Secure Outsourced Attribute-Based Signatures

ABSTRACT
Attribute-based signature (ABS) is a useful variant of digital signature, which enables users to sign messages over attributes without revealing any information other than the fact that they have attested to the messages. However, heavy computational cost is required during signing in existing work of ABS, which grows linearly with the size of the predicate formula. As a result, this presents a significant challenge for resource-limited users (such as mobile devices) to perform such heavy computation independently. Aiming at tackling the challenge above, we propose and formalize a new paradigm called OABS, in which the computational overhead at user side is greatly reduced through outsourcing such intensive computation to an untrusted signing-cloud service provider (S-CSP). Furthermore, we apply this novel paradigm to existing ABS to reduce complexity and present two schemes, i) in the first OABS scheme, the number of exponentiations involving in signing is reduced from $O(d)$ to $O(1)$ (nearly three), where $d$ is the upper bound of threshold value defined in the predicate; ii) our second scheme is built on Herranz et al's construction with constant-size signatures. The number of exponentiations in signing is reduced from $O(d^2)$ to $O(d)$ and the communication overhead is $O(1)$. Security analysis demonstrates that both OABS schemes are secure in terms of the unforgeability and attribute-signer privacy definitions specified in the proposed security model. Finally, to allow for high efficiency and flexibility, we discuss extensions of OABS and show how to achieve accountability and outsourced verification as well.

EXISTING SYSTEM:
We specify that existing work of ABS requires a large number of exponentiations in signing. The complexity commonly grows linearly with the size of the predicate formula in threshold ABS6. Such inefficiency becomes even more serious for ABS with more expressive predicate. The problem that how to securely outsource different kinds of expensive computations has drew considerable attention from theoretical computer science community.

**PROPOSED SYSTEM:**
The proposed OABS scheme with outsourced verification reduces the computation load at signer side through delivering computation to V-CSP but only letting two exponentiations locally. Because the outsourcing verification method is the same as, the security can be also guaranteed based on the assumption that the S-CSP does not collude with the V-CSP. In another word, V-CSP cannot cheat to let an invalid signature pass the verification algorithm because is blinded and not available to V-CSP

**PROBLEM STATEMENT:**
There are three entities involved in our OABS system, namely, the attribute authority, users (include signers and verifiers), and S-CSP. Typically, the signers obtain their private keys from attribute authority, with which they are able to sign messages later for any predicate satisfied by the possessed attributes. Verifiers will be convinced of the fact that whether a signature is from one of the users whose attributes satisfy the signing predicate, but remaining completely ignorant of the identity of the signer. Different from the definition of traditional ABS an additional entity S-CSP is introduced. Specifically, S-CSP is to finish the outsourced expensive tasks in signing phase and relieve the computational burden at signer side.

**SCOPE:**
The proposed scheme of OABS must satisfy outsource able requirement. Specifically, the running time of Sign must be less than directly computing the signature itself. In original ABS construction, it requires single-based exponentiations to generate the signature. However, since multiple exponentiations have been delivered to S-CSP, in OABS-I, the signing algorithm Sign simply requires 3 single-based exponentiations, which is independent of the attribute to be signed. We also specify that our technique in OABS-I allows S-CSP to perform delegated signing by employing an AND gate at private key for each user. Therefore, to generate an outsourcing key, attribute authority has to compute exponentiations in G, which is linear with the size of request attribute set \( \Omega \). Fortunately, in practical, the generation is allowed to be performed once for all. After obtaining private key and outsourcing key from authority, user is able to (delegated) sign any message with it. Such amortized computation cost of generating the outsourcing key is rather low cost. Moreover, we consider a scenario that user has limited computation and storage ability. In this case, the outsourcing key can be firstly generated by authority and sent to S-CSP. Therefore, user only needs to store a small-sized component locally but still maintaining signing capability.

**MODULE DESCRIPTION:**

**Number of Modules**

After careful analysis the system has been identified to have the following modules:

2. Attribute Based Signature Module.
4. OABS With Outsource Verification Module.

1. Cloud Computing Module:
Cloud computing, provides the feasibility to reduce the computation overhead at user side by outsourcing the computation of signing to a signing-cloud service provider (S-CSP). This presents a significant challenge for users that manage and view private data on mobile devices where processors are often one to two orders of magnitude slower than their desktop counterparts. We employ a hybrid private key by introducing a default attribute for all the users in the system. The private key component for user's attributes (denoted as outsourcing key OK in this paper) which is to be utilized by S-CSP to compute the outsourced signature; ii) the private key component for the default attribute which is to be utilized by signer to generate a normal ABS signature from the outsourced signature returned from S-CSP.

2. Attribute Based Signature Module:
Attribute-based signature (ABS) enables a party to sign a message with _fine-grained access control over identifying information. Specifically, in an ABS system, users obtain their attribute private keys from an attribute authority, with which they can later sign messages for any predicate satisfied by their attributes. A verifier will be convinced of the fact that whether the signer's attributes satisfy the signing predicate while remaining completely ignorant of the identity of signer. ABS is much useful in a wide range of applications including private access control, anonymous credentials, trust negotiations, distributed access control for ad hoc networks, attribute-based messaging.

3. Outsource ABS Computation Module:
Outsourced attribute-based signature scheme OABS consists of five probabilistic polynomial-time algorithms below:
**Setup:** It takes as input the security parameter _, attribute universe U and an auxiliary information d. It outputs the public key PK and the master key MK.

**Key Gen (MK; Ω):** For each user's private key request on attribute set Ω, the private key generation algorithm takes as input the master key MK and the attribute set Ω. It outputs the user's private key SK and the outsourcing key OK.

**Sign out (OK; Ω; _):** The outsourced signing algorithm takes as input the outsourcing key OK, the corresponding attribute set Ω and the predicate _. It outputs the partial signature _part.

**Sign (SK;M; _part; _) :** The signing algorithm takes as input the private key SK, the message M, the partial signature _part and the corresponding predicate _. It outputs the signature _ of message M with the predicate _.

**Verify (M; _; _; PK):** The verifying algorithm takes as input a message M, the signature _, the predicate _ and public key PK. It outputs 1 if the original signature is deemed valid and 0 otherwise.

---

**5. OABS With Outsource Verification Module:**

This technique can only guarantee the correctness of outsourced computation with accountability, it cannot check the correctness and detect the misbehaves of S-CSP on spot. To solve this problem, we provide another solution to verify the outsourced signature with low computational cost by introducing another independent entity called verifying-cloud service provider (V-CSP). We also introduce an assumption that the S-CSP and V-CSP will not collude. Actually, such assumption has also appeared to deal with the problem of secure outsourcing computation as well. Accordingly, an outsourced verification protocol, including the transformation algorithm for outsourced verification Transfer, the outsourced verifying algorithm Verifyout and the verifying algorithm Verify, replaces the original verifying algorithm in OABS definition.
SOFTWARE REQUIREMENTS:

- Operating System : Windows
- Technology : Java and J2EE
- Web Technologies : Html, JavaScript, CSS
- IDE : My Eclipse
- Web Server : Tomcat
- Tool kit : Android Phone
- Database : My SQL
- Java Version : J2SDK1.5

HARDWARE REQUIREMENTS:

- Hardware : Pentium
- Speed : 1.1 GHz
- RAM : 1GB
- Hard Disk : 20 GB
- Floppy Drive : 1.44 MB
- Key Board : Standard Windows Keyboard
- Mouse : Two or Three Button Mouse
- Monitor : SVGA