ARTICLE IN PRESS

Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

An efficient RSA-based certificateless public key encryption scheme

Xi-Jun Lin [a,*], Lin Sun [b], Haipeng Qu [a]

[a] Department of Computer Science and Technology, Ocean University of China, Qingdao 266100, PR China
[b] College of Liberal Arts, Qingdao University, Qingdao 266071, PR China

ARTICLE INFO

Article history:
Received 8 January 2016
Received in revised form 11 August 2016
Accepted 20 February 2017
Available online xxxx

Keywords:
CL-PKE
RSA
Encryption
Bilinear pairing

ABSTRACT

In order to resolve the key escrow in identity-based scheme and the significant cost of using a PKI system in traditional public key scheme, the notion of certificateless public key cryptography (CL-PKC) was introduced. The first certificateless public key encryption scheme (CL-PKE) was proposed by Al-Riyami and Paterson, and then further schemes were developed. However, most of them are constructed from the bilinear pairing which is a time costing operation. In this paper, we construct an efficient CL-PKE scheme from RSA since RSA is the *de facto* Internet standard and is widely used in many applications. The security is based on Kilian–Petrank's RSA assumption which is a variant of RSA.

1. Introduction

In order to resolve the key escrow in identity-based scheme [12] and the significant cost of using a PKI system in traditional public key scheme, the notion of certificateless public key cryptography (CL-PKC) was introduced and developed.

The difference between CL-PKC [1,2,4–7,10,13–15] and traditional public key scheme is that the public key in CL-PKC does not need to be explicitly certified since it is constructed with partial private key from the master key of a trusted agency (TA), while the private key is only known to the user, i.e. no one except the private key holder can decrypt messages constructed with his public key, not even the TA.

In some sense, CL-PKC schemes are between the ID-based schemes which provide less privacy as the private keys are generated by the key distribution center, and the traditional PKI approaches which are quite complex.

After the first certificateless public key encryption scheme (CL-PKE) was introduced by Al-Riyami and Paterson [1] based on the bilinear pairing and Boneh–Franklin's ID-based scheme [3], and then further schemes were developed. However, most of them are constructed from the bilinear pairing which is a time costing operation. Some CL-PKE schemes without pairing were introduced in [2,13].

On the other hand, RSA is the *de facto* Internet standard and is widely used in many applications. Hence, it is highly desirable to construct CL-PKE scheme based on RSA. However, the scheme in [2] is not based on RSA and our scheme is more efficient than that in [13].

Our Contributions. In this paper, we construct an efficient CL-PKE scheme from RSA. The security is based on Kilian–Petrank's RSA assumption (a variant of RSA) and DDH assumption, where all operations are over $\mathbb{Z}_n^*$.

* Corresponding author.
E-mail address: linxj77@163.com (X.-J. Lin).

http://dx.doi.org/10.1016/j.dam.2017.02.019
0166-218X/

Please cite this article in press as: X.-J. Lin, et al., An efficient RSA-based certificateless public key encryption scheme, Discrete Applied Mathematics (2017), http://dx.doi.org/10.1016/j.dam.2017.02.019.

2. Preliminaries

2.1. Kilian–Petrank's RSA assumption

In the RSA encryption scheme the public key consists of $n = pq$, where p and q are primes, and an exponent e, where e is relatively prime to $\phi(n) = (p-1)(q-1)$. For security purposes, e should be chosen randomly. A message M is encrypted as $M^e \pmod n$. The private key d satisfies that $ed \equiv 1 \pmod{\phi(n)}$, and M^e can be decrypted by computing $M = (M^e)^d \pmod n$.

An additional assumption beyond the security of RSA is made in [8]: It is assumed that for a random number δ, it is hard to find (a, b) such that $a^e - b^e = \delta \pmod n$. Furthermore, it is assumed that given a set of such pairs $\{(a_i, b_i)\}$ satisfying that $a_i^e - b_i^e = \delta \pmod n$, it is hard to generate such a new pair. Given d, it is easy to compute (a, b) by computing $a = (a^e)^d \pmod n$ and $b = (a^e - \delta)^d \pmod n$.

It should be noted that the assumption is not true for very small e (e.g. 2 or 3); the pairs (a_i, b_i) fall on a low degree curve, which can be used as a basis for an attack. However, a large e does not seem to be vulnerable to such an attack.

2.2. Decision Diffie–Hellman problem (DDH)

In the following, G denotes a multiplicative finite cyclic group generated by an element g from G, and let prime p be the order of G.

Definition 1 (*DDH Problem*)**.** Let g^x, g^z and $T \in G$ be given where x and z are chosen randomly from $\mathbb{Z}/p\mathbb{Z}$. DDH problem is to decide whether $T = g^{xz} \in G$.

Definition 2 (*DDH Assumption*)**.** For every probabilistic, polynomial-time algorithm, the probability of solving DDH problem is negligible, i.e., DDH problem is hard.

2.3. Definition of CL-PKE

A generic CL-PKE scheme [1] consists of the following 7 algorithms.

- Setup: The Trusted Agency (TA) runs this algorithm to generate the system parameters and a master key. Note that the parameters are given to all interested parties.
- Partial-Private-Key-Extract: TA runs this algorithm to generate a partial private key for entity A with input the system parameters, master key and A's identity.
- Set-Secret-Value: This algorithm takes as inputs the system parameters and entity A's identity and outputs A's secret value.
- Set-Private-Key: This algorithm takes the system parameters, entity A's partial private key and A's secret value as input. The secret value is used to transform the partial private key into the (full) private key S_A. The algorithm returns S_A.
- Set-Public-Key: This algorithm takes the system parameters and entity A's secret value as input and from these constructs the public key for entity A.
  Normally both Set-Private-Key and Set-Public-Key are run by entity A for itself, after running Set-Secret-Value.
- Encrypt: This algorithm takes as inputs the system parameters, a message and entity A's public key and identity. It returns either a ciphertext or the null symbol indicating an encryption failure.
- Decrypt: This algorithm takes as inputs the system parameters, the ciphertext and A's private key. It returns a message or a null symbol indicating a decryption failure.
  Naturally, the output message should result from applying algorithm Decrypt with inputs the system parameters and A's private key on a ciphertext generated by using algorithm Encrypt with inputs the system parameters, the public key and A's identity on the message.

3. Security model

3.1. Security model for Kilian–Petrank's RSA assumption

This model is described through the following game between a challenger C and an adversary A.

- *Setup*: The challenger takes a security parameter k, and generates the RSA public parameter (n, e) and a random number $\delta \in \mathbb{Z}_n^*$, where $n = pq$ (p, q are two primes and $|p| \approx |q| \approx k/2$). The private key is d, where $ed \equiv 1 \pmod{\phi(n)}$. (n, e, δ) is sent to A.
- *Query*: At any time of the game, C can act as an oracle by answering A's queries as follows:
  A sends a query to C (no input is provided, only a query signal is sent to C). C outputs a pair (a, b) randomly to satisfy $a^e - b^e = \delta \pmod n$. (a, b) is distinct from the previous pairs output by C.

Please cite this article in press as: X.-J. Lin, et al., An efficient RSA-based certificateless public key encryption scheme, Discrete Applied Mathematics (2017), http://dx.doi.org/10.1016/j.dam.2017.02.019.