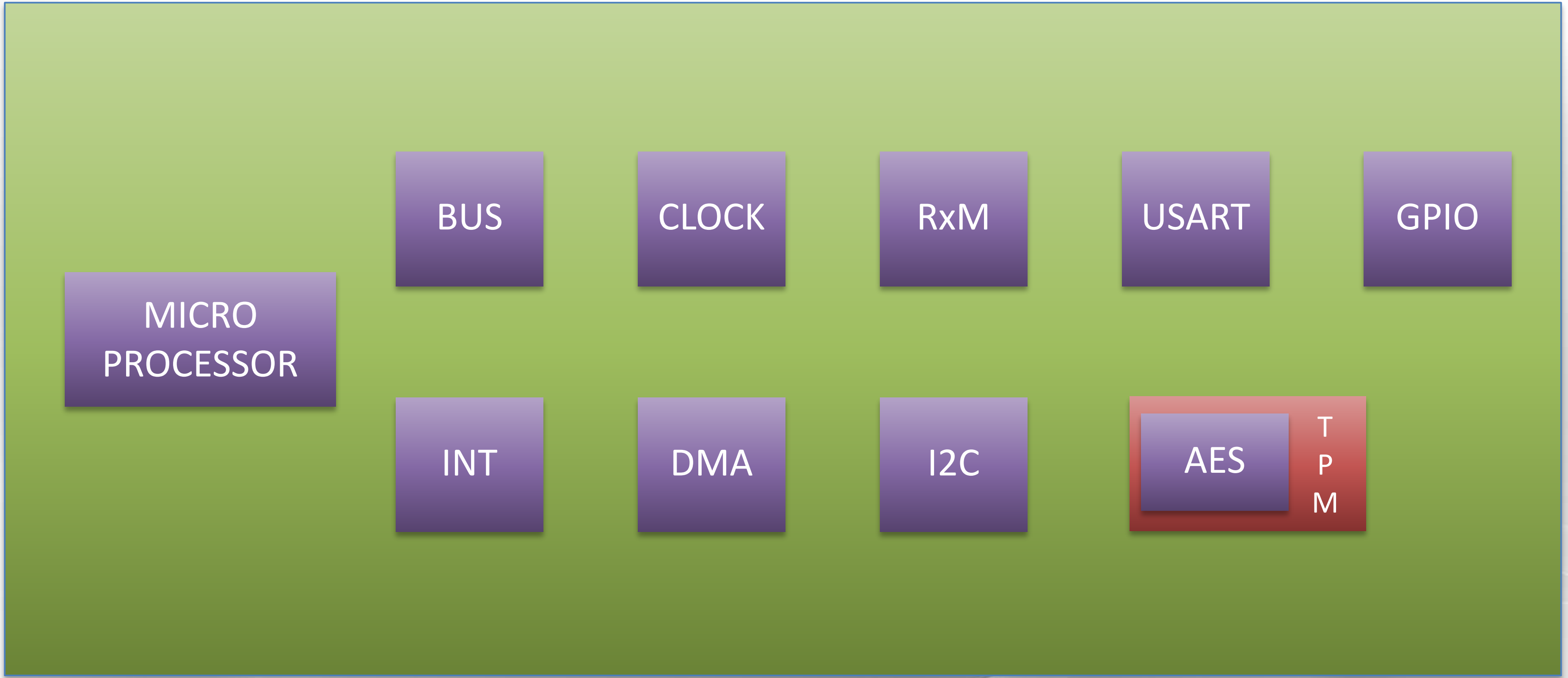
# “The Tiniest TPM”

- RTS
  - TPM2_PCR_Extend
  - TPM2_PCR_Read
- RTR
  - TPM2_Quote
- Need lightweight hashing and symmetric signing
- Would LOVE to have lightweight <u>asym</u> signing

# MARS activities

- Use Cases
  - Identity
  - Integrity measuring, storing, reporting
  - Seal, Unseal
- Profile
  - Requirements to construct MARS
- Provisioning, rekeying, zeroizing, …

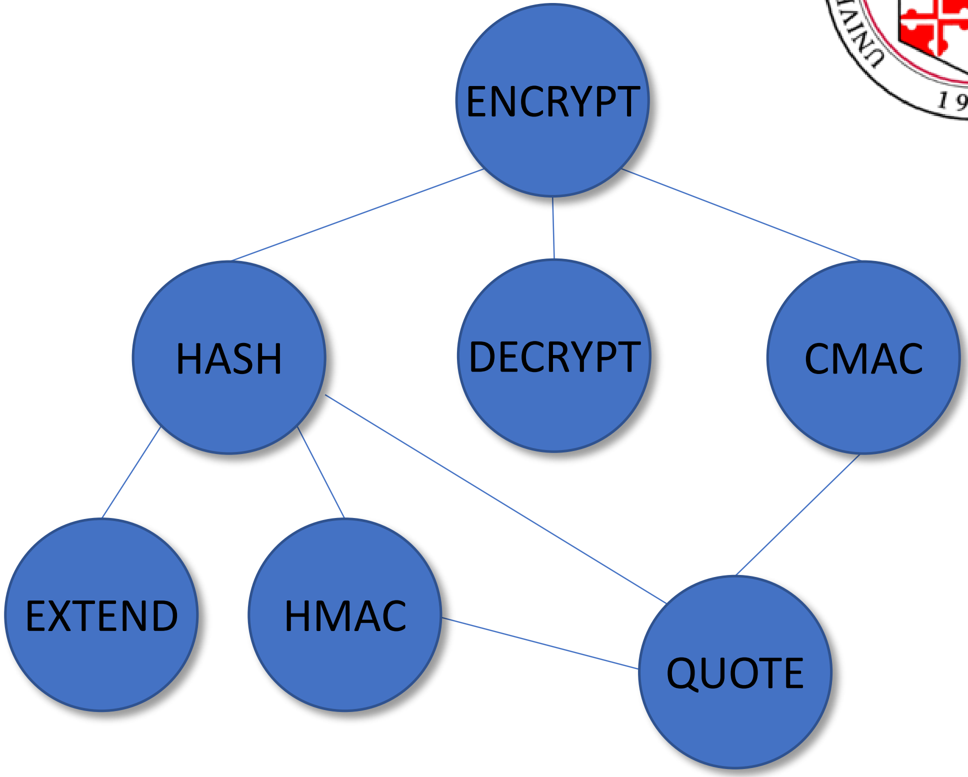
# MICRO-CONTROLLER (SoC?)



# Research w/ UMBC

- FPGA Prototype
- Project Radicle
- ARM + RoT
- Encrypt = Simon

- ASIC Prototype
- RISC-V + RoT



# Results

- Intel/Altera Cyclone V FPGA resources
  - Adaptive Logic Modules (ALM)
  - Block Memory Bits (BMB)

| APPROACH | ENGINE | CORE | WRAPPER | TOTAL |
|---|---|---|---|---|
| CONVENTIONAL | SHA-256 | 1009\ 384 | 256\0 | 1265\ 384 |
| | AES-256 | 648\75776 | 186\0 | 834\75776 |
| | Total | 1657\76160 | 442\0 | 2099\76160 |
| OPTIMIZED | Simon | 106\ 0 | 165\0 | 271\ 0 |

ALM\BMB Consumption of Conventional and Optimized Prototypes

# Acknowledgments

*Thanks to the Laboratory for Advanced Cybersecurity Research in the National Security Agency's Research Directorate who sponsored this work.*

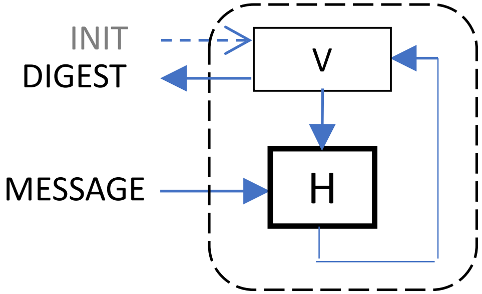
# Thanks!

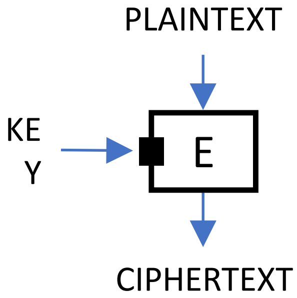
# Q & A

mars-chair@trustedcomputinggroup.org

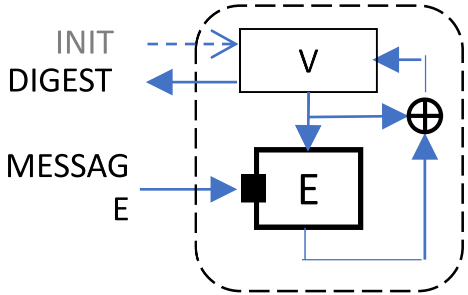
# Hash Methods

## CONVENTIONAL




## OPTIMIZED



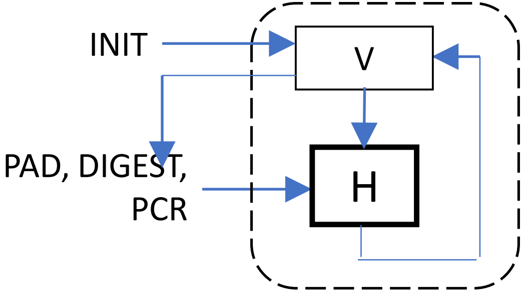

- $V_i = E_{M_i}(V_{i-1}) \oplus V_{i-1}$
- Davies–Meyer Compression
- SHA-3 Semi-finalists
  - SHAvite-3
  - SIMD

# EXTEND Methods

## CONVENTIONAL

$PCR_i = H(\ldots H( H(0 \,||\, D_1) \,||\, D_2) \ldots \,||\, D_i)$

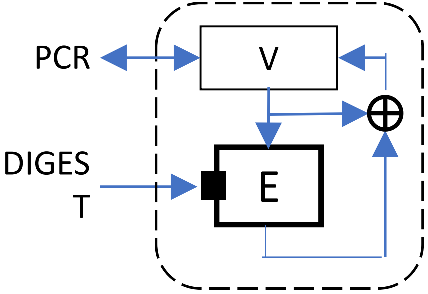
$PCR_i = H(PCR_{i-1} \,||\, D_i)$

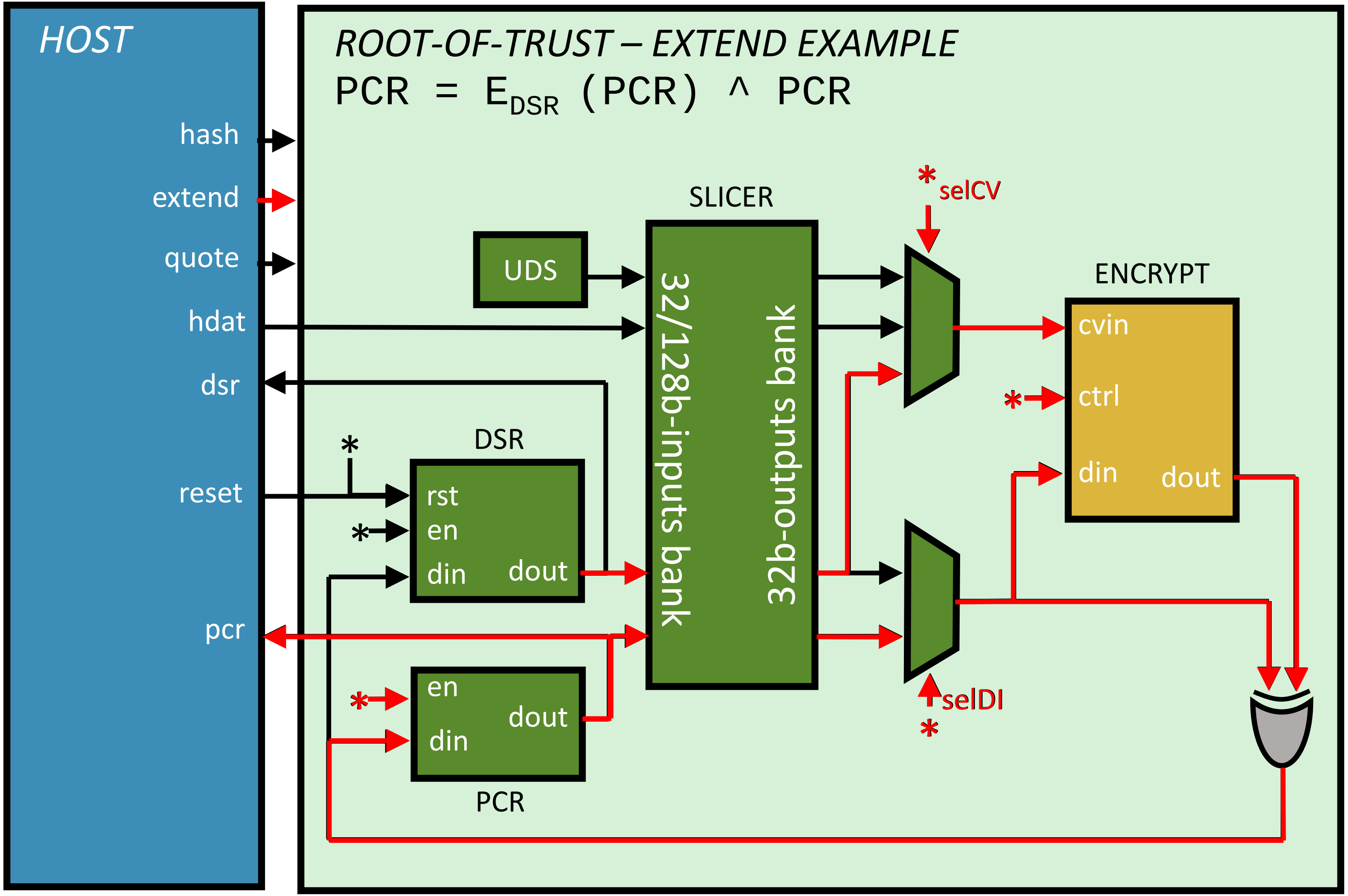



## OPTIMIZED

$PCR_i = H(D_1 \,||\, D_2 \ldots \,||\, D_i)$

- Eliminates redundant hash initializations and padding
- "digest of digests"
- Simplified state machine




HOST
hash
extend
quote
hdat
dsr
reset
pcr
ROOT-OF-TRUST – EXTEND EXAMPLE
PCR = E$_{DSR}$ (PCR) ^ PCR
SLICER
UDS
32/128b-inputs bank
32b-outputs bank
*selCV
ENCRYPT
cvin
ctrl
din
dout
DSR
rst
en
din
dout
*
selDI
en
dout
din
PCR