Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Policy controlled system with anonymity

Pairat Thorncharoensri*, Willy Susilo, Yi Mu

Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2522, Australia

ARTICLE INFO

Article history:
Received 8 January 2018
Received in revised form 26 April 2018
Accepted 30 May 2018
Available online xxxx
Communicated by G. Yang

Keywords:
Attribute-based
Policy-based
Signature
Signcryption
Designated verifier
Anonymity
Authorisation

ABSTRACT

The revelation in April 2018 on Mark Zuckerberg's testimony to the congress raises the question about how much control people have over their data in the cloud. The big data privacy risks lead to the question of how to securely share the information among an assigned group or set of peoples. Furthermore, anonymity is an equally important issue in which the disclosed information should not be linked to the owner. The policy controlled signature and signcryption were presented in this paper to provide an affirmative answer to the aforementioned privacy issues. The primitives ensure the user's privacy, especially confidentiality and anonymity. Limiting only the permitted verifiers constricted by a verifier policy to validate a signature without revealing the identity of a signer, our policy controlled signature schemes provide both privacy and anonymity. An additional property of our policy controlled signcryption scheme provides not only privacy and anonymity, but also the confidentiality, where the information delivered to the receiver is encrypted and cannot be traced back to the sender's identity. Furthermore, our policy controlled signature scheme was proven to be secure against unforgeability and collision-resistant. Additionally, our policy controlled signcryption scheme was proven to be secure against indistinguishability and it is equivalent to a adaptive chosen ciphertext attack model of an encryption scheme, which is the strongest model in the existing literature.

1. Introduction

The growth of network technology causes the problem of information disclosure. The attribute-based (and policy-based) signature and encryption have been the most well known cryptographic primitives to support fine-grained access control systems. The access control systems, such as Attribute-based access control (ABAC) and role-based access control (RBAC), are systems that use a policy (set of attribute) to limit or grant a user an access to the services. To put it simply, gaining an access to the systems or services, a user must prove that he/she hold secrets corresponding to the attributed stated in the policy. Nevertheless, there are some services that a system must provide confidentiality, privacy and anonymity, such as anonymous VPN. In particular, the mentioned services should not log user activities and anyone must not be able to reveal the user identity and the validity of the access (even it was logged by other parties). Specifically, to provide confidentiality, privacy and anonymity, a user first logins to the registered server to obtain credentials (secret key) related to his/her attributes. Then, he/she use these credentials to communicate with the appropriated service servers. To secure the communication, such that one must not be able to prove the existing of this communication and its content cannot be revealed,

* Corresponding author.
E-mail addresses: pairat@uow.edu.au (P. Thorncharoensri), wsusilo@uow.edu.au (W. Susilo), ymu@uow.edu.au (Y. Mu).

https://doi.org/10.1016/j.tcs.2018.05.038
0304-3975/© 2018 Published by Elsevier B.V.

the system needs a protocol that provides the deniability property (i.e., a designated verifier signature) together confidentiality from an encryption scheme. It may sound simple to construct the scheme to enable the aforementioned protocol, but unfortunately combining designated verifier signature schemes, encryption schemes and attributed-based identity cannot be achieved easily due to the security issue. Hence, we propose the notion of policy controlled system with anonymity to tackle the above problem, where confidentiality, privacy and anonymity are required.

Let us review another scenario where the application involves sensitive contents, such as medical records, which only the authorised doctors can review them. A group of doctors conducts a study on a sensitive illness which cannot be known by other irrelevant people. If doctor D wants to access this information, then D will need to ask the patient and his doctor to grant D an access to this information. Consequently, D must ask every patient and their doctor for the permission. Conversely, let's assume that patients agree to participate in a research study and to reveal their conditions and physical attributes, but not their identity, hence, doctors can access this information directly. However, doctors should not be able to link or convince others about the identity of a patient. The recently-introduced notion of a cyber-physical system (CPS) in medical helps doctors to closely monitor patients at all time. Accessing patient's condition and physical attributes at real-time are greatly benefiting from the medical research. Hence, a system that provides confidentiality, privacy and anonymity is a significant factor for the patients to participate in the medical studies. At a glance, the above problem can be solved by a policy-controlled signature together with a policy-based encryption. On the contrary, a policy-controlled signature can be used to reveal the identity of a signer by comparing the public key. As a result, the anonymity property cannot be achieved in the above solution. Similarly, a designated verifier signatures and ring signature do not support for the designated multi-verifier setting and the identity of a signer can be revealed as such, it is not the right solution either. Policy-based system, hierarchical identity-based system, and attribute-based system are similar to the above solution which is not supported for the designated multi-verifier.

In conclusion, the answer to the above scenarios is a policy-controlled signcryption with anonymity, which allows policy satisfied verifiers to decrypt and verify the ciphertext generated by a sender, who reveals nothing, but its attributes. That is, a policy-controlled signcryption reveals only the message after the decryption process, which cannot be traced back to the identity of a signer. Moreover, those, who does not satisfy the policies, cannot decrypt and verify this ciphertext.

1.1. Related work

At the first glance, the above scenario seems easy to achieve. We will describe one by one and show that the existing primitives are not the solution.

Introduced by Rivest, Shamir and Tauman [45], a ring signature scheme aims to provide the anonymity of a signer in a ring. A single signer can generate a signature that is definitely signed by one of the signers in a ring. Therefore, from the verifier's point of view, the authentication of a message is provided by a signer in this ring. Following this notion, many works had been proposed and thoroughly studied [10,57,21,61,5,48,16,35,34]. Regarding the multi-signer, a threshold ring signature scheme aims to provide a multi-signer setting for a ring signature. The scheme provides authenticity, non-repudiation, and anonymity in a multi-signer setting. It was first formalised by Bresson, Stern and Szydlo in [10]. Two-party ring signatures are indeed giving the concrete construction to a designated verifier signature scheme. However, when the application required a multi-verifier setting, it is unachievable by any ring signature schemes.

A digital signature that provides both authenticity and deniability properties at the same time is a designated verifier signature proposed by Jakobsson, Sako and Impagliazzo in [25]. The deniability property ensures a signer that the validity of this digital signature inspired by only a designated verifier and this conviction cannot be transferred to any other third party. The authenticity property ensures a designated verifier that this digital signature is indeed signed by a signer, however, other parties cannot validate this digital signature. The topic has been widely studied and expanded [27,26,31,33,23,53,51,30]. Nevertheless, the above schemes do not provide a scheme in a multi-verifier setting, so it cannot use to construct a solution for the early mentioned problems.

Attribute-Based Signatures scheme (ABS) was first proposed by Maji et al. in [37]. The primitive is similar to the identity-based signature. This primitive's attribute works as a public key, where, in an identity-based signature, an identity is a public key. However, many users might hold the same attribute, so signer only needs to prove that he/she holds a secret key related to the attribute but does not need to reveal his/her true identity. To be precise, it allows a signer, who want to reveal no information about his/her identity, to sign a message using only the specified attributes that he/she is possessed of. Based on the results of Maji et al.'s works, many variant ABS schemes were conferred [49,19,20,14,40,41,39,47,38]. The ABS schemes in the standard model were later presented in [38]. The attribute-based signature with threshold predicate was independently and simultaneously presented by Shahandashti and Safavi-Naini [49], and Li et al. [29]. Escala et al. introduced a revocable ABS with threshold predicate and an adaptive unforgeability property for ABS schemes in [14]. Later, Herranz et al. proposed a constant size of an ABS scheme with threshold predicate in [20]. Sakai et al. presented an efficient ABS scheme with arbitrary circuits (when the number of gates is increased) in [47]. Their constructions are based on the combination of an extractable non-interactive proof system and a witness indistinguishable and an existentially unforgeable signature scheme. Once again, the above schemes do not limit a verifier to covey the verdict of validation of the signature to other parties, so it cannot use to construct a solution for the early mentioned problems.

The first signcryption scheme was introduced by Zheng in [64]. The primitive provides both secrecy and authenticity. Later, Gagné et al. adopted this concept and first to propose the attribute-based signcryption Scheme (ABSC) with threshold

Please cite this article in press as: P. Thorncharoensri et al., Policy controlled system with anonymity, Theoret. Comput. Sci. (2018), https://doi.org/10.1016/j.tcs.2018.05.038