Research Journal of Applied Sciences, Engineering and Technology 4(1): 79-81, 2012
ISSN: 2040-7467

Submitted: September 23, 2011 Accepted: October 24, 2011 Published: January 01, 2012

A Novel Universally Composable Threshold Signature Protocol for Mobile Ad-Hoc Network

Hong Xuan
Computer Science Department, Shanghai Normal University, Shanghai 200234, China

Abstract: Mobile ad-hoc network has received a lot of attention recently, adapting threshold signature schemes to work in such environments is challenging. In this study, we propose a novel threshold RSA signature protocol. The proposed protocol is suitable for the mobile ad-hoc networks, for it is completely non-interactive and has simple algorithm. Furthermore, we will give the concrete analysis of the reduction to prove the security of the proposed protocol. The proposed protocol is also secure under the universal composability framework, it can be applied to the mobile ad-hoc networks regardless what the environment it interacts with.

Key words: Mobile Ad-Hoc network, threshold signature, universal composability framework

INTRODUCTION

Mobile ad-hoc networks (MANET) have received a lot of attention for its rapid expanding range of capabilities and various uses. The mobile ad hoc network (Schiller, 2000; Huang *et al*., 2004) is a collection of nodes, while the nodes communicate amongst each other using wireless radios and operate by following a peer-to-peer network model. Applications of mobile ad hoc networks are very extensive, such as data collection, sensor networks, and meeting room applications.

Security of mobile ad hoc networks has become a more sophisticated problem than security in other networks. In mobile ad-hoc networks, the set of parties is formed in dynamic and ad-hoc manners. Large numbers of nodes may be deployed in the network, and yet at a given time a node may be in the communication range of only a few other nodes. In these environments nodes are receptive to being captured, compromised, and hijacked since they are units capable of roaming independently. In many such applications, communication bandwidth may be constrained, transmitting large amount of data or heavy interaction may be infeasible, and expensive communication primitives like broadcast may not be available. We consider a scenario wherein relatively small subsets of very large and dynamic groups report data, which is aggregated and certified by means of a signature. Such signatures are referred to as threshold signatures in cryptography.

Threshold signatures provide a robust, flexible and secure way for the nodes to report and certify data that can be verified, by preventing single node of corruption A t out of n threshold signature scheme is a protocol that allows any subset of t parties out of n to generate a signature, but that disallows the creation of a valid signature if fewer than t parties participate in the protocol. It should also be robust, meaning that corrupted parties should not be able to prevent uncorrupted parties from generating signature. Desmedt (Desmedt, 1987) introduced the general concept of threshold cryptography. Though threshold schemes based on the discrete logarithm problem are relatively straightforward to build, Basing threshold schemes on RSA is more difficult due to the fact that the modulus Φ (N) cannot be leaked to any of the shareholders. These earlier protocols additively share the signing key d among the parties, and they tend to be more complex and less efficient. Later, Shoup (2000) described his practical threshold signatures, which is widely regarded as the most efficient threshold RSA signature scheme. None of these schemes seems practical enough for realistic use in the mobile ad-hoc networks. Gennaro *et al*. (2008) propose the solution of threshold signature protocol for dynamic and communication-constrained scenarios.

The universal composability framework maintains the security, regardless of execution environment. That is suitable for analyzing the mobile ad-hoc networks. Canetti introduced the Universal Composability (UC) framework (Canetti and Rabin, 2003; Canetti, 2004) as a new approach for designing and analyzing the security of cryptographic primitives and protocols. The main concern is to create a new approach for the assessment of cryptographic protocol. It is guaranteed that a protocol with UC security maintains its security even when running concurrently with others. When analyzing multi-protocol systems, we analyze each protocol as if it is tand alone Then the composition theorem is used to deduce the security of all instances when running concurrently.

Security of the protocol is achieved via comparing the protocol execution in the real-life model to the ideal model. This is formalized by considering an environment Z, which represents all the other protocols running in the

system, including the protocols that provide inputs to, and obtain outputs from. Security is required that no environment can distinguish interactions with protocol π from interactions with ideal functionality. Almansa *et al*. (Almansa *et al*., 2006) proposed a simplified threshold RSA in the universal composability framework.

Contribution: In the study, we proposed a novel efficient threshold RSA signature protocol, and circumstantiate the proposed scheme is suitable for the mobile agent system. The scheme is efficient, fully non-interactive and the security satisfies the universal composablity framework. Due to the fact that Shoup scheme has a parameter n, which is the number of potential parties in the protocol, the parameter n must be fixed. As n grows, the calculations of protocol become expensive or even infeasible. However, we easily adopt Gennaro *et al*. (2008) scheme, without using the extra cryptographic techniques. Each user only needs one pair of RSA keys to participate in the threshold signature scheme. The proposed scheme shares the signing key by using Lagrange formula. Its signature generation and combination protocol are completely non-interactive. The size of the partial signing key and that of the partial signature are constant and independent to the number of the proxy signers. Owing to its simple algorithm and fewer parameter requirements, the proposed scheme requires fewer calculations and fewer communications, and is suitable for the mobile ad-hoc network.

□ THE PROPOSED PROTOCOL

In this section, we describe the proposed (t,n) threshold signature scheme. The proposed threshold signature scheme consists of four stages: key generation stage, signature share generation stage, signature share verification stage and signature share combination and signature verification stage. The details of the new protocol are depicted as follows.

Key generation: When activated with input (KeyGen,sid), Party Si verifies sid = (Si,sid , Si calls the dealer for generating the secret key ski, the verification public key PK and the partial verification key pki. Outputs (VerificationAlgorithms,sid,pki,PK).

The dealer operates as follows: Performs RSA key generation with secureparameter k to obtain modulus N, where N = pq, p = 2p +1, q = 2q 1, p, q, p q themselves prime. Lets M = p computes the components e, d, where ed = 1 mode M. The verification public key PK= (n,e). Next sets a0 = d and chooses ai at random from {0, 1, M-1} for $1 \le i \le k-1$. The number a0, a1, ak-1 define the polynomial $f(x) = \Sigma^{t-1}_{i=0} \alpha_i x^i$, the dealer computes $sk_i = f_i$ for each signer Si. Random select $v \in N$ (subgroup of squares in ZN), set $v_i = v^{ski} \in N$. The partial verification key is $pk_i = (v, v_i)$.

Signature share generation: When activated with input (ThSign,sid,m) where sid = (S,sid'), Signer Si let x = H(m). Computes $\sigma i = x^{2kt.}sk_i \bmod N$, where k is the secure parameter, t is the threshold parameter. Computes the proof (z,c) of the signature share σ_i, where

$v' = v^r$, $x = x^{4\Delta}{}_{s.r}$
$z = Sk_i.\ c+r.(v,x4\Delta,vi,\sigma 2i,v',x',),$
$z = sk_i .c + r$

Signer Si outputs (The Signature, sid,m,σi,(z,c)).

Signature share verification: When activated with input (ThVerify,sid,m,σi,(c,z),pki), any third party V can check whether $c = H'(v, x^{4\Delta}, v_i, \sigma_i^2, v'.v_i^{-c}, x^{4\Delta s.z}, \sigma_i^{-2c})'$, c. If so, output (ThVerified,sid,m,σ,(z,c),1), otherwise, output (ThVerified,sid,m,σ,(z,c),0).

-Signature share combination: When activated with input (The Combine, sid, m, σ1, (z1,c1),…,σt,(zt,ct)), if all these signature share are valid. Any third Party C outputs (ThCombined,sid,m,δ), where δ is computed as follows:
Lets

$$\Delta_s = \text{lcm}\left\{\left(\prod_{j \in S,\, j \neq i}(i-j)\right): i \in S\right\}$$

where S = {a1,…,at-1}. Computes

$$\sigma = \prod_{j=1}^{t+1} \sigma_{a_i}^{\Delta_S . \lambda_0^S, a_i} = x^{\Delta_S . 2^{kt} . d} \bmod N$$

Since $\gcd(e, 2kt.\Delta_S) = 1$, we can compute a, b easily using extended Euclidean algorithm, such that $a.e+b(2^{kt}.\Delta_S) = 1$. Finally, the threshold signature δ is computed as:

$$\delta = x^a . \sigma^b = \left(x^{1/e}\right)^{a.e} . \left(x^{1/e}\right)^{b\left(2^{kt}.\Delta s\right)} = x^{1/e}$$

Signature verification: When activated with input (Verify,sid,m,δ,PK), third party V checks whether $H(m) = \delta^e \bmod N$ If so,outputs (Verified,m,δ,1), else outputs (Verified,m,δ,0).

DISCUSSION

In this section, we examine the security properties and analyze the performance of the proposed (t,n) threshold signature protocol. The proposed protocol satisfies the universal composability security framework.

Security: We adopt the Almansa et al. ideal functionality for threshold signature, which they had proved to be equivalent to the standard notion.

Theorem 1: The protocol π securely realizes the ideal functionality of threshold signature □ThSig, under the RSA assumption.

Briefly, this result is shown by constructing a UC □simulator , which will generate on its own a set of keys for the signature scheme by executing internally an instance of π. Let □ be an adversary that interacts with parties running π in the ideal model. We construct an ideal process adversary (simulator) □ such that the view of any environment □ of an interaction with □ and π is distributed identically to its view of an interaction with □ in the ideal process of □ThSig. Generally speaking, simulator S runs an internal copy of □ and each of the involved parties.

Thus using the private keys, it can trivially simulate the environment □ 's view of π by simply following the protocol to generate signature. We can observes that the only way it could differ from actual execution is if □ can produce a valid signature that was not legally generated. However, the unsolvable of the RSA assumption ensures that such event occur with negligible probability.

Theorem 2: The protocol π is well-formed, correct, consistent and unforgeable relative to the environments which corrupt and adaptively, at most t-1 parties.

It can be easily proved following the work of Almansa et al.'s ideal functionality.

Performance: The study shares the signing key by using a simple Lagrange formula but not extra cryptographic techniques. We hide the secret information M with the subgroup of squares N. The size of the partial signing key is constant O (|M|), those are independent to the number of the signers. Furthermore, the signature generation stage and the signature combining stage are completely non-interactive. Owing to its simple algorithm and fewer parameter requirements, the proposed scheme requires fewer calculations and transactions.

Application to mobile agent system: In the mobile ad-hoc networks, the set of parties is formed in dynamic and ad-hoc manners. Large numbers of nodes may be deployed in the network, and yet at a given time a node may be in the communication range of only a few other nodes. In these environments nodes are receptive to being captured, compromised, and hijacked since they are units capable of roaming independently. In many such applications, communication bandwidth may be constrained, transmitting large amount of data or heavy interaction may be infeasible, and expensive communication primitives like broadcast may not be available. Adapting threshold signature schemes to work in such environments is challenging.

We can easily apply the traditional RSA cryptosystem to the proposed scheme without using additional cryptographic techniques. Each user only needs one pair of RSA keys to carry out the threshold signature scheme. The proposed scheme can satisfy all the security requirements of the threshold signature scheme, and its overhead is lower than that of the existing schemes. Only when more than t nodes are corrupted, the protocol becomes insecure. Furthermore, the signature generation stage and the signature combining stage are completely non-interactive. Moreover, the proposed protocol is also secure under the universal composability framework, it can be applied to the mobile ad-hoc networks regardless what the environment it interacts with. These characteristics make our scheme very attractive in mobile agent system.

Summary: In this study, we proposed a novel threshold RSA signature protocol, which is secure depends on the underlying RSA assumption within universal composability framework. We believe that the proposed protocol should be both secure and efficient. In addition, we evaluated the computational overhead. The proposed protocol is suitable for the mobile ad-hoc networks, for it is completely non-interactive and has simple algorithm.

ACKNOWLEDGMENT

This research is partially supported by the National Natural Science Foundation of China under Grant No. 61003215 and No. 60903188, the shanghai normal university general project No. A-3101-10-037.

REFERENCES

Almansa, J., I. Damgard and J. Nielsen, 2006. Simplified threshold RSA with adaptive and proactive security. EUROCRYPT 6, LNCS, 4004: 593-611.

Canetti, R., 2004. Universally Composable Signature, certification and authentication. Proceedings of the 17th IEEE workshop on Computer Security Foundations, IEEE Computer Society Press, New York, pp: 219-233.

Canetti, R. and T. Rabin, 2003. Universal Composition with Joint State. Crypto 2003, LNCS, 2729: 265-281.

Desmedt, Y., 1987. Society and group oriented cryptography: A new concept. CEYPTO 7, LNCS, 293L: 20-127.

Gennaro, R., S. Halevi, H. Krawczyk and T. Rabin, 2008. Threshold RSA for dynamic and ad-hoc group. EUROCRYPT 8. LNCS, 4965: 88-107.

Huang, E., J. Crowcraft and I. Wassell, 2004. Rethinking incentives for mobile ad hoc Networks, Proc. SIGCOMM 4 Workshops. Portland, United States, pp: 191-196.

Schiller, J., 2000. Mobile Communication.1st Edn., Addison-Wesley Professional.