Cluster Comput (2013) 16:845–859
DOI 10.1007/s10586-013-0258-7

Simultaneous authentication and secrecy in identity-based data upload to cloud

Bo Qin · Huaqun Wang · Qianhong Wu · Jianwei Liu · Josep Domingo-Ferrer

Received: 21 January 2013 / Accepted: 26 March 2013 / Published online: 23 April 2013

Abstract Most existing works to secure cloud devote to remote integrity check, search and computing on encrypted data. In this paper, we deal with simultaneous authentication and secrecy when data are uploaded to cloud. Observing that cloud is most interesting to companies in which multiple authorized employees are allowed to upload data, we propose a general framework for secure data upload in an identity-based setting. We present and employ identity-based signcryption (IBSC) to meet this goal. As it is shown that it is challenging to construct IBSC scheme in the standard model and most IBSC schemes are realized in the random oracle model which is regarded weak to capture the realistic adversaries, we propose a new IBSC scheme simultaneously performing encryption and signature with cost less than the signature-then-encryption approach. The identity based feature eliminates the complicated certificates management in signcryption schemes in the traditional public-key infrastructure (PKI) setting. Our IBSC scheme exploits Boneh et al.'s strongly unforgeable signature and Paterson et al.'s identity-based signature. The scheme is shown to satisfy semantic security and strong unforgeability. The security relies on the well-defined bilinear decision Diffie-Hellman (BDDH) assumption and the proof is given in the standard model. With our IBSC proposal, a secure data upload scheme is instantiated with simultaneous authentication and secrecy in a multi-user setting.

Keywords Cloud Computing · Authentication · Secrecy · Bilinear pairings

This paper is partly supported by the European Commission under FP7 projects "DwB" and "Inter-Trust", the Spanish Government through projects CTV-09-634, PTA2009-2738-E, TSI-020302-2010-153, TIN2009-11689, TIN2011-27076-C03-01, CONSOLIDER INGENIO 2010 "ARES" CSD2007-0004 and TSI2007-65406-C03-01, by the Catalonia Government through grant SGR2009-1135, and by the NSF of China through grants 60970116, 91018008, 61173154, 61003214, 61173192, 61272501 and 61272522, by MOST of China through National Key Basic Research Program under grant 2012CB315905, by Shaanxi Provincial Education Department through Scientific Research Program 2010JK727, by the NSF of Liaoning Province in China through project 20102042 and by the Program for Liaoning Excellent Talents in University through project LJQ2011078. The fifth author is partially supported as an ICREA-Acadèmia researcher by the Catalan Government.

B. Qin
School of Information, Renmin University of China, Beijing, P.R. China
e-mail: bo.qin@urv.cat

B. Qin · H. Wang (✉) · Q. Wu · J. Domingo-Ferrer
Department of Computer Engineering and Mathematics, UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, Tarragona, Catalonia
e-mail: huaqun.wang@urv.cat

J. Domingo-Ferrer
e-mail: josep.domingo@urv.cat

H. Wang
School of Information Engineering, Dalian Ocean University, Dalian, China
e-mail: wanghuaqun8@gmail.com

Q. Wu · J. Liu
School of Electronic and Information Engineering, Beihang University, Beijing, China

Q. Wu
e-mail: qianhong.wu@urv.cat

J. Liu
e-mail: liujianwei@buaa.edu.cn

1 Introduction

With the fast advances in networking [14, 25] and computing technologies, there is a great demand for many organizations to outsource their storage and computing needs on demand. This new economic and computing paradigm is commonly referred to as cloud computing [22]. It brings appealing benefits including relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc. There are however barriers hindering customers to migrate to the cloud. First, a cloud user will lack physical control over the outsourced data and may worry about their data loss of leakage incidents. Second, in addition to the risk of remote malicious attacks on the cloud, the traditional concerns posed by malicious insiders are now compounded by the even more hazardous threat of malicious outsiders who are given the power of insiders. Third, legal obstacles may also prevent enterprises and e-government applications from moving to clouds. A recent EU bill will force companies migrating to the cloud to be liable for any privacy breaches into which their cloud service provider (CSP) may incur, even when they do not retain control over their data.

In order to reach the full potential of could computing, it is essential to provide security mechanisms to establish trustworthiness for users in their outsourced data and computation to the cloud without imparting the functionality and the cost-saving benefits. The challenge is therefore to provide sound information security mechanisms in the face of potentially intrusted or unreliable clouds that are under the control of the cloud customers and without losing the functionality and economy provided by these technologies [44]. The basic idea is to physically outsource data and their processing but not digital control over data. To this end, this paper will provide cloud customers with the means to supervise the security and privacy of data storage and processing. This paper proposes to secure cloud service that enables users to keep their data private from the CSP by performing security preserving operations outside the cloud that nevertheless do not prevent them from transparently recovering the original data.

1.1 Related work

One of the main obstacles for costumers to move to clouds is their security concerns on the outsourced data. A number of works have been done to secure the clouds. The US national Institute of Standards and technology (NIST) is one of them, having defined the cloud as composed of four deployment modes and identifying the security requirements. The Cloud Security Alliance (SCA) [37] releasing a white paper entitled "Security guidance for critical areas of focus in cloud computing", has taken these definitions to work through its guidance, explaining that the motivation is "to bring coherence and consensus around a common language so we can focus on use cases rather than semantic nuance". Most of the existing works are focused on securing the cloud from the CSP perspectives, e.g., prevent external attacks from unauthorized access the data stored in the clouds.

This paper focused on securing the outsourced data to clouds from the customer's perspectives. Security can be generally interpret as confidentiality and integrality of the outsourced data and privacy of the customer processing the data. There are numerous cryptographic studies to achieve these security properties in traditional networking and computing scenarios. However, the traditional cryptographic primitives cannot be directly applied to secure clouds. For example, using traditional encryption method to encrypt the outsourced data will disable the basic functionalities provided by clouds. Without downloading the encrypted files, the costumer cannot search the files containing a specific key word. Also, it does allow any third party to re-compute on the encrypted data. Hence, advanced cryptographic technologies have to be envisioned and developed to enable functional secure clouds.

There have been a number of proof-of-concept studies to support secure clouds from the customer's perspective while keep the functionalities of the clouds. The first function needs to be preserved is to allow the customer to check the outsourced data have been kept intact. This is usually referred to as Provable Data Possession (PDP), which is used for remote data checking where a client that has stored data at an untrusted server can verify that the server possesses the original data without retrieving it. A part of the natural solution of replicating the data, several results on PDP ([3, 4, 34, 35]) and on privacy-preserving MapReduce by Di Pietro [17] can be leveraged. The adopted probabilistic proofs of possession can be improved by leveraging knowledge over stored data type and would aim to guarantee that the cloud service provider is performing the required operation. In particular, by locally simulating (on the client or proxy side) the same operation on a sample subset of remote data in the cloud we can increase trust in the cloud provider itself.

A basic function in secure clouds is accessing, in which is, according to a policy, to allow some users to read the encrypted data. The up-to-date notion about this is the attribute-based encryption [36] which can be classified into two categories [20]. One is ciphertext-policy attribute-based encryption in which the secret key represents a set of attributes and the ciphertexts contain the access control policy. A user can decrypt only if the attributes of the secret key assigned to him/her satisfying the access policy. Another is the key-policy attribute-based encryption in which the ciphertexts define a set of attributes while the secret key contains the access policy. A user can decrypt a ciphertext only if the

attributes of the ciphertexts are consistent with the access policy contained in the user's secret key.

Another basic functionality that it is interesting to maintain is searching, in which the problem is to find a means to efficiently search over encrypted data, since performing effective searches over encrypted information is considered to be a difficult problem. Most existing works do not support efficient searches with complex query conditions, and care needs to be taken when using them because of the potential privacy leakages about the data owners. Li et al. [26] show the necessity of search capability authorization that reduces the privacy exposure resulting from the search results, and establish a scalable framework for Authorized Private Keyword Search (APKS) over encrypted cloud data. They propose two novel solutions for APKS based on a recent cryptographic primitive, Hierarchical Predicate Encryption (HPE), providing solutions for efficient multi-dimensional keyword searches with range query, allow delegation and revocation of search capabilities. We note that although the problem of searching over encrypted data is very old, in the last years a considerable research effort has been put into making encryption-based solutions practical, [24] sometimes at the price of reducing a bit the very strong security guarantees offered by standard public-key encryption.

The ability to do some computation on numerical data is also an interesting function to be remained for some data. For this a possible venue to explore is partially homomorphic encryption. This type of encryption only allows a limited operations on the ciphertext, like for example, evaluation of multivariate polynomials of some bounded degree and is more efficient than its fully homomorphic counterpart, see for example ([2]). To minimize the efficiency loss a possible solution would be to encrypt only sensitive numerical data. To compute over encrypted data, Sadeghi et al. propose [33] to use a trusted hardware token combined with Secure Function Evaluation (SFE) to compute arbitrary functions on secret (encrypted) data where the computation leaks no information and is verifiable using symmetric encryption primitives only and without any interaction with other entities. The token is used in the setup phase only whereas in the time-critical online phase the cloud computes the encrypted function on encrypted data. Finally, the recent fully homomorphic encryption [12, 19] allows the computation of both addition and multiplication, thus allowing the computation of any boolean circuit. This new approach theoretically provides an ultra solution to re-computation on encrypted data stored on CSP. However, the major obstacle of this approach is up-to-date fully homomorphic encryption schemes are too inefficient to be deployed in clouds while preserve the cost-saving benefits.

As reviewed above, most existing works on securing clouds devote their efforts to private operations on outsourced data, e.g., remote integrity check, encrypted data retrieval and re-computation on encrypted data. Few attentions have been paid to provide security countermeasures when the data are outsourced. To secure data outsourced to clouds, the first step should be to guarantee security and privacy when the data are upload. In this case, two security requirements of authentication and secrecy are essential. The authentication property means that only authorized users can upload data to a given account in the cloud. The latter guarantees that only the owner of the cloud account can read the uploaded data. That is, even the CSP cannot understand the uploaded data if he is not the account owner. The authentication and secrecy requirements can be met by separately leveraging signature and encryption. However, a more practical solution is to employ the cryptographic primitive of signcryption.

The concept of public key signcryption was introduced by Zheng [47]. The underlying idea is to simultaneously perform signature and encryption in a single logic step to enjoy computational costs and communication overheads lower than the signature-then-encryption approach. This is very meaningful in applications where both authentication and confidentiality are required. Since Zheng's introduction, many efficient signcryption schemes have been presented [1, 5, 6]. Baek et al. proposed a security model [5] for signcryption that admits rigorous formal proofs for the confidentiality and unforgeability in signcryption schemes. Their model formally defines existential unforgeability which is slightly weaker than the strong unforgeability notion in some signature schemes. Specifically, for an existential forgery adversary to success, he has to forge a valid signature on a message which has never been signed. This implies that the existential unforgeability notion cannot capture the attacks where the adversary forges signatures on signed messages. That is, the adversary, knowing a message/signature pair (M, σ), may be able to forge a new valid signature $\sigma' \neq \sigma$ on M. The existential unforgeability cannot cope with this kind of attacks.

The strong unforgeability notion of signatures guarantees that an adversary can not even produce a new signature for a previously signed message. In [10], Boneh et al. proposed a generic transformation which converts an existentially unforgeable signature into a strongly unforgeable one. Since then, a number of strongly unforgeable signatures have been proposed [8, 21, 30, 38, 39]. In signcryption, strong unforgeability is needed to ensure that the adversary can not modify the challenge ciphertext. This is necessary to prove that a signcryption scheme, used for encryption, is IND-CCA2 (indistinguishable against adaptively chosen ciphertext attack) secure. Without stronger unforgeability, the attacker can modify the challenge signcryption ciphertext and use the valid modified challenge ciphertext to query the challenger; and then with this legal decryption query for the

forged ciphertext, the attacker can always break the signcryption scheme. That is, a signcryption cannot be proven secure if it is not strongly unforgeable.

The early signcryption schemes are realized in the PKI setting. Certificates are required to authenticate the senders and the receivers. That is, before sending a confidential message, the sender has to first retrieve the public key and its corresponding certificate of the receiver from a trusted certificate authority. The sender can signcrypt to the receiver only after validating the receiver's public key and certificate. For the receiver, he also needs to retrieve and validate the sender's public key and certificate from a trusted certificate authority before unsigncrypting the message from the sender. The certificates management may incur considerable overheads in practice. Identity based signcryption (IBSC) does not suffers from this problem because in IBSC, the recognizable identities of the users (senders and receivers) are used as their public keys and no extra certificates are required to associate a public key with a user. Recently, a number of IBSC schemes have been presented [7, 11, 15, 16, 27, 29]. These signcryption schemes are proved secure in the random oracle model.

It has been shown that there exist signature and encryption schemes that are secure in the random oracle model, but any implementation of the random oracle results in insecure schemes [13]. Hence, it is desirable to construct provably secure IBSC schemes in the standard model (i.e., without relying on random oracles). Although several efforts [23, 28, 42, 45] have been made recently, it is shown to be challenging to obtain secure IBSC schemes in the standard model. In 2009, Yu et al. proposed an identity based signcryption scheme [42] in the standard model but it was later shown insecure [23]. Another challenge is that existing IBSC schemes in the standard model suffer from complexity linear with the binary length of identities of the users. Note that the primary goal of the signcryption primitive is to achieve better efficiency by simultaneously performing signature and encryption. Hence, it is desirable to achieve secure IBSC schemes with constant complexity in the standard model.

1.2 Our contribution

In this paper, we extend our IBSC work in [32] and investigate efficient cryptographic schemes to secure multi-user data upload in cloud. Specifically, our contribution includes the following aspects.

First, we present a security framework of data upload by multiple users of companies in the cloud storage setting. The cloud sever creates a storage account for each company; each user is authorized with a secret key from the company. Then a user can upload data to the account in a secure way so that the cloud server can validate that the data is from an authorized user while cannot read the content. Finally, the intended user can download and read the data if necessary. We show that the IBSC primitive is perfectly suitable for such applications.

Second, we revisit recent IBSC schemes in the standard model and show that they cannot achieve security as expected. In 2009, Yu et al. proposed an IBSC scheme in the standard model [18]. It is regret that this scheme is insecure. In 2010, Jin et al. improved Yu et al.'s signcryption scheme [19]. Through cryptanalysis, we found Jin et al.'s scheme is still insecure. Both Yu et al.'s scheme and Jin et al.'s scheme can not satisfy the indistinguishability against adaptive chosen identity and chosen ciphertext attacks (i.e., IND-IBSC-CCA2).

Third, we present efficient IBSC schemes which can be proven secure without relying on random oracles. By exploiting Boneh et al.'s strongly unforgeable signature [10] and Paterson et al.'s identity-based signature [31], this paper proposes a new IBSC scheme in the standard model. It is proven that our IBSC scheme satisfies semantic security and strong unforgeability under the bilinear decision Diffie-Hellman (BDDH) assumption. The proofs do not rely on random oracles. As for efficiency, our scheme enjoys complexity independent of the scale of the users in the system or the binary length of the users' identities. Specifically, the signcryption and unsigncryption needs only constant number of pairings/expontiations, and the signcryption ciphertext contains only constant number of group elements. This implies that our IBSC scheme is efficient and practical. With our IBSC scheme, one can efficiently and securely realize simultaneous authentication and secrecy for data upload in clouds.

Finally, we instantiate data upload scheme in company-oriented cloud storage applications. The scheme follows our generic data upload framework and the instantiation employs our IBSC proposal. The instantiated scheme simultaneously achieves authentication and secrecy in an efficient way. Only the authorized company employees can upload data and only the intended authorized employees can read the digital content. By including expiry date information into each employee's identity, the scheme also allows the company to efficiently manage the issued credentials to its employees.

1.3 Paper organization

The rest of the paper is organized as follows. In Sect. 2, we present an ISBC based security framework of distributed data upload in clouds. We review and analyze two recent IBSC schemes in the standard model in Sect. 3. Section 4 presents our IBSC scheme in the standard model. We propose a new IBSC scheme and prove its security in the standard model, followed by concluding remarks in Sect. 5.

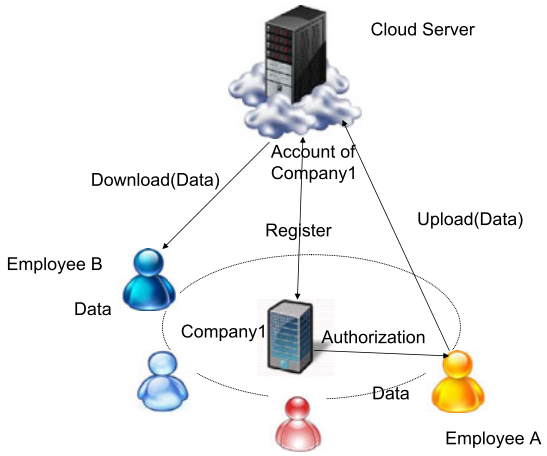


Fig. 1 System model of data upload in cloud

2 System model

2.1 Problem statement

We consider the following scenario. A number of companies would like to outsource their data to a cloud server maintained by a third party called CSP. The CSP creates a storage account for each company and allows each company's employees to upload data the company's account. If necessary, some employees of the company can download the data and work on the content of the data.

As shown in Fig. 1, the system model of data upload in cloud can be described as follows.

- **Setup**: In this procedure, the CSP first generates the global system parameters to be used by all the companies subscribing the cloud storage service. To use the storage service, each company needs to register to CSP and the CSP will create a storage account for each company.
- **Authorization**: The company who subscribed the storage service generates a credential for its employees.
- **Upload**: With a valid credential, an employee can upload data to the company's account and designate the intended receiver.
- **Read**: Any employee can download the data. However, only the intended receiver can read the content.

In such an application, we have three basic security requirements:

Authentication: The authentication requirement states that only authorized company's employees can upload data to that company's storage account in the cloud. This implies unauthorized users cannot send any digital content to the cloud, which prevents spams for the companies.

Secrecy: The secrecy requirement says that, except the intended receiver (and the company), anyone including CSP cannot understand the digital content of the data. This requirement is essential since the outsourced data may contain much private information of the employees and the company's business. This is necessary as CSP may not be fully trusted or be hacked by attackers.

Availability: The availability means that the intended receiver can download and understand the data anywhere anytime. This is essential for the system to be functional.

2.2 Syntax of ID-based signcryption schemes

Now we recall Yu et al.'s security model for IBSC schemes [42].

Definition 1 An ID-Based signcryption scheme consists of the following algorithms.

- *Setup*: Given a security parameter k, PKG generates a master key s and common parameters *params*. *params* is made public while s is kept secret.
- *Extract*: Given an identity ID, the PKG runs this algorithm to generate the private key S_{ID} associated with ID and transmits it to ID via a secure channel.
- *Signcrypt*: To send a message m to Bob whose identity is ID_B, Alice with identity ID_A obtains a ciphertext σ by computing $\mathit{Signcrypt}(m, S_{\mathrm{ID}_A}, \mathrm{ID}_B)$.
- *Unsigncrypt*: After Bob receives the ciphertext σ, he computes $\mathit{Unsigncrypt}(\sigma, S_{\mathrm{ID}_B}, \mathrm{ID}_A)$ and obtains the message m or the symbol $\perp$ indicating that the ciphertext is invalid.

Definition 2 An IBSC scheme is said to have indistinguishability against adaptively chosen ciphertext attack (IND-IBSC-CCA2) if no polynomially bounded adversary has a non-negligible advantage in the following game between the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$.

1. Taking into as input a security parameter k, the challenger $\mathcal{C}$ runs the *Setup* procedure. $\mathcal{C}$ obtains the common parameter *params* and a master key s. He sends *params* to the adversary $\mathcal{A}$ and keeps s secret.
2. The adversary $\mathcal{A}$ performs a polynomially bounded number of queries. These queries may be made adaptively, i.e., each query may depend on the answers to previous queries.
   - *Extract queries*: The adversary $\mathcal{A}$ produces an identity ID and receives the extracted private key $S_{\mathrm{ID}} = \mathit{Extract}(\mathrm{ID})$ from $\mathcal{C}$.
   - *Signcrypt queries*: The adversary $\mathcal{A}$ produces two identities $\mathrm{ID}_i, \mathrm{ID}_j$ and a plaintext m. By computing $\sigma = \mathit{Signcrypt}(m, S_{\mathrm{ID}_i}, \mathrm{ID}_j)$, the challenger $\mathcal{C}$ obtains a ciphertext σ. He sends σ to $\mathcal{A}$.
   - *Unsigncrypt queries*: The adversary $\mathcal{A}$ produces two identities $\mathrm{ID}_i, \mathrm{ID}_j$ and a ciphertext σ. By computing

Unsigncrypt$(\sigma, \mathrm{ID}_i, S_{\mathrm{ID}_j})$, the challenger $\mathcal{C}$ gets the plaintext M. He sends M to $\mathcal{A}$. This result may be the symbol $\perp$ if σ is an invalid ciphertext.

3. The adversary $\mathcal{A}$ chooses two plaintexts, m_0 and m_1, and two identities, ID_A and ID_B, on which he wishes to be challenged. He can not have queried the corresponding private key on ID_B in the first stage.
4. The challenger $\mathcal{C}$ chooses randomly a bit $\gamma \in \{0, 1\}$ and computes

$$\sigma = \mathit{Signcrypt}(m_\gamma, S_{\mathrm{ID}_A}, \mathrm{ID}_B)$$

He sends σ to $\mathcal{A}$.
5. The adversary $\mathcal{A}$ asks a polynomial number of queries adaptively again as in Step 2, with a constraint that $\mathcal{A}$ is not allowed to query for the private key corresponding to ID_B or to make an unsigncryption query for σ under ID_B.
6. Finally, the adversary $\mathcal{A}$ produces a bit $\gamma' \in \{0, 1\}$ and wins in the game if $\gamma' = \gamma$.

$\mathcal{A}$'s advantage is defined as

$$\mathit{Adv}(\mathcal{A}) = |2\Pr[\gamma' = \gamma] - 1|$$

where $\Pr[\gamma' = \gamma]$ denotes the probability that $\gamma' = \gamma$.

Definition 3 An IBSC scheme is said to be secure against a strong forgery for adaptive chosen identity and chosen message attacks (SUF-IBSC-CMA) if no polynomially bounded adversary has a non-negligible advantage in the following game.

1. The challenger $\mathcal{C}$ runs the *Setup* procedure with a security parameter 1^k. The *Setup* procedure outputs the common parameters *params* and a master key s. He sends *params* to the adversary $\mathcal{A}$ and keeps s secret.
2. The adversary $\mathcal{A}$ performs a polynomially bounded number of queries adaptively just like in the definition 2.
3. Finally, $\mathcal{A}$ produces a new triple $(m, \sigma, \mathrm{ID}_A, \mathrm{ID}_B)$ (i.e., it does not belong to the query/response quadruple set) where the private key of ID_A was not asked. We say that $\mathcal{A}$ wins in the game if the result of *Unsigncrypt*$(\sigma, \mathrm{ID}_A, S_{\mathrm{ID}_B})$ is not the $\perp$ symbol.

The adversary's advantage is defined as the probability that the adversary wins.

2.3 An ISBC based security framework

As shown in Fig. 2, we present an ISBC based security framework for data upload in clouds as follows.

– **Setup:** In this procedure, the CSP and the companies jointly run the *Setup* procedure of the ISBC scheme to setup the system. Specifically, the CSP partially runs the *Setup* procedure of an ISBC scheme to generate the global parameters excluding the public key of each company; each company partially run the *Setup* procedure of the ISBC scheme to generate its respective master public/secret key; a subscribing company registers to the CSP by letting the CSP know the company's public key; then the CSP creates a storage account for the subscribing company.
– **Authorization:** Taking into as input an employee's identity A, the company generates a secret credential SK_A by running the *Extract* procedure of the underlying ISBC scheme. The employee gets successful authorization if he/she is assigned with SK_A.
– **Upload:** With a valid credential SK_{ID} and the data *Data* to be sent to another employee with identity B, an employee runs the *Signcrypt* to generate $\sigma = \mathit{Signcrypt}(\mathit{Data}, SK_A, B)$. The employee uploads *Data* in an signcrypted form σ to the company's account.
– **Read:** The employee B can download σ the data anywhere anytime. If employee B has been authorized by the company, then the employee B can read the original digital content *Data* by computing $\mathit{Data} = \mathit{Unsigncrypt}(\mathit{Data}, SK_B, A)$.

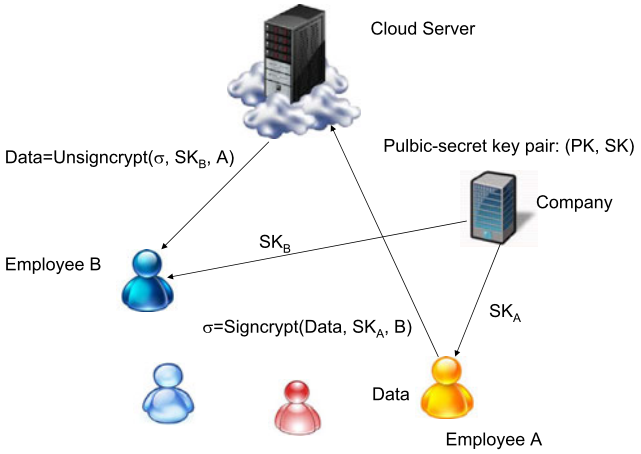


Fig. 2 An ISBC based security framework

The availability of the framework follows from the Definition 1 of IBSC. From the security properties captured in Definitions 2 and 3, the secrecy and authentication requirements are well met in the above IBSC based framework.

3 On the security of two recent IBSC schemes

Yu et al.'s IBSC scheme [18] and Jin et al.'s IBSC scheme [19] are the starting point of our proposed scheme. First, we review these two IBSC schemes. Second, we analyze the two IBSC schemes in the security model of IBSC.

3.1 Bilinear groups and difficult problems

The schemes in [18, 19] and our scheme are built from the bilinear groups which have been shown a powerful mathematical tools for versatile cryptosystems [9, 40, 41]. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicative cyclic groups of prime order p. A map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is a bilinear pairing map if e has the following properties:

1. Bilinearity: For all $u, v \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p^*$, it holds that

$$e\big(u^a, v^b\big) = e(u, v)^{ab}$$

2. Non-degeneracy: $e(g, g) \neq 1$ if $g \neq 1$.
3. Computability: There exists an efficient algorithm to compute $e(u, v)$ for all $u, v \in \mathbb{G}_1$.

Then $\mathbb{G}_1$ and $\mathbb{G}_2$ are said to be bilinear groups.

The security of our IBSC scheme relies on the following difficult problem(s) on finite cyclic groups which may or may not be equipped with a bilinear pairing map.

Definition 4 (Discrete Logarithm (DL) Problem) Given a group $\mathbb{G}$ of prime order p with generator g and element $g^a \in \mathbb{G}$ where a is selected uniformly at random from $\mathbb{Z}_p^*$, the DL problem is to compute a in $\mathbb{G}$.

Definition 5 (Computational Diffie-Hellman (CDH) Problem) Given a group $\mathbb{G}$ of prime order p with generator g and elements $g^a, g^b \in \mathbb{G}$, where a, b are randomly sampled from $\mathbb{Z}_p^*$, the CDH problem is to compute g^{ab} in $\mathbb{G}$.

Definition 6 (Bilinear Diffie-Hellman (BDH) Problem) Given bilinear groups $\mathbb{G}_1$ and $\mathbb{G}_2$ as defined above, and g, g^a, g^b, g^c in $\mathbb{G}_1$ for some randomly chosen $a, b, c \in \mathbb{Z}_p^*$, the BDHP problem is to compute $e(g, g)^{abc}$ in $\mathbb{G}_2$.

Definition 7 (Bilinear Decision Diffie-Hellman (BDDH) Problem) Given bilinear groups $\mathbb{G}_1$ and $\mathbb{G}_2$ as defined above, and g, g^a, g^b, g^c in $\mathbb{G}_1$ and h in $\mathbb{G}_2$ for some randomly chosen $a, b, c \in \mathbb{Z}_p^*$, decide whether $h = e(g, g)^{abc}$.

Our scheme also requires a hash function in a standard way. That is, we just need the collision-resistance of the hash function without modeling the hash function as a random oracle. In practice, one may use a standard hash function such as SHA-256 for which no known collision has been found so far.

Definition 8 (Collision-Resistant Hashing) A hash family H is (t, ϵ)-collision-resistant if no t-time adversary has advantage at least ϵ in breaking the collision-resistance of H.

3.2 Review of Yu et al.'s IBSC scheme

Yu et al.'s IBSC scheme consists of four phases: *Setup*, *Keygen*, *Signcrypt*, *Unsigncrypt*.

– *Setup*: Let $H_u : \{0,1\}^* \to \{0,1\}^{n_u}$, $H_m : \{0,1\}^* \to \{0,1\}^{n_m}$ be two collision-resistant hash functions for some $n_u, n_m \in \mathbb{Z}$. Select a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ where the order of $\mathbb{G}_1, \mathbb{G}_2$ is p. Let g be a generator of $\mathbb{G}_1$. Randomly select $\alpha \in_R \mathbb{Z}_p$, $g_2 \in_R \mathbb{G}_1$ and compute $g_1 = g^\alpha$. Also select randomly the elements u', v', u_i, $v_j \in \mathbb{G}_1$, where $i = 1, \ldots, n_u$, $j = 1, \ldots, n_m$. Let $U = \{u_i\}$, $V = \{v_j\}$. The public parameters are

$$param = \big(e, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, u', v', U, V\big)$$

and the master secret key is g_2^α.

– *Keygen*: Let u be a bit string of length n_u and let $u[i]$ be the i-th bit of u, where u represents an identity. Define $X_u \subseteq \{1, \ldots, n_u\}$ to be the set of indices such that $u[i] = 1, i \in X_u$. Randomly selects $r_u \in \mathbb{Z}_p^*$ and computes

$$d_u = \left(g_2^\alpha \left(u' \prod_{i \in X_u} u_i\right)^{r_u}, g^{r_u}\right) = (d_{u1}, d_{u2}).$$

Therefore, the sender Alice and the receiver Bob's respective private keys are

$$d_A = (d_{A1}, d_{A2}) = \left(g_2^\alpha \left(u' \prod_{i \in X_A} u_i\right)^{r_A}, g^{r_A}\right)$$

$$d_B = (d_{B1}, d_{B2}) = \left(g_2^\alpha \left(u' \prod_{i \in X_B} u_i\right)^{r_B}, g^{r_B}\right)$$

– *Signcrypt*: To sign a message $M \in \mathbb{G}_2$ to Bob, Alice randomly selects $r_m \in \mathbb{Z}_p^*$ and executes the steps as follows.

1. Compute $\sigma_1 = e(g_1, g_2)^{r_m} M$, $\sigma_2 = g^{r_m}$, and

$$\sigma_3 = \left(u' \prod_{i \in X_B} u_i\right)^{r_m}$$

2. Compute $M' = H_m(M)$. Let $M'[i]$ denote the i-th bit of M'. $Y \subset \{1, 2, \ldots, n_m\}$ denotes the set of i for which $M'[i] = 1$. Compute

$$\sigma_4 = d_{A1}\left(v' \prod_{j \in Y} v_j\right)^{r_m}$$

3. Let $\sigma_5 = d_{A2}$. The ciphertext is

$$\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$$

– *Unsigncrypt*: Receiving a ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, Bob decrypts the ciphertext as follows.

1. Compute $\sigma_1 e(d_{B2}, \sigma_3) e(d_{B1}, \sigma_2)^{-1} \to M$;
2. Compute $M' = H_m(M)$ and generates the corresponding set Y, where Y denotes the set of all i for which $M'[i] = 1$;
3. Accept the message if

$$e(\sigma_4, g) = e(g_1, g_2) e\left(u' \prod_{i \in X_A} u_i, \sigma_5\right) e\left(v' \prod_{j \in Y} v_j, \sigma_2\right)$$

3.3 Review of Jin et al.'s improved IBSC scheme

In 2010, Jin et al. found that Yu et al.'s scheme actually does not satisfy the semantic security. To make up for this defect, they proposed a rescue scheme and showed their improvement is really secure in the standard model based on DBDH problem.

– *Setup*: $\phi : \mathcal{R} \to \mathbb{G}_2$ is a bijection, where ϕ^{-1} is its inverse mapping, $\mathcal{R}$ is a subset of $\{0,1\}^{k+l}$ with p elements. $H : \{0,1\}^k \to \{0,1\}^l$ is a hash function. Pick a secret value $\alpha \in \mathbb{Z}_p$ and a public element $g_2 \in \mathbb{G}_1$, compute $g_1 = g^\alpha$. The public parameters are

$$param = \left(e, \mathbb{G}_1, \mathbb{G}_2, \phi, \phi^{-1}, g_1, g_2, h, u', v', U, V\right)$$

The master secret key is g_2^α. The other elements in *param* are the same as Yu et al.'s scheme.

– *Keygen*: Same as Yu et al.'s Keygen step.

– *Signcrypt*: To send a message $M \in \{0,1\}^k$ to Bob, Alice randomly picks $r \in \mathbb{Z}_p$ and $R \in \{0,1\}^l$ such that $M||R \in \mathcal{R}$, and does the following:

1. Compute

$$\sigma_1 = e(g_1, g_2)^r \phi(M||R), \qquad \sigma_2 = g^r$$

$$\sigma_3 = \left(u' \prod_{i \in X_B} u_i\right)^r$$

2. Compute

$$\sigma_4 = d_{A1}\left(v' \prod_{j \in Y} v_j\right)^r$$

where Y denotes the set of indices j for which the j-th bit of $H(M) \oplus R$ is 1.

3. Set $\sigma_5 = d_{A2}$. The ciphertext is

$$\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$$

– *Unsigncrypt*: Receiving a ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, Bob decrypts the ciphertext and verifies it as follows.

1. Compute

$$\phi^{-1}\left(\sigma_1 e(d_{B2}, \sigma_3) e(d_{B1}, \sigma_2)^{-1}\right) \to M||R$$

2. Generate

$$\left\{j \in Z : H(M)[j] \oplus R[j]\right\} \to Y$$

3. Accept the message M if

$$e(\sigma_4, g) = e(g_1, g_2) e\left(u' \prod_{i \in X_A} u_i, \sigma_5\right) e\left(v' \prod_{j \in Y} v_j, \sigma_2\right)$$

3.4 Analysis of the above two IBSC schemes

From the above two IBSC schemes, they are insecure as implied by the following two claims.

Claim 1 *The above two IBSC schemes are existentially forgeable under adaptive chosen identity and chosen message attacks.*

Proof Let the attacker be $\mathcal{A}$. Suppose $\mathcal{A}$ gets the signcryption $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$ of some message M which was sent to the receiver Bob by the sender Alice. $\mathcal{A}$ can construct another signcryption σ' on the same message M in Yu et al.'s scheme (and the same random number R in Jin et al.'s scheme) as follows.

Based on $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, $\mathcal{A}$ computes $\sigma' = (\sigma_1', \sigma_2', \sigma_3', \sigma_4', \sigma_5')$ as follows:

$$\sigma_1' = \sigma_1 e(g_1, g_2), \qquad \sigma_2' = \sigma_2 g, \qquad \sigma_3' = \sigma_3 \left(u' \prod_{i \in X_A} u_i\right)$$

$$\sigma_4' = \sigma_4 \left(u' \prod_{i \in X_A} u_i\right)\left(v' \prod_{j \in Y} v_j\right), \qquad \sigma_5' = \sigma_5 g$$

We next show that the forged ciphertext can pass the verification.

We take Yu et al.'s IBSC scheme as example. Following the *unsigncrypt* step, we do the following:

1. Compute

$$\begin{aligned}
&\sigma_1' e\left(d_{B2}, \sigma_3'\right) e\left(d_{B1}, \sigma_2'\right)^{-1} \\
&\quad = \sigma_1 e(g_1, g_2) e\left(d_{B2}, \sigma_3 \left(u' \prod_{i \in X_A} u_i\right)\right) \\
&\qquad \times e(d_{B1}, \sigma_2 g)^{-1} \\
&\quad = M e(g_1, g_2) e\left(d_{B2}, u' \prod_{i \in X_A} u_i\right) e(d_{B1}, g)^{-1} \\
&\quad = M e(g_1, g_2) e\left(g^{r_B}, u' \prod_{i \in X_A} u_i\right) \\
&\qquad \times e\left(g_2^\alpha \left(u' \prod_{i \in X_B} u_i\right)^{r_B}, g\right)^{-1} = M
\end{aligned}$$

2. Compute $M' = H_m(M)$ and generates the corresponding set Y, the set of all i for which $M'[i] = 1$;
3. The verification holds because

$$
\begin{aligned}
&e\left(\sigma_4', g\right) \\
&= e\left(\sigma_4\left(u' \prod_{i\in X_A} u_i\right)\left(v' \prod_{j\in Y} v_j\right), g\right) \\
&= e(g_1, g_2)e\left(u' \prod_{i\in X_A} u_i, \sigma_5\right)e\left(v' \prod_{j\in Y} v_j, \sigma_2\right) \\
&\quad \times e\left(u' \prod_{i\in X_A} u_i, g\right)e\left(v' \prod_{j\in Y} v_j, g\right) \\
&= e(g_1, g_2)e\left(u' \prod_{i\in X_A} u_i, \sigma_5'\right)e\left(v' \prod_{j\in Y} v_j, \sigma_2'\right)
\end{aligned}
$$

Finally, Jin et al.'s IBSC scheme is also forgeable by using the similar attack method above. □

Claim 2 *The plaintexts in the above two IBSC schemes are distinguishable under adaptively chosen identity and chosen message attacks.*

Proof Yu et al.'s IBSC scheme has been attacked in [22]. Hence we focus on Jin et al.'s IBSC scheme [22]. Our attack methods come from a different view. Our cryptanalysis can also be used for other IBSC schemes that can not satisfy strong unforgeability.

Adversary $\mathcal{A}$ chooses two plaintexts, m_0 and m_1, and two identities, ID_A and ID_B, on which he wishes to be challenged.

Challenger $\mathcal{C}$ chooses randomly a bit $\gamma \in \{0, 1\}$, computes $\sigma = Signcrypt(m_\gamma, S_{\mathrm{ID}_A}, \mathrm{ID}_B)$ and sends σ to the attacker $\mathcal{A}$.

According to the forgery attack proposed above, $\mathcal{A}$ can get another ciphertext σ' on the same message m_γ. Then, $\mathcal{A}$ sends the *unsigncryption* query $(\sigma', \mathrm{ID}_A, \mathrm{ID}_B)$ to the challenger $\mathcal{C}$. $\mathcal{C}$ unsigncrypts $(\sigma', \mathrm{ID}_A, \mathrm{ID}_B)$ and gets m_γ. $\mathcal{C}$ sends m_γ to $\mathcal{A}$. $\mathcal{A}$ compares the response m_γ to m_0. If they are equal, the signcrypted message is m_0. Otherwise, the signcrypted message is m_1.

Thus, the above two IBSC schemes are distinguishable against adaptive chosen identity and chosen ciphertext attacks. □

Due to the above two attack methods, we showed that Yu et al.'s IBSC scheme and Jin et al.'s IBSC scheme are insecure.

4 The proposed IBSC scheme in the standard model

In this section, we describe an IBSC scheme in the standard model. Our starting point is Boneh et al.'s strongly unforgeable signature scheme [10] and Paterson et al.'s identity-based signature (IBSC) scheme [31].

4.1 Building blocks

Partitioned Signature [10] A signature system is said to be partitioned if it satisfies two properties:

- **Property 1.** The signing algorithm can be divided into two deterministic algorithms F_1 and F_2 so that a signature on a message m using secret key SK is computed as follows:
  1. Select a random r in R.
  2. Set $\sigma_1 \leftarrow F_1(m, r, SK)$ and $\sigma_2 \leftarrow F_2(r, SK)$.
  3. Output the signature $\sigma \leftarrow (\sigma_1, \sigma_2)$.
- **Property 2.** Given m and σ_2 there is at most one σ_1 so that (σ_1, σ_2) verifies as a valid signature on m under PK.

Generic Conversion to Strongly Unforgeable Signature In [10], Boneh et al.'s presented a generic conversion from an existentially unforgeable partitioned signature scheme to a strongly unforgeable one. Let $\Sigma = (Keygen, Sign, Verify)$ be a partitioned signature where the signing algorithm is partitioned using functions F_1 and F_2. Suppose the randomness for signature generation is picked from some set R. A new strongly unforgeable signature system

$$\Sigma_{new} = (Keygen_{new}, Sign_{new}, Verify_{new})$$

can be built as follows:

- $Keygen_{new}$. To generate the public key, select random generators $g, h \in \mathbb{G}_1$ and a hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$. Next, run $Keygen$ to obtain the secret key SK and the public key PK. The public key and secret key for the new system are: $PK' = (PK, g, h)$ and $SK' = (SK)$.
- $Sign_{new}(SK, M)$. A signature on a message $M \in \{0, 1\}^*$ is generated as follows.
  1. Select a random exponent $s \in \mathbb{Z}_p$ and a random $r \in R$;
  2. Set $\sigma_2 \leftarrow F_2(r, SK)$;
  3. Compute $t \leftarrow H(M, \sigma_2) \in \mathbb{Z}_p$, $m \leftarrow g^t h^s \in \mathbb{G}$, $\sigma_1 \leftarrow F_1(m, r, SK)$;
  4. Output the signature $\sigma \leftarrow (\sigma_1, \sigma_2, s)$.
- $Verify_{new}(PK, M, \sigma)$. A signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ on a message M is verified as follows:
  1. Compute $\tilde{t} \leftarrow H_k(M, \sigma_2)$ and $\tilde{m} \leftarrow g^{\tilde{t}} h^{\sigma_3}$.
  2. Output $Verify(PK, \tilde{m}, (\sigma_1, \sigma_2))$.

Paterson et al.'s IBSC Scheme [31] Paterson et al.'s signature consists of *Setup*, *Keygen*, *Sign* and *Verify*.

- *Setup*: Let $H_u : \{0,1\}^* \to \{0,1\}^{n_u}$, $H_m : \{0,1\}^* \to \{0,1\}^{n_m}$ be two collision-resistant hash functions where $n_u, n_m \in \mathbb{Z}$. Pick a secret value $\alpha \in \mathbb{Z}_p$ and a public element $g_2 \in \mathbb{G}_1$, and compute $g_1 = g^\alpha$. The public parameters are

  $$param = \big(e, \mathbb{G}_1, \mathbb{G}_2, g, g_1, g_2, u', v', U, V\big)$$

  and the master secret key is g_2^α.
- *Keygen*: Let $\mathbf{u}$ be a bit string of length n_u, representing an identity and let $\mathbf{u}[i]$ be the i-th bit of $\mathbf{u}$. Define $X_u \subseteq \{1, \ldots, n_u\}$ to be the set of indices such that $\mathbf{u}[i] = 1$ for $i \in X_u$. Randomly select $r_u \in \mathbb{Z}_p^*$ and compute

  $$d_u = \left(g_2^\alpha \left(u' \prod_{i \in X} u_i\right)^{r_u}, g^{r_u}\right) = (d_{u1}, d_{u2}).$$

- *Sign*: To sign a message m, a sender with identity $\mathbf{u}$ randomly selects $r_m \in \mathbb{Z}_p^*$ and computes

  $$\sigma = \left(d_{u1}\left(v' \prod_{j \in Y} v_j\right)^{r_m}, d_{u2}, g^{r_m}\right) \in \mathbb{G}_1^3$$

  where $Y \subseteq \{1, \ldots, n_m\}$ to be the set of indices such that $m[i] = 1$.
- *Verify*: Given a purported signature $\sigma = (\sigma_1, \sigma_2, \sigma_3) \in \mathbb{G}_1^3$ of an identity $\mathbf{u}$ on a message m, a verifier accepts σ if the following equality holds:

  $$e(\sigma_1, g) = e(g_2, g_1) e\left(\left(u' \prod_{i \in X_u} u_i\right), \sigma_2\right) \times e\left(v' \prod_{j \in Y} v_j, \sigma_3\right)$$

4.2 Our IBSC scheme in the standard model

Our scheme consists of four procedures: *Setup*, *Keygen*, *Signcrypt*, *Unsigncrypt*.

- *Setup*: Let $H : \{0,1\}^* \to \mathbb{Z}_p^*$, $H_u : \{0,1\}^* \to \{0,1\}^{n_u}$, $H_m : \{0,1\}^* \to \{0,1\}^{n_m}$ be three collision-resistant hash functions for some $n_u, n_m \in \mathbb{Z}$. Select a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ where the order of $\mathbb{G}_1, \mathbb{G}_2$ is a large prime p. Let g be a generator of $\mathbb{G}_1$. Randomly select $\alpha \in \mathbb{Z}_p$, and $g_2, u', v', u_i, v_j, h \in \mathbb{G}_1$ and compute $g_1 = g^\alpha$, where $i = 1, \ldots, n_u$, $j = 1, \ldots, n_m$. Denote $U = \{u_i\}$, $V = \{v_j\}$. The public parameters are

  $$param = \big(e, \mathbb{G}_1, \mathbb{G}_2, g, g_1, g_2, h, u', v', U, V, H_u, H_m, H\big)$$

  and the master secret key is g_2^α.
- *Keygen*: It is the same as Paterson et al.'s *Keygen* phase. Specifically, let $\mathbf{u}$ be a bit string of length n_u, representing an identity and let $\mathbf{u}[i]$ be the i-th bit of $\mathbf{u}$. Define $X_u \subseteq \{1, \ldots, n_u\}$ to be the set of indices such that $\mathbf{u}[i] = 1$ for $i \in X_u$. Randomly select $r_u \in \mathbb{Z}_p^*$ and compute

  $$d_u = \left(g_2^\alpha \left(u' \prod_{i \in X} u_i\right)^{r_u}, g^{r_u}\right) = (d_{u1}, d_{u2}).$$

  Therefore, the sender Alice and the receiver Bob's private keys are

  $$d_A = (d_{A1}, d_{A2}) = \left(g_2^\alpha \left(u' \prod_{i \in X_A} u_i\right)^{r_A}, g^{r_A}\right)$$

  $$d_B = (d_{B1}, d_{B2}) = \left(g_2^\alpha \left(u' \prod_{i \in X_B} u_i\right)^{r_B}, g^{r_B}\right)$$

- *Signcrypt*: To send a message $M \in \mathbb{G}_2$ to Bob, Alice randomly picks $r_m \in \mathbb{Z}_p$ in a uniform distribution and follows the steps as follows.

  1. Compute

     $$\sigma_1 = e(g_1, g_2)^{r_m} M, \qquad \sigma_2 = g^{r_m},$$

     $$\sigma_3 = \left(u' \prod_{i \in X_B} u_i\right)^{r_m}$$

  2. Denote $\sigma_5 = d_{A2}$;
  3. Compute $t = H(\sigma_1, \sigma_3, \sigma_2, \sigma_5)$;
  4. Randomly select $s \in \mathbb{Z}_p^*$ in a uniform distribution and compute $m = H_{n_m}(g^t h^s)$. Let $m[i]$ denote the i-th bit of m, and $Y \subset \{1, 2, \ldots, n_m\}$ denote the set of i for which $m[i] = 1$. Compute

     $$\sigma_4 = d_{A1}\left(v' \prod_{j \in Y} v_j\right)^{r_m}.$$

     The ciphertext is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, s)$.

- *Unsigncrypt*: Receiving a ciphertext $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, s)$, Bob decrypts the ciphertext as follows.

  1. Compute $t = H(\sigma_1, \sigma_3, \sigma_2, \sigma_5), m = H_m(g^t h^s)$ and generates the corresponding set Y, where Y denotes the set of all i for which $m[i] = 1$.
  2. Check that the equality

     $$e(\sigma_4, g) = e(g_1, g_2) e\left(u' \prod_{i \in X_A} u_i, \sigma_5\right) e\left(v' \prod_{j \in Y} v_j, \sigma_2\right)$$

  If it does not hold, output $\perp$. Otherwise, output

  $$M = \sigma_1 e(d_{B2}, \sigma_3) e(d_{B1}, \sigma_2)^{-1}$$

5 Analysis of our IBSC scheme

5.1 Security analysis

We prove that our IBSC scheme is SUF-IBSC-CMA secure as signature scheme and IND-IBSC-CCA2 secure as an encryption scheme in the standard model.

Theorem 1 *The proposed IBSC scheme is SUF-IBSC-CMA secure in the standard model.*

Proof Paterson et al.'s signature system is known to be existential unforgeable assuming that the CDH problem is difficult [31].

It is straightforward to verify that Paterson et al.'s signature is partitioned. The function F_1 and F_2 are:

$$F_1(m, r_m, SK) = \left(d_{A1}\left(v' \prod_{j \in Y} v_j\right)^{r_m}, d_{A2}\right),$$

$$F_2(r_m, SK) = g^{r_m}$$

where $v', v_1, \ldots, v_{n_m} \in \mathbb{G}_1$ are part of the public key and $m = m_1, \ldots, m_{n_m} \in \{0,1\}^{n_m}$. The second property of partitioned signatures holds since given m and σ_5 there is only one $F_1(m, r_m, SK)$ for which the verification equation will hold. We assume that each element $g \in \mathbb{G}_1$ has a unique encoding (otherwise an attacker can invalidate property 2 by simply changing the encoding of a group element).

According to Boneh et al.'s conversion from existentially unforgeable signature to strongly unforgeable signature, we can derive that the signature part $(\sigma_2, \sigma_4, \sigma_5, s)$ on the message $M = (\sigma_1, \sigma_3)$ is strongly unforgeable, i.e., the ciphertext σ is SUF-IBSC-CMA secure. □

Theorem 2 *Our proposed IBSC scheme is IND-IBSC-CCA2 secure in the standard model if the BDDHP is hard.*

Proof Suppose $\mathcal{A}$ is a forger against our IBSC scheme in the standard model. We are going to construct another algorithm $\mathcal{C}$ that makes use of $\mathcal{A}$ to solve the BDDHP. $\mathcal{C}$ is given as input a random 5-tuple (g, g^a, g^b, g^c, T). Algorithm $\mathcal{C}$'s goal is to output 1 if $T = e(g,g)^{abc}$ and 0 otherwise. $\mathcal{C}$ runs $\mathcal{A}$ executing the steps as follows.

Setup: The challenger $\mathcal{C}$ sets $l_u = 2(q_e + q_s + q_u)$ and $l_m = 2q_u$ and chooses randomly two integers k_u and k_m $(0 \le k_u \le n_u, 0 \le k_m \le n_m)$; an integer $x' \in Z_{l_u}$, an n_u-dimensional vector $X = (x_i)$ $(x_i \in Z_{l_u})$; an integer $z' \in Z_{l_m}$, an n_m-dimensional vector $Z = (z_j)$ $(z_j \in Z_{l_m})$; two integers $y', w' \in \mathbb{Z}_p$, an n_u-dimensional vector $Y = (y_i)(y_i \in \mathbb{Z}_p)$ and an n_m-dimensional vector $W = (w_j)$ $(w_j \in \mathbb{Z}_p)$, where q_e, q_s, q_u denote the number of *Keygen queries, Signcrypt queries, Unsigncrypt queries*. Let $g_1 = g^a, g_2 = g^b$. $\mathcal{A}$ is first given the public

$$param = \left(e, \mathbb{G}_1, \mathbb{G}_2, g, g_1, g_2, h, u', v', U, V, H_u, H_m, H\right).$$

Suppose $\mathbf{u}$ is an identity and $\mathbf{m}$ is a message. $\mathcal{C}$ defines the functions as follows.

$$F(\mathbf{u}) = (p - l_u k_u) + x' + \sum_{i \in \mathcal{U}} x_i,$$

$$J(\mathbf{u}) = y' + \sum_{i \in \mathcal{U}} y_i,$$

$$K(\mathbf{m}) = (p - l_m k_m) + z' + \sum_{j \in Y} z_j,$$

$$L(\mathbf{m}) = w' + \sum_{j \in Y} w_j.$$

$\mathcal{C}$ assigns the public parameters as follows

$$u' = g_2^{p - l_u k_u + x'} g^{y'}, \qquad u_i = g_2^{x_i} g^{y_i} \quad (1 \le i \le n_u),$$

$$v' = g_2^{p - l_m k_m + z'} g^{w'}, \qquad v_j = g_2^{z_j} g^{w_j} \quad (1 \le j \le n_m)$$

For any identity $\mathbf{u}$ and any message $\mathbf{m}$, we have

$$u' \prod_{i \in \mathcal{U}} u_i = g_2^{F(\mathbf{u})} g^{J(\mathbf{u})}, \qquad v' \prod_{j \in \mathcal{M}} v_j = g_2^{K(\mathbf{m})} g^{L(\mathbf{m})}$$

Keygen queries. When $\mathcal{A}$ asks for the private key corresponding to the identity $\mathbf{u}$, $\mathcal{C}$ first checks if $F(\mathbf{u}) = 0$ and aborts in this situation. Otherwise, it chooses a random $r_u \in \mathbb{Z}_p^*$ in the uniform distribution and gives $\mathcal{A}$ the pair

$$d_u = (d_0, d_1) = \left(g_1^{\frac{-J(\mathbf{u})}{F(\mathbf{u})}} \left(u' \prod_{i \in \mathcal{U}} u_i\right)^{r_u}, g_1^{\frac{-1}{F(\mathbf{u})}} g^{r_u}\right)$$

Signcrypt queries. At any time, the adversary $\mathcal{A}$ can perform a signcryption query for a plaintext M and identities u_A and u_B. If $F(u_A) \neq 0 \bmod l_u$, $\mathcal{C}$ first generates a private key for u_A just calling the *Keygen query* phase described above, and then runs $Signcrypt(M, d_A, u_B)$ to answer $\mathcal{A}$'s query. Otherwise, $\mathcal{C}$ will simply abort.

Unsigncrypt queries. At any time, the adversary $\mathcal{A}$ can perform an unsigncryption query on a ciphertext σ for identities u_A and u_B. If $F(u_B) \neq 0 \bmod l_u$, $\mathcal{A}$ first generates a private key for u_B just calling the *Keygen query* phase described above, and then runs $Unsigncrypt(\sigma, d_B, u_A)$ to answer $\mathcal{A}$'s query. If $F(u_B) = 0 \bmod l_u$, $F(u_A) \neq 0 \bmod l_u$ and $K(H(\sigma_1, \sigma_3, \sigma_2, \sigma_5)) \neq 0 \bmod l_m$, which is denoted as $m = H(\sigma_1, \sigma_3, \sigma_2, \sigma_5)$, $\mathcal{A}$ can derive the secret key d_A of u_A and compute as follows.

$$g_2^{r_m} = \left(\frac{\sigma_4}{d_{A1} \sigma_2^{L(m)}}\right)^{\frac{1}{K(m)}}, \qquad M = \frac{\sigma_1}{e(g_1, g_2^{r_m})}$$

Then $\mathcal{C}$ can get M and send it to $\mathcal{A}$. Otherwise, abort.

After a polynomially bounded number of queries, the adversary $\mathcal{A}$ chooses two distinct identities $\{u_A, u_B\}$ on which he wishes to be challenged, with a constraint that $\mathcal{A}$ has not asked a *Keygen* query on u_B. Then $\mathcal{A}$ submits two identities $\{u_A, u_B\}$ and two equal length messages $M_0, M_1 \in \mathbb{G}_2$ to $\mathcal{C}$. If $F(u_B) \neq 0 \bmod l_u$, $\mathcal{C}$ aborts. Otherwise, $\mathcal{C}$ flips a fair coin $\gamma \in \{0, 1\}$, and constructs a ciphertext of M_γ as follows.

Set

$$\sigma_1 = TM_\gamma, \qquad \sigma_2 = g^c, \qquad \sigma_3 = \left(g^c\right)^{J(u_B)}$$

Select a random number $t_A \in \mathbb{Z}_p^*$ and set

$$\sigma_5 = g_1^{-\frac{1}{F(u_A)}} g^{t_A}$$

Denote

$$\mathbf{m}_\gamma = H(\sigma_1, \sigma_3, \sigma_2, \sigma_5),$$
$$Y_\gamma = \left\{ j | \mathbf{m}_\gamma[j] = 1,\ j = 1, 2, \ldots, n_m \right\}$$

Set

$$\sigma_4 = g_1^{-\frac{J(u_A)}{F(u_A)}} \left(u' \prod_{i \in \mathcal{U}_\mathcal{A}} u_i \right)^{t_A} C^{L(\mathbf{m}_\gamma)}$$

Return $\mathcal{A}$ with

$$\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$$

The adversary $\mathcal{A}$ can continue to query the *Keygen*, *Signcrypt* and *Unsigncrypt* oracles. But he is not allowed to make an *Unsigncrypt* query for σ under u_A and u_B. At the end of the simulation, the adversary $\mathcal{A}$ outputs a guess bit γ'. If $\gamma' = \gamma$, $\mathcal{C}$ outputs 1 indicating that $T \neq e(g, g)^{abc}$. Otherwise, $\mathcal{C}$ outputs 0 indicating that $T \neq e(g, g)^{abc}$.

The above analysis shows that if the adversary $\mathcal{A}$ can break the IND-IBSC-CCA2 security of our IBSC scheme, then the algorithm $\mathcal{C}$ can solve the underlying BDDH problem. Since the BDDH problem is assumed to be difficult, the successful probability of the algorithm $\mathcal{C}$ is negligible. The ciphertext part $(\sigma_1, \sigma_2, \sigma_3)$ of σ is CCA2 secure. On the other side, the signature part $(\sigma_2, \sigma_4, \sigma_5, s)$ of σ on the message $m = H_m(g^t h^s)$ is strongly unforgeable, where $t = H(\sigma_1, \sigma_3, \sigma_2, \sigma_5)$. Thus, $\mathcal{A}$ can not get new challenge ciphertext on the chosen message M_γ. In the meanwhile, the signature part is independent of the receiver private key d_B. It will not expose any information on the plaintext M_γ. Therefore, our IBSC scheme is IND-IBSC-CCA2 secure. □

5.2 Efficiency analysis

For fairness, we compare the efficiency of our scheme with that of Zheng's schemes [46] and Fan's scheme [18] which are also shown secure in the standard model. The comparison is in terms of number pairing map operations, number of exponentiations on $\mathbb{G}_1$ and $\mathbb{G}_2$, signcryption size, as summarized in Table 1 where n denotes biometric string length. It can be seen that only our scheme has complexity independent of the parameters n, n_m, n_u which may be up to hundreds to guarantee the security of these schemes in practice. This implies that our scheme will be more efficient when these schemes are implemented in the real world.

Table 1 Efficiency comparison

	Pair	Exp. on $\mathbb{G}_1$	Exp. on $\mathbb{G}_2$	Size
[43]	3n	$1 + n_m$	n	$5\mathbb{G}_1$
[46]	5	$8 + n_u$	1	$2\mathbb{G}_1 + 1\mathbb{G}_2 + 1Z_p$
Ours	7	7	1	$4\mathbb{G}_1 + 1\mathbb{G}_2 + 1Z_p$

5.3 Instantiating IBSC-based data upload in clouds

Following our ISBC based security framework in Sect. 2.3, this section instantiates a secure data upload scheme based on our IBSC proposal. The proposed scheme consists of the following procedures.

- **Setup:** In this procedure, the CSP and the companies jointly run the *Setup* procedure of the ISBC scheme to setup the system.
  1. The CSP partially runs the *Setup* procedure of an ISBC scheme to generate the global parameters excluding the public key of each company. Let $H : \{0, 1\}^* \to \mathbb{Z}_p^*$, $H_u : \{0, 1\}^* \to \{0, 1\}^{n_u}$, $H_m : \{0, 1\}^* \to \{0, 1\}^{n_m}$ be three collision-resistant hash functions for some n_u, $n_m \in \mathbb{Z}$. The CSP selects a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, where the order of $\mathbb{G}_1, \mathbb{G}_2$ is a large prime p. The CSP selects g as a generator of $\mathbb{G}_1$, and randomly chooses $g_2, u', v', u_i, v_j, h \in \mathbb{G}_1$, where $i = 1, \ldots, n_u$, $j = 1, \ldots, n_m$. Denote $U = \{u_i\}$, $V = \{v_j\}$. The public parameters are
  $$param = \left(e, \mathbb{G}_1, \mathbb{G}_2, g, g_2, h, u', v', U, V, H_u, H_m, H\right).$$
  2. A company randomly chooses $\alpha \in \mathbb{Z}_p$ and computes its public key $g_1 = g^\alpha$. The company subscribe storage services from the CSP.
  3. The CSP records g_1 and creates a storage account for the company.
- **Authorization:** Taking into as input an employee's identity, the company generates a secret credential by running the *Extract* procedure of the underlying ISBC scheme. Let $\mathbf{u}$ be a bit string of length n_u, representing an identity and let $\mathbf{u}[i]$ be the i-th bit of $\mathbf{u}$. Define $X_u \subseteq \{1, \ldots, n_u\}$

to be the set of indices such that $\mathbf{u}[i] = 1$ for $i \in X_u$. Randomly select $r_u \in \mathbb{Z}_p^*$ and compute

$$d_u = \left(g_2^{\alpha}\left(u' \prod_{i \in X} u_i\right)^{r_u}, g^{r_u}\right) = (d_{u1}, d_{u2}).$$

Therefore, the employee with identity A and, similarly, another employee with identity B's respective secret credentials are

$$d_A = (d_{A1}, d_{A2}) = \left(g_2^{\alpha}\left(u' \prod_{i \in X_A} u_i\right)^{r_A}, g^{r_A}\right)$$

$$d_B = (d_{B1}, d_{B2}) = \left(g_2^{\alpha}\left(u' \prod_{i \in X_B} u_i\right)^{r_B}, g^{r_B}\right)$$

– **Upload:** With a valid credential and the data to be sent to another employee with identity B, an employee runs the *Signcrypt* to generate the resulting signcryption ciphertext. The employee uploads the data in an signcrypted form to the company's account. Specifically, to send a message $M \in \mathbb{G}_2$ to employee B, the employee A randomly picks $r_m \in \mathbb{Z}_p$ in a uniform distribution and follows the steps as follows.

1. Compute $\sigma_1 = e(g_1, g_2)^{r_m} M$, $\sigma_2 = g^{r_m}$,

$$\sigma_3 = \left(u' \prod_{i \in X_B} u_i\right)^{r_m}$$

2. Denote $\sigma_5 = d_{A2}$;
3. Compute $t = H(\sigma_1, \sigma_3, \sigma_2, \sigma_5)$;
4. Randomly select $s \in \mathbb{Z}_p^*$ in a uniform distribution and compute $m = H_{n_m}(g^t h^s)$. Let $m[i]$ denote the i-th bit of m, and $Y \subset \{1, 2, \ldots, n_m\}$ denote the set of i for which $m[i] = 1$. Compute

$$\sigma_4 = d_{A1}\left(v' \prod_{j \in Y} v_j\right)^{r_m}.$$

The ciphertext is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, s)$.

5. Upload σ to the company's storage account maintained by the CSP.

The CSP executes the following steps:

1. Compute

$$t = H(\sigma_1, \sigma_3, \sigma_2, \sigma_5), \qquad m = H_m\left(g^t h^s\right)$$

and generates the corresponding set Y, where Y denotes the set of all i for which $m[i] = 1$.

2. Check that the equality

$$e(\sigma_4, g) = e(g_1, g_2) e\left(u' \prod_{i \in X_A} u_i, \sigma_5\right) e\left(v' \prod_{j \in Y} v_j, \sigma_2\right)$$

and add σ to the according company's account if and only the equality holds.

– **Read:** The employee B can download σ anywhere anytime. If employee B has been authorized by the company, then the employee B can read the original digital content *Data* executing the *Unsigncrypt* procedure, i.e., by computing

$$M = \sigma_1 e(d_{B2}, \sigma_3) e(d_{B1}, \sigma_2)^{-1}$$

The availability of the scheme follows from the correctness of IBSC. From the security properties proven in Theorems 1 and 2, the secrecy and authentication requirements are simultaneously achieved in the above proposed scheme.

6 Conclusion

In this paper, we justified that IBSC is an appropriate cryptographic primitive for secure data upload in clouds. Based IBSC, we proposed a generic framework to simultaneously achieve secrecy and authentication in company-oriented cloud storage applications. After analyzing two recent IBSC schemes in the standard model, and motivated by Boneh et al.'s strongly unforgeable signature and Paterson et al.'s identity-based signature, we proposed a new IBSC scheme provably secure in the standard model. Our scheme has constant complexity in terms of computation and communication. By exploiting our IBSC proposal, we instantiated an distributed data upload scheme in clouds.

Acknowledgements For the authors with the UNESCO Chair in Data Privacy, this paper does not necessarily reflect the position of UNESCO nor does it commit that organization.

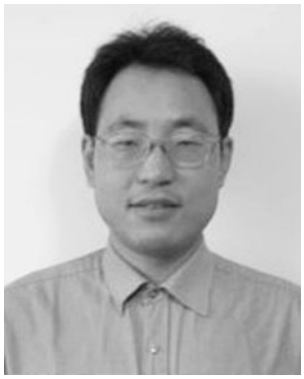
References

1. An, J.H., Dodis, Y., Rabin, T.: On the security of joint signature and encryption. In: Proceedings of EUROCRYPT'02, vol. 2332, pp. 83–107 (2002)
2. Armknecht, F., Augot, D., Perret, L., Sadeghi, A.: On constructing homomorphic encryption schemes from coding theory. In: Proceedings of Cryptography and Coding—13th IMA International Conference, Oxford, UK, December 2011, pp. 23–40 (2011)
3. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Khan, O., Kissner, L., Peterson, Z., Song, D.: Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur. **14**(1), 12.1–12.34 (2011)
4. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., Song, D.: Provable data possession at untrusted stores. In: Proc. of ACM CCS'07, pp. 598–609 (2007)
5. Baek, J., Steinfeld, R., Zheng, Y.: Formal proofs for the security of signcryption. In: Proc. of PKC'02, vol. 2274, pp. 80–98 (2002)
6. Baek, J., Steinfeld, R., Zheng, Y.: Formal proofs for the security of signcryption. J. Cryptol. **20**(2), 203–235 (2007)

7. Barreto, P.S.L.M., Libert, B., McCullagh, N., Quisquater, J.J.: Efficient and provably-secure identity based signatures and signcryption from Bilinear maps. In: Proc. of ASIACRYPT'05, vol. 3788, pp. 515–532 (2005)
8. Bellare, M., Shoup, S.: Two-tier signatures, strongly unforgeable signatures, and fiat-shamir without random oracles. In: Proc. of PKC'07, vol. 4450, pp. 201–216 (2007)
9. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Proc. of ASIACRYPT'01, vol. 2248, pp. 514–532 (2011)
10. Boneh, D., Shen, E., Waters, B.: Strongly unforgeable signatures based on computational diffie-hellman. In: Proc. of PKC'06, vol. 3958, pp. 229–240 (2006)
11. Boyen, X.: Multipurpose identity based signcryption: a swiss army knife for identity based cryptography. In: Proc. of CRYPTO'03, vol. 2792, pp. 383–399 (2003)
12. Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Proc. of CRYPTO'11, vol. 6841, pp. 505–524 (2011)
13. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology. J. ACM **51**(4), 557–594 (2004)
14. Chatterjee, P., Sengupta, I., Ghosh, S.K.: STACRP: a secure trusted auction oriented clustering based routing protocol for MANET. Clust. Comput. **15**, 303–320 (2012)
15. Chen, L., Malone-Lee, J.: Improved identity-based signcryption. In: Proc. of PKC'05, vol. 3386, pp. 362–379 (2005)
16. Chow, S.S.M., Yiu, S.M., Hui, L.C.K., Chow, K.P.: Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. In: Proc. of ICISC'03, vol. 2971, pp. 352–369 (2004)
17. Di Pietro, R., Blass, E.-O., Molva, R., Onen, M.: PRISM—privacy-preserving searches in MapReduce. In: Proc. of PET'02, vol. 7384, pp. 180–200 (2012)
18. Fan, J., Zheng, Y., Tang, X.: Signcryption with non-interactive non-repudiation without random oracles. In: Transactions on Computational Science X, vol. 6340, pp. 202–230 (2010)
19. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proc. of STOC 2009, pp. 169–178 (2009)
20. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proc. of ACM CCS'06, pp. 89–98 (2006)
21. Huang, Q., Wong, D.S., Li, J., Zhao, Y.: Generic transformation from weakly to strongly unforgeable signatures. J. Comput. Sci. Technol. **23**(2), 240–252 (2008)
22. Itani, W., Kayssi, A., Chehab, A.: SNUAGE: An Efficient Platform-as-a-service Security Framework for the Cloud. Cluster Comput. Accessed: 1 December (2012). Retrieved from: http://link.springer.com/article/10.1007%2Fs10586-012-0223-x
23. Jin, Z.P., Wen, Q.Y., Du, H.Z.: An improved semantically-secure identity-based signcryption scheme in the standard model. Comput. Electr. Eng. **36**(3), 545–552 (2010)
24. Kamara, S., Lauter, K.: Cryptographic cloud storage. In: Proc. of Financial Cryptography Workshops 2010. Lecture Notes in Computer Science, vol. 6054, pp. 136–149 (2010)
25. Kim, I., Lee, D., Kim, K.J., Lee, J.: Flexible authorization in home network environments. Clust. Comput. **15**, 3–15 (2012)
26. Li, M., Yu, S., Cao, N., Lou, W.: Authorized private keyword search over encrypted data in cloud computing. In: Proc. of the 2011 31st International Conference on Distributed Computing Systems (ICDCS'11), pp. 383–392. IEEE Comput. Soc., Washington (2011)
27. Libert, B., Quisquator, J.J.: A new identity based signcryption scheme from pairings. In: Proc. of IEEE Information Theory Workshop, Paris, France, pp. 155–158 (2003)
28. Liu, Z.H., Hu, Y.P., Zhang, X.S., Ma, H.: Certificateless signcryption scheme in the standard model. Inf. Sci. **180**(3), 452–464 (2010)
29. Malone-Lee, J.: Identity Based Signcryption, Cryptology ePrint Archive. IACR Report 2002/098. Accessed: 1 December (2012). Retrieved from: http://eprint.iacr.org/2002/098.pdf
30. Matsuda, T., Attrapadung, N., Hanaoka, G., Matsuura, K., Imai, H.: A CDH-based strongly unforgeable signature without collision resistant hash function. In: Proc. of International Conference on Provable Security. Lecture Notes in Computer Science, vol. 4784, pp. 68–84 (2007)
31. Paterson, K.G., Schuldt, J.C.N.: Efficient identity-based signatures secure in the standard model. In: Proc. of ACISP'06. Lecture Notes in Computer Science, vol. 4058, pp. 207–222 (2006)
32. Qin, B., Wang, H., Wu, Q., Liu, J., Domingo-Ferrer, J.: An identity based signcryption scheme in the standard model. In: Proc. of the 4-th International Conference on Intelligent Networking and Collaborative Systems—INCOS 2012, Bucharest, Romania, September 2012, pp. 606–611 (2012)
33. Sadeghi, A.-R., Schneider, T., Winandy, M.: Token-based cloud computing. In: Proc. of TRUST'10, Berlin, Germany, June 2010, pp. 417–429 (2010)
34. Wang, H.: Proxy Provable Data Possession in Public Clouds. IEEE Transactions on Services Computing. IEEE computer Society Digital Library, 07 December (2012). http://doi.ieeecomputersociety.org/10.1109/TSC.2012.35
35. Wang, H., Zhang, Y.: On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage. IEEE Trans. Parallel Distrib. Syst. **PP**(99), 1. doi:10.1109/TPDS.2013.16
36. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Proc. of Eurocrypt'05. Lecture Notes in Computer Science, vol. 3494, pp. 457–473 (2005)
37. Security Guidance for Critical Areas of Focus in Cloud Computing. Accessed: 12 November (2012). Retrieve from: www.cloudsecurityalliance.org
38. Steinfeld, R., Pieprzyk, J., Wang, H.X.: How to strengthen any weakly unforgeable signature into a strongly unforgeable signature. In: Proc. of CT-RSA'07. Lecture Notes in Computer Science, vol. 4377, pp. 357–371 (2007)
39. Wang, L.L., Zhang, G.Y., Ma, C.G.: A secure ring signcryption scheme for private and anonymous communication. In: Proc. of IFIP International Conference on Network and Parallel Computing—NPC Workshops 2007, Dalian, China, September 2007, pp. 107–111 (2007)
40. Wu, Q., Mu, Y., Susilo, W., Qin, B., Domingo-Ferrer, J.: Asymmetric group key agreement. In: Proc. of EUROCRYPT'09, vol. 5479, pp. 153–170 (2009)
41. Wu, Q., Qin, B., Zhang, L., Domingo-Ferrer, J., Farràs, O.: Bridging broadcast encryption and group key agreement. In: Proc. of ASIACRYPT'11. Lecture Notes in Computer Science, vol. 7073, pp. 143–160 (2011)
42. Yu, Y., Yang, B., Sun, Y., Zhu, S.L.: Identity based signcryption scheme without random oracles. Comput. Stand. Interfaces **31**(1), 56–62 (2009)
43. Zhang, M., Li, P., Yang, B., Wang, H., Takagi, T.: Towards confidentiality of ID-based signcryption schemes under without random oracle model. In: Proc. of PAISI'10. Lecture Notes in Computer Science, vol. 6122, pp. 98–104 (2010)
44. Zhang, G., Parashar, M.: Cooperative detection and protection against network attacks using decentralized information sharing. Clust. Comput. **13**, 67–86 (2010)
45. Zhang, B., Xu, Q.L.: An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model. In: Proc. of AST/UCMA/ISA/ACN 2010. Lecture Notes in Computer Science, vol. 6059, pp. 15–27 (2010)
46. Zhang, M., Yang, B., Takagi, T., Shen, Y., Zhang, W.: Fuzzy biometric signcryption scheme with bilinear pairings in the standard model. In: Proc. of PAISI'10. Lecture Notes in Computer Science, vol. 6122, pp. 77–87 (2010)

47. Zheng, Y.: Digital signcryption or how to achieve cost (Signature & Encryption) ≤ Cost (Signature) + Cost (Encryption). In: Proc. of CRYPTO'97. Lecture Notes in Computer Science, vol. 1294, pp. 165–179 (1997)

Bo Qin received her Ph.D. degree in Cryptography from Xidian University in 2008 in China. Since then, she has been with Xi'an University of Technology (China) as a lecturer, and with Universitat Rovira i Virgili (Catalonia) as a postdoctoral researcher. Her research interests include pairing-based cryptography, data security and privacy, and VANET security. She has been a holder/co-holder of 5 China/Spain funded projects. She has authored over 50 publications and served in the program committee of several international conferences in information security.



Huaqun Wang received the BS degree in mathematics education from the Shandong Normal University and the MS degree in applied mathematics from the East China Normal University, both in China, in 1997 and 2000, respectively. He received the Ph.D. degree in Cryptography from Nanjing University of Posts and Telecommunications in 2006. Since then, he has been with Dalian Ocean University (China) as an associate professor. His research interests include applied cryptography, network security, and cloud computing security. He has published more than 40 papers. He has served in the program committee of several international conferences and the editor board of international journals.

Qianhong Wu received his Ph.D. in Cryptography from Xidian University in 2004. Before he joins to Beihang University (China) as a full professor in 2013, he has been with Wollongong University (Australia) as an associate research fellow, with Wuhan University (China) as an associate professor, and with Universitat Rovira i Virgili (Spain) as a research director. His research interests include cryptography, information security and privacy, ad hoc network security and cloud computing security. He has been a holder/co-holder of 6 domestic and international funded projects. He has authored 5 patents and over 90 publications. He has served in the program committee of several international conferences in information security and privacy. He is a member of IACR and IEEE.

Jianwei Liu received his Ph.D. in communication engineering from Xidian University, China in 1998, and his B.S. and M.S. degrees in electronic engineering from Shandong University, China in 1985 and 1988. He is currently a professor and the head of School of Electronic and Information Engineering of Beihang University. His research interests are the security of wireless and mobile communication network and computer network. He is a senior member of the Chinese Institute of Electronics and director of the Chinese Association for Cryptologic Research.

Josep Domingo-Ferrer is a Distinguished Professor of Computer Science and an ICREA-Acadèmia Researcher at Universitat Rovira i Virgili, Tarragona, Catalonia, where he holds the UNESCO Chair in Data Privacy. His research interests are in data privacy and data security. He received his M. Sc. and Ph. D. degrees in Computer Science from the Autonomous University of Barcelona in 1988 and 1991, respectively. He also holds an M. Sc. in Mathematics. He has won several research and technology transfer awards, including the IEEE Fellow Grade, the Academia Europaea membership, the "Narcís Monturiol" Medal to the scientific merit and the 1st Edition of the ICREA Acadèmia Prize 2008, the last two awarded by the Government of Catalonia. He has authored 5 patents and over 300 publications. He has been the co-ordinator of projects funded by the European Union and the Spanish government, among which the CONSOLIDER ARES project on security and privacy, one of Spain's 34 strongest research teams. He has been the PI of US-funded research contracts. He has held visiting appointments at Princeton, Leuven and Rome. He is a co-Editor-in-Chief of the journal "Transactions on Data Privacy".