Lightweight Cryptography for RFID Systems

Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
CANADA
<http://comsec.uwaterloo.ca/~ggong>

Part III. Design of Authentication Protocols for RFID Systems

- **Security** and **Privacy** threats in RFID systems
- **Lightweight** Crypto Solutions to Authentication for RFIDs
- **LPN Based** Entity Authentication Protocol for RFIDs
- **WG-7** Based Authentication Protocol for RFIDs

Security Threat Classification

- Information Leakage
- Privacy Violation
- Tag Impersonation Attack
- Relay Attack
- Denial of Service Attack
- Backward and Forward Traceability
- Server Impersonation Attack

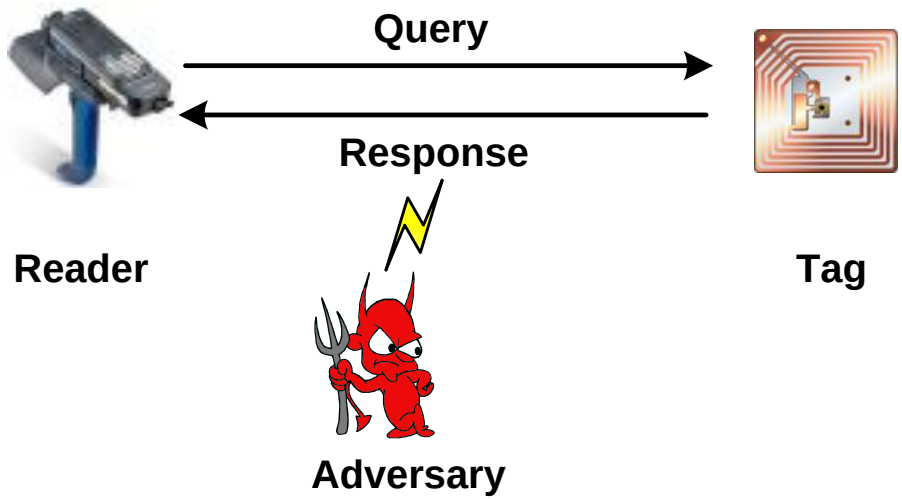
Information Leakage

Problem

☞ An adversary should not be able to **obtain useful information** about the tagged object.

Attacking Method

☞ The adversary can **query** the target tag or **eavesdrop** communications between the tag and readers.



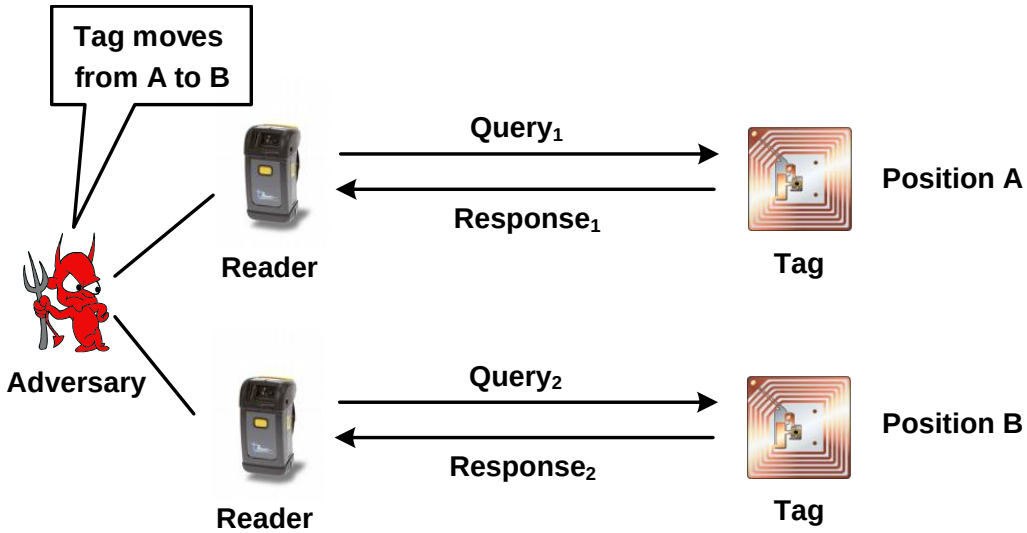
Privacy Violation

Problem

☞ An adversary should not be able to **track** the movement of a tagged item, and by extension, the person associated with it.

Attacking Method

☞ The adversary can **query** the target tag and **correlate** data from multiple RFID readers.



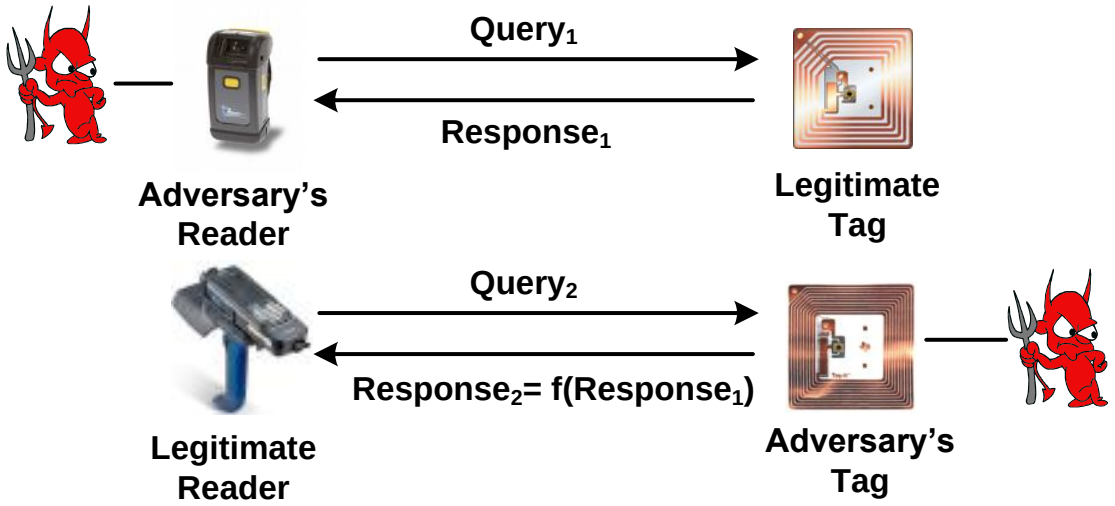
Tag Impersonation Attack

Problem

☞ An adversary should not be able to **impersonate** a tag.

Attacking Method

☞ The adversary can **query** the target tag or **eavesdrop** communications between the tag and readers. Then the adversary tries to use the **responses from the victim** to fool a legitimate reader.



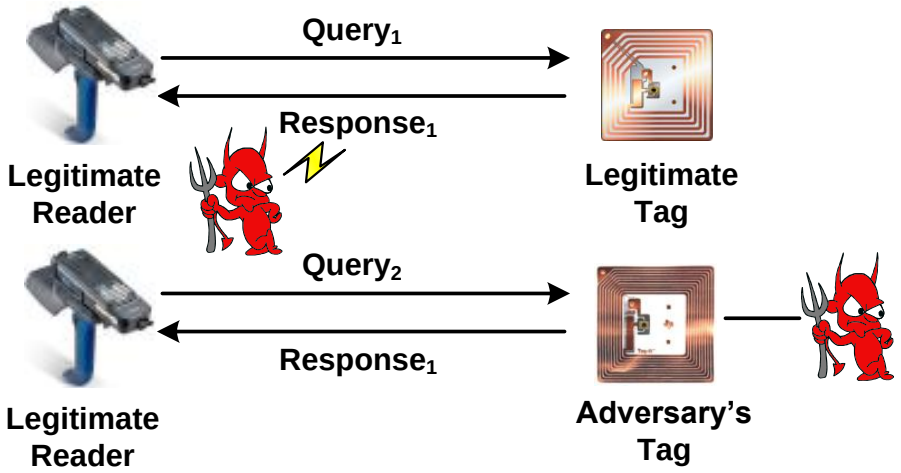
Replay Attack

Problem

☞ An adversary should not be able to **reuse** the communications from **previous sessions** to perform a successful authentication between a tag and a reader.

Attacking Method

☞ The adversary can **intercept** the valid authenticators from a **past transaction** and use them to finish the authentication.



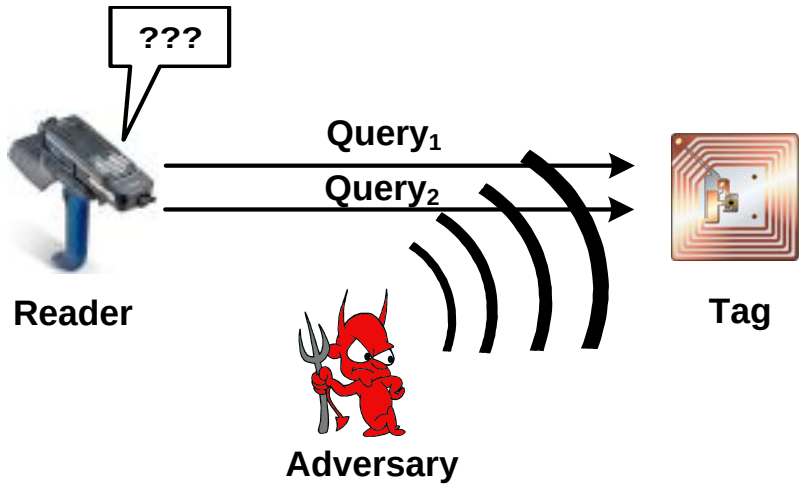
Denial of Service Attack

Problem

☞ An adversary should not be able to **disturb** the interactions between a tag and a reader.

Attacking Method

☞ The adversary can **intercept** or **block** the transmitted messages which might lead to the **desynchronization** of the shared secret between a reader and a tag.



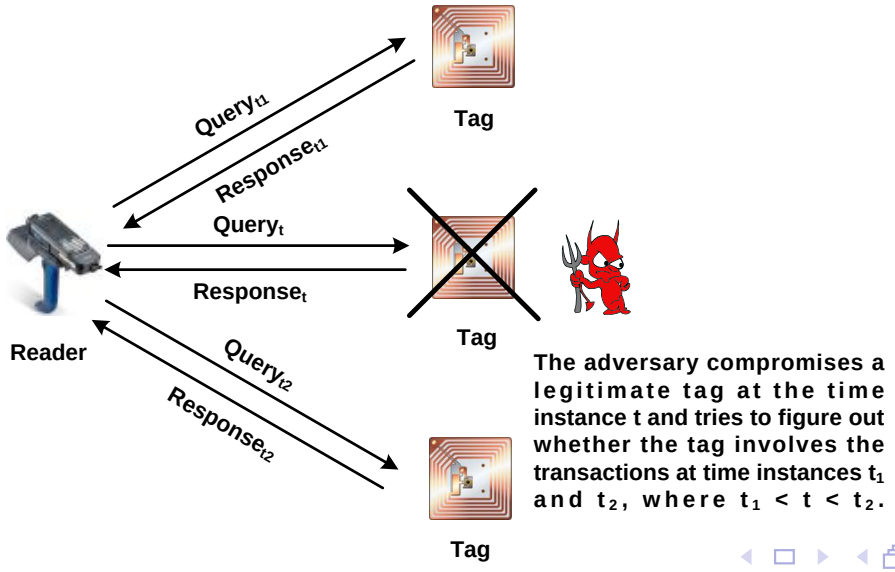
Backward and Forward Traceability

Problem

☞ An adversary should not be able to **link** a tag with **past** and **future** actions performed on the tag, even after compromising the tag.

Attacking Method

☞ The adversary can **compromise** a tag and try to track the victim's **past** and **future** transactions.



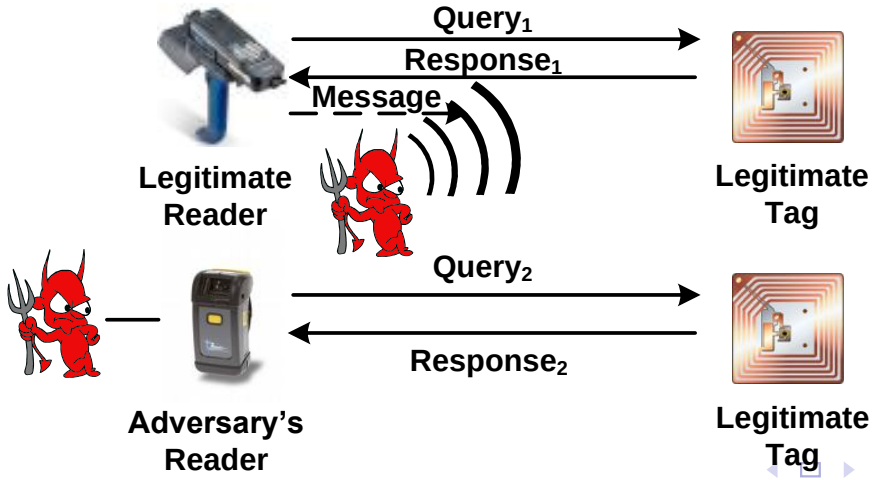
Server Impersonation Attack

Problem

☞ An adversary should not be able to **impersonate** a legitimate server to the tag without knowledge of a tag's secret.

Attacking Method

☞ The adversary can **eavesdrop** a valid session and **block** some messages from reaching the tag. Then the adversary **initiates another session** as an impersonated reader.



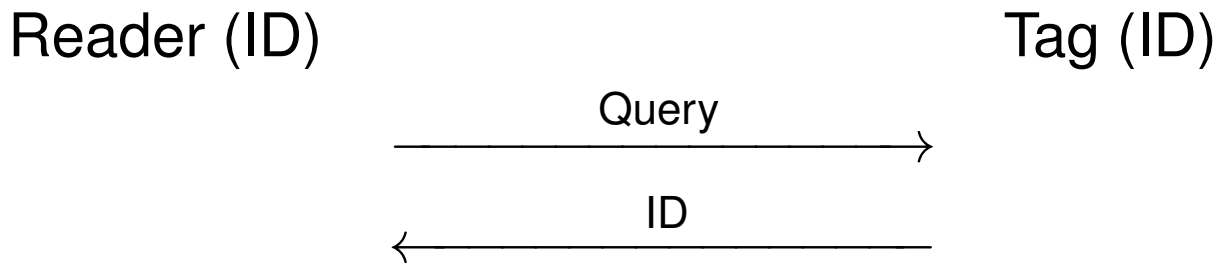
Countermeasures

Physical Protection	Distance measurement, Faraday cage approach
Deactivation	Killing, sleeping, hash lock
Re-naming	Relabeling or effacing, minimalist cryptography, re-encryption
User-Oriented	Light Crypto based approaches
Proxy Or Filter	Watchdog tag, RFID guardian
Jamming	Blocking, soft-blocking tag
Entity authentication	PRG-based, hash-based, private authentication

Identification and Authentication

Identification Protocol

An identification protocol allows a reader to obtain the identity of a queried tag, but no proof is required.

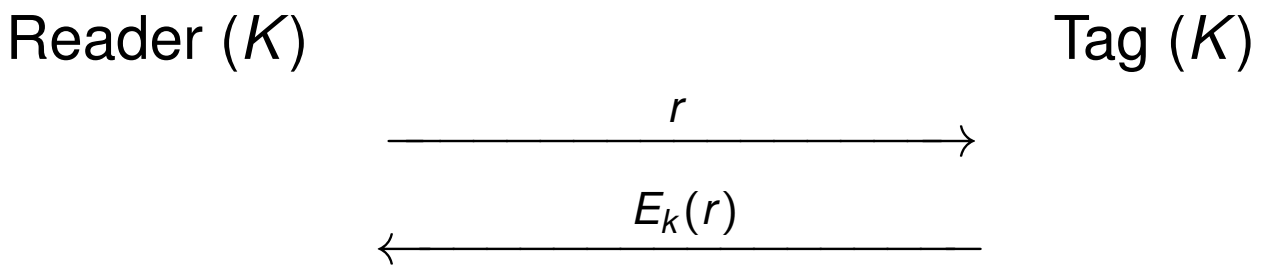


- Primal goal of identification protocols is to provide functionality and privacy.
- Examples: Localization, stock management, etc.

Tag Authentication

Authentication Protocol

An authentication protocol allows a reader to be convinced of the identity of a queried tag. Conversely, it can allow a tag to be convinced of the identity of a querying reader. If both properties are ensured, we speak of mutual authentication.



- Primal goal of authentication protocols is to provide security.
- Examples: Access control, e-documents, anti-clone, anti-counterfeiting, etc.

Performance Requirements

- **Low Computational Cost**: The computational overhead of authentication protocols in the tag side should be small due to the limited power available to RFID tags.
- **Low Communication Cost**: The message transmitted in the authentication phase should be minimized because of the limited bandwidth available to RFID tags.
- **Low Storage Requirement**: The data stored in a RFID tag should be kept as small as possible since the tag memory is extremely constrained.
- **Scalability**: The back-end database should be able to efficiently identify an individual tag even though the tag population is huge.

Privacy-Preserving RFID Authentication Protocols

- **Block Cipher** Based Authentication Protocols
- **Public-key** Based Authentication Protocols
- **HB-family** Based Authentication Protocols

Block Cipher based Authentication Protocols

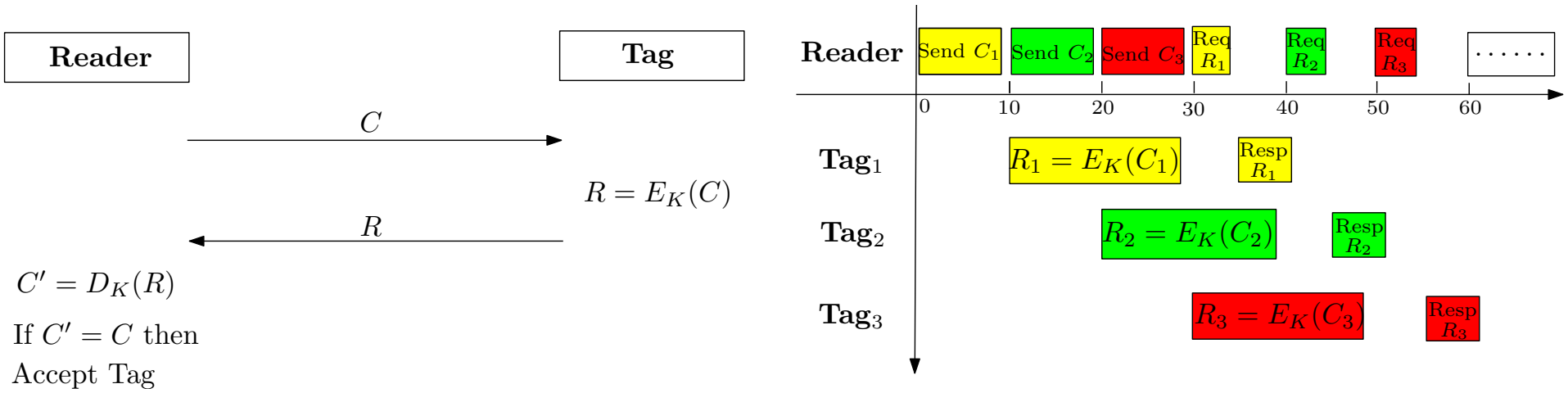


Figure: Interleaved Challenge-Response Protocol Using AES [Feldhofer et al.'04]

- HF tags running at a frequency of 100KHz are considerted.
- The standard requires that a reponse must follow $320\mu s$ after a request. Otherwise, the tag has to stay quiet.
- AES is too slow (1032 cycles/block) to meet the requirement of the standard and therefore an interleaving authentication method is used.

Lightweight Identification Schemes based on Public-key Schemes

- **The most** commonly public-key schemes, such as those based on the difficulty of factorization, discrete logarithms, or elliptic curve discrete logrithms, are not suitable for RFID applications.
- The **hardware** implementations of public-key schemes usually require many tens of thousands of logical gates.
- Two types of **identification schemes** can provide public-key functionality to RFID tags at a low cost.
  - Use a variation of the Rabin cryptosystem (i.e., SQUASH [Shamir'08] and WIPR [Oren et al.'08])
  - Use a token (coupon)-based approach (i.e., cryptoGPS [Girault'07, Mcloone et al.'07])

Public-key Based Authentication Protocols

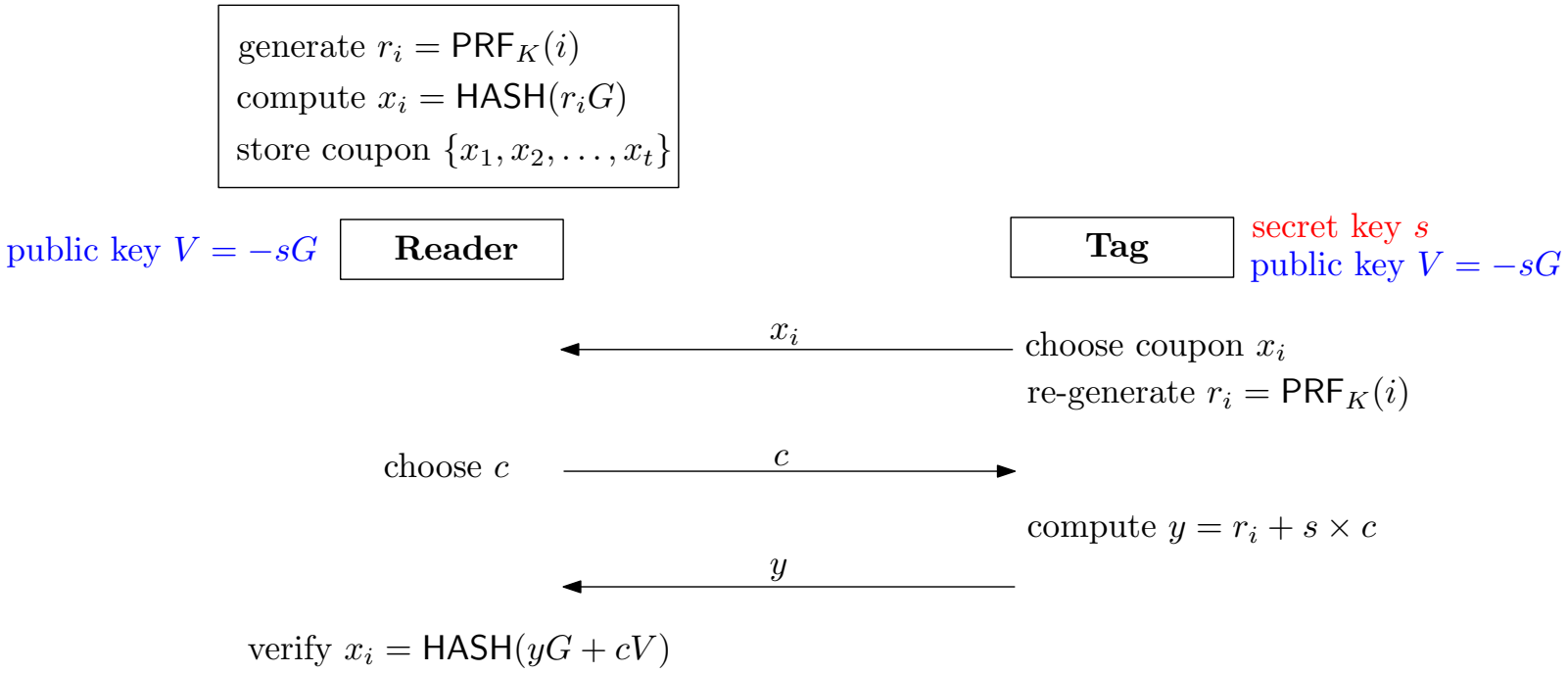


Figure: The Elliptic Curve Variant of cryptoGPS [Mcloone et al.'07]

- The computation on the tag is simple.
- There are a variety of implementation trade-offs. For example, we can use a sparse challenge c to "change" multiplication into a small number of additions (but still cost).

HB$^+$ Protocol [Juels & Weis '05]

Tag $(\boldsymbol{k}_1, \boldsymbol{k}_2)$		Reader $(\boldsymbol{k}_1, \boldsymbol{k}_2)$
$\boldsymbol{b} \in_R \{0,1\}^m$	$\xrightarrow{\boldsymbol{b}}$	
	$\xleftarrow{\boldsymbol{a}}$	$\boldsymbol{a} \in_R \{0,1\}^m$
$v \in_R \{0,1 \mid \Pr[v=1] = \eta\}$;		
$y = (\boldsymbol{a} \cdot \boldsymbol{k}_1) \oplus (\boldsymbol{b} \cdot \boldsymbol{k}_2) \oplus v$	$\xrightarrow{y}$	
		$(\boldsymbol{a} \cdot \boldsymbol{k}_1) \oplus (\boldsymbol{b} \cdot \boldsymbol{k}_2) \stackrel{?}{=} y$

- Based on **Learning Parity with Noise** (LPN) problem
- $\boldsymbol{k}_1$ and $\boldsymbol{k}_2$ are two m-bit vectors as **authentication key**, $\eta \in (0, \frac{1}{2})$, $\boldsymbol{b}$ is a **blinding vector**, $\boldsymbol{a}$ is a **challenge vector**

LCMQ Protocol (Li-Gong10)

Definition of Circulant-P2 Matrix

($m \times m$) Square Circulant Matrix

$$\begin{bmatrix} \theta_0 & \theta_1 & \cdots & \theta_{m-1} \\ \theta_{m-1} & \theta_0 & \cdots & \theta_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1 & \theta_2 & \cdots & \theta_0 \end{bmatrix}$$

Circulant-P2 Matrix

- m is a prime number satisfying that 2 is a primitive element of finite field $GF(m)$.
- Square, landscape, and portrait: $\mathbf{C}_{\boldsymbol{\theta}}$, $\mathbf{C}_{\boldsymbol{\theta}}^{[n\times m]}$, and $\mathbf{C}_{\boldsymbol{\theta}}^{[m\times n]}$

Linear Independence of Circulant-P2 Matrix

- All row vectors in a landscape circulant-P2 matrix (and all column vectors in a portrait circulant-P2 matrix) are **linearly independent**.
- A landscape circulant-P2 matrix always has a **right inverse**. Likewise, an portrait circulant-P2 matrix always has a **left inverse**.
- All m row vectors in a square circulant-P2 matrix $\mathbf{C}_\theta$ are **linearly independent** if and only if the **Hamming weight** of θ is **odd**. Consequently, $\mathbf{C}_\theta$ is invertible if only if the Hamming weight of θ is odd.

A Secure Encryption Against Ciphertext-Only Attack

A symmetric-key encryption scheme

$$\boldsymbol{z} = \mathrm{Enc}(\boldsymbol{\theta}, \boldsymbol{\kappa}) = \boldsymbol{\theta} \circ \mathbf{C}_{\boldsymbol{\kappa}}^{[(m-1)\times m]} \ ,$$

- Plaintext $\boldsymbol{\theta}$: $(m-1)$-bit random vector, $\boldsymbol{\theta} \neq \mathbf{0}_{m-1}$
- Encryption key $\boldsymbol{\kappa}$: randomly selected from $\mathbb{S}_m^{\mathrm{e}}$
- Ciphertext $\boldsymbol{z}$: an element in $\mathbb{S}_m^{\mathrm{e}}$
- $\mathbb{S}_m$: Set of all m-bit vectors except $\mathbf{0}_m$ and $\mathbf{1}_m$
- $\mathbb{S}_m^{\mathrm{e}}$: Set of all vectors in $\mathbb{S}_m$ whose Hamming weights are even

LCMQ Protocol Specification

Tag $(\boldsymbol{k}_1, \boldsymbol{k}_2)$		Reader $(\boldsymbol{k}_1, \boldsymbol{k}_2)$
	$\xleftarrow{\boldsymbol{a}}$	$\boldsymbol{a} \in_R \mathbb{S}_m^e$
$\boldsymbol{b} \in_R \mathbb{S}_m$;		
$\boldsymbol{v} \in_R \{\{0,1\}^n \mid \Pr[v_j = 1] = \eta$, where $0 \le j \le n-1\}$;		
$\boldsymbol{y} = (\boldsymbol{b} \circ \mathbf{C}_{\boldsymbol{k}_1}^{[m \times n]}) \oplus \boldsymbol{v}$;		
$\boldsymbol{r} \in_R \{0,1\}^{m-n-1}$;		
$\boldsymbol{z} = (\boldsymbol{y} \| \boldsymbol{r}) \circ \mathbf{C}_{\boldsymbol{k}_2 \oplus \boldsymbol{a}}^{[(m-1) \times m]}$	$\xrightarrow{\boldsymbol{b}, \boldsymbol{z}}$	
		$\boldsymbol{y} \| \boldsymbol{r} = \mathrm{Dec}(\boldsymbol{z}, \boldsymbol{k}_2 \oplus \boldsymbol{a})$;
		? $\mathrm{Hwt}((\boldsymbol{b} \circ \mathbf{C}_{\boldsymbol{k}_1}^{[m \times n]}) \oplus \boldsymbol{y}) \le \tau$

$\boldsymbol{k}_1 \xleftarrow{\$} \mathbb{S}_m$ and the parity of $\mathrm{Hwt}(\boldsymbol{k}_1)$ is public, $\boldsymbol{k}_2 \xleftarrow{\$} \mathbb{S}_m^e$, interaction expansion$n < m$, noise level $\eta \in (0, \frac{1}{2})$, integer pass-threshold $\tau \in (\eta n, \frac{n}{2})$

Security of LCMQ Protocol

An LCMQ authentication system is denoted by a pair of probabilistic functions $(\mathcal{T}_{\boldsymbol{k}_1,\boldsymbol{k}_2,\eta,n}, \mathcal{R}_{\boldsymbol{k}_1,\boldsymbol{k}_2,n,\tau})$.

Definition (DET-Model)

Adversary $\mathcal{A}$ interacts q times with the tag $\mathcal{T}_{\boldsymbol{k}_1,\boldsymbol{k}_2,\eta,n}$.

Definition (MIM-model)

Adversary $\mathcal{A}$ manipulates any communications between the tag $\mathcal{T}_{\boldsymbol{k}_1,\boldsymbol{k}_2,\eta,n}$ and the reader $\mathcal{R}_{\boldsymbol{k}_1,\boldsymbol{k}_2,n,\tau}$ for q executions

- LCMQ protocol is **provably secure** in both **DET-model** and **MIM-model**!

Practical Parameters

- According to the LCMQ security proofs in the DET model, $m \geq 81$ would suffice to provide 80-bit security.
- Security proof in the MIM-model demands negligible false rates, ruling out too small choices of m.

Recommended Parameter Set for 80-bit Security

- $m = 163, n = 162, \eta = 0.08, \tau = 19$
- Key size: 326-bit

WG-7 based Authentication Protocol (Luo-Qi-Gong-Lai 10)

Reader		Tag
Randomly pick n_R	$\xrightarrow{(n_R)}$	
	$\xleftarrow{(M_1, M_2)}$	Randomly pick n_T $M_1 = id \oplus n_T$ $M_2 = WG7(k, n_R \oplus n_T)$
Search a valid (id, k) such that $WG7(\hat{k}, n_R \oplus M_1 \oplus \hat{id}) = M_2$	$\xrightarrow{(M_3)}$	
Continuously execute WG7 for 80 clock cycles and obtain M_3		Verify M_3

- A **privacy-preserving** challenge-response protocol

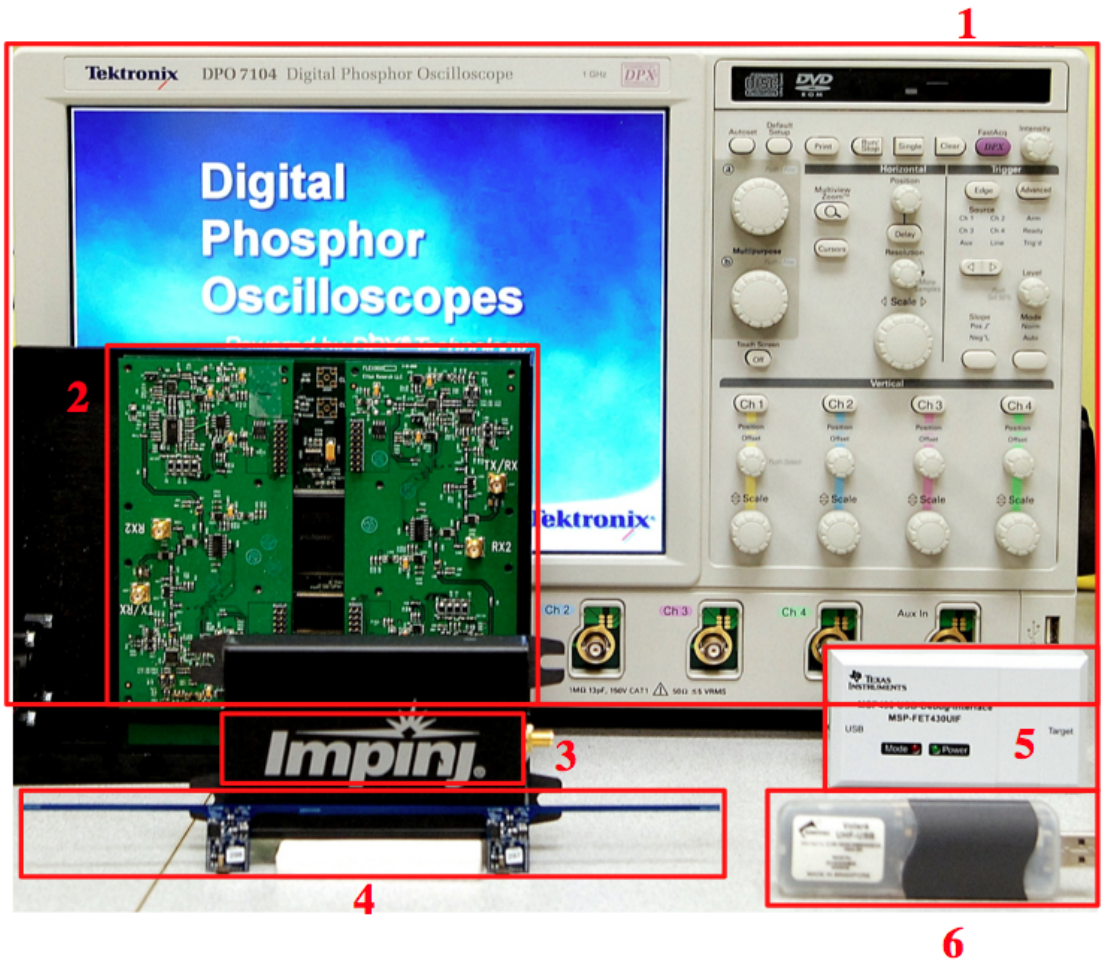
Security Properties

- The protocol has the following privacy and security properties:
  - **Tag untraceability**
  - **Tag impersonation**
  - **Reader impersonation**
- An adversary can obtain at most 160 consecutive keystream bits for a successful mutual authentication.
- For a **chosen IV attack**, the adversary can get at most 80 keystream bits for each IV, thus it is **impossible** for the adversary to obtain 224 consecutive keystream bits in this protocol.

Devices for Implementation

Devices Employed for Our Implementation

- **1.** DPO7104 oscilloscope
- **2.** USRP motherboard with two RFX900 daughter-boards, in conjunction with software radio GNU Radio
- **3.** A mini-guardrail antenna from Impinj
- **4.** Two WISP tags from Intel Research Seattle
- **5.** USB Debugger -- MSP430-FET430UIF from Texas Intrument
- **6.** A Volare UHF-USB reader as an auxulary reader to debug the WISP tags



Concluding Remarks

- **RFID** is one of the most promising technologies in the field of ubiquitous and pervasive computing.
- **EPC standard** has put forward austere challenge for designing security mechanisms for RFID systems.
- **Lightweight** cryptographic algorithms and protocols are crucial for RFID security.

Related Work

Z. Li and G. Gong

Secure and Efficient LCMQ Entity Authentication Protocol .

Centre for Applied Cryptographic Research (CACR) Technical Reports, CACR 2010-21, available at `http://www.cacr.math.uwaterloo.ca/`.

Y. Luo, Q. Chai, G. Gong, and X. Lai

A Lightweight Stream Cipher WG-7 for RFID Encryption and Authentication.

IEEE Global Communications Conference (IEEE GLOBECOM 2010), December 6-10, 2010, Mimami, Florida, USA.

The other references can be found in the above two papers.


RED
GREEN
HI-SPEED
RFID-SATA SOLUTION
2.5" SECURITY HD ENCLOSURE
SERIAL ATA
RFID

Questions?