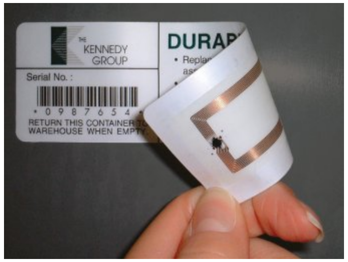
# Lightweight Authentication Protocols on Ultra-Constrained RFIDs – Myths and Facts

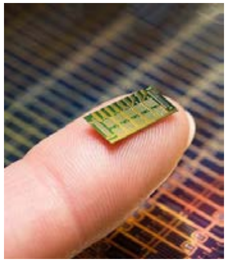
*(presented at RFIDsec 2014, Oxford, UK)*

Frederik Armknecht Matthias Hamann Vasily Mikhalev

University of Mannheim, Germany

# Lightweight Authentication on RFIDs

- <u>Situation:</u>
  Most **standard cryptographic algorithms too expensive** (hardware, money) for low-cost RFID tags.
  → **New, “sufficiently secure” approaches needed.**

- <u>Problem:</u>
  Specific **hardware capabilities** (at a certain cost level) often **hardly known** to the academic community.
  → **Public designers can’t evaluate their protocols accordingly!**

# “Lightweight!” – Well, opinions differ…

*Former Mr. Olympia Ronnie Coleman screaming his motto: “Lightweight, baby!”*

# Our Contribution

- Hardware Capabilities:
  - Comprehensive, **public list of practical limits on ultra-constrained low-cost RFID tags.**
  - Sources: Literature, **discussions with experts from industry and academia**.

- Protocol Evaluation:

| Approach | Feasible? |
|---|---|
| Cipher-based | YES |
| LPN-based / HB-type | NO |

# Ultra-constrained RFID Hardware

- Targeted Platform:
  Passively powered, **low-cost RFID tags in the range of $0.05 to $0.10** like Electronic Product Codes (EPCs).

- Technology:
  **Application-specific Integrated Circuits (ASICs)**
  - Integrated circuit customized for a particular use, rather than intended for general-purpose use.
  - Typical component in the low-cost RFID context, e.g., due to low per-unit costs (for large batches).

- Implementation:
  Hardware Description Languages like **Verilog**.

# Hardware Constraints (1)

1. Area:
   - Measured in Gate Equivalents (GEs): 1 GE = area of a two-input NAND gate.
   - Common design tradeoff: area vs. speed.
   - **Limit: ~ 2,000 GEs (security budget).**
   - (AES ~ 3,400 GEs, PRESENT ~ 1,100 GEs, KTANTAN64 ~ 700 GEs.)

2. Non-volatile Memory (NVM):
   - Volatile memory limits included in area constraints (e.g., for flip-flops).
   - Prevalent technology: EEPROMs (costly in terms of money and power).
   - Alternatives w.r.t. key storage: masks, fuses.
   - **Limit: ~ 2,048 bit.**

# Hardware Constraints (2)

3. Power:
   - (Low-cost / Ultra-constrained) Tags are passively powered.
   - Limiting factors: transmission power of RFID readers (e.g., due to legal regulations), temperature issues in medicine ($\Delta < 1$ °C), …
   - Numbers strongly depend on the technology library.
   - **Limit: ~ 10 µW.**

4. Clock Speed:
   - Limited esp. by power constraints.
   - Important w.r.t. to authentication times (max. 150 msec).
   - **Limit: ~ 100 KHz (→ 15,000 clock cycles per authentication).**

# Hardware Constraints (3)

5. <u>Operating Frequency and Transmission Bandwidth:</u>
   – **Limit: 200 kbit/s (→ 30,000 bits per authentication, i.e., within 150 msec).**

| Waveband | Utilization | Bandwidth | Distance |
|---|---|---|---|
| **Low Frequency (LF), 30-300 kHz** | Animal Identification | < 10 kbit/s | 0.1-0.5 m |
| **Medium Frequency (MF), 300 kHz - 3 MHz** | Contactless Payment | < 50 kbit/s | 0.5-0.8 m |
| **High Frequency (HF), 3-30 MHz** | Access Control | < 100 kbit/s | 0.05-3 m |
| **Ultra HF (UHF), 300 MHz - 3 GHz** | Range Counting | < 200 kbit/s | 1-5 m |
| **Super HF (SHF), 3 GHz - 30 GHz** | Vehicle Identification | < 200 kbit/s | ca. 10 m |

*(Source: H. Chabanne, P. Urien, and J. Susini; RFID and the Internet of Things; 2011.)*

# Hardware Constraints (4)

6. Random Number Generator (RNG):
   - Hardware sources: thermal noise, shot noise, diode breakdown noise, metastability, oscillation jitter, …
   - **But:** hardware cost of respective components and of checking/ensuring entropy.
   - Further problems: RNG speed, probability distribution, …
   - Practical specifications/numbers for low-cost RNGs hard to obtain (well-guarded business secret w.r.t. ultra-constrained devices).
   - **According to major RFID hardware suppliers: at most 128 (truly) random bits per authentication available on low-cost tags (i.e., in the range of $0.05 to $0.10).**

# Hardware Constraints - Summary

| Hardware/Usability Property | Limit | Sources (i. a.) |
|---|---|---|
| **Area** | ~ 2,000 GEs | [5], [14], [17], [10], [6], ([11]), [3], [2] |
| **Non-volatile Memory** | ~ 2,048 bit | [2], [7], [5] |
| **Power** | ~ 10 µW | [12], [5], [14], [13] |
| **Clock Speed** | ~ 100 KHz | [19], [4], [8] |
| **Bandwidth** | < 200 kbit/s | [15], [2] |
| **Random Numbers (TRNG)** | < 128 bits/authentication | [16], [1], [8] |
| **Authentication Time** | < 150 msec | [2], [11], [4] |

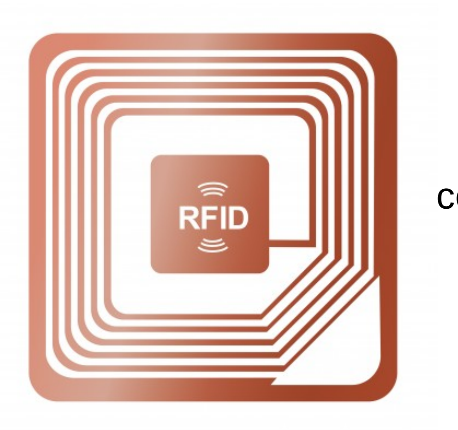
# Lightweight Authentication Protocols

- **Basic Scenario:**
  - **Prover** (RFID tag) and **verifier** (RFID reader) share common **secret key**.

- **Design Approaches:**
  1. Conventional:
     Protocols which use established primitives, e.g., **lightweight block ciphers** like PRESENT or KATAN, as basic cryptographic operations.
  2. Approaches invented specially for Lightweight Authentication:
     - **HB-type protocols**, based on the well-researched **Learning Parity with Noise (LPN) problem**.
     - **Linear protocols**, based on the **Principle of Random Selection**.
     - …

# Conventional Cipher-based Approach (1)

**Prover($E_k$)**
RFID tag




compute
$z = E_k(a)$

**Verifier($E_k$)**
RFID reader


choose
$a \in_U \{0,1\}^n$

$a$ ←
challenge

$z$ →
response

accept if
$E_k(a) = z$

Simple cipher-based challenge-response authentication protocol (1 round).
($E_k$ = encryption function using a secret key $k$)

# Conventional Cipher-based Approach (2)

- (Tag-side) Costs at the example of PRESENT ($n = 64$, $|k| = 80$, 1 round):
  - **Area:** 1,080 GEs **< 2,000 GEs**
  - **NVM:** key size $|k|$ = 80 bit **< 2,048 bit**
  - **Power:** as low as 2.52 µW (at 100 KHz) **< 10 µW**
  - **Computation:** 563 clock cycles per block **< 15,000 clock cycles**
  - **Communication:** 2*64 = 128 bits (per protocol round) **< 30,000 bits**
  - **Random Numbers:** no RNG needed on the tag's side! **(< 128 bits)**

**→ Feasible on low-cost RFID tags!**

# LPN-based Protocols: HB+ as an example

| **Prover (RFID tag)** | ***Common Secrets:*** $x \in \{0,1\}^{k_x}, y \in \{0,1\}^{k_y}$ | **Verifier (RFID reader)** Error Counter: $E := 0$ |
| --- | --- | --- |

*$\times$ r rounds*

*Round $i$*

| | | |
| --- | --- | --- |
| **Generates:** $b^{(i)} \in_U \{0,1\}^{k_y}$, $\nu \in \{0,1 \mid Prob\ [\nu = 1] = \eta\}$ | $\xrightarrow{b^{(i)}}$ blinding factor | |
| | $\xleftarrow{a^{(i)}}$ challenge | **Generates:** $a^{(i)} \in_U \{0,1\}^{k_x}$ |
| **Computes**: $z^{(i)} := a^{(i)} \cdot x + b^{(i)} \cdot y + \nu$ | $\xrightarrow{z^{(i)}}$ response | |
| | | **Checks:** If $a^{(i)} \cdot x + b^{(i)} \cdot y \neq z^{(i)}$, then $E := E + 1$. |

If the **number of errors $\boldsymbol{E}$** is less than the **threshold $\boldsymbol{t} = \boldsymbol{u} \cdot \boldsymbol{r}$** for some fixed parameter $u$ ($\eta \in (0, 0.5)$, $u \in (\eta, 0.5)$ and $r$ are publicly known), then the verifier accepts the tag.

# Parameter Choices for LPN-based Protocols

- General Observation:
  - **If** the noise probability $\boldsymbol{\eta \approx 0.5}$, then the **number of rounds has to be large** for **reliability** reasons.
  - **If** $\boldsymbol{\eta \approx 0}$, then the **key size has to be huge** for **security** reasons (i.e., to ensure the hardness of the underlying LPN problem).

- Our Approach for Protocol Evaluation:
  Were **parameters suggested by the respective authors** (or in follow-up publications)?
  - **YES** → Use those.
  - **NO** → Determine resource-optimal parameters subject to certain restrictions like sufficiently low false acceptance/rejection rates and security against state-of-the-art LPN algorithms.

# Example: Costs of HB+

Round $i$. The Operations of the Prover (Tag):

Knows secrets: $x \in \{0,1\}^{80}$, $y \in \{0,1\}^{512}$

Generates: $b^{(i)} \in_U \{0,1\}^{512}$, $\nu \in \{0,1 | Prob\,[\nu = 1] = 0.125\}$

Sends: $b^{(i)}$ to the verifier

Receives: $a^{(i)} \in \{0,1\}^{80}$ from the verifier

Computes: $z^{(i)} = a^{(i)} \cdot x + b^{(i)} \cdot y + \nu$

Sends: $z^{(i)}$ to the verifier

× 441 rounds per authentication instance

Key storage = *80 + 512 = 592* *≤ 2,048* ✓

Uniformly distributed random bits for blinding factors = *512 × 441 = 225,792*

Uniformly distributed random bits for noise = $-Log_2(0.125) \times 441 = 1{,}323$

Total number of random bits = *225,792 + 1323 = 227,115 > 128* X

Total communication complexity = *(512 + 80 + 1) × 441* = *261,513 > 30,000* X

# Evaluation results for the considered HB-type protocols

| Protocol | Storage | Rnd. Bits | Comm. | Clk. Cycles | Area | Security |
|---|---|---|---|---|---|---|
| **HB** | ✓ | X | X | ✓ | ✓ | X |
| **HB+** | ✓ | X | X | ✓ | ✓ | X |
| **HB++** | ✓ | X | X | ✓ | X | X |
| **HB-MP** | ✓ | X | X | ✓ | X | X |
| **HB-MP+** | ✓ | X | X | ? | ? | ? |
| **HB*** | ✓ | X | X | ✓ | ✓ | X |
| **HB*(1)** | ✓ | X | X | ✓ | X | X |
| **Random HB#** | X | X | ✓ | X | X | X |
| **HB#** | ✓ | X | ✓ | ✓ | X | X |
| **HB-MAC** | X | X | ✓ | ✓ | X | X |
| **GHB#** | X | X | ✓ | ✓ | X | ✓ |
| **$HB^N$** | X | X | X | ? | X | ✓ |
| **$HB^b$** | X | ? | ✓ | ✓ | X | ? |
| **NL-HB** | ✓ | X | X | ✓ | ✓ | X |
| **AUTH** | X | ? | X | X | ? | ✓ |
| **$MAC_1$** | X | ? | X | X | ? | ✓ |
| **$MAC_2$** | X | ? | X | X | ? | ✓ |

# Conclusion

- Revisited **lightweight authentication schemes for ultra-constrained RFID devices** in the cost range of **$0.05 to $0.10**.
- Specified and argued a **comprehensive set of hardware conditions** to be met.
- **No** **unbroken LPN-based/HB-type protocol feasible** for ultra-constrained devices currently exists.
- **Feasible solutions based on lightweight block ciphers do exist**, i.e., using PRESENT or KATAN/KTANTAN.

# References w.r.t. Hardware Constraints (1)

1. G. K. Balachandran and R. E. Barnett: *A 440-nA true random number generator for passive RFID tags*, 2008.
2. P. H. Cole and D. C. Ranasinghe: *Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting*, 2008.
3. M. Feldhofer, J. Wolkerstorfer, and V. Rijmen.: *AES implementation on a grain of sand*, 2005.
4. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer: *Strong authentication for RFID systems using the AES algorithm*, 2004.
5. A. Juels and S. A. Weis: *Authenticating pervasive devices with human protocols*, 2005.
6. J. Melià-Seguí, J. Garcia-Alfaro, and J. Herrera-Joancomartí: *J3Gen: A PRNG for low-cost passive RFID*, 2013.
7. A. Nuykin, A. Kravtsov, S. Timoshin, and I. Zubov: *A low cost EEPROM design for passive RFID tags*, 2012.
8. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda: *LAMED - a PRNG for EPC Class-1 Generation-2 RFID specification*, 2009.
9. A. Poschmann: *Lightweight cryptography: Cryptographic engineering for a pervasive world*, 2009.

# References w.r.t. Hardware Constraints (2)


10. A. Poschmann, A. Moradi, K. Khoo, C. Lim, H. Wang, and S. Ling : *Side-channel resistant crypto for less than 2,300 GE*, 2011.
11. D. C. Ranasinghe, D. W. Engels, and P. H. Cole : *Low-cost RFID systems: Confronting security and privacy*, 2005.
12. C. A. Repec: *Regulatory status for using RFID in the EPC Gen 2 band (860 to 960 MHz) of the UHF spectrum*, 2013.
13. C. Rolfes, A. Poschmann, G. Leander, and C. Paar: *Ultralightweight implementations for smart devices - security for 1000 gate equivalents*, 2008.
14. M.-J. O. Saarinen and D. W. Engels: *A do-it-all-cipher for RFID: Design requirements (extended abstract)*, 2012.
15. J. Susini, H. Chabanne, and P. Urien: *RFID and the Internet of Things*, 2011.
16. C. Tokunaga, D. Blaauw, and T. Mudge: *True random number generator with a metastability-based quality control*, 2007.
17. W. Wu and L. Zhang: *LBlock: A lightweight block cipher*, 2011.

# Thank you for your attention!