

Simple Threshold RSA Signature Scheme Based on Simple Secret Sharing

Shaohua Tang

School of Computer Science and Engineering, South China University of Technology,
Guangzhou 510640, China
csshtang@scut.edu.cn

Abstract. A new threshold RSA signature scheme is presented, which is based on a newly proposed simple secret sharing algorithm. The private key of RSA algorithm is divided into N pieces, and each piece is delivered to different participant. In order to digitally sign a message, each participant should calculate the partial signature for the message by using its own piece of shadow. Any K or greater than K participants out of N can combine the partial signatures to form a complete signature for the message. At the phase of signature combination, each participant's partial secret (shadow) is not necessary to expose to others and the RSA private key is not required to reconstruct, thus the secret of the private key will not be exposed. Besides, fast computation and simple operation are also the features of this scheme.

1 Introduction

The threshold cryptosystem was first introduced by Desmedt [1] in 1987. The threshold signature is very similar to the threshold cryptosystem. In a (t, n) threshold signature scheme, the signature can only be generated when the number of participating members is not less than the threshold value t . Anyone can use the public key to verify the signature. The most attractive feature of threshold signature is that the private key is never reconstructed but the signature can be calculated. There are some schemes can realize this feature. But almost all related works adopt complex algorithm or narrow the range that the parameters can choose. For example, Frankel's scheme [2] brings the complexity of algorithm design and security proof. Shoup's scheme [3] brings the hardness of computation to the combiner. People may think of designing a threshold RSA signature based upon classical Shamir's secret sharing scheme [6], however, as Desmedt and Frankel briefly addressed in [4], there are some technical obstructions to doing this.

In this paper, we propose a new threshold RSA signature scheme based on a newly proposed simple secret sharing algorithm [5]. The mathematical theory adopted by this simple secret sharing scheme is the union operation in set theory and the addition operation in arithmetic. Since the principle and the operations invoked by our scheme are extremely simple, thus we call it "simple" scheme, which possesses the following features: (1) It is easy to implement. (2) Fast computation of the threshold signature is ensured, because only simple addition and union operations are adopted by the underlying secret sharing algorithm. (3) It requires no strict preconditions and can apply to almost all circumstances requiring threshold signature. (4) It is secure. Though the

scheme is simple, it still possesses the security of threshold cryptography. The rest of this paper is organized as follows: A brief review of Tang's simple secret sharing scheme [5] is presented in Section 2. Our proposed threshold RSA signature scheme is described in Section 3. The security, performance, and the comparisons with related works are analyzed in Section 4. Finally, we summarize the results of this paper in Section 5.

2 Review of Simple Secret Sharing Scheme

Recently, Tang proposed a simple secret sharing scheme [5], which invokes only simple addition and union operations. The secret is divided into N pieces, and each piece is delivered to different participants. Any K or greater than K participants out of N can reconstruct the secret, but any $(M-1)$ or less than $(M-1)$ participants would fail to recover the secret, where $M = \lceil N/(N-K+1) \rceil$, and $\lceil x \rceil$ denotes the smallest integer greater than or equal to x . Tang's scheme is characterized by fast computation as well as easy implementation and secure operation.

Tang's scheme consists of three stages: the shadow generation stage, the shadow distribution stage, and the stage of reconstructing the secret. Suppose F is an arbitrary field, d is the secret data, and $d \in F$. The original N participants are P_0, P_1, \dots, P_{N-1} .

Shadow Generation Stage: $(N-2)$ random numbers d_0, d_1, \dots, d_{N-2} are selected from F , then d_{N-1} is computed by the equation $d_{N-1} = d - \sum_{i=0}^{N-2} d_i$.

Shadow Distribution Stage: For $j=0, 1, \dots, N-1$, the shadow A_j is defined as $A_j = \{ (i \bmod N, d_{i \bmod N}) \mid j \leq i \leq N-k+j \}$. Then each A_j is delivered to the j -th participant P_j .

Stage of Secret Reconstruction: Randomly select K participants whose shadow is not damaged, and then each one should present their own A_j . Any one among the K selected participants can act as a combiner to find $(0, d_0), (1, d_1), \dots, (n-1, d_{N-1})$ from

the presented A_j . Let $d = \sum_{i=0}^{N-1} d_i$, which is the solution.

3 Threshold Signature Scheme

Our proposed threshold RSA signature scheme consists of five stages: the initial stage, the shadow generation stage, the shadow distribution stage, the stage to generate partial signatures, and the stage to combine the partial signatures.

3.1 Initial Stage

Parameters for RSA cryptosystem are generated at the initial stage. Randomly select two large primes p and q , and let $n=p \times q$, n is the public parameter. Compute