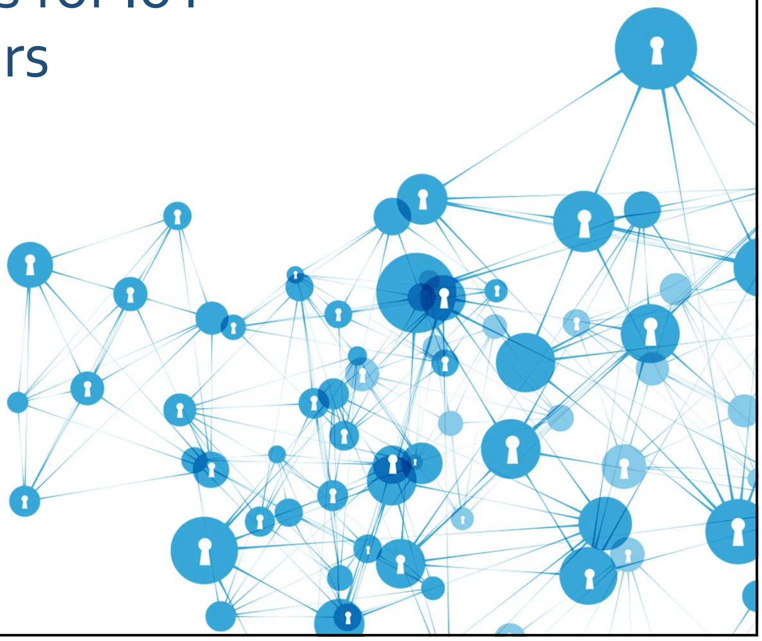
Security Essentials for IoT Product Developers

Intel Global
IoT DevFest 2017

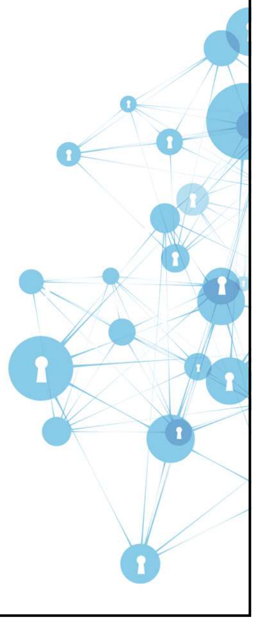


Louis Parks, CEO
LParks@SecureRF.com

Derek Atkins, CTO
Datkins@SecureRF.com

SECURE RF
Securing the Internet of Things®

Authentication and Data Protection For the "Smallest" Internet of Things



"Innovation Award: Best Contribution to IoT Security"
ARM TechCon 2017

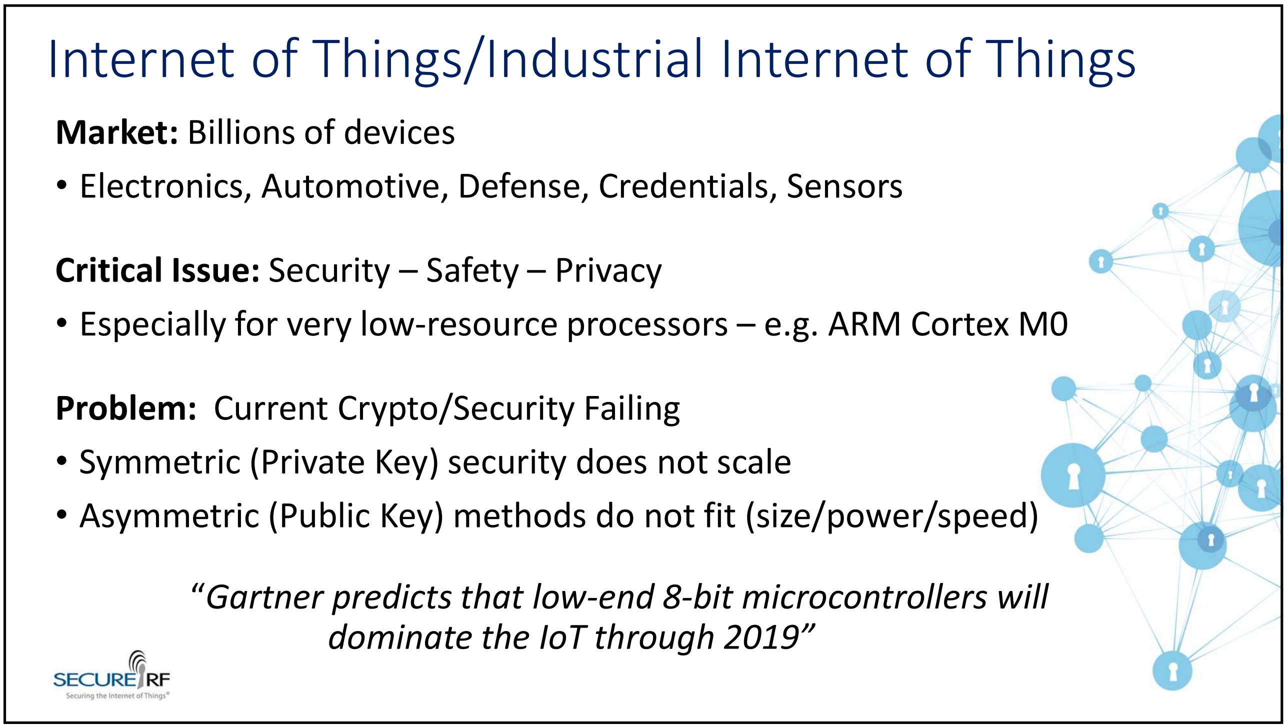
"Cybersecurity 500 World's hottest and most innovative"
Cybersecurity Ventures, Q2 2017

"Cool Vendors in Mobile Security and IoT Security, 2015"
Gartner, Inc.

"10 Most Influential Internet of Things Companies"
Forbes Article/Appinions Survey July 8, 2014

"Top 16 Emerging U.S. Cybersecurity Companies"
SINET 16 2014

SECURE RF
Securing the Internet of Things®



Internet of Things/Industrial Internet of Things

Market: Billions of devices

- Electronics, Automotive, Defense, Credentials, Sensors

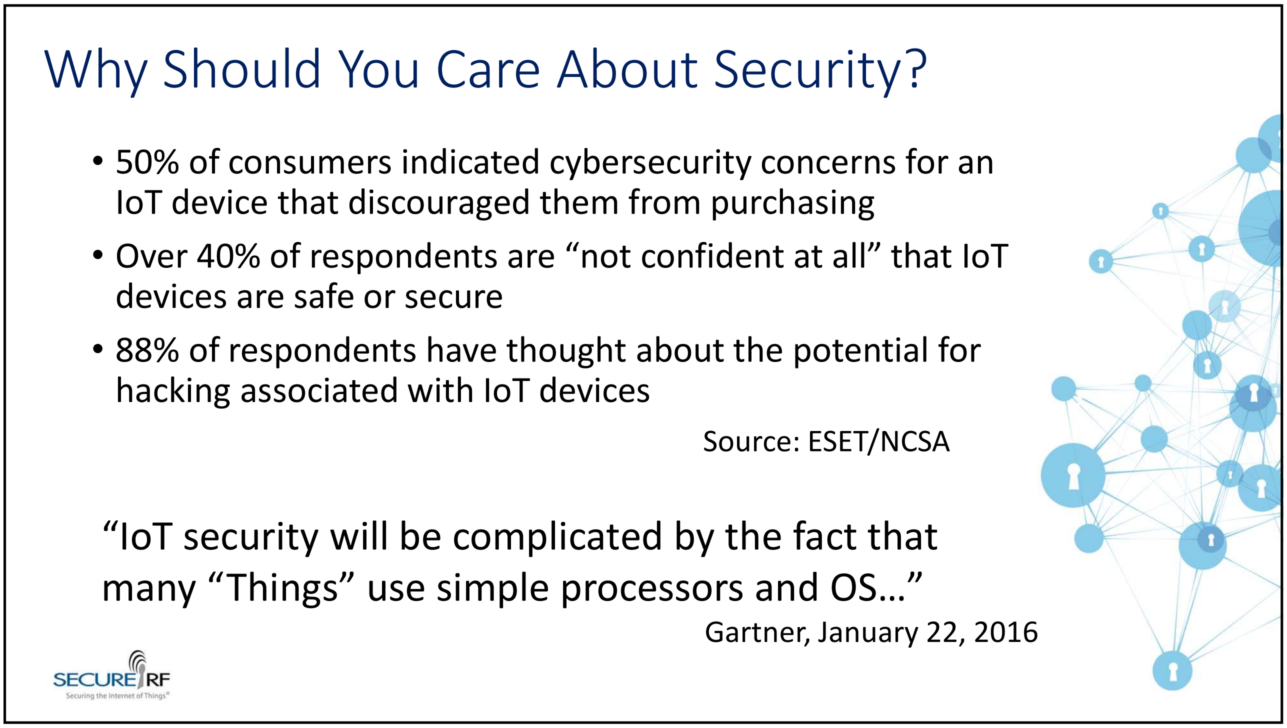
Critical Issue: Security – Safety – Privacy

- Especially for very low-resource processors – e.g. ARM Cortex M0

Problem: Current Crypto/Security Failing

- Symmetric (Private Key) security does not scale
- Asymmetric (Public Key) methods do not fit (size/power/speed)

"Gartner predicts that low-end 8-bit microcontrollers will dominate the IoT through 2019"



Why Should You Care About Security?

- 50% of consumers indicated cybersecurity concerns for an IoT device that discouraged them from purchasing
- Over 40% of respondents are "not confident at all" that IoT devices are safe or secure
- 88% of respondents have thought about the potential for hacking associated with IoT devices

Source: ESET/NCSA

"IoT security will be complicated by the fact that many "Things" use simple processors and OS…"

Gartner, January 22, 2016

How Bad is it?

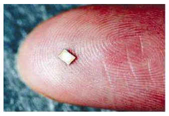
- LG Hom-Bot robotic vacuum
- Over 1 million in market
- Hack of LG SmartThinq App
- Remotely control and access video

- UBTech Home Assistant Robot
- No authentication on updates
- Able to remotely update firmware
- Create "Killer" and surveillance robots

Why is Securing the IoT so hard...

"...good security tools developed over the last 45 years won't fit into the hardware that's (now) available..."

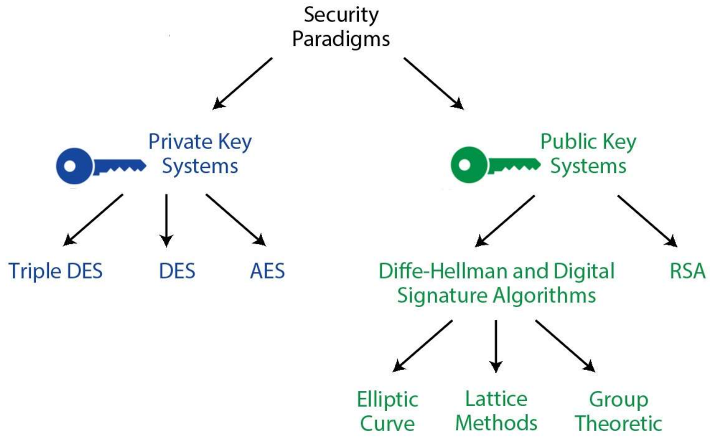
Burt Kaliski
Founding Scientist RSA Laboratories
Director, EMC Innovations Network



Challenges in Securing IoT

- Little or no power
- Small computing platform
- Time to compute
- No common computing environment

Cryptographic Taxonomy



Security Paradigms

Private Key Systems

Triple DES

DES

AES

Public Key Systems

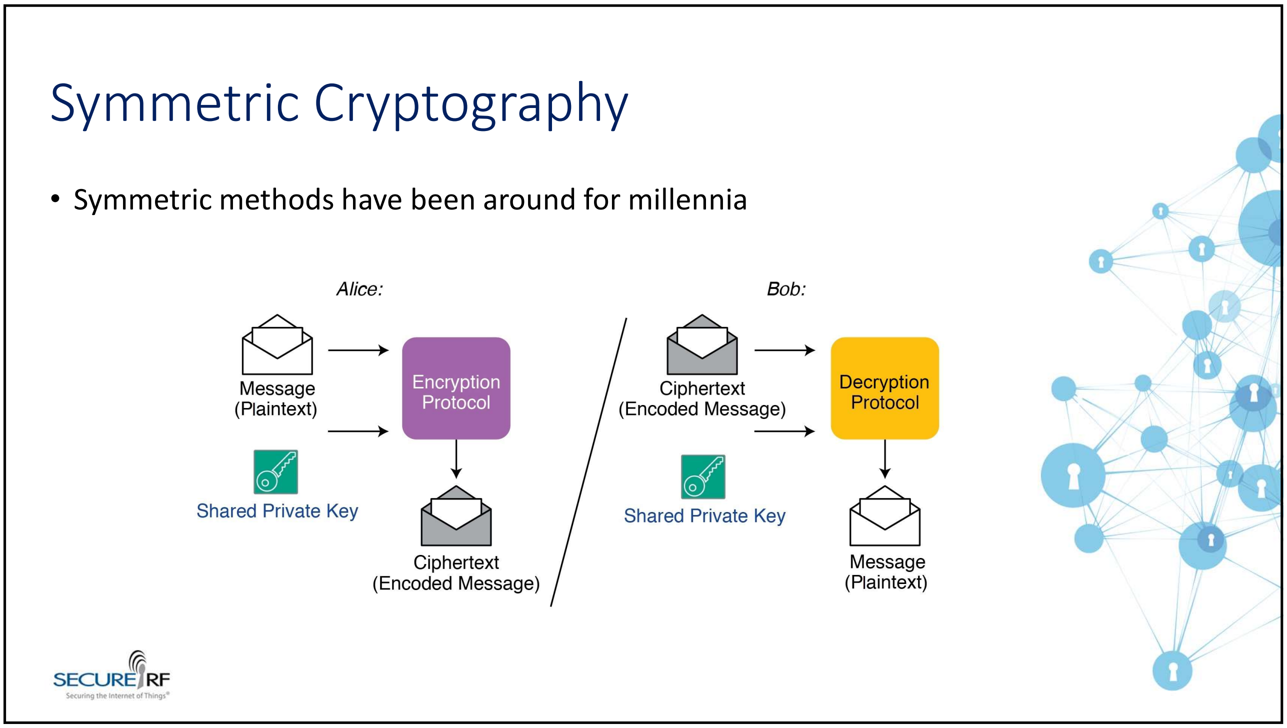
Diffe-Hellman and Digital Signature Algorithms

RSA

Elliptic Curve

Lattice Methods

Group Theoretic



Symmetric Cryptography

- Symmetric methods have been around for millennia

Alice:

Message
(Plaintext)

Encryption
Protocol

Shared Private Key

Ciphertext
(Encoded Message)

Bob:

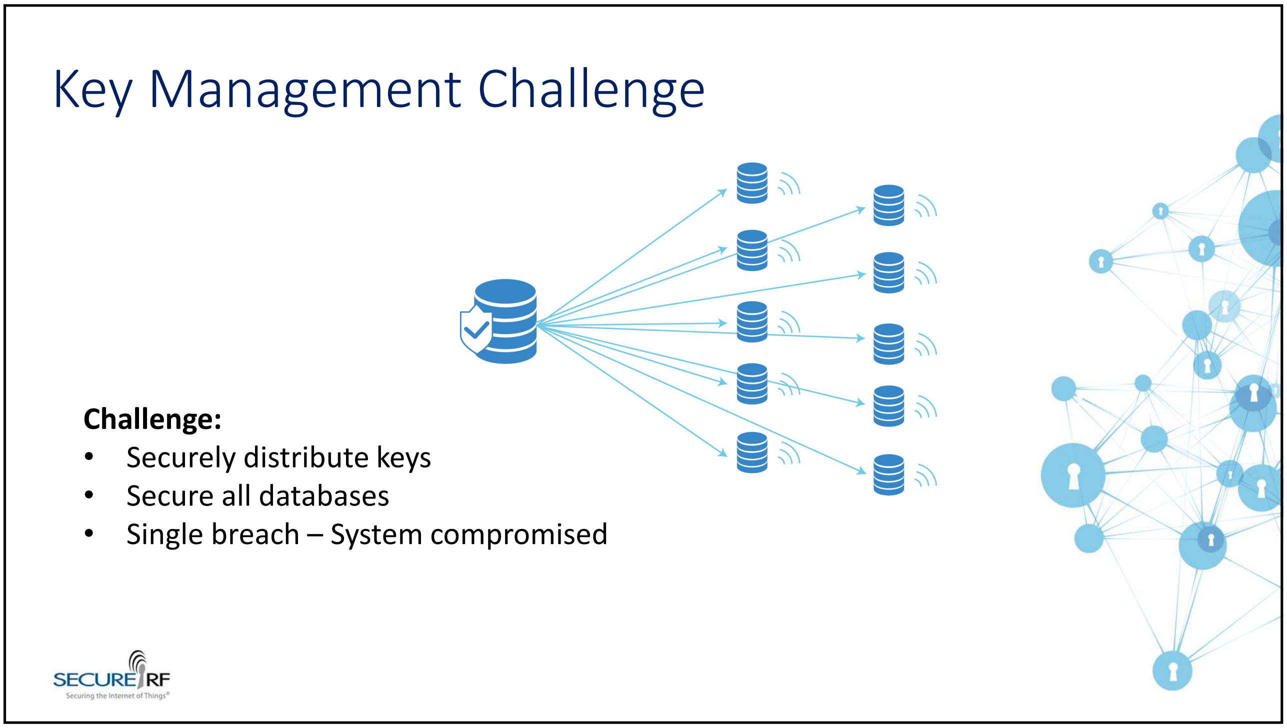
Ciphertext
(Encoded Message)

Decryption
Protocol

Shared Private Key

Message
(Plaintext)

SECURE RF
Securing the Internet of Things®



Key Management Challenge

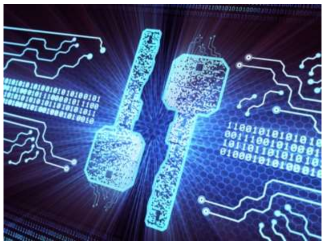
Challenge:

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

SECURE RF
Securing the Internet of Things®

Solution: Asymmetric Cryptography

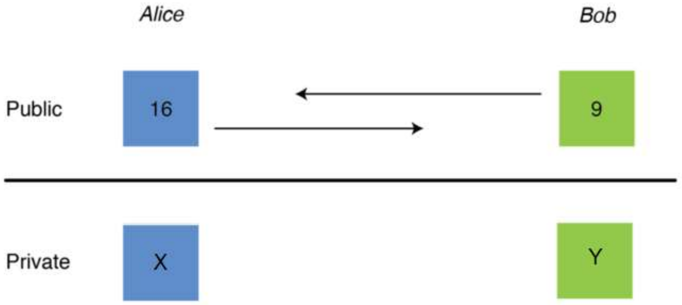
- Solves the key management problem
- Several methods to choose from:
  - RSA
  - Diffie-Hellman (DH)
  - Elliptic Curve (ECC)
  - Group Theoretic
  - Lattice Based



SECURE RF
Securing the Internet of Things®

Asymmetric Cryptography

Exchange Public Keys



SECURE RF
Securing the Internet of Things®

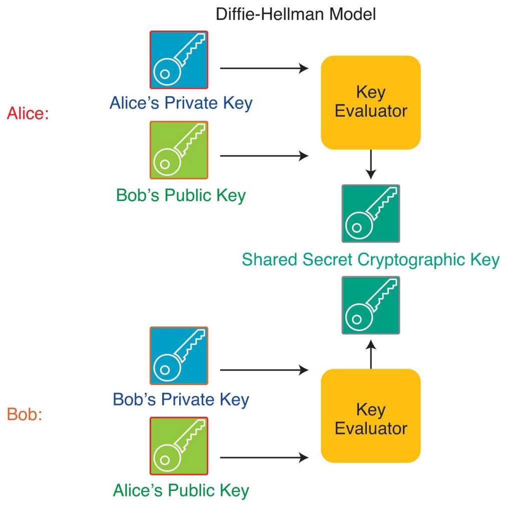
Asymmetric Cryptography

Calculate Shared Secret

	Alice		*Bob*	
Public	9		16	
Private	X	= 34#D82	Y	= 34#D82

SECURE RF
Securing the Internet of Things®

Asymmetric Cryptography



Diffie-Hellman Model

Alice:

Alice's Private Key

Bob's Public Key

Key Evaluator

Shared Secret Cryptographic Key

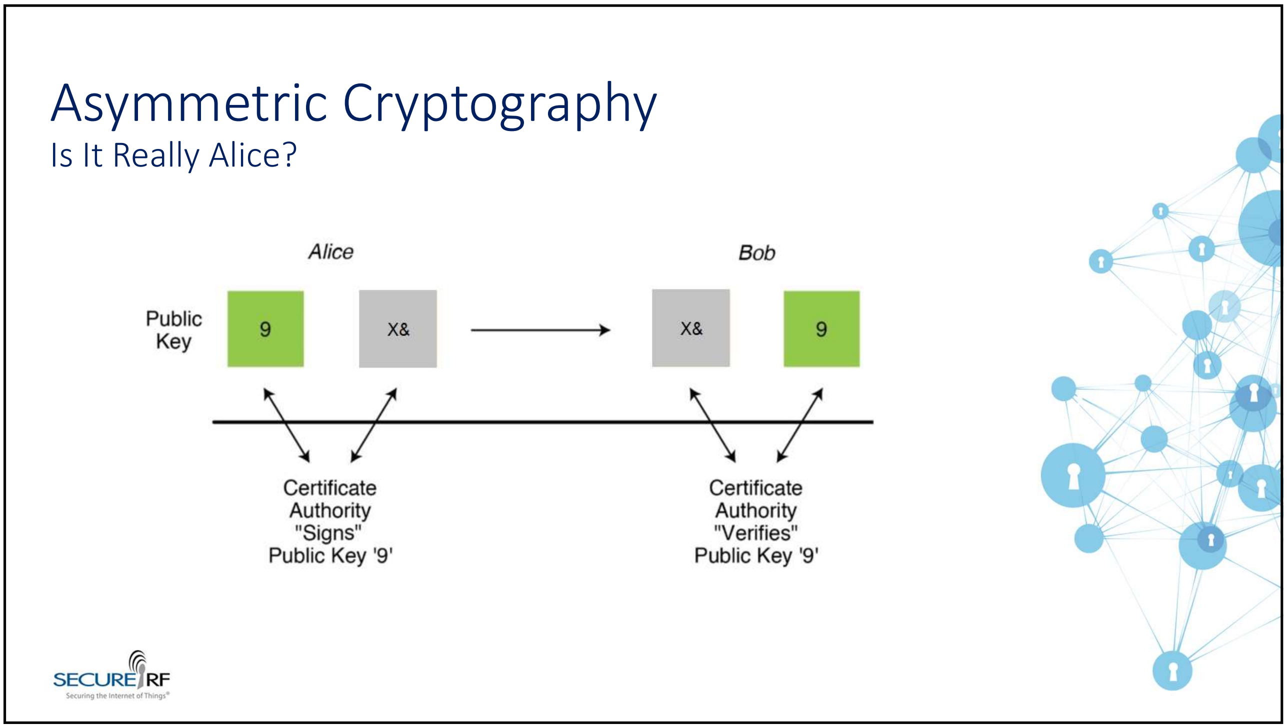
Bob:

Bob's Private Key

Alice's Public Key

Key Evaluator

SECURE RF
Securing the Internet of Things®



Asymmetric Cryptography

Is It Really Alice?

Alice

Bob

Public Key

9

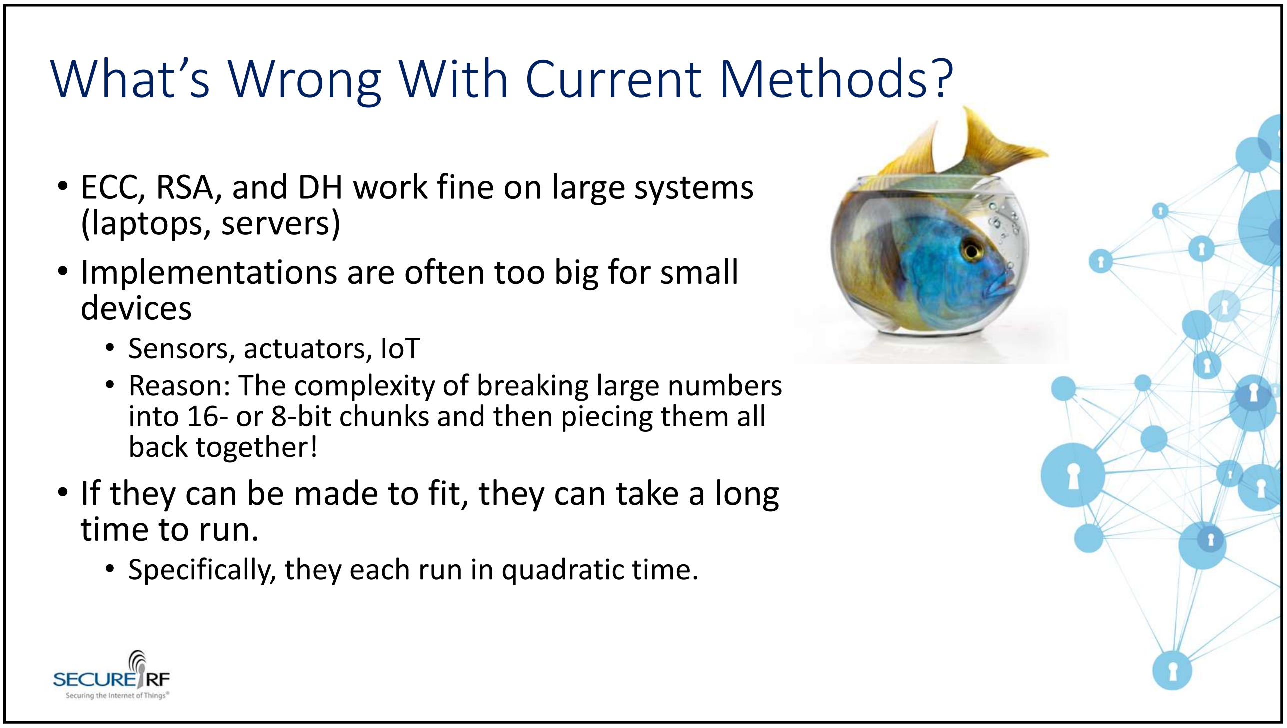
X&

X&

9

Certificate Authority "Signs" Public Key '9'

Certificate Authority "Verifies" Public Key '9'

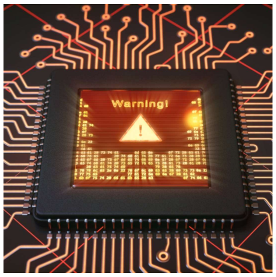


What's Wrong With Current Methods?

- ECC, RSA, and DH work fine on large systems (laptops, servers)
- Implementations are often too big for small devices
  - Sensors, actuators, IoT
  - Reason: The complexity of breaking large numbers into 16- or 8-bit chunks and then piecing them all back together!
- If they can be made to fit, they can take a long time to run.
  - Specifically, they each run in quadratic time.

Where does this leave IoT Device Security?

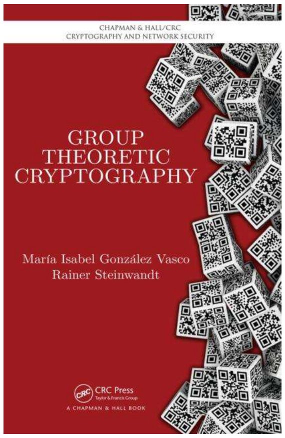
- Small devices that power the IoT are insecure
- These devices provide few, if any, options for authentication and data integrity
- They lack the computing, memory, and/or energy resources needed to implement today's standard security methods.
- Current IoT systems are vulnerable to attack



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-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


CHAPMAN & HALL/CRC
CRYPTOGRAPHY AND NETWORK SECURITY

GROUP
THEORETIC
CRYPTOGRAPHY

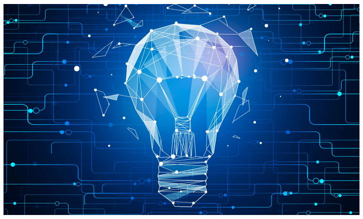
María Isabel González Vasco
Rainer Steinwandt

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

SECURE RF
Securing the Internet of Things®

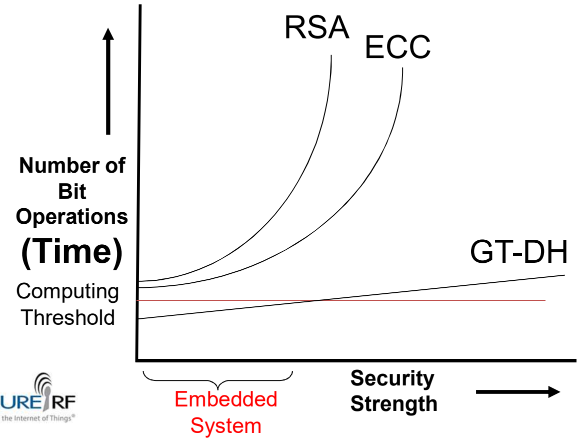
Our Breakthrough: *E*-Multiplication

- Group-Theoretic-based One-Way Function
- First published in 2005
- Designed for low-resource/constrained environments
- 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



Group Theoretic Cryptography

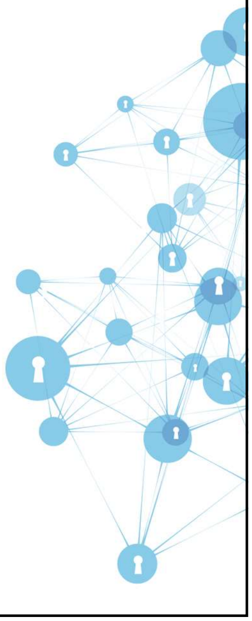
SecureRF ***Group Theoretic Diffie-Hellman (GT-DH)*** *delivers breakthrough size, speed, and power performance over Number Theoretic methods*



- Diffie-Hellman type method
- Based on Infinite Groups
- Platform Agnostic
- “Linear-in-Time” Security Strength
- Safe against known Quantum Attacks

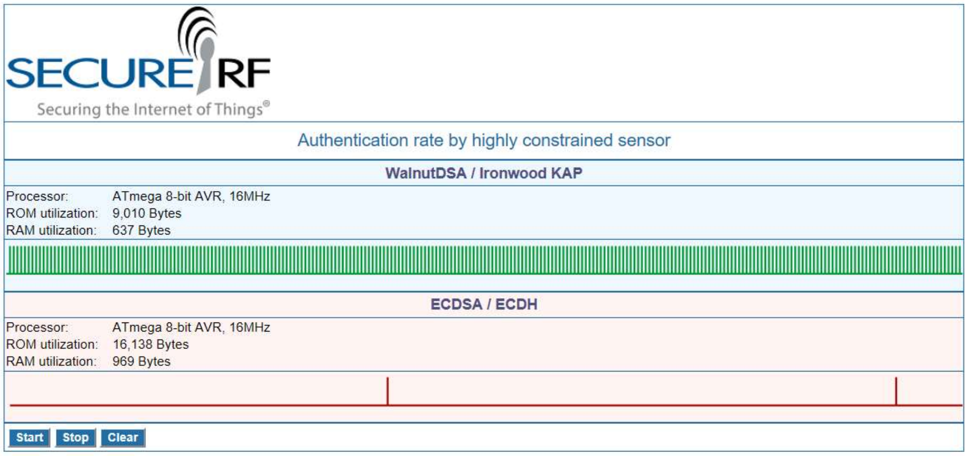
SecureRF Cryptographic Constructions

- All constructions are based on *E*-Multiplication and are quantum-resistant
  - Ironwood Key Agreement Protocol
  - Walnut Digital Signature Algorithm
  - Kayawood Key Agreement Protocol
  - Hickory Hash



SECURE RF
Securing the Internet of Things®

Performance: Authentication



SECURE RF
Securing the Internet of Things®

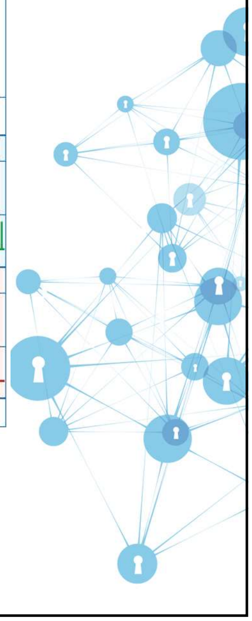
Authentication rate by highly constrained sensor

WalnutDSA / Ironwood KAP

Processor: ATmega 8-bit AVR, 16MHz
ROM utilization: 9,010 Bytes
RAM utilization: 637 Bytes

ECDSA / ECDH

Processor: ATmega 8-bit AVR, 16MHz
ROM utilization: 16,138 Bytes
RAM utilization: 969 Bytes



<u>ATmega 8-bit AVR, 16MHz:</u>

100x faster than ECC (0.068 s per authentication versus 7.69 s per authentication for ECC
This represents major energy savings and system simplification.

SECURE RF
Securing the Internet of Things®

Performance: WalnutDSA versus ECDSA

Security Level: 2^{128}

	WalnutDSA				ECDSA			
Platform	**Clock (MHz)**	**ROM (bytes)**	**RAM (bytes)**	**Time (ms)**	**ROM (bytes)**	**RAM (bytes)**	**Time (ms)**	**GAIN**
MSP430	8	3244	236	46	20-30K	2-5K	1,000 to 3,000	**21X to 63X**
8051	24.5	3370	312	35.3	N/A	N/A	N/A	**N/A**
ARM M3	48	2952	272	5.7	7168	540	233	**40.8X**
FPGA	50			0.05			2.08	**41.6x**

Quantum Resistant: Future-Proof Now

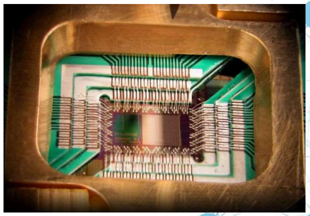
SecureRF's methods are quantum-resistant to all known attacks

"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

Quantum Resistance

- Two important quantum methods: Shor's Algorithm and Grover's Search Algorithm
- Grover's Search Algorithm reduces 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/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 - Shor does not apply

SECURE RF
Securing the Internet of Things®

Side Channel Attacks

- Types of attacks:
  - Differential Power Analysis
  - Glitching
  - Timing
- SecureRF has:
  - the tools to measure many side-channel attacks
  - IP to protect against side channel analysis
- Whitening techniques

SECURE RF
Securing the Internet of Things®

Secure Boot / Secure Firmware Update

- Ensure firmware has not been modified
- Verify origin authenticity during boot sequence (signature verification is VERY fast)
- Protect devices from malware or modified configuration
- Ensure firmware updates are authentic from origin and not modified in transit

Securing 8-bit, 16-bit, and 32-bit Processors

Future-Proof Identification, Authentication, and Data Protection for IoT Gateway and Endpoint devices

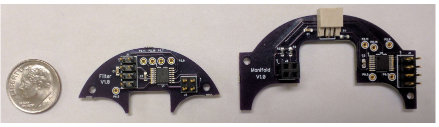
Platform Examples

ST Micro

Intel

Infineon

Arrow Electronics

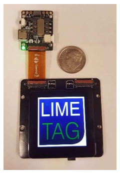


ARM Cortex M0

Microsemi

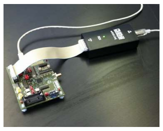
Securing Your Devices

- Software Libraries:
  - For 8/16/32 bit embedded processors
- Hardware Cores (IP):
  - Ironwood (Key Agreement Protocol)
  - WalnutDSA (Digital Signature)
- IoT Solutions:
  - Wireless Sensors
    - UHF, NFC, BLE, 433MHz
  - Smartphone Apps
    - Android, Apple
  - IoT Windows SDK
  - Cloud Dashboard



Multi-Mode Tags

Sensor Solutions



Custom Solutions

Smartphone Apps

Secure
Passive Tags

SecureRF 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
- Request your SDK: info@securerf.com
- Information: www.securerf.com/products/security-tool-kits/

Need to Secure Your Solution? Let's Talk.

100 Beard Sawmill Road, Suite 350, Shelton, CT 06484
75 E Santa Clara St., Floor 6, San Jose, CA 95113
www.SecureRF.com Twitter: @SecureRF

ARM
codasip
RENESAS
intel
TEXAS INSTRUMENTS
incits
NSF
ALTERA
ANDES TECHNOLOGY
United Technologies
U.S. AIR FORCE
ARROW
Microsemi
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
Raytheon
Member AIM NORTH AMERICA Association for Automatic Identification and Mobility
RISC-V
EM MICROELECTRONIC
ST life.augmented Authorized Partner
SECURE RF Securing the Internet of Things