RFID Authentication Protocols based on Elliptic Curves

A Top-Down Evaluation Survey

Michael Hutter

IAIK TU Graz

Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology

Presentation Outline

- Introduction
- Cryptographic-Enabled RFID Tags
- Public-Key Authentication Techniques
- Authentication Protocols for RFID tags
  - Schnorr, Okamoto, and GPS
- Performance Evaluation
  - Identification Schemes
  - Signature Schemes
  - X.509 Certificates
- Conclusions

Introduction

- Radio-Frequency Identification (RFID)
  - Wireless technology
  - Identification of objects/entities
  - Increases the performance of internal processes
  - Improves supply-chain management and inventory control

- State-of-the-Art RFID Security
  - No security: low-cost tags answer with a fixed identifier
  - Reasonable security: tags use shared secrets/symmetric keys
    - Memory write/read protection (e.g. iCode, …)
    - Access control, ticketing (e.g. Mifare, CryptoRF, …)
  - Enhanced security: electronic payment, e-passports, …

Cryptographic-Enabled RFID Tags

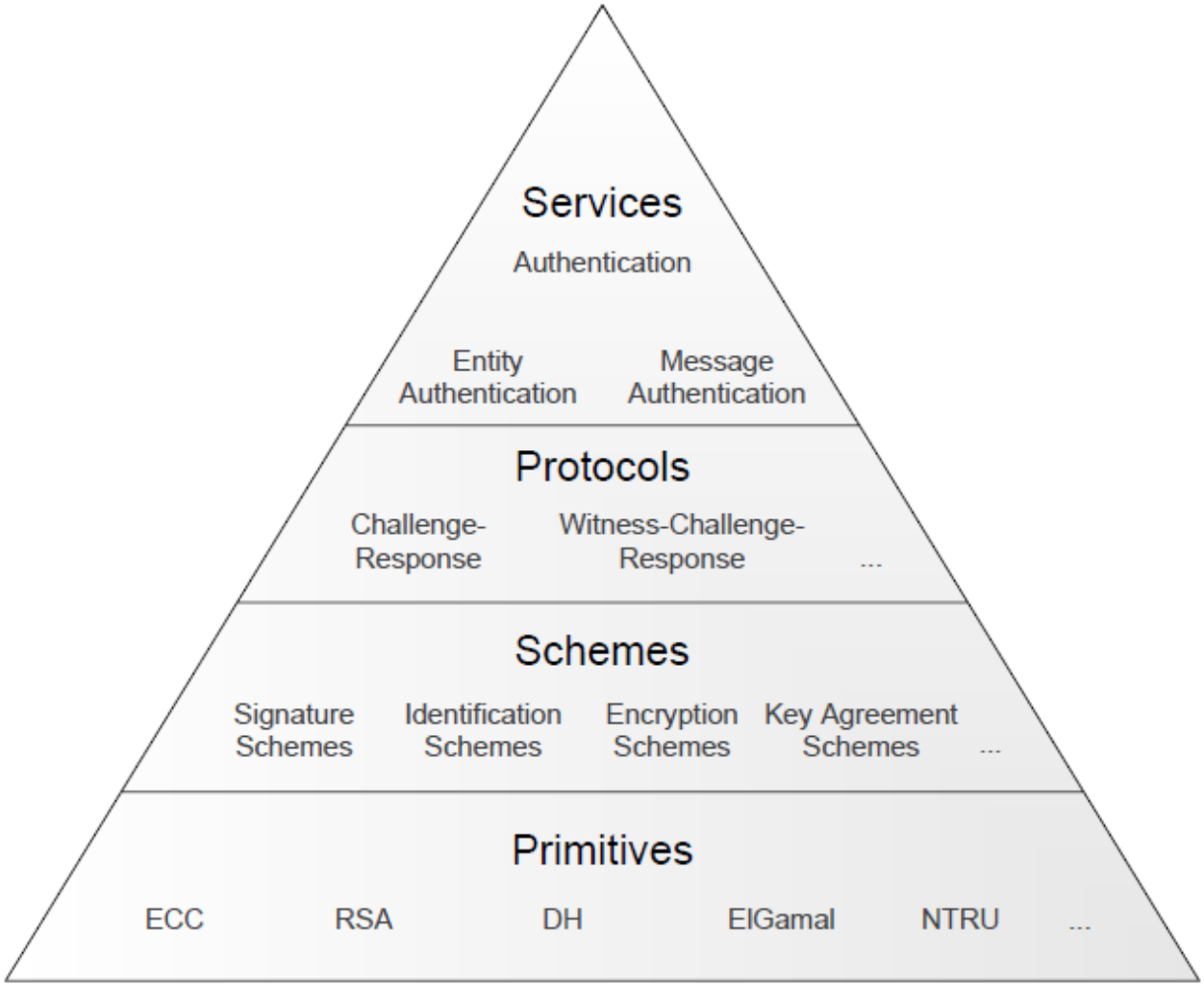
- ..would solve a lot of issues
  - RFID is an effective tool to tackle the **problem of counterfeited products**
  - International Chamber of Commerce estimates **$650 billion** a year (worldwide)
- ..but
  - Cryptographic units need additional HW area = costs
  - Key-distribution problem: more than 2 billion RFID tags will be sold worldwide in 2009 (according to IDTechEx)
- Symmetric vs. asymmetric cryptography

	Symmetric Crypto	**Asymmetric Crypto**
Keys	1 secret key	2 (1 private key, 1 public key)
Key length	128-bit	300-2000-bit
Key management	Complicated (secure channel)	Manageable (PKI)
Computational complexity	Reasonable	High
Power consumption	Reasonable	High

Our Objectives

- Cryptographic service
  - Tag authentication (instead of identification)
- Key Management
  - Asymmetric techniques (instead of symmetric)
- Light-weight implementations
  - Low resources available (low power, area,…)
- Low costs
  - Large deployment of tags (some billion tags)

- Challenge: find light-weight public-key authentication protocols for low-cost RFID tags


Services
Authentication
Entity Authentication
Message Authentication
Protocols
Challenge-Response
Witness-Challenge-Response
...
Schemes
Signature Schemes
Identification Schemes
Encryption Schemes
Key Agreement Schemes
...
Primitives
ECC
RSA
DH
ElGamal
NTRU
...

Questions for RFID Applications:

- Which protocol/scheme/primitive to choose?
- What is the performance of existing RFID authentication protocols?
  - Security, memory, computational complexity, communication
- Complexity of signature schemes compared to identification schemes?
  - Entity vs. message authentication capabilities for RFID tags?
- What are the costs for storing X.509 certificates on the tag?
- …

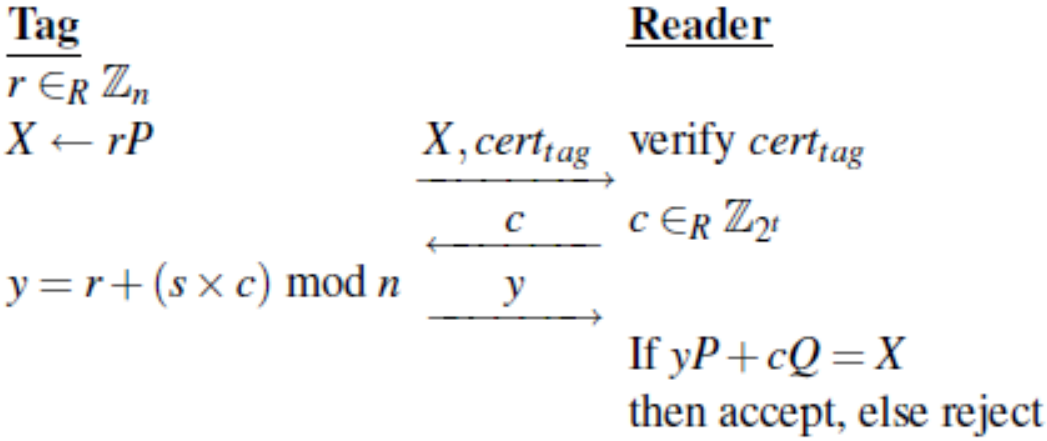
Performance Evaluation

- Simulation of different RFID scenarios using Java
  - Model of components (reader, tags, air-interface, TTP, …)

1) Performed certificate-size estimations for RFID tags

2) Evaluated different authentication protocols/schemes
   - Schnorr, Okamoto, GPS
   - Both identification and signature schemes
   - All schemes are based on the recommended NIST elliptic curve over GF(p192)

Schnorr's Identification Scheme



- Introduced by C.P.Schnorr in 1979
- Interactive identification scheme
- Three-way witness-challenge-response protocol
- Provides a zero-knowledge proof-of-knowledge
- Can be applied using ECC (ECSchnorr)

Okamoto's Identification Scheme

Tag		**Reader**
$r_1, r_2 \in_R \mathbb{Z}_n$		
$X \leftarrow r_1 P_1 + r_2 P_2$	$\xrightarrow{X, cert_{tag}}$	verify $cert_{tag}$
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_{2^t}$
$y_1 = r_1 + (s_1 \times c) \bmod n$		
$y_2 = r_2 + (s_2 \times c) \bmod n$	$\xrightarrow{y_1, y_2}$	
		If $y_1 P_2 + y_2 P_2 + cQ = X$ then accept, else reject

- Introduced by T.Okamoto in 1993
- Provides additional security against active attacks
- Two scalar multiplications needed (Shamir's trick can be applied)
- Provides a witness-indistinguishable proof-of-knowledge

GPS Identification Scheme

Tag		**Reader**
$r \in_R \mathbb{Z}_{2^\rho}$		
$X \leftarrow rP$	$\xrightarrow{X, cert_{tag}}$	verify $cert_{tag}$
	$\xleftarrow{c}$	$c \in_R \mathbb{Z}_{2^t}$
$y = r + (s \times c)$	$\xrightarrow{y}$	
		If $yP + cQ = X$ then accept, else reject

- Introduced by M.Girault, G.Poupard, J.Stern in 2001
- Standardized in ISO/IEC 9798-5 in 2004
- Eliminates modular reduction
- Allows fast “on-the-fly” authentication

X.509 Certificate-Evaluation Results

- Evaluated 3 scenarios:
  - 1. store entire X.509 certificate
  - 2. store compressed certificate
  - 3. store only variable part

```
Certificate
  Version: 1
  Serial Number: 4660
  Signature Algorithm: ecdsaWithSHA1 (1.2.840.10045.4.1)
  Issuer: CN=TestCA
  Valid not before: Thu Feb 12 18:08:14 CET 2009
        not after: Tue Feb 12 18:08:14 CET 2019
  Subject: CN=14443A00,EMAIL=test@test.com
  SubjectPublicKeyInfo:
    Algorithm: ecPublicKey, NISTp192 (1.2.840.10045.2.1)
    SubjectPublicKey:
      03:32:00:04:62:B1:2D:60:69:0C:DC:F3:30:BA:BA:B6:
      E6:97:63:B4:71:F9:94:DD:70:2D:16:A5:63:BF:5E:C0:
      80:69:70:5F:FF:F6:5E:5C:A5:C0:D6:97:16:DF:CB:34:
      74:37:39:02
SignatureAlgorithm: ecdsa-with-SHA1 (1.2.840.10045.4.1)
Signature:
  30:35:02:18:1F:91:F5:89:8B:4F:C5:D3:47:D8:7C:F2:5D:8F:
  AE:53:6F:F7:39:3E:B2:D3:18:92:02:19:00:B4:F5:9A:F7:3B:
  13:80:48:B3:86:82:42:62:C8:23:57:7A:C5:A9:A6:B5:96:C2:
  D9
```

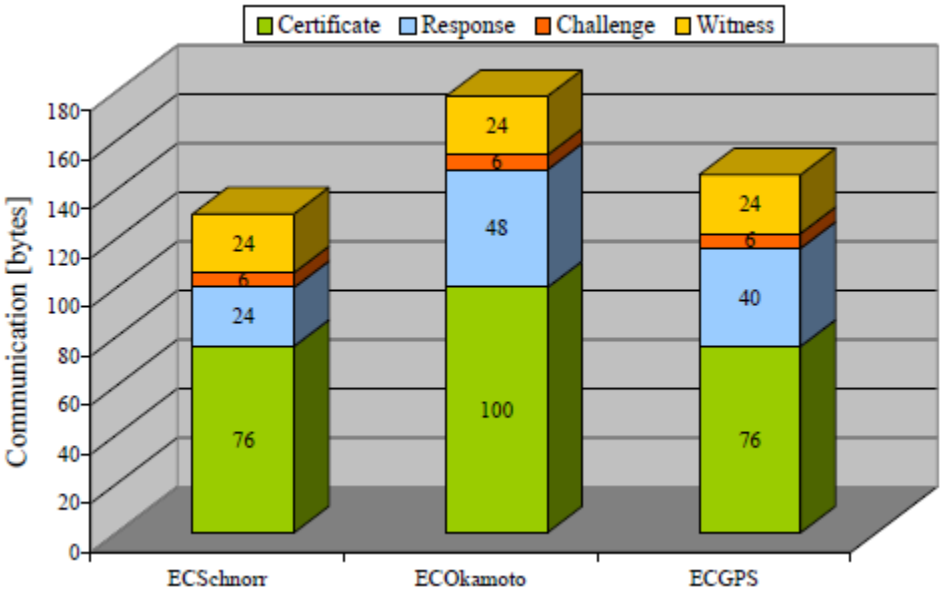
[bytes]	Schnorr	Okamoto	GPS
Scenario 1	268	292	268
Scenario 2	243	267	243
Scenario 3	76	100	76

Identification-Schemes Performance

Service, memory usage, and computational complexity

	Schnorr	Okamoto	GPS
Crypt. Service			
Entity auth.	Yes	Yes	Yes
Message auth.	No	No	No
Memory [byte]			
Private key	24	48	24
Computation			
Size of scalar	24	48	40
#Additions	771	1,544	1,283
#Subtractions	769	1,536	1,281
#Multiplications	3,271	6,542	5,447
#Squarings	962	1,924	1,602
#Inversions	2	4	2
#Hash comp.	0	0	0
Total Operations	**5,775**	**11,550**	**9,615**
Estim. Cycle Count	**993,432**	**1,986,864**	**1,630,872**

Communication bandwidth

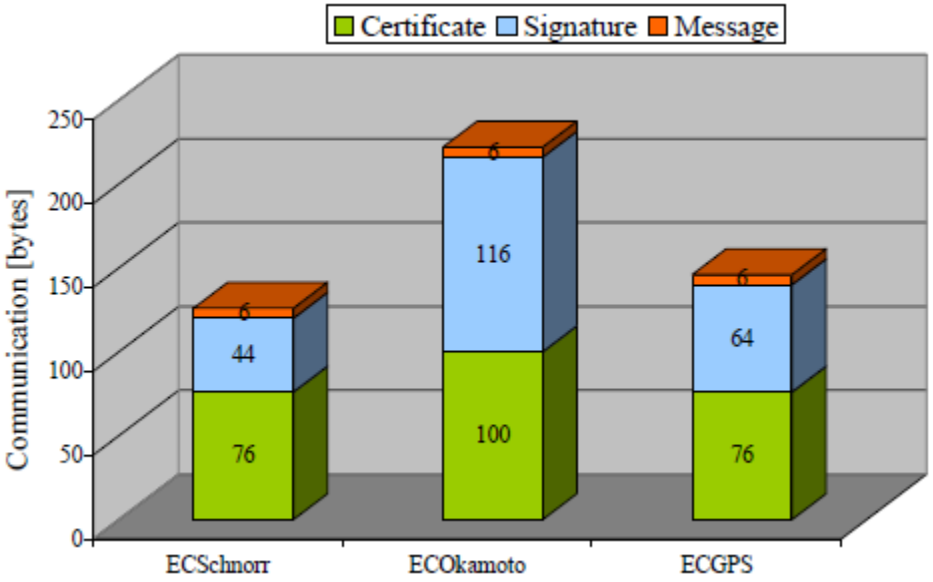


Signature-Schemes Performance

Service, memory usage, and computational complexity

	Schnorr	Okamoto	GPS
Crypt. Service			
Entity auth.	Yes	Yes	Yes
Message auth.	Yes	Yes	Yes
Memory [byte]			
Private key	24	48	24
Computation [byte]			
Hash-input size	30	30	30
#FF Operations	5,775	11,550	9,615
#Hash comp.	1	1	1
Total Operations	**5,793**	**11,568**	**9,633**
Estim. Cycle Count	**997,392**	**1,990,824**	**1,634,832**

Communication bandwidth



Conclusions

- Analyzed different authentication protocols for low-cost RFID tags
- Each protocol provides different tradeoffs
  - Schnorr provides best performance (100 bytes memory, ~1M cycles, ~130 bytes for communication)
  - Okamoto provides enhanced security features (148 bytes memory, ~2M cycles, ~180 bytes for communication)
  - GPS provides fast challenge-response computation (100 bytes memory, ~1.6M cycles, ~150 bytes for communication)
- ECC-based identification and signature schemes have nearly the same complexity
  - Hash computation needs about 4000 additional clock cycles

Thanks for your attention!

Questions?

http://www.iaik.tugraz.at/