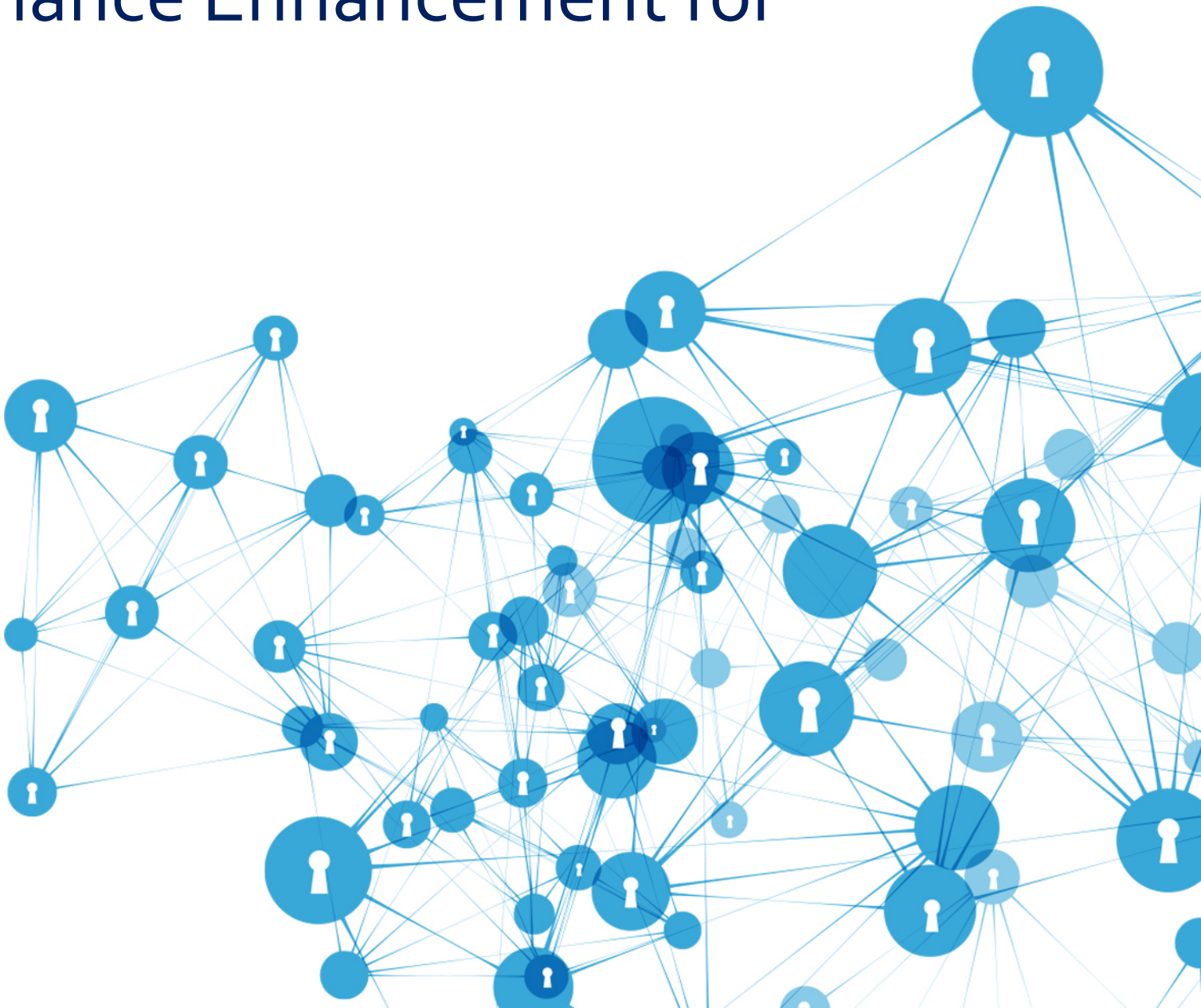
A Future-Proof Performance Enhancement for Secure MCUboot



embeddedworld
Exhibition&Conference
...it's a smarter world

Derek Atkins, Chief Technology Officer

SECURE RF
Securing the Internet of Things®

February 28, 2019

The IoT Has a Problem

FEB 21, 2018 @ 07:06 AM 2,783 The Little Black Book of Billionaire Secrets

Warning: 50,000 Mi-Cam Baby Monitors Can Be Spied On With Ease

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms.
FULL BIO

A Basic Z-Wave Hack Exposes Up To 100 Million Smart Home Devices

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms.
FULL BIO

PRIVACY AND SECURITY FANATIC
By Ms. Smith, CSO | MAY 8, 2018 7:37 AM PT

About
Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

NEWS

'I'm hacked' message left on dozens of defaced Canon IoT security cameras in Japan

If you don't at least change the default passwords for IoT devices, don't be surprised when it gets hacked.

Posted on June 1, 2018 at 3:52 PM

BMW'S WITH AN INTERNET CONNECTION IN DANGER OF BEING HACKED

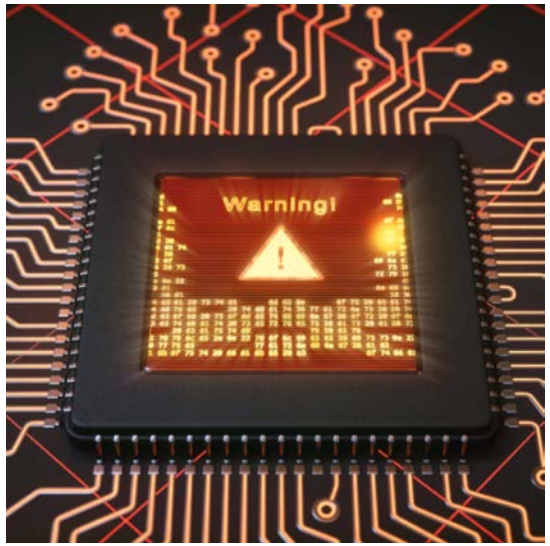
According to researchers, BMW vehicles with an internet connection seem to be in danger of being hacked. So far, up to 14 different vulnerabilities have been detected.

"Little or No Security"

SECURE RF
Securing the Internet of Things®

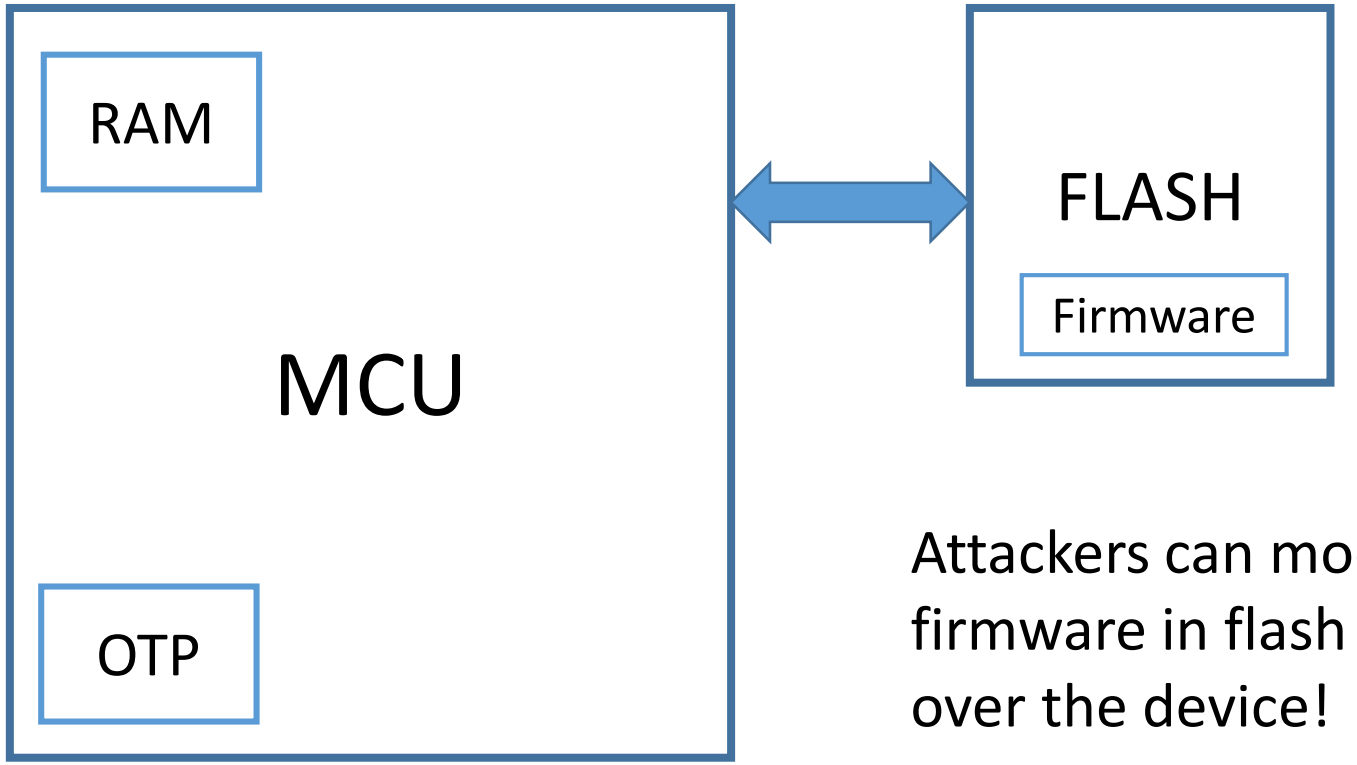
The IoT Has a Problem

- The small devices that power the IoT are insecure.
- These devices provide few, if any, options for authentication and data integrity.
- They lack the computing, memory, and/or energy resources needed to implement today's standard security methods.
- This leaves most IoT systems vulnerable to attack.



SECURE RF
Securing the Internet of Things®

Real-World Problem: Securing Device Firmware



Attackers can modify the firmware in flash and take over the device!

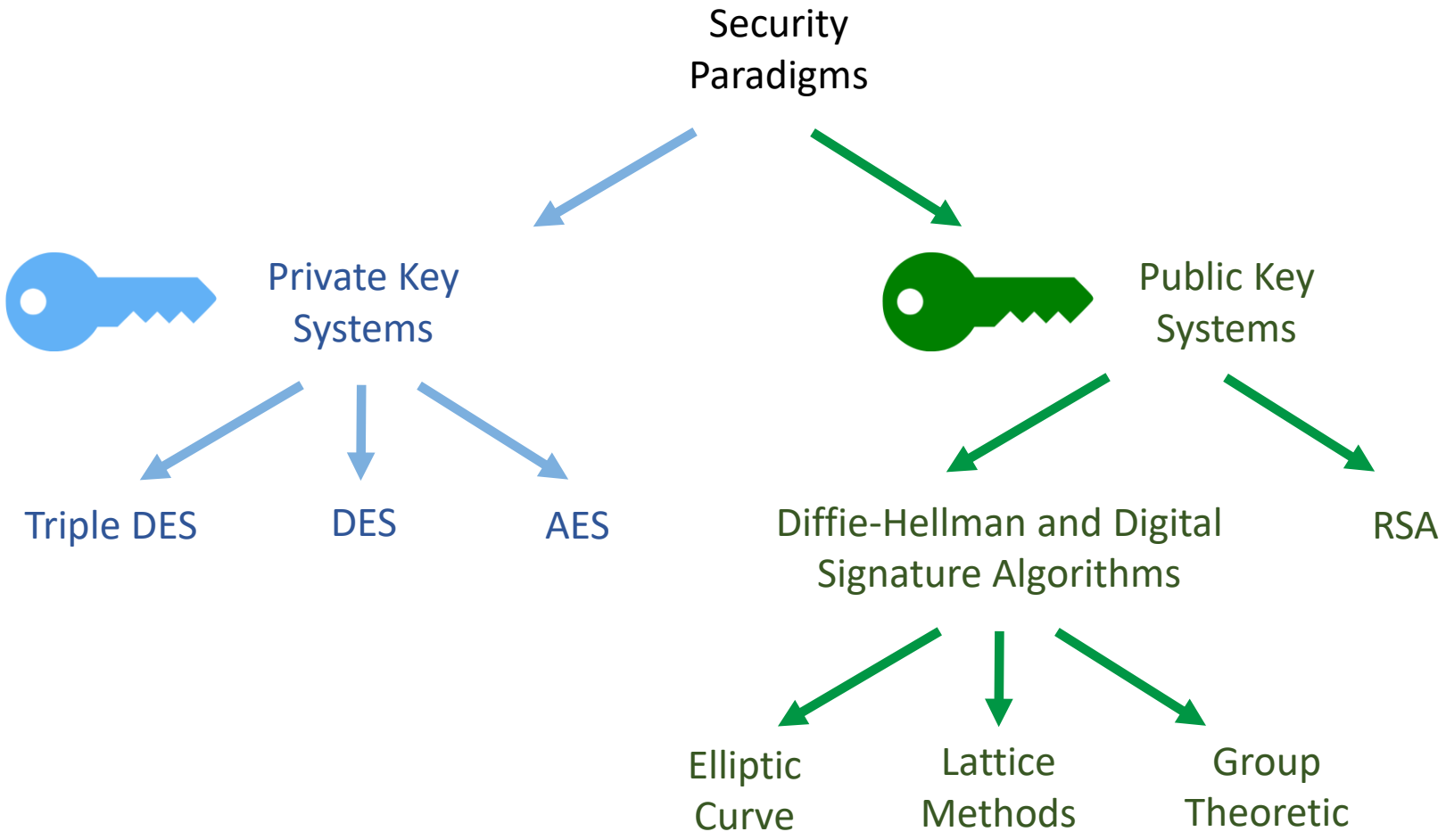
SECURE RF
Securing the Internet of Things®

Firmware Security Solution Architectures

- Do nothing
  - Be an Ostrich!
- Hashing
  - Too brittle (can’t update code)
- Symmetric Cipher / Message Authentication Codes (MAC)
  - Key management problem
- Public-Key Signature
  - Too slow!

SECURE RF
Securing the Internet of Things®

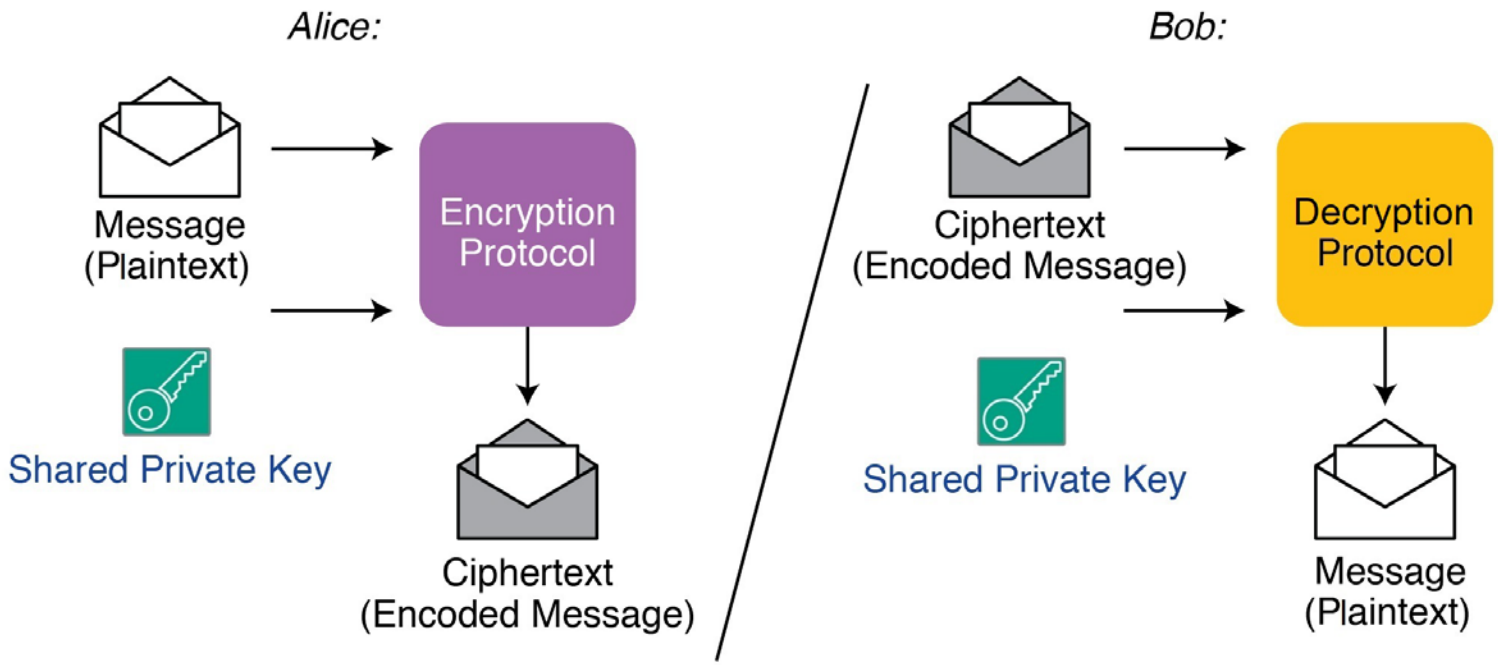
Cryptographic Taxonomy



SECURE RF
Securing the Internet of Things®

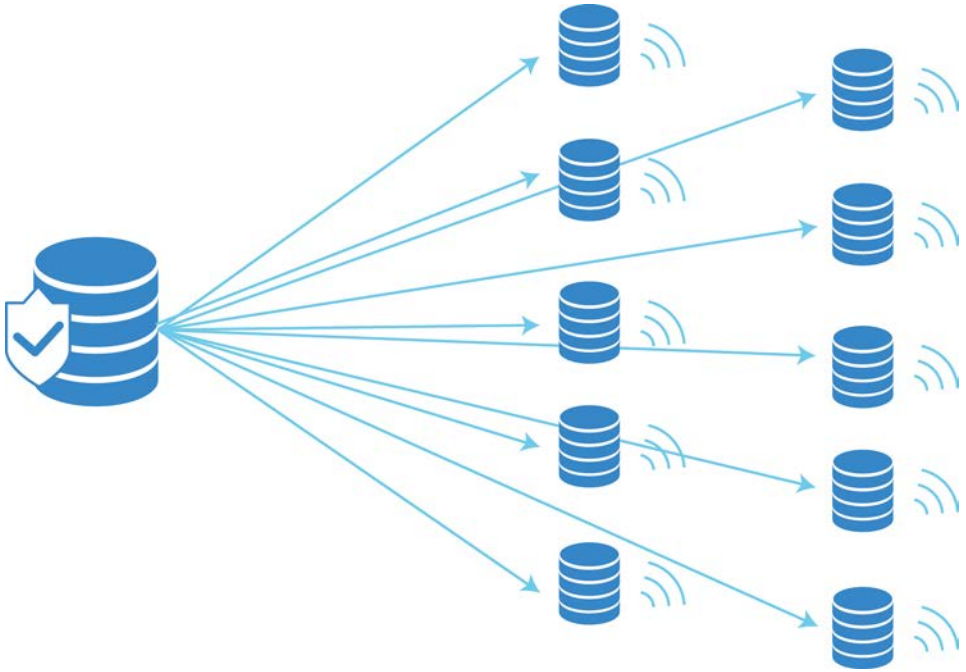
Symmetric Cryptography

- Symmetric methods have been around for millennia



SECURE RF
Securing the Internet of Things®

Key Management Challenge



Challenge:

- Securely distribute keys
- Secure all databases
- Single breach – System compromised

SECURE RF
Securing the Internet of Things®

Solution: Asymmetric (Public-Key) Cryptography

- Solves the key management problem
- Several methods to choose from:
  - RSA
  - Elliptic Curve (ECC)
  - Diffie-Hellman (DH)
  - Lattice Methods

SECURE RF
Securing the Internet of Things®

What's Wrong With Current Methods?

- ECC, RSA, and DH work fine on large systems (laptops, servers)
- Implementations are often too big for small devices
  - Sensors, actuators, IoT
- If they can be made to fit, they can take a long time to run.
  - Specifically, they each run in quadratic time.

SECURE RF
Securing the Internet of Things®

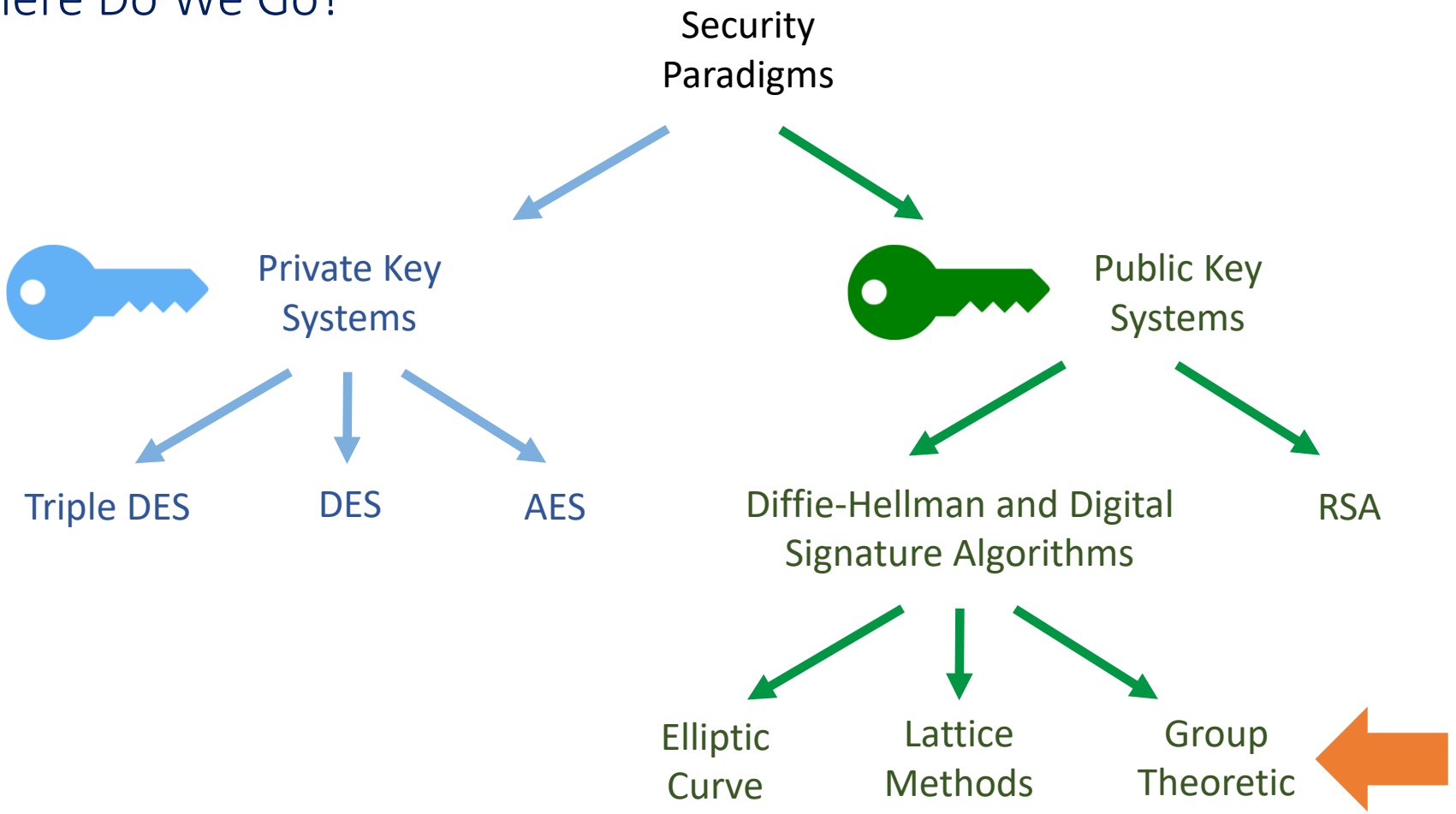
Why Is This Hard?

- Legacy systems like ECC, RSA, and DH multiply very large (256-4096 bits) numbers.
- This is even harder on 16- or even 8-bit processors!
- Reason: The complexity of breaking large numbers into 16- or 8-bit chunks and then piecing them all back together!

SECURE RF
Securing the Internet of Things®

Cryptographic Taxonomy

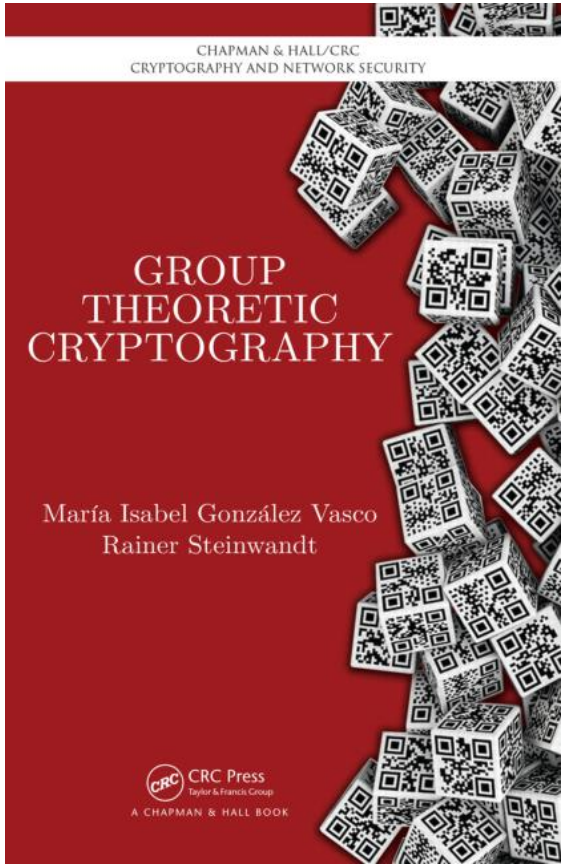
So Where Do We Go?



SECURE RF
Securing the Internet of Things®

Group Theoretic Cryptography

- Hard problem over 100 years old
- GTC studied since mid-1970s
  - Same timeframe as RSA and DH
- Calculates using small numbers (operands)
  - 8-32-bits vs 256-4096 in ECC, RSA, and DH
- Small, fast, and ultra-low-energy
- Leverages:
  - Structured groups
  - Matrices and permutations
  - Arithmetic over finite fields



SECURE RF
Securing the Internet of Things®

GTC Deconstructed

- Every public-key method is based on several math foundations.
  - GTC is no different.
- GTC leverages structured groups, matrices, permutations, and arithmetic over finite fields.
- The structures group used for GTC is the Braid Group.
- Note: there have been other uses of the Braid Group for cryptography (some of which have been broken). GTC is different than those.
- Note: not to be confused with “Braid Group Cryptography”

SECURE RF
Securing the Internet of Things®

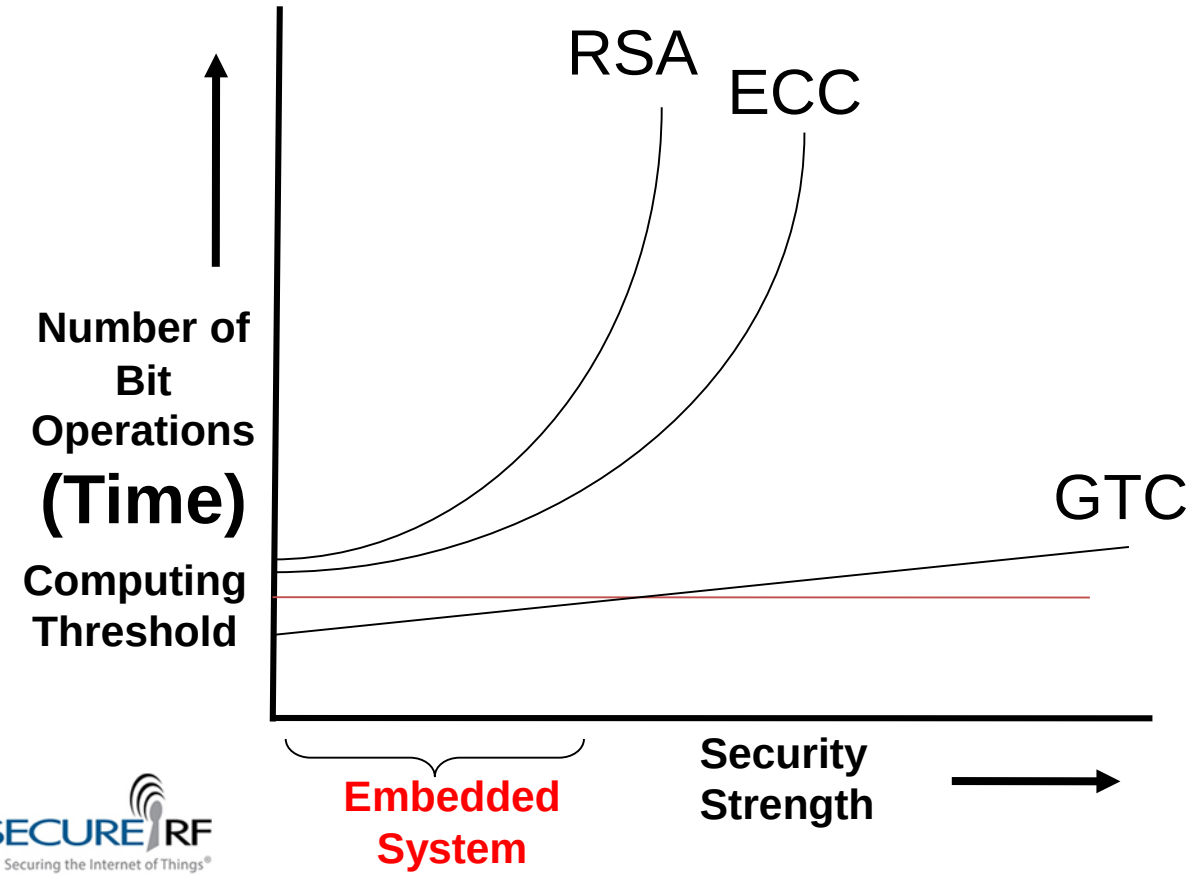
Our Breakthrough: *E*-Multiplication

- A Group-Theoretic, One-Way Function designed for low-resource/constrained environments
- First published in 2005, subject to significant analysis and never broken
- Quantum-resistant to all known attacks
- Runtime grows *linearly* with increase in security level
- Rapidly computable (due to a sparse matrix)
  - Requires *n* multiplies and *2n* additions, which can be completed in a single clock cycle in lightweight hardware
- Building block for our cryptographic methods

SECURE RF
Securing the Internet of Things®

E-Multiplication: The Basis of GTC

E-*Multiplication (published in 2005), SecureRF's cryptography building block, is based on GTC to deliver size, speed, and power breakthroughs*

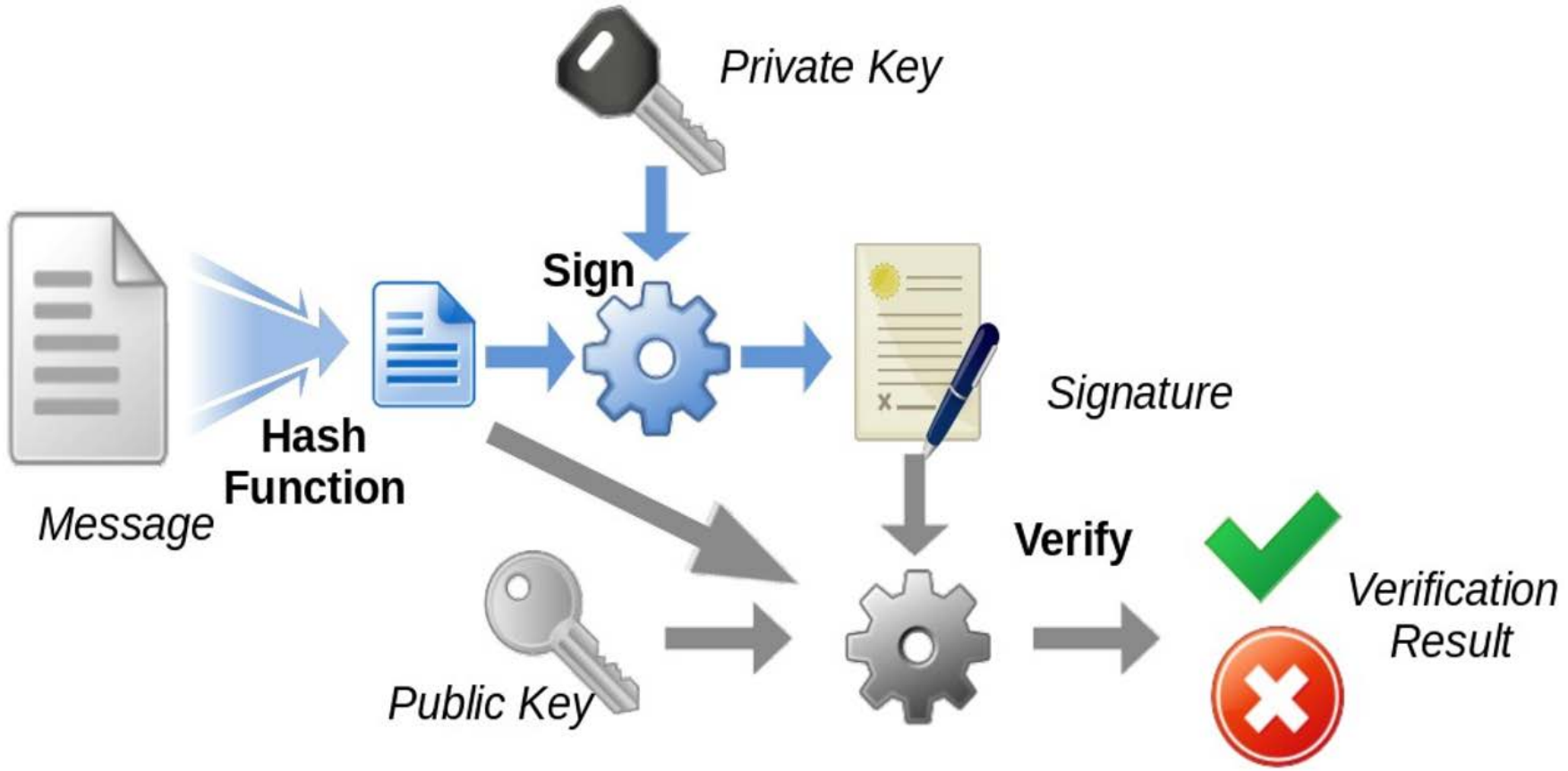


Group Theoretic Cryptography (GTC)

- Hard problem over 100 years old
- GTC studied since mid-1970s
- Calculates using small numbers
  - 8-32-bits vs 256-4096 in ECC, RSA, DH
- Small, fast, and ultra-low-energy
- Leverages:
  - Structured groups
  - Matrices and permutations
  - Arithmetic over finite fields

SECURE RF
Securing the Internet of Things®

Walnut Digital Signature Algorithm Process



Quantum Resistant: Future-Proof Now

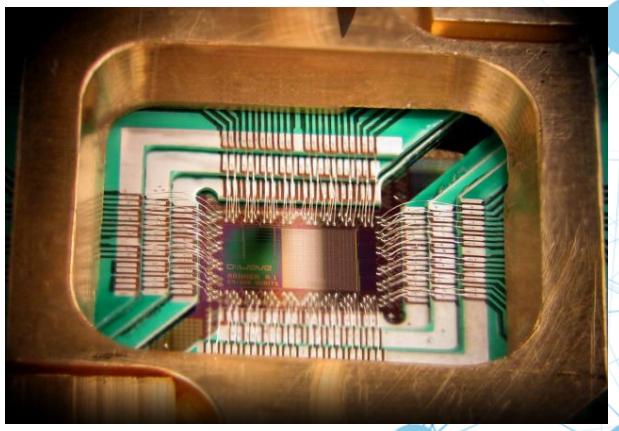
SecureRF's methods are quantum-resistant to all known attacks

"The National Security Agency is advising US agencies and businesses to prepare for a time in the not-too-distant future when the cryptography protecting virtually all e-mail, medical and financial records, and online transactions is rendered obsolete by quantum computing."

Source: Ars Technica, August 21, 2015

"…We must begin now to prepare our information security systems to be able to resist quantum computing."

Source: NIST Report on Post-Quantum Cryptography February 2016



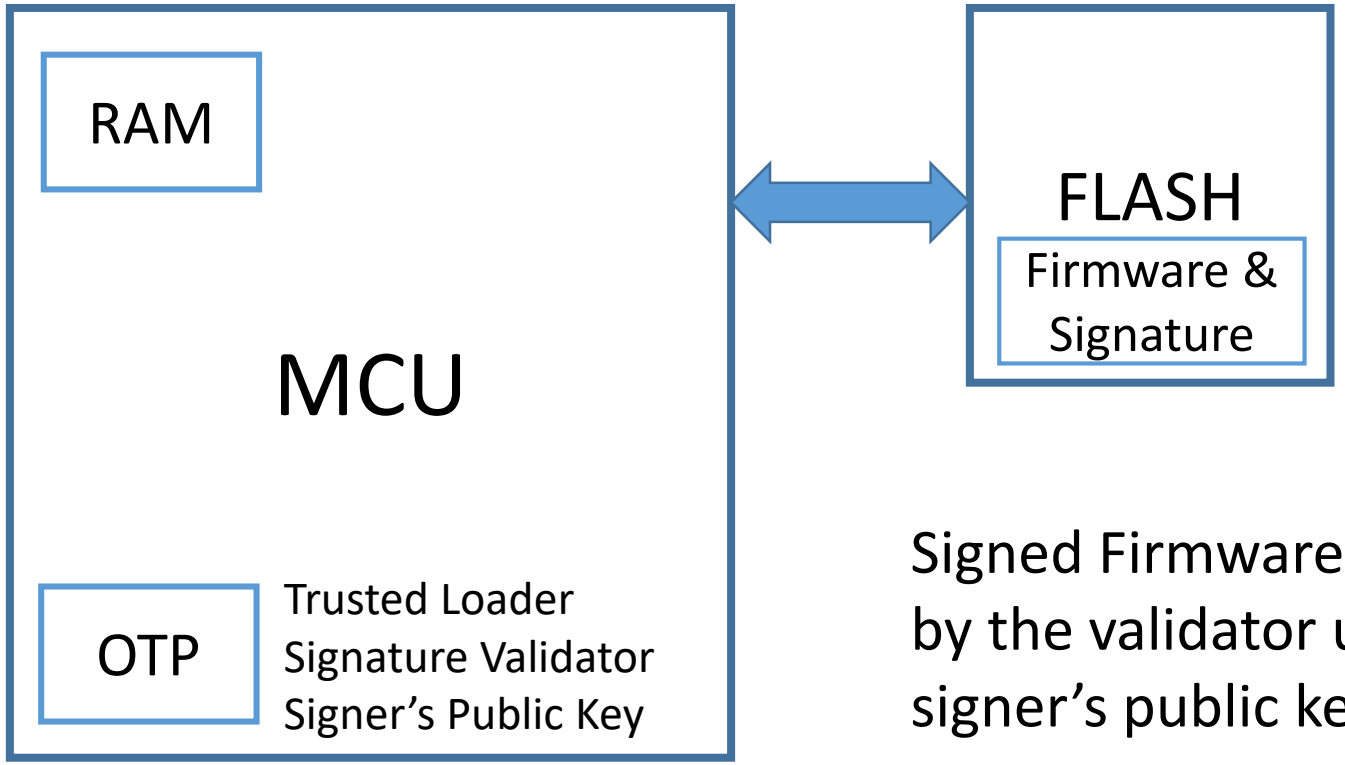
D-Wave System Chip with quantum Properties

SECURE RF
Securing the Internet of Things®

Quantum Resistance

- Two important quantum methods: Shor's Algorithm and Grover's Search Algorithm
- Grover's Search Algorithm reduces the security level (e.g., AES-128 becomes 64-bit secure)
  - Doubling the security of GTC requires doubling the key size which only doubles the runtime
- Shor: Breaks ECC, RSA, and DH by quickly factoring or solving the discrete log problem
  - Requires the method's math be Finite, Cyclic, and Commutative
  - GTC is neither Cyclic nor Commutative, and the underlying group is Infinite, so Shor does not apply

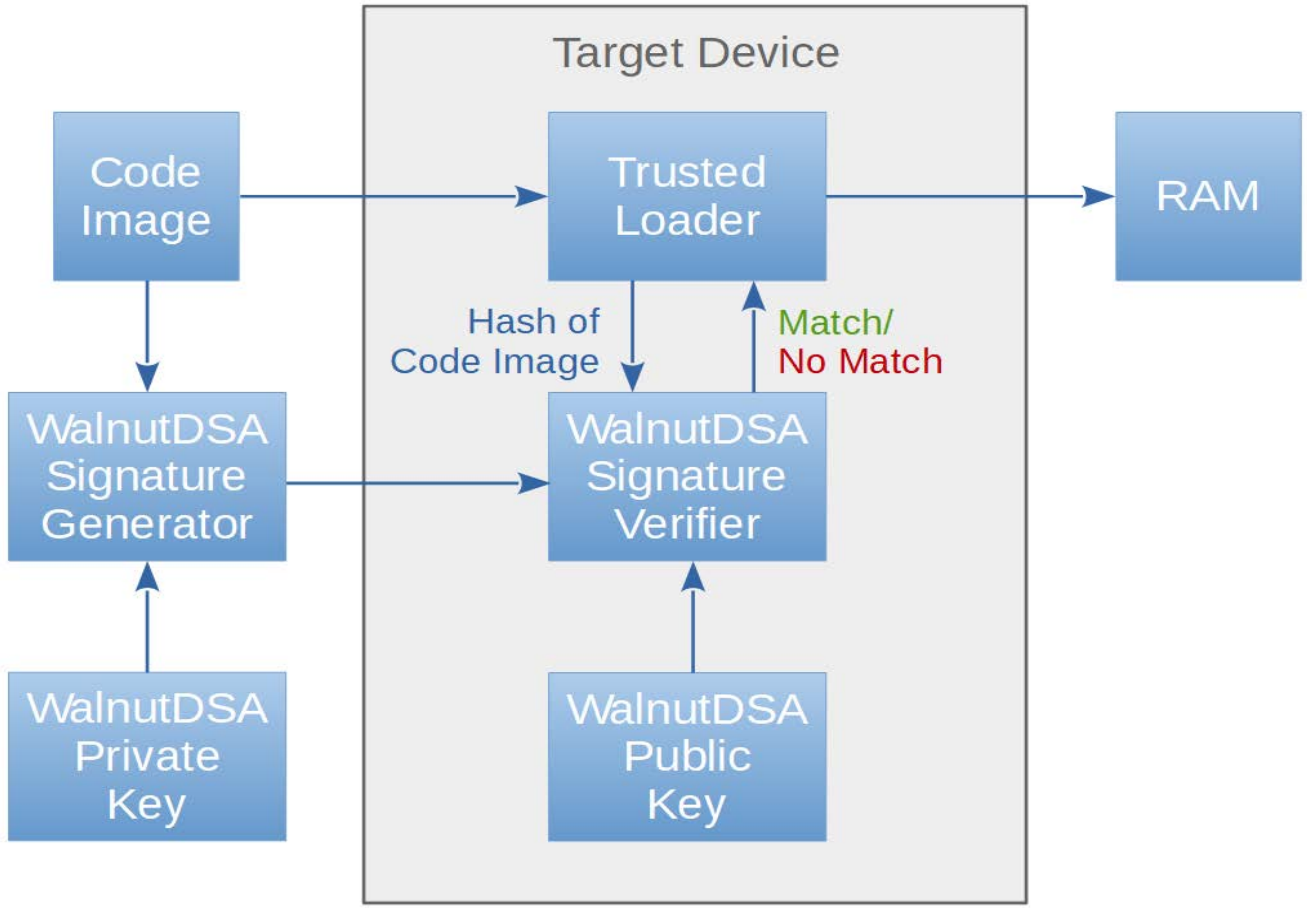
Securing Device Firmware



Signed Firmware is checked by the validator using the signer's public key.

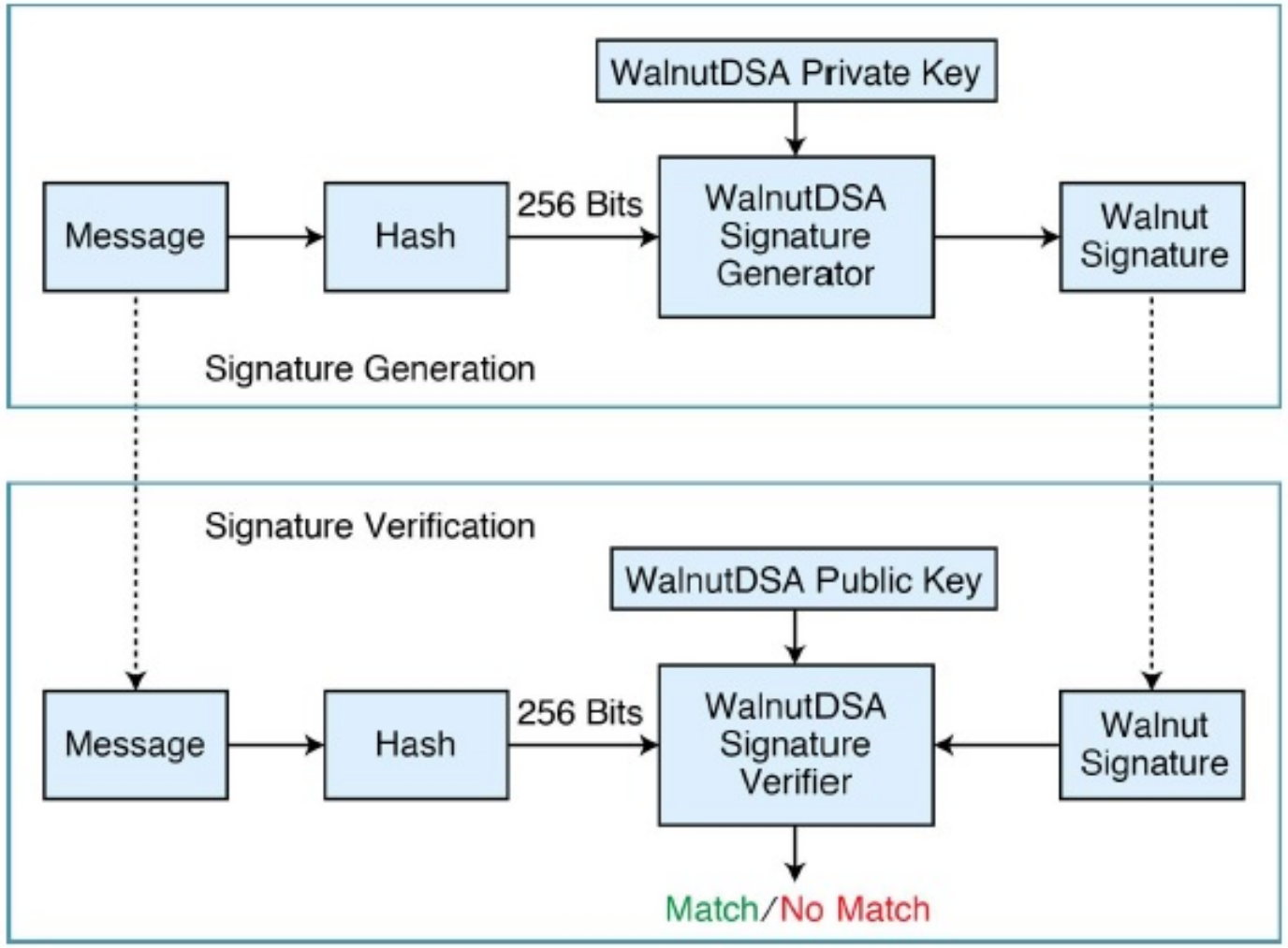
SECURE RF
Securing the Internet of Things®

Our Secure Boot Architecture



SECURE RF
Securing the Internet of Things®

WalnutDSA in Practice



SECURE RF
Securing the Internet of Things®

Integrating WalnutDSA into MCUboot

- MCUboot comes with TinyCrypt ECDSA
- We added support for WalnutDSA

- WalnutDSA ROM: 1,852 Bytes
- ECDSA ROM: 6,062 Bytes

- Code size went down by over 4KB with WalnutDSA!

SECURE RF
Securing the Internet of Things®

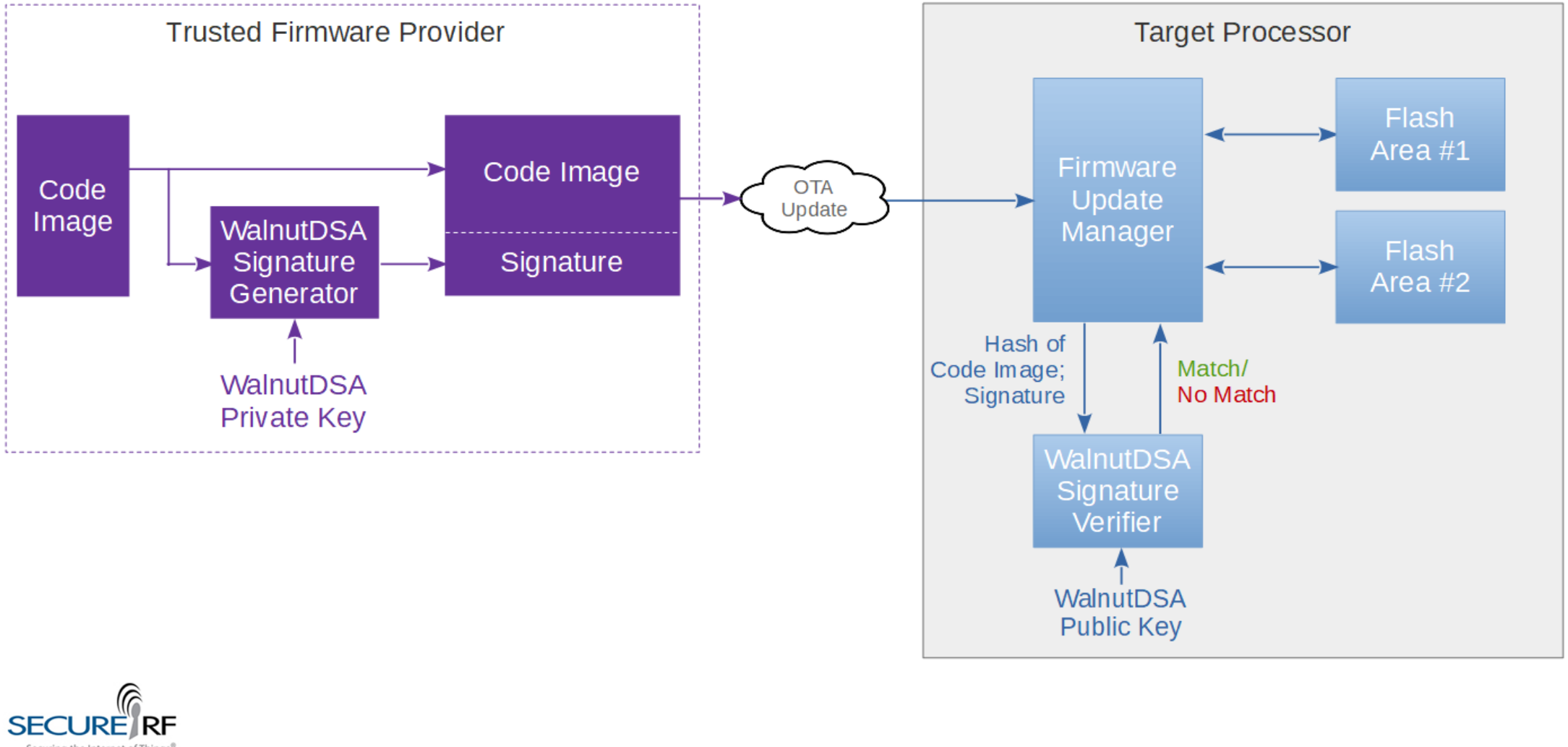
WalnutDSA + MCUboot Performance

- Instrumented code to obtain boot-time cycle counts:
  - ECDSA: 15,884,979 cycles
  - WalnutDSA: 634,224 cycles (25x faster!)

- Faster, Smaller, **and** quantum-resistant!

SECURE RF
Securing the Internet of Things®

Secure Firmware Boot/Update Ecosystem



SECURE RF
Securing the Internet of Things®

How you can use WalnutDSA with MCUboot

A. Configure Mynewt
   1. Add mcuboot repository to your project.yml file
   2. Update your bootloader's pkg.yml to add MCUboot as a dependency
   3. Create a new target for the bootloader targeting MCUboot
   4. Add syscfg variable BOOTUTIL_SIGN_WALNUT to syscfg.yml

B. Add WalnutDSA public key to MCUboot
   1. Define a new Mynewt package for exporting WalnutDSA public key
   2. Replace ECDSA public key in image_sign_pub.c with WalnutDSA key

C. Alter MCUboot to detect & verify WalnutDSA signatures
   1. Introduce WalnutDSA verification code
   2. Add BOOTUTIL_SIGN_WALNUT preprocessor definitions

(see *A Future-Proof Performance Enhancement for Secure MCUboot* for more details)

SECURE RF
Securing the Internet of Things®

IoT Embedded SDKs

- Available for your development and assessment:
  - IoT embedded SDKs for a wide range of 8-, 16-, and 32-bit processors
  - Android SDK
  - Windows SDK
  - Linux SDK
  - iOS SDK
- Request your SDK: info@securerf.com
- More information: www.securerf.com/products/security-tool-kits/

SECURE RF
Securing the Internet of Things®

Any Questions?

SecureRF Corporation

Company Headquarters
100 Beard Sawmill Road, Suite 300
Shelton, CT 06484 USA
1-203-227-3151
info@securerf.com

California Office
75 East Santa Clara, Floor 6
San Jose, CA 95113 USA
1-203-227-3151
info@securerf.com

SECURE RF
Securing the Internet of Things®