ECC based Mutual Authentication Scheme for RFID

Parshuram Budhathoki
Cameron University

Topic

- RFID
- Mutual Authentication
- Elliptic Curve Cryptography
- One Example
- Implementation
- Ongoing Work

RFID

“friend or foe” Identification system used in World war II on aircraft

RFID

RFID

RFID Tag

RFID

RFID Reader

RFID

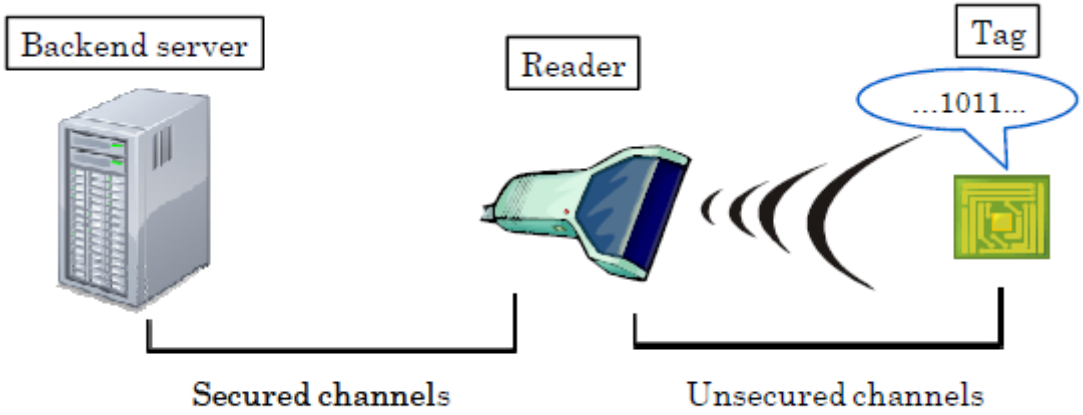
RFID

RFID

RFID

RFID

Mutual Authentication

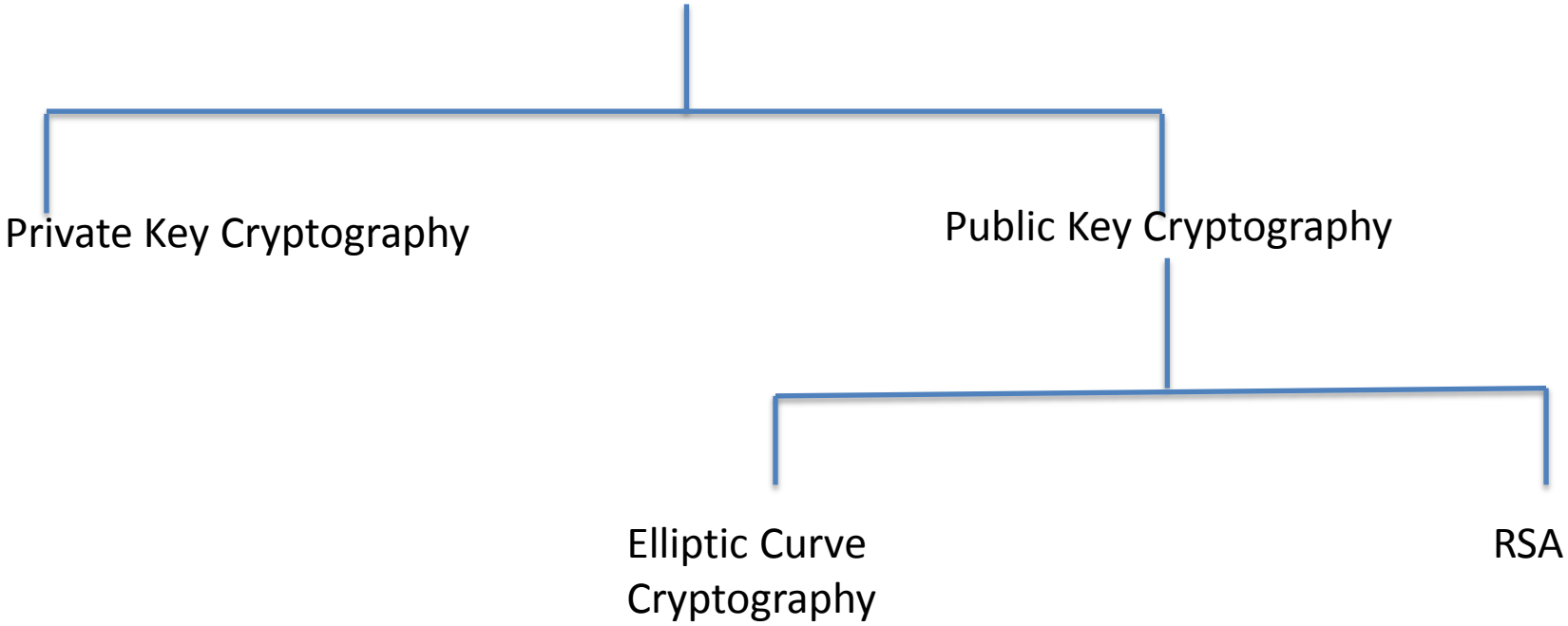


Cryptography

Private Key Cryptography

Public Key Cryptography

Cryptography



Elliptic Curve Cryptography

In 1985, Victor Miller and Neal Koblitz independently proposed public key cryptography based on the group structure of elliptic curves over finite fields.

Elliptic Curve Cryptography

ECC Key Size	RSA Key Size	Key Size Ratio
163	1024	1:6
256	3072	1:12
384	7680	1:20
512	15360	1:30

One Example

$\mathbb{G}$	An additive group of prime order q on an elliptic curve
P	A generator of $\mathbb{G}$
X_i	The identifier of ith tag which is a random point in $\mathbb{G}$
y	The private key of the server
Y	The public key of the server which is $Y = yP$
h	A one-way hash function

One Example

Tag$_i$ $\{X_i, Y, P\}$		Server $\{y, Y = yP, P\}$
		$r \in \mathbb{Z}_q$ $C_0 = rY$
	$\{C_0\}$ ←	
$k \in \mathbb{Z}_q$ $K = kP$ $C_1 = kC_0$ $R = K + K$ $C_2 = X_i + R$ $C_3 = h(X_i, K)$		
	$\{C_1, C_2, C_3\}$ →	
		$K' = y^{-1}r^{-1}C_1$ $X' = C_2 - 2K'$ $h(X', K')? = C_3$ $C_4 = h(X_i, 3K')$
	$\{C_4\}$ ←	
$R = R + K = 3K$ $h(X_i, R)? = C_4$		

Chou's RFID mutual authentication scheme

Implementation

- Scalar Multiplication
- Hash Functions
- Addition

Implementation

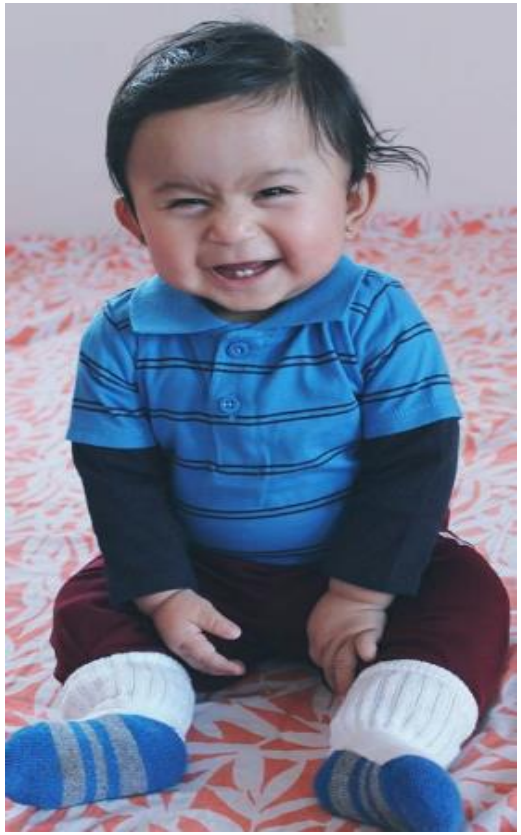
	Tuyls (Tag, Server)	Batina (Tag, Server)	Lee (Tag, Server)	Chou (Tag, Server)	Farash (Tag, Server)	Ours (Tag, Server)
Hash	(0, 0)	(0, 0)	(0, 0)	(2, 2)	(2, 2)	(3, 3)
Scalar Multiplication	(1, 2)	(2, 4)	(3,3)	(2, 2)	(2, 3)	(0, 4)

On Going Work

- Randomness
- Security Proof
- Implementation

Reference

1. J.S. Chou et al “An efficient RFID mutual authentication scheme based on ECC”
2. L. Batina et al “RFID-tags for Anti-Counterfeiting”
3. P. Tuyls et al “Public-Key Cryptography for RFID tags”
4. Y.K. Lee et al “Anti-counterfeiting Untraceability and Other Security Challenges for RFID Systems-Public-Key-Based Protocols and Hardware”
5. M.S. Farash “Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography”
6. Chin-I Lee et al “An Elliptic Curve Cryptography-Based RFID Authentication Securing E-Health System”
7. Md. Endadul Hoque, Protecting Privacy and Ensuring Security of RFID Systems Using Private Authentication Protocols
8. Picture Source: Internet



Thank you!