



# **RAIN RFID and the Internet of Things: Industry Snapshot and Security Needs**

Matt Robshaw and Tyler Williamson  
Impinj  
Seattle, USA

# Overview

- RAIN RFID
- The product and standardization landscape
- Security, performance, and looking forward
- Questions

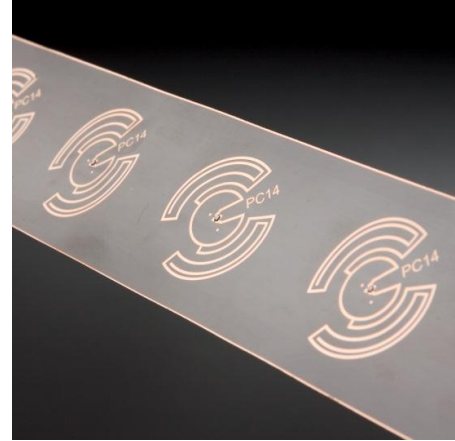
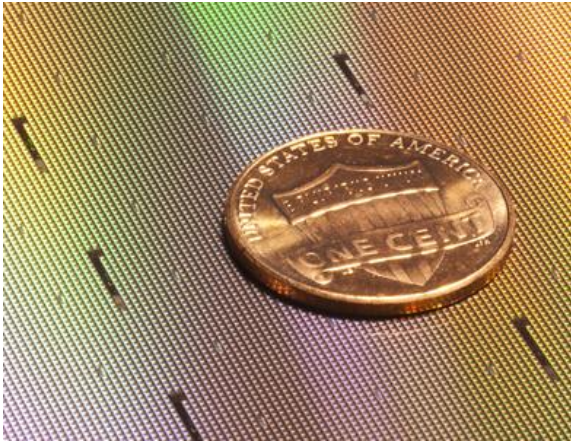
*Note : This presentation outlines the personal views of the authors*

# RAIN RFID

- Radio-frequency identification
  - Item identification using EM waves
  - Many different systems at different frequencies
  - Low frequency (LF), High frequency (HF), Ultra-high frequency (UHF) , ...
  - UHF is now an established technology, solutions can be reliably deployed
    - Long read range, passive, and cheap
- The original motivation for the term “Internet of Things”
  - The cheapest way to provide connectivity to an object or device
- RAIN: Radio-frequency IdentificationN
  - Industry alliance to promote UHF RFID



# RAIN RFID



# What Does a RAIN RFID Chip Currently Do?

- Chips communicate wirelessly, *i.e.* not line-of-sight
  - Bar-code scanning < 500 units/hour; RFID scanning > 10,000 units/hour
- Chips store a chip identifier (TID) and a product identifier (EPC)
  - TID is fixed by the chip manufacturer
  - Electronic Product Code (EPC) identifies the individual object; not just the product type
- Most RAIN RFID chips, but not all, have a small amount of user memory
  - 512 bits is a lot, typically  $\leq 64$  bits
  - Some specialty chips provide  $\geq 2k$  bits
- Current deployments are built around reading and writing product identifiers and/or small amounts of application data

# Example RAIN RFID Applications



The diversity of RAIN RFID applications is rapidly increasing ...

# What Could a RAIN RFID Chip Do?

- RAIN RFID capabilities are defined by the *over-the-air* protocol
- The revision of EPCglobal Gen2v1 to Gen2v2 brings 12 additional (optional) commands
  - Support for cryptographic solutions
  - Gen2v2.0.1 is available for download at [www.gs1.org/epc-rfid](http://www.gs1.org/epc-rfid)
- Services such as tag/reader/mutual authentication and authenticated/encrypted communication are now possible
  - However Gen2v2.0.1 is crypto-agnostic so more work is needed
- ISO/IEC SC31 is working on a multi-part standard 29167-x
  - NIST and ISO/IEC SC27, among others, define cryptographic primitives
  - Goal is to integrate crypto technologies within Gen2v2.0.1
  - Includes a mix of encryption technologies

# What Are The Issues?

- RAIN RFID is typically used for its low tag cost and long read-range
- RAIN RFID is *extremely* cost- and performance-sensitive and so adding any feature requires careful analysis
- Different use-cases may prioritize different performance attributes
  - e.g. sensitivity/read range, throughput, cost/area, security
- The deployment eco-system is complex
  - There are different chip vendors and different reader vendors
  - Different solution providers might address very different markets
  - Much more than just choosing an algorithm

# First Steps

- The majority of chips by volume will continue to be simple “license-plate” models
- First generation RAIN RFID cryptographic chips are likely to support tag authentication
  - *e.g.* NXP UCODE DNA provides tag authentication using AES-128
- However more sophisticated chips will appear as the range of applications—and their security requirements—broaden

# The Case for Lightweight Encryption

- For symmetric encryption 3DES and AES are excellent algorithms
  - But they bring a performance compromise to RAIN RFID
- Looking at alternatives currently provided in SC31 we see, *for example*, that ...
  - ... the total transaction time for block cipher-based tag authentication can be halved when using 29167-11 (PRESENT-80) instead of AES
  - ... secure channel solutions can be provided by 29167-13 (Grain-128a)
- 29167-11 and 29167-13 represent “first-generation” lightweight algorithms
  - Perhaps these are sufficient, perhaps other proposals offer more advantages
- Lightweight needn't compromise security
- Providing the developer with sufficient implementation flexibility is key

# The Case for Guidance from NIST

- There are many different initiatives to add cryptography to IoT applications
  - These are not always taking place where cryptographic expertise is available
  - Existing industry and standards bodies are not always well-equipped to deal with this
- Even something as simple as a technical survey that identifies – without formal approval – some “interesting” new designs could be helpful
  - A nudge to avoid people choosing poor or un-reviewed solutions
- At the other extreme, a full-scale competition has been successful in the past
  - Formulating the scope of such an effort would require some care (see over)
  - Likely too late for current/near-future products
  - However results would likely be of lasting value

# Issues and Complexities

- Framing the parameters for a “competition” could be difficult
  - A block cipher? A stream cipher?
  - Asymmetric? Symmetric?
- To support what goals?
  - More than the primitive
  - *e.g.* symmetric-key authenticated encryption optimized for short payloads
- Evaluation parameters are hard to establish for the full generality of the “IoT”
- The most useful outcome could be a small portfolio of technologies addressing complementary parts of the IoT eco-system

# Conclusions

- Billions of RAIN RFID tags will be sold this year
  - This is just one part of the IoT
- As deployments take hold and applications proliferate, the need for robust security with exceptional performance characteristics will grow
- There is a risk that “poor cryptography” will rush into the vacuum
  - Bad for everyone
- The expertise and reputation of NIST would be very beneficial in either guiding industry choice or in offering well-founded complements to existing standards