Novel construction of Secure RFID Authentication Protocol

Shafiqul Abidin *shafiqulabidin@yahoo.co.in*
Department of Information Technology
Northern India Engineering College
(GGSIP University)
Shastri Park, Delhi - 110053, India

Abstract

This article proposes an efficient and secure authentication protocol for secure and low-cost RFID systems in random oracles. Security is one of the prime concerns of RFID system. Proposed protocol relies on Elliptic Curve Discrete Logarithm Problem (ECDLP) to achieve security. The protocol achieves the most important security goals scalability, anonymity and anti-cloning for RFID system. A password based protocol has vulnerability on fixed password. This can be exploited by threats. In the proposed protocol, there is a provision to change the password of the Tags. Hence the vulnerability can be reduced in an acceptable level. Computation cost is very less as compare to the other protocols.

Keywords: Authentication, ECDLP, Counterfeiting, Multicast.

1. INTRODUCTION

RFID systems have many continuing and emerging applications like access controls, tool management, supply chains, airline baggage management, livestock or inventory tracking and so on. It can also be used to distinguish between counterfeits and authentic products. The important security and operational problems such as cloning problem, tracing problem and scalability can be solved by RFID system with cheaper RFID tags for commercial applications. Security can be CMOS technologies progressively efficient and the production costs decrease, which allows stronger security solutions on tags. More expensive tags with constraints power source, less memory, gate can be used for certain commercial applications such as access control systems and costly goods for security [1] [2].

2. SECURITY MODEL FOR RFID SYSTEM

This section describes a security model. The system consists of three components: a trusted server S, reader R, and tag T.

- Typically Tags do not have its own power. It operates on electromagnetic field. These are wireless Trans ponders.

- The fields are generated by the transceiver that is the Reader. There exits two kind of broadcast challenges by responding the tags. These are unicast and multi-cast. Under the range of reader, these are addressed to all tags. But unicast challenges are addressed to particular tags.

- Server: The system has a trusted Server communicates with the reader and also reader communicates with the server. We consider that all honest tags T follow the protocol's requirements and system specifications. The parameters fixed are applied to the honest readers R and the trusted server S. Both Tag T and reader R interact by sending and receiving of data as an authentication transcript. We assume that the communication

takes place through secure channel. Since two parties involve in this communication, we can consider it as two party protocols.

3. SECURITY PROPERTIES AND ADVERSARY

This section describes the security properties and the adversary model. The protocol can be modeled in terms of the following four games with players the PPT adversary A against the honest tags T and the readers R. We have followed the Chatmon et.al [3] protocol for this model.

- Gauth : Game for authentication
- Ganon : Game to achieve anonymity
- Gtrace : Game for tracing
- Gavail: Game for availability

The game runs by the following steps.

- Initialization: In this phase the adversary A interacts with the tags and the readers in arbitrary manner.

- The knowledge of A will be examined. AdvG(A) denotes the score of A in game G . The adversary A that has no negligible advantage A to win the game G. Formally we can say

$$Adv_G(A) = \epsilon(k) \leq k^{-\mu} \; \forall \; k > k_{\mu}, \mu > 0$$

3.1 Authentication

The process of authentications is to be performed in two ways. The reader is to be authenticated by the Tag and the tag is authenticated by the reader [4] [5]. Attackers can reveal the secret information by compromising and capturing only one tag [6]. After the reveled of the information, the tags which share the secret information are a threat that can be exploited by the attacker. Attackers may replicate the same to other tags. In the game for authentication Gauth, A must masquerade as some tag T to some reader R. During this masquerade step, A will be allowed to interact arbitrarily with all other tags and readers, except the one tag T that A is trying to masquerade. The advantage of the adversary advA on game Gauth is the probability that A succeeds in authenticating itself to R. An authenticated protocol is said to be secure under Gauth, if there does not exist PPT adversary that has no negligible advantage i.e

$$Adv_{Gauth}(A) = \epsilon(k) \leq k^{-\mu} \; \forall \; k > k_{\mu}, \mu > 0$$

3.2 Untraceability

In this game Gtrace, A traces various tags T. The attacker A is allowed to access to a challenge tag $\check{T}$ and pass the information whether $\check{T}$ is T or not, better than guessing. During the tracing, A is give to interact with all tags and readers, in particular, interacting with T. The advantage advA Gtrace of the adversary in this game is The protocol face untracebility if advA Gtrace is negligible i.e

$$adv^A G_{trace} = \epsilon(k) \leq k^{-\mu} \; \forall \; k > k \mu \, , \mu > 0$$

3.3 Unlinkability

This is a strong notion of anonymity. The advantage of the adversary is denoted by advAGanon. Here there will be two different interactions to the same tag in the linking. In the initial step of the game, the adversary has the knowledge about the tag T from the previous interaction. In Ganon both T and $\check{T}$ are challenge tags. Through interacting with T and $\check{T}$ as well as all other normal tags and readers, A must tell whether it is interacting with identical tags or not i.e whether T and $\check{T}$ have the same key or not.

3.4 Availability

In this game Gavail, the adversary A must thwart a tag T from being authenticated by a reader R in a challenge session ses, without interacting with this session ses. The advantage advAGanon of A in this game is the probability that R rejects T in the challenge session ses.

4. PROPOSED PROTOCOL

The proposed authentication protocol comprises five phases Registration, login, Verification and Mutual Authentication phases. The following phases are described bellow:

- **Registration Phase**
  1. The Tag T with identity IDi chooses a random password pwi and a random number t in Z*n. Computes pwj = H($pw_i \oplus t$).
  2. The tag T sends pw_j as registration request, after receiving the request, server S computes the tag authentication key as $K_{IDi} = q_s \cdot H_1(ID_i)$.
  3. Server S chooses the base point the P on the elliptic curve of order n and computes the public and private key pairs (q_s,Q_s), where $Q_s = q_s \cdot P$.
  4. S computes $\lambda_i = H(_{IDi} \oplus pw_j)$, $\mu_i = H(pw_j \| ID_i) \oplus K_{IDi}$.
  5. S stores the Tag's smart card <λ_i, μ_i>.

- **Login Phase**
  T sends the pairs <ID_i, pw_i> to obtain the S's message transcript and computes pw_j = H($pw_i \oplus t$), $\lambda'_i = H(ID_i \oplus pw_j)$ and check the equality $\lambda_i = \lambda'_i$. When the login phase has been accepted, the Tag T proceeds the following steps with the Reader R.
  1. T obtains its authenticated key K_{IDi} and selects a point $U_i = (x_i, y_i)$
  2. Computes $\theta_1 = H_2(T_1)$,$m_i = U_i + \theta_1 \cdot K_{IDi}$ and $\hat{U}_i = x_i \cdot P$ at time stamp T_i
  3. Sends the message transcript <T_1, ID_i, m_i, $\hat{U}_i$ > to S.

- **Verification Phase**
  After receiving the transcript message <T_1, ID_i, m_i, $\hat{U}_i$ > through the reader R, S performs the following steps to verify the tag:
  1 Computes $Q_{IDi} = H_1(IDi)$, $\theta_1 = H_2(T_1)$ and $U_i' = m_i - q_s\theta_1 Q_{IDi}$.
  2 S verifies whether $\hat{U}_i = x'_i \cdot P$. If holds then the tag is authenticated by the server.
  3 S sends the transcript message <T_2,m_s,m_k> through the reader R, S chooses a point U_s on the elliptic curve and computes $\theta_2 = H_2(T_2)$, $m_s = U_s + \theta_2 qs Q_{IDi}$ mod n. session key $SK = H_3(x_Q, x_i, x_s)$ and $m_k = (k + x_s) \cdot P$.

Finally S sends the message transcript <T_2,m_s,m_k> through the public channel in order to respond the request of R at time stamp T_2.

- **Mutual Authentication Phase**
  This phase performs the following steps:
  1. S sends the transcript <T_2,m_s,m_k> to the reader R, R sends a login request to S.

2. Computes $Q_{IDi} = H_1(ID_i)$, $\theta_2 = H_2(T_2)$, $U_s' = m_s - \theta_2 \cdot K_{IDi}$.
3. R computes $SK' = H_3(xQ \| x_i \| x'_s)$ and $m'_k = (k' + x'_s) \cdot P$.
4. Verify whether $m'_k = m_k$. If holds then S is authenticated by R.

5. PERFORMANCE ANALYSIS

We can evaluate the performance of the proposed protocol in term of its computation cost. Computation time for authentication can be evaluated in two phases, verification and mutual authentication [7] [8] [9]. Consider the following notation to compute computation time.

- T_H : time required to compute hash function.
- T_{add} : time required for addition of points on Elliptic curve.
- T_{PK} : time required to compute private key.
- T_{PU} : time required to compute public key.
- T_{mul} : time for point multiplication.
- Te : Elliptic curve polynomial computation time.

Total computation time is $T = 11T_H + 4T_{add} + 6T_{mul} + 2T_e$

In this research article, I have proposed an authentication protocol with provable security. It is resistant to insider attack, masquerade attack and provides mutual authentication. Security of the protocol relies on ECDLP. The protocol is also susceptible to forgery attacks. Since more expensive tags with constraints power source, less memory, gate can be used for certain commercial applications such as access control systems, the protocol is most suitable for implementation.

6. REFERENCES

[1] E.K. Ryu, and T. Takagi A hybrid approach for privacy-preserving RFID tags,Computer Standards & Interfaces, Vol. 31, 2009, pp. 812-815.

[2] 10. H.yeh, T.Ho Chen, Pin-Chuan Liu, Tai Hoo Kim and Hsin-Wen Wei A Secure Authenticated Protocol for Wireless Sensor Networks Using ECC, Sensor pp 4767-4779, 2011.

[3] C.Chatmon and T.Burmester Secure Anonymous RFID Authentication Protocols, available at www.cs.fsu.edu/ burmeste/TR-060112.pdf

[4] D. N. Duc, and K. Kim Defending RFID authentication protocols against DoS attacks, Computer Communications, 2010.

[5] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, V. Khandelwal Design and implementation of PUF-based unclonable RFID ICs for anti-counterfeiting and security applications, Proceedings of the IEEE International Conference on RFID, April 2008, pp. 58–64.

[6] Wenbo Mao Modern Cryptography - Theory And Practice, 2003, Prentice Hall, pp.196-203.

[7] D. Hankerson, A .Menezes and S.Vanstone. Guide to Elliptic Curve Cryptography, Springer Verlag, 2004

[8] "Certicom ECC Challenge and The Elliptic Curve Cryptosystem" available :http://www.certicom.com/index.php.

[9] Murat Fiskiran A and B Ruby Lee Workload characterization of elliptic curve cryptography and other network security algorithms for constrained environments.