An Improved RSA-based Certificateless Signature Scheme for Wireless Sensor Networks

Gaurav Sharma, Suman Bala, and Anil K. Verma
(Corresponding author: Gaurav Sharma)
Computer Science and Engineering Department, Thapar University, Patiala 147004, India
(Email: gaurav.sharma@thapar.edu)
(Received Aug. 15, 2013; revised and accepted Jan. 7 & Apr. 28, 2014)

Abstract

The entire world is looking to fulfill the need of the hour in terms of security. Certificateless cryptography is an efficient approach studied widely due to two reasons: first, it eliminates the need of certificate authority in public key infrastructure and second, it can resolve key escrow problem of ID-based cryptography. Recently, Zhang et al. proposed a novel security scheme based on RSA, applicable to real life applications but could not cope up with the well defined attacks. This paper, presents an RSA-based CertificateLess Signature (RSA-CLS) scheme applicable to wireless sensor networks. The security of RSA-CLS is based on the hardness assumption of Strong RSA. The scheme is proven to be secure against Type I and Type II attack in random oracle model.

Keywords: Certificateless public key cryptography, digital signature, RSA

1 Introduction

Express progress in the field of technology made it feasible to foster wireless sensor networks technology [1, 7, 21]. Wireless Sensor Networks (WSN) are comprised of large number of tiny sensor nodes with constrained resources in terms of processing power, energy and storage. WSN can be used in various applications mainly environmental monitoring, medical, military, and agriculture [1]. Since, devices used in sensor networks is not tamper resistant, so adversary can gain its physical access easily. Hence, the main objective is to protect the data from unauthorized access, which can be done by using some security mechanisms [6, 9, 29]. The technology faces lots of security problems as it has a wireless mode of communication and access to such sensor devices is quite easy. There are two approaches to restrict the unauthorized access in to the network: symmetric cryptography [39] and asymmetric cryptography [30]. Initially, symmetric algorithms are preferable to asymmetric algorithms, as they are simple and less computational for 8-bit micro-controller. Symmetric algorithms need key pre-distribution. The problem with this approach is the number of keys stored in each sensor node and the network is not forward secure after the compromising of the key. Moreover, it causes greater configuration effort before deployment and generating ample traffic, thus consequently higher energy consumption [8]. As a result, researchers are redirecting their attention to asymmetric algorithms but asymmetric algorithms are very challenging for constrained resources in WSN.

In traditional Public Key Infrastructure (PKI), the user selects a public key but it needs to be validated by a trusted third party known as Certificate Authority (CA) [3]. The CA provides a digital certificate to tag the public key with the user's identity. PKI has a problem of high computation and storage. To avoid this, Shamir [24] introduced the concept of Identity-based Infrastructure. It allows the user to choose a public key of its own choice such as email-id, phone number, name, etc. and the private key is generated by trusted third party server, Private Key Generator (PKG) causing a key escrow problem. Then, Al-Riyami et al. [2] presented a novel approach to solve the key escrow problem familial to Identity-based Cryptography (IBC) and eliminated the use of certificates in traditional Public Key Cryptography (PKC) known as CertificateLess Public Key Cryptography (CL-PKC). In CL-PKC, the trusted third party server, Key Generation Centre (KGC) generates a partial private key for the user wherein user's secret key and partial private key are used to generate public key of the user. In other words, CL-PKC differs from IBC in terms of arbitrary public key and when a signature is transmitted, user's public key is attached with it but not certified by any of the trusted authority. Thus, the KGC does not come to know the secret key of the user.

Thereafter, lots of CertificateLess Signature (CLS) schemes based on Discrete Logarithm Problem (DLP) have been presented and cryptanalyzed [12, 15, 17, 36]. Later, CLS schemes based on Elliptic Curve Discrete Logarithm Problem (ECDLP) has been presented and cryptanalyzed such as [10, 27, 28, 35, 40, 41]. Xu et al. [33, 34] presented two CLS schemes for emergency mobile wireless

cyber-physical systems and mobile wireless cyber-physical systems respectively. But Zhang et al. [37] proved it insecure against public key replacement attack. Another, authenticated scheme for WSN was presented by Li et al. [19].

Since, the pairing operation is the most expensive operation among all, so there was a need to find the solution. In 2009, Wang et al. [31] presented a scheme which need not to compute the pairing at the sign stage, rather it precomputes and publishes as the system parameters. But, this is not the solution for the removal of pairing operation. In 2011, He et al. [13] developed an efficient short CLS scheme without pairing. After a while, few schemes have been presented and cryptanalyzed based on ECDLP without pairing [11, 26].

Another aspect of pairing free CLS scheme was presented by Zhang et al. [38] in 2012, based on Strong RSA assumption and proven to be secure against Super Type I adversary in random oracle model. But, proved insecure in [14, 25] independently against key replacement attack. Watro et al. [32] initiated the concept of RSA based cryptography in public-key based protocols for wireless sensor networks known as TinyPK. Bellare et al. [5] presented an Identity-Based Multi-Signature (IBMS) scheme based on RSA, which is secure under the one-wayness of RSA in the random oracle model.

This paper presents a new RSA-based Certificateless Signature (RSA-CLS) scheme for WSN based Strong RSA assumption and proven to be secure against Super Type I and Super Type II attacks in random oracle model.

1.1 Organization of the Paper

The rest of the paper is organized as follows: In the next section, we will discuss motivation and our contribution. Section 2 describes preliminaries, which includes complexity assumptions, formal model and security model of CLS scheme. Section 3, describes the proposed RSA-based CertificateLess Signature (RSA-CLS) scheme. Section 4 discusses about the analysis of the proposed RSA-CLS scheme, including security proofs against Type I and Type II adversary in the random oracle model and performance analysis w.r.t WSN followed by conclusion.

1.2 Motivation and Our Contribution

The real truth is far from imagination, i.e. there are many theories proposed for secure transmission. At present most of the theories are on paper but far from the real application. RSA has been implemented already in various applications like WSN, cloud computing etc. So, it would be preferable to upgrade the existing system rather implementing a new system. In present scenario, CL-PKC is the most convincing approach to provide secure communication. The main benefits of RSA based CertificateLess Signature (RSA-CLS) scheme is to avoid pairing operations which is the most expensive operation for resource-constrained WSN. Zhang et al. [38] proposed a scheme and claimed that their scheme based on Strong RSA assumption, is: (i) more practical as far as industry standard goes, (ii) secure in random oracle model, (iii) more efficient than existing schemes as no pairing operation is involved, (iv) secure against Super Type I (discuss in Section 2.3) adversary [16] (which implies the security against Strong and Normal Type both) and left an open problem of designing of CLS scheme secure in standard model. Sharma et al. [25] and He et al. [14] independently found that the scheme [38] is not secure against key replacement attack. Sharma et al. [25] proved that the [38] is insecure against Strong Type I attack. In Strong Type I attack, the adversary has a privilege to choose a private key, and query the challenger to replace the public key and breach the security of the scheme. We have avoid such kind of attack in scheme [38], by modifying the value of $R_1 = H_0(ID)^{r_1}$ to $R_1 = x_{ID}^e H_0(ID)^{r_1}$ and the corresponding value of u_1.

2 Preliminaries

In this section, we briefly review some fundamental concepts akin to CLs, which includes formal model and security notions. We further state the hardness assumptions required in the proposed RSA-CLS scheme.

2.1 Complexity Assumptions

In this section, we describe the complexity assumptions which are requisite for the security proof of the proposed scheme. The security of our proposed signature scheme will be attenuated to the hardness of the Strong RSA Assumption [22] in the group in which the signature is constructed. We briefly review the definition of the Strong RSA Assumption and Discrete Logarithm Problem (DLP) [20]:

Definition 1. *(Strong RSA Assumption). Let $n = pq$ be an RSA-like modulus and let G be a cyclic subgroup of Z_n^* of order $\#G, \lceil \log_2(\#G) \rceil = l_G$. Given (n, e) and $z \in G$, the strong RSA problem consists of finding $u \in Z_n$ satisfying $z = u^e \mod n$.*

Definition 2. *(Discrete Logarithm Problem). Let $n = pq$ be a RSA modular number which satisfying $p = 2p' + 1$, $q = 2q' + 1$, $g \in Z_n^*$ is a generator of order $p'q'$, for given elements g, y, n, its goal is to compute the exponent x such that $y = g^x \mod n$.*

2.2 Formal Model of Certificateless Signature Scheme

This section describes the formal model of a certificateless signature scheme, which consists of seven polynomial-time algorithms. These are:

Setup. This algorithm is run by the KGC to initialize the system. It takes as input a security parameter 1^k and outputs a list of system parameters *params*

and the master secret key d. The system parameters $params$ is public to all where as the master secret key d is known to KGC only.

Partial-Private-Key-Extraction. This algorithm is run by the KGC, takes the system parameters $params$, master secret key d, and an identity $ID \in \{0,1\}^*$ as input, and outputs the partial private key d_{ID}, which is sent to the user via a secure channel.

Set-Secret-Value. This is a probabilistic algorithm, run by the user. It takes the system parameters $params$ and the user's identity ID as input and outputs a secret value x_{ID}.

Set-Private-Key. This is a deterministic algorithm, run by the user. It takes the system parameters $params$, a partial private key d_{ID}, and a secret value x_{ID} as inputs and outputs a full private key SK_{ID} .

Set-Public-Key. This is a deterministic algorithm, run by the user. It takes the system parameters $params$, the user's identity d_{ID}, and the private key $SK_{ID} = (d_{ID}, x_{ID})$ as inputs and outputs a public key PK_{ID}.

CL-Sign. This algorithm is run by the user, takes the system parameters $params$, the user's identity ID, and the private key SK_{ID} and a message M as input and outputs a correct certificateless signature δ on message M.

CL-Verify. This algorithm is run by the user, takes the system parameters $params$, the user's identity ID, public key PK_{ID}, message M, and the signature δ as input and outputs $true$ if the signature is correct, or else $false$.

2.3 Security Models

As for security model [16], a CLS scheme is different from an ordinary signature scheme. Certificateless signature scheme is vulnerable to two types (Type I and Type II) of adversaries. The adversary $\mathcal{A}_I$ in Type I represents a normal third party attacker against the CLS scheme. That is, $\mathcal{A}_I$ is not allowed to access to the master key but $\mathcal{A}_I$ may request public keys and replace public keys with values of its choice. The adversary $\mathcal{A}_{II}$ in Type II represents a malicious KGC who generates partial private keys of users. The adversary $\mathcal{A}_{II}$ is allowed to have access to the master-key but not replace a public key.

3 Proposed RSA-based Certificateless Signature Scheme (RSA-CLS)

In this section, we describe the proposed certificateless signature scheme based on Strong RSA assumption. The scheme works as follows.

Setup: Given a security parameter 1^k as input, a RSA group (n, p, q, e, d) is generated, where p' and q' are two large prime numbers which satisfy $p = 2p' + 1$ and $q = 2q' + 1$, $n = pq$ is a RSA modular number, $e < \phi(n)$ is the public key of Key Generation Center (KGC) and satisfies $gcd(e, \phi(n) = 1$ and $ed \equiv 1 \bmod \phi(n)$, where $\phi(n)$ denotes the Euler Totient function. Choose two cryptographic hash functions H and H_0 which satisfy $H_0 : \{0,1\}^* \to Z_n^*$ and $H : Z_n^4 \times \{0,1\}^* \to \{0,1\}^l$, where l is a security parameter. The master secret key is d and the public parameters of system is $params = \{n, e, H, H_0\}$.

Partial-Key-Extract: For a user with identity $ID \in \{0,1\}^*$, KGC computes partial private key by using the master secret key as $d_{ID} = H_0(ID)^d \bmod n$.

Set-Secret-Value: Given $params$ and an identity ID, the user randomly chooses $x_{ID} \in Z_{2^{|n|/2-1}}$, where $|n|$ denotes the binary length of n.

Set-Private-Key: Given the partial private key d_{ID} and the secret value x_{ID} of a user with identity ID, output $SK_{ID} = (x_{ID}, d_{ID})$.

Set-Public-Key: Given the partial private key d_{ID} and the secret value x_{ID} of a user with identity ID, output $PK_{ID} = H_0(ID)^{x_{ID}} \bmod n$.

Sign: Given a message m and system parameters $params$, a user with identity ID computes the following steps by using its private key.

1) Randomly choose two numbers r_1, $r_2 \in Z_{2^{|n|/2-1}}$.
2) Compute $R_1 = x_{ID}^e H_0(ID)^{r_1} \bmod n$ and $R_2 = H_0(ID)^{r_2} \bmod n$.
3) Compute $h = H(R_1, R_2, ID, PK_{ID}, m)$.
4) Set $u_1 = x_{ID} d_{ID}^{r_1 - h} \bmod n$ and $u_2 = r_2 - x_{ID} h$.
5) Finally, the resultant certificateless signature on message m is $\delta = (u_1, u_2, h)$.

Verify: Given a certificateless signature $\delta = (u_1, u_2, h)$ on message m, a verifier executes as follows:

1) Compute $R_1' = u_1^e H_0(ID)^h \bmod n$ and $R_2' = H_0(ID)^{u_2} PK_{ID}^h \bmod n$.
2) Accept, if and only if the following equation holds $h = H(u_1^e H_0(ID)^h \bmod n, H_0(ID)^{u_2} PK_{ID}^h \bmod n, ID, PK_{ID}, m)$.

Correctness: In the following, we show that our scheme is correct and satisfies completeness.

$$
\begin{aligned}
& H(u_1^e H_0(ID)^h, H_0(ID)^{u_2} PK_{ID}^h \bmod n, ID, PK_{ID}, m) \\
= \; & H((x_{ID} d_{ID}^{r_1 - h})^e H_0(ID)^h, \\
& \quad H_0(ID)^{r_2 - x_{ID} h} PK_{ID}^h \bmod n, ID, PK_{ID}, m) \\
= \; & H(x_{ID}^e H_0(ID)^{d(r_1 - h)e} H_0(ID)^h, \\
& \quad H_0(ID)^{r_2 - x_{ID} h + x_{ID} h} \bmod n, ID, PK_{ID}, m) \\
= \; & H(x_{ID}^e H_0(ID)^{r_1}, H_0(ID)^{r_2} \bmod n, ID, PK_{ID}, m) \\
= \; & h.
\end{aligned}
$$

4 Analysis of RSA-CLS Scheme

4.1 Security Analysis

In this section, we prove that the proposed scheme is secure against Type I and Type II adversaries defined in Section 2.3 in the random oracle model H_0 and H. The following theorems are provided for the security.

Theorem 1. *If there exists a Type I adversary $\mathcal{A}_I$ who can ask at most q_{H_0} and q_H* ***Hash*** queries *to random oracles H_0 and H, q_s* ***Sign*** queries, *q_{ppk}* ***Partial-Private-Key-Extract*** queries, *and q_p* ***Private-Key-Extract*** queries, *and can break the proposed scheme in polynomial time τ with success probability ϵ, then there exists an algorithm β that solves the RSA problem with advantage, $\eta > \frac{(q_s+1)(q_s+q_{H_0})\epsilon}{2^l q_H \tau(q_{ppk}+q_p+q_s+1)}$.*

Proof. If there exists an adversary $\mathcal{A}_I$, who can break the proposed certificateless signature scheme. Then, we can construct another adversary β, known as RSA adversary, such that β can use $\mathcal{A}_I$ as a black-box and solve the RSA problem. The aim is to find $y^e = z$, where $y \in Z_n^*$ in n RSA modulus and (n, e, z) is an instance of RSA problem.

Setup: The adversary β selects two hash functions H_0 and H as random oracle. d is the master secret key, which satisfies $ed \equiv 1 \bmod \phi(n)$ and is unknown to β. The system parameters (e, n) is public to all. The adversary β maintains three lists *H_0-list*, *H-list* and *KeyList*, which are initially empty. The adversary β sends (e, n, z, H_0, H) as a final output to the adversary $\mathcal{A}_I$.

Queries: At any time, $\mathcal{A}_I$ is allowed to access the following oracles in a polynomial number of times. Then, β simulates the oracle queries of $\mathcal{A}_I$ as follows:

1) **H_0-Hash Queries:** $\mathcal{A}_I$ can query the random oracle H_0 at any time with an identity ID. In response to these queries, β flips a biased $coin \in \{0, 1\}$ at random such that $Pr[coin = 0] = \rho$. Then, β randomly chooses $t_{ID} \in Z_n$ and compute $h_{ID}^0 = z_{coin} t_{ID}^e$ and send it to $\mathcal{A}_I$. β add $(ID, h_0, t_{ID}, coin)$ to the *H_0-list*.
2) **H-Hash Queries:** $\mathcal{A}_I$ can query the random oracle H at any time with $h = H(R_1, R_2, ID, PK_{ID}, m)$. For each query $(R_1, R_2, ID, PK_{ID}, m)$, β first checks the *H-list*:
   a. If $(R_1, R_2, ID, PK_{ID}, m, h)$ exists in the *H-list*, then β sets $H(R_1, R_2, ID, PK_{ID}, m) = h$ and returns h to $\mathcal{A}_I$.
   b. Else, β randomly chooses $h \in Z_n^*$, and add the record $(R_1, R_2, ID, PK_{ID}, m, h)$ to the *H-list*. β sends h to $\mathcal{A}_I$ as the corresponding response.
3) **Partial-Private-Key-Extract Queries:** At any time, $\mathcal{A}_I$ can query the oracle by giving an identity ID. β outputs a symbol $\perp$ if ID has not been created. Else, if ID has been created and $coin = 0$, then β returns t_{ID} to the adversary $\mathcal{A}_I$. Otherwise, β returns failure and terminates the simulation.
4) **Public-Key-Request Queries:** At any time, $\mathcal{A}_I$ can query the oracle by giving an identity ID. β randomly chooses $x_{ID} \in Z_{2^{|n|/2-1}}$ and searches the *H_0-list* for $(ID, h_{ID}^0, t_{ID}, coin)$. Then, β adds $(ID, PK_{ID} = {h_{ID}^0}^{x_{ID}}, x_{ID}, coin)$ to *KeyList* and send PK_{ID} to $\mathcal{A}_I$.
5) **Private-Key-Extract:** For a given identity ID chosen by $\mathcal{A}_I$, β searches (ID, h_{ID}^0, t_{ID}, $coin$) in the *H_0-list*. If $coin = 1$, then β aborts it, else, β searches (ID, $PK = {h_{ID}^0}^{x_{ID}}$, x_{ID}, $coin$) in the *KeyList*. β return $SK_{ID} = (x_{ID}, t_{ID})$ to $\mathcal{A}_I$ as a final output.
6) **Public-Key-Replace Queries:** $\mathcal{A}_I$ can request a query to replace public key PK_{ID} of an identity ID with a new public key PK'_{ID} chosen by $\mathcal{A}_I$ itself. As a result, β replaces the original public key PK_{ID} with PK'_{ID} if ID has been created in the *H_0-list*. Otherwise, output $\perp$.
7) **Sign Queries:** For each query on an input (m, ID), output $\perp$ if ID has not been queried before. For any input (m, ID) with ID which has already been queried, β searches *H_0-list* and *KeyList* for $(ID, h_{ID}^0, t_{ID}, coin)$ and $(ID, PK_{ID}, x_{ID}, coin)$. If $coin = 0$, then β produces a certificateless signature δ on message m by the returned private key (x_{ID}, t_{ID}). Otherwise, β computes as follows:
   a. β randomly chooses $u_1 \in Z_n^*$, $h \in \{0, 1\}^l$, and $u_2 \in Z_{2^{|n|/2-1}}$.
   b. β computes $R_1 = u_1^e H_0(ID)^h$ and $R_2 = H_0(ID)^{u_2} {PK_{ID}}^h$, where PK_{ID} may be a replaced public key.
   c. β searches whether $(R_1, R_2, ID, PK_{ID}, m)$ exists in the *H-list*. If it exists, then abort it. Else, β sets $H(R_1, R_2, ID, PK_{ID}, m) = h$ and adds $(R_1, R_2, ID, PK_{ID}, m, h)$ in the *H-list*.
   d. The resultant signature $\delta = (u_1, u_2, h)$ is returned to $\mathcal{A}_I$.

Output: After all the queries, $\mathcal{A}_I$ outputs a forgery $(ID^\star, PK_{ID}^\star, m^\star, \delta^\star = (u_1{}^\star, u_2{}^\star, h^\star))$ and win this game. It must satisfy the following conditions:

1) If $\delta^\star$ is a valid forgery, then $h^\star = H(R_1{}^\star, R_2{}^\star, PK_{ID^\star}, ID^\star, m)$, which is in the *H-list*, where $R_1{}^\star = {u_1{}^\star}^e H_0(ID^\star)^{h^\star}$ and $R_2{}^\star = H_0(ID^\star)^{{u_2}^\star} PK_{ID^\star}^{h^\star}$).
2) $coin^\star = 1$ of the record $(ID^\star, h_{ID^\star}^0, t_{ID^\star}, coin^\star)$ in the *H_0-list*.

By applying Forking Lemma [22], after replaying $\mathcal{A}_I$ with the same random tape but different choices of oracle H, β can obtain another valid certificateless signature $(ID^\star, PK_{ID^\star}, m^\star, \delta'^\star = (u_1'^\star, u_2'^\star, h'^\star))$. Then, they should satisfy ${R_1}^\star = {u_1}^{\star e} H_0(ID^\star)^{h^\star}$ and ${R_1}^\star = {u_1'}^{\star e} H_0(ID^\star)^{h'^\star}$. Thus, we have the following relation

$$
\begin{aligned}
{u_1}^{\star e} H_0(ID^\star)^{h^\star} &= {u_1'}^{\star e} H_0(ID^\star)^{h'^\star} \\
(\frac{{u_1}^\star}{{u_1'}^\star})^e &= H_0(ID^\star)^{h'^\star - h^\star} \\
(\frac{{u_1}^\star}{{u_1'}^\star})^e &= (z {t_{ID^\star}}^e)^{h'^\star - h^\star} \\
(\frac{{u_1}^\star}{{t_{ID^\star}}^{h'^\star - h^\star} {u_1'}^\star})^e &= (z)^{h'^\star - h^\star}.
\end{aligned}
$$

Because e is a prime number, it means that $gcd(e, h'^\star - h^\star) = 1$, then there exists two numbers a, b satisfying $ae + b(h'^\star - h^\star) = 1$. Thus, we can obtain

$$
\begin{aligned}
z &= z^{ae + b(h'^\star - h^\star)} \\
&= z^{ae} z^{b(h'^\star - h^\star)} \\
&= z^{ae} (\frac{{u_1}^\star}{{t_{ID^\star}}^{h'^\star - h^\star} {u_1'}^\star})^{eb} \\
&= (z^a (\frac{{u_1}^\star}{{t_{ID^\star}}^{h'^\star - h^\star} {u_1'}^\star})^b)^e.
\end{aligned}
$$

This shows that the RSA problem can be solved by β. Hence, it is in contradiction to the RSA problem.

Analysis: We show that β solves the given instance of the RSA problem with the probability η. We will observe that β does not abort during the whole simulation, $\mathcal{A}_I$ can forge the signature and the valid certificateless signature $(ID^\star, PK_{ID^\star}, m^\star, \delta'^\star = (u_1'^\star, u_2'^\star, h'^\star))$ satisfies ${R_1}^\star = {u_1}^{\star e} H_0(ID^\star)^{h^\star}$ and ${R_1}^\star = {u_1'}^{\star e} H_0(ID^\star)^{h'^\star}$. In **Partial-Private-Key-Extract** phase and **Private-Key-Extract** phase, the probability of β does not abort is at most $(1-\rho)^{q_{ppk}}$ and $(1-\rho)^{q_p}$, respectively. In **Signing phase**, the probability of no aborting is at most $(1-\rho)^{q_s}/q_H$. Thus, the probability of β does not abort in the simulation is at most $(1-\rho)^{q_{ppk}+q_p+q_s}(1-\rho)\cdot 1/q_H$ which is maximized at $\rho = 1-1/(q_{ppk}+q_p+q_s+1)$. That is to say, the probability of β does not abort is at most $1/\tau(q_{ppk}+q_p+q_s+1)$, where τ denotes the base of the natural logarithm. Therefore, the probability of solving the RSA problem is $\eta > \frac{(q_s+1)(q_s+q_{H_0})\epsilon}{2^l q_H \tau(q_{ppk}+q_p+q_s+1)}$.

□

Theorem 2. *In the random oracle model, if there exists a type II adversary $\mathcal{A}_{II}$, who is allowed to request at most q_{H_0}, q_H* ***Hash*** queries *to random oracles H_0 and H, respectively, and q_s* ***Sign*** queries*, can break the proposed certificateless signature scheme with probability ϵ and within a time bound τ, then there exists another algorithm β who can make use of $\mathcal{A}_{II}$ to solve the discrete logarithm problem.*

Proof. Suppose there exists a Type II adversary $\mathcal{A}_{II}$ can break the proposed scheme. We are going to construct an adversary β that makes use of $\mathcal{A}_{II}$ to solve the discrete logarithm problem. Let us recall the discrete logarithm problem: for a given number $g \in Z_n^*$ and (n, p, q), y is a random number of Z_n, its goal is to compute x which satisfies $y = g^x \bmod n$. In order to solve this problem, β needs to simulate a challenge and the **Secret-Key-Extract** queries, **Hash** queries and **Sign** queries for $\mathcal{A}_{II}$. Thereby, β does in the following ways:

Setup: β maintains three lists H_0-*list*, *H-list* and *KeyList* which are initially empty. Let (e, n) be the system parameters. The master secret key is d and satisfies $ed \equiv 1 \bmod \phi(n)$, and the master secret key d and (p, q) are known for β, where $n = pq$. Choose two hash functions H_0 and H as random oracle. Let $PK_{ID^\star} = y$ be a challenged user $U^\star$'s public key and $ID^\star$ be the identity of the challenged user $U^\star$. Finally, β sends public parameters (e, d, n, g, H_0, H) to the adversary $\mathcal{A}_{II}$.

Queries: At any time, $\mathcal{A}_{II}$ is allowed to access the following oracles in a polynomial number of times. Then, β simulates the oracle queries of $\mathcal{A}_{II}$ as follows:

1) H_0**-Hash Queries:** $\mathcal{A}_{II}$ can query this oracle by given an identity ID. β randomly chooses $t_{ID} \in \phi(n)$ to set $H_0(ID) = g^{t_{ID}}$ and returns it to $\mathcal{A}_{II}$, where $\phi(n)$ is the Euler totient function and can be obtained by p, q. Finally, add $(ID, H_0(ID), t_{ID})$ to the H_0-*list*.
2) H**-Hash Queries:** In this process, $\mathcal{A}_{II}$ can request at most q_H Hash queries. For each query (R_1, R_2, ID, PK_{ID}, m), β randomly chooses $k_{ID} \in \{0,1\}^l$ and sets $H(R_1, R_2, ID, PK_{ID}, m) = k_{ID}$. Finally, return k_{ID} to $\mathcal{A}_{II}$ and add (R_1, R_2, ID, PK_{ID}, m, k_{ID}) to the *H-list*.
3) **Public-Key-Request Queries:** At any time, $\mathcal{A}_{II}$ can query the oracle by given an identity ID. If $ID \neq ID^\star$, β randomly chooses $x_{ID} \in \phi(n)$ to compute $PK_{ID} = H_0(ID)^{x_{ID}}$, then add $(ID, PK_{ID} = H_0(ID)^{x_{ID}}, x_{ID})$ to *KeyList*. Otherwise, β searches the H_0-*list* for $(ID^\star, H_0(ID^\star), t_{ID^\star})$ and computes $PK_{ID^\star} = y^{t_{ID^\star}}$. And add the record $(ID^\star, PK_{ID^\star}, \perp)$ to *KeyList*. Finally, send PK_{ID} to $\mathcal{A}_{II}$.
4) **Private-Key-Extract Queries:** When $\mathcal{A}_{II}$ makes this query with ID, if $ID \neq ID^\star$, β searches (ID, PK_{ID}, x_{ID}) in the *KeyList*, and computes $d_{ID} = H_0(ID)^d$. Then, $\mathcal{A}_{II}$ returns (d_{ID}, x_{ID}) to the adversary $\mathcal{A}_{II}$. If $ID = ID^\star$, then β aborts it.

Table 1: Performance analysis of proposed RSA based certificateless signature scheme

Process	Running Time (s)	Energy Consumption (mJ)	ROM (KB)	RAM (Static + Stack) (KB)
Sign	1.45	34.8	1.7	2.3
Verify	1.37	32.88	1.7	2.3

5) **Sign Queries:** For each query on an input (m, ID), if $ID \neq ID^\star$, then β firstly obtains private key associated with ID by **Private-Key-Extract** queries on ID, then it produces a signature by using the obtained private key. If $ID = ID^\star$, then β computes as follows:
   a. β randomly choose $u_1 \in Z_n$ and $h \in \{0,1\}^l$, $u_2 \in Z_{\phi(n)}$.
   b. β computes $R_1 = {u_1}^e H_0(ID)^h$ and $R_2 = H_0(ID)^{u_2} PK_{ID}^h$.
   c. β searches whether $(R_1, R_2, ID, PK_{ID}, m)$ exists in the *H-list*. If it exists, then abort it. Otherwise, β sets $H(R_1, R_2, ID, PK_{ID}, m) = h$ and adds $H(R_1, R_2, ID, PK_{ID}, m, h)$ in the *H-list*.
   d. The resultant signature $\delta = (u_1, u_2, h)$ is returned to $\mathcal{A}_{II}$.

Output: After all the queries, $\mathcal{A}_{II}$ outputs a forgery $(ID^\star, PK_{ID^\star}, m^\star, \delta^\star = ({u_1}^\star, {u_2}^\star, h^\star))$ and win this game. It must satisfy the following conditions:

1) If $\delta^\star$ is a valid forgery, then $h^\star = H({R_1}^\star, {R_2}^\star, PK_{ID^\star}, ID^\star, m)$ which is in the *H-list*, where ${R_1}^\star = {u_1}^{\star e} H_0(ID^\star)^{h^\star}$ and ${R_2}^\star = H_0(ID^\star)^{{u_2}^\star} PK_{ID^\star}^{h^\star})$.
2) $ID^\star$ is the challenger's identity and $H_0()$ is queried by $ID^\star$.

By applying Forking Lemma [22], after replaying $\mathcal{A}_{II}$ with the same random tape but different choices of oracle H, β can obtain another valid certificateless signature $(ID^\star, PK_{ID^\star}, m^\star, \delta'^\star = ({u_1'}^\star, {u_2'}^\star, h'^\star))$. Then, they should satisfy ${R_2}^\star = H_0(ID^\star)^{u_2} PK_{ID^\star}^{h^\star}$ and ${R_2}^\star = H_0(ID^\star)^{u_2'} PK_{ID^\star}^{h'^\star}$. Thus, we have the following relation:

$$\begin{aligned} H_0(ID^\star)^{u_2} PK_{ID^\star}^{h^\star} &= H_0(ID^\star)^{u_2'} PK_{ID^\star}^{h'^\star} \\ (H_0(ID^\star))^{u_2 - u_2'} &= PK_{ID^\star}^{h'^\star - h^\star} \\ (g)^{t_{ID^\star}(u_2 - u_2')} &= y^{h'^\star - h^\star} \\ (g)^{t_{ID^\star}(u_2 - u_2')/h'^\star - h^\star} &= y. \end{aligned}$$

Obviously, the discrete logarithm of y to the base g is $t_{ID^\star}(u_2 - u_2')/h'^\star - h^\star$. It denotes that the discrete problem can be solved by β. Obviously, it is in contradiction to the difficulty of solving the discrete logarithm problem.

□

4.2 Performance Analysis

The proposed RSA based CLS scheme has been evaluated for WSN based on few parameters like running time and energy consumption, ROM and RAM including static RAM and stack RAM. The results are shown in Table 1. The scheme has been implemented on MICAz platform [23] using TinyOS-2.1.1 [18] operating system for embedded devices and RELIC-0.3.3 [4] cryptographic library. The running time of the proposed scheme is 1.45 seconds and 1.37 seconds in sign and verify phase respectively. The energy consumption is 34.8 milliJoules and 32.88 milliJoules in sign and verify phase respectively. Further, the proposed scheme consumes 1.7 KB of ROM and 2.3 KB of RAM (static and stack) excluding the space used by cryptographic library.

5 Conclusion

RSA is a well defined industry implemented security approach. Also certificateless schemes have their own benefits. In this paper, we proposed an RSA-based efficient certificateless signature scheme and proved it to be secure under some well-studied assumptions. We believe the new scheme is more suitable for systems with low-bandwidth channels and/or low-computation power making it suitable for WSN, on the basis of implementation results on WSN environment.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks*, vol. 38, pp. 393–422, Mar. 2002.
[2] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology (ASIACRYPT'03)*, LNCS 2894, pp. 452–473, Springer, 2003.
[3] F. Amin, H. Jahangir, and H. Rasifard, "Analysis of public-key cryptography for wireless sensor networks security," vol. 2, no. 5, pp. 403–408, 2008.
[4] D. Aranha and C. Gouvêa, "RELIC is an Efficient LIbrary for Cryptography," June 15, 2015. (`http://code.google.com/p/relic-toolkit/`)
[5] M. Bellare and G. Neven, "Identity-based multi-signatures from rsa," in *Topics in Cryptology (CT-RSA 2007)*, LNCS 4377, pp. 145–162, Springer, 2006.
[6] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Communications Surveys Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[7] Y. Chen and Q. Zhao, "On the lifetime of wireless sensor networks," *IEEE Communications Letters*, vol. 9, no. 11, pp. 976–978, 2005.

[8] L. Chun-Ta, H. Min-Shiang, and C. Yen-Ping, "Improving the security of a secure anonymous routing protocol with authenticated key exchange for ad hoc networks," *International Journal of Computer Systems Science and Engineering*, vol. 23, no. 3, pp. 227–234, 2008.

[9] L. Chun-Ta, H. Min-Shiang, and C. Yen-Ping, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803–2814, 2008.

[10] H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings," *Computer Standards and Interfaces*, vol. 31, no. 2, pp. 390–394, 2009.

[11] P. Gong and P. Li, "Further improvement of a certificateless signature scheme without pairing," *International Journal of Communication Systems*, vol. 27, no. 10, pp. 2083–2091, Oct. 2014.

[12] M. Gorantla and A. Saxena, "An efficient certificateless signature scheme," in *Computational Intelligence and Security*, LNCS 3802, pp. 110–116, Springer, 2005.

[13] D. He, J. Chen, and R. Zhang, "An efficient and provably-secure certificateless signature scheme without bilinear pairings," *International Journal of Communication Systems*, vol. 25, no. 11, pp. 1432–1442, 2012.

[14] D. He, M. Khan, and S. Wu, "On the security of a rsa-based certificateless signature scheme," *International Journal of Network Security*, vol. 15, no. 6, pp. 408–410, 2013.

[15] B. Hu, D. Wong, Z. Zhang, and X. Deng, "Key replacement attack against a generic construction of certificateless signature," in *Information Security and Privacy*, LNCS 4058, pp. 235–246, Springer, 2006.

[16] X. Huang, Y. Mu, W. Susilo, D. Wong, and W. Wu, "Certificateless signatures: New schemes and security models," *The Computer Journal*, vol. 55, no. 4, pp. 457–474, 2012.

[17] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes from asiacrypt 2003," in *Cryptology and Network Security*, LNCS 3810, pp. 13–25, Springer, 2005.

[18] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler, "Tinyos: An operating system for sensor networks," in *Ambient Intelligence*, pp. 115–148, 2005.

[19] C. Li, M. Hwang, and Y. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks," *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107–2124, 2009.

[20] K. McCurley, "Discrete logarithm problem," in *Proceedings of Symposia Applied Mathematics*, pp. 49–74, 1990.

[21] S. Olariu and Q. Xu, "Information assurance in wireless sensor networks," in *Proceedings of the IEEE International Symposium on Parallel and Distributed Processing*, vol. 13, pp. 236a, Los Alamitos, CA, USA, 2005.

[22] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Advances in Cryptology (EUROCRYPT'96)*, LNCS 1070, pp. 387–398, Springer, 1996.

[23] A. Rev, "MPR-MIB series user manual," 2004. (`http://www-db.ics.uci.edu/pages/research/quasar/MPR-MIB%20Series%20User%20Manual%207430-0021-06_A.pdf`)

[24] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, LNCS 196, pp. 47–53, Springer, 1985.

[25] G. Sharma and A. Verma, "Breaking the rsa-based certificateless signature scheme," *Information-An International Interdisciplinary Journal*, vol. 16, no. 11, pp. 7831–7836, 2013.

[26] J. Tsai, N. Lo, and T. Wu, "Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings," *International Journal of Communication Systems*, vol. 27, no. 7, pp. 1083–090, July 2014.

[27] R. Tso, X. Huang, and W. Susilo, "Strongly secure certificateless short signatures," *Journal of Systems and Software*, vol. 85, no. 6, pp. 1409–1417, 2012.

[28] R. Tso, X. Yi, and X. Huang, "Efficient and short certificateless signatures secure against realistic adversaries," *The Journal of Supercomputing*, vol. 55, no. 2, pp. 173–191, 2011.

[29] J. Walters, Z. Liang, W. Shi, and V. Chaudhary, *Security in Distributed, Grid, and Pervasive Computing*, Chap. 17 Wireless Sensor Network security: A survey, pp. 1–51, CRC Press, 2007.

[30] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications (PERCOM'05)*, pp. 324–328, Washington, DC, USA, 2005.

[31] C. Wang, D. Long, and Y. Tang, "An efficient certificateless signature from pairings," *International Journal of Network Security*, vol. 8, no. 1, pp. 96–100, 2009.

[32] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: Securing sensor networks with public key technology," in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04)*, pp. 59–64, New York, NY, USA, 2004.

[33] Z. Xu, X. Liu, G. Zhang, and W. He, "Mccls: Certificateless signature scheme for emergency mobile wireless cyber-physical systems," *International Journal*

of Computers Communications and Control, vol. 3, no. 4, pp. 395–411, 2008.

[34] Z. Xu, X. Liu, G. Zhang, W. He, G. Dai, and W. Shu, "A certificateless signature scheme for mobile wireless cyber-physical systems," in *Proceedings of the 8th International Conference on Distributed Computing Systems Workshops (ICDCS'08)*, pp. 489–494, 2008.

[35] W. Yap, S. Heng, and B. Goi, "An efficient certificateless signature scheme," in *Emerging Directions in Embedded and Ubiquitous Computing*, LNCS 4097, pp. 322–331, Springer, 2006.

[36] D. Yum and P. Lee, "Generic construction of certificateless signature," in *Information Security and Privacy*, LNCS 3108, pp. 200–211, Springer, 2004.

[37] F. Zhang, S. Li, S. Miao, Y. Mu, W. Susilo, and X. Huang, "Cryptanalysis on two certificateless signature schemes," *International Journal of Computers Communications and Control*, vol. 5, no. 4, pp. 586–591, 2010.

[38] J. Zhang and J. Mao, "An efficient rsa-based certificateless signature scheme," *Journal of Systems and Software*, vol. 85, no. 3, pp. 638–642, 2012.

[39] X. Zhang, H. Heys, and L. Cheng, "Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks," in *25th Biennial Symposium on Communications (QBSC'10)*, pp. 168–172, 2010.

[40] Z. Zhang, D. Wong, J. Xu, and D. Feng, "Certificateless public-key signature: Security model and efficient construction," in *Applied Cryptography and Network Security*, LNCS 3989, pp. 293–308, Springer, 2006.

[41] M. Zhou, M. Zhang, C. Wang, and B. Yang, "Cclas: A practical and compact certificateless aggregate signature with share extraction," *International Journal of Network Security*, vol. 16, no. 2, pp. 157–164, 2014.

Gaurav Sharma received his Ph.D and M.E degree in Computer Science & Engineering from Thapar University, Patiala, India. He had received M. Sc. as well as B. Sc. Degree from CCS University, Meerut, India. Presently he is working as an Asst. Professor at Galgotias University, India. His area of interests is routing and security in Ad hoc networks.

Suman Bala received her Ph.D and M.E degree in Computer Science & Engineering from Thapar University, Patiala, India. She had received B.Tech degree from Punjab Technical University, Jalandhar, India. Her areas of interest are: Wireless Sensor Networks, Security, Cryptography and Key Management.

Anil K. Verma is currently working as Associate Professor in the department of Computer Science and Engineering at Thapar University, Punjab (INDIA). He has more than 20 years of experience. He has published over 150 papers in referred journals and conferences (India and Abroad). He is member of various program committees for different International/National Conferences and is on the review board of various journals. He is a senior member (ACM), LMCSI (Mumbai), GMAIMA (New Delhi). He is a certified software quality auditor by MoCIT, Govt. of India. His research interests include wireless networks, routing algorithms and securing ad hoc networks.