Efficient Trust Based Information Sharing Schemes over Distributed Collaborative Networks

Huang Lin, Xiaoyan Zhu, Yugang Fang, *Fellow, IEEE*, Dongsheng Xing, Chi Zhang, and Zhenfu Cao

***Abstract*—In distributed collaborative networks such as peer-to-peer systems, privacy preserving information sharing and dissemination heavily relies on effective trust management. Trust based encryption (TBE) has been proposed to be a solution to enabling privacy preserving information sharing and dissemination for such networks. Unfortunately, the previously proposed schemes are not efficient in terms of communications overhead, and require a constantly online trust authority. In this paper, we propose two trust based encryption schemes with significantly improved efficiency. In the first scheme, we develop a generic transformation approach based on the recently proposed identity based broadcast encryption (IBBE) technique, which can significantly reduce both memory space and communication overhead when static reputation is considered. For the dynamic reputation scenarios, we present a trust based encryption scheme which is based on a recently proposed revocable identity based encryption technique, resulting in significantly reduced communication overhead at the central trust authority.**

***Index Terms*—Trust management, privacy preserving information sharing, trust based encryption, identity based encryption.**

I. Introduction

REPUTATION systems have served as an important tool in establishing trust in distributed networks, such as peer-to-peer networks. Based on their interaction experience in such networks, users can offer their reputation rating on a network node, a service or a product. They can also derive evidence from other nodes' ratings or feedback and come up with their own opinion on how much they should trust a node and/or a service. In the recently emerging distributed networks, such as peer-to-peer (P2P) networks, various rating systems based on reputation are designed to achieve different security goals. In all the existing reputation based systems, an individual user or entity will be evaluated and assigned with a reputation value (score) and treated accordingly. This bears some similarities to the real world scenario in which people tend to have trust evaluation on others and react differently.

Reputation systems have also been applied to access control for private information dissemination over other emerging distributed networks, such as mobile social networks (MSN). Nowadays, people share various personal profile information with friends or even strangers in MSNs. Based on the data privacy levels of the profile information, different security levels can be defined. Apparently, user's reputation or trust levels between different users gathered from users' interactions or feedback from other users' interactive experience could serve as a base to realize privacy preserving information sharing and dissemination.

Thus, given a reputation system in place for a distributed network, how to efficiently enable privacy preserving information sharing and dissemination based on the reputation rating is a challenging problem. For instance, a user may wish to share the private information with those with reputation level higher than certain threshold while hiding his information from those with rating lower than the threshold, how can this be done efficiently? This problem is vital in various application scenarios. For instance, a server's multicast/broadcast service might only be allowed to be accessed by those with good reputation during the service delivery. A user in a P2P network may only allow users with good reputation to access its upload files. These issues have been posed in [2], and trust based encryption (TBE) technique has been used to design a solution. In this TBE scheme, each user is evaluated and assigned with a reputation rating value, say, r, where $r \in [0, 1)$ is a rational number equivalent to $r = a/2^{\kappa}, a \in [0, 2^{\kappa})$ and $u = 2^{\kappa}$ is the granularity of reputation rating. In this paper, we assume the lower the user rating value, the more trustworthy this user is. This correspondence could vary according to the concrete application scenario. A trusted authority (TA) in this system is responsible for distributing a private key for each user according to its identity and rating value. The concrete TBE system works as follows. Suppose a message sender Bob wants to communicate with a receiver $Alice$, he will encrypt his message using $Alice$'s identity, a reputation requirement $[0, R]$ and the current communication round t. The encrypted message can be successfully decrypted by $Alice$ if and only if her reputation rating value r falls into

Manuscript received February 29, 2012; revised July 14, 2012.

H. Lin and Y. Fang are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, 32611, USA (e-mail: linhuangsame@gmail.com; fang@ece.ufl.edu).

X. Zhu is with the National Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China (e-mail: xyzhu@mail.xidian.edu.cn).

D. Xing and A. Cao are with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China (e-mail: homer.xing@gmail.com; zfcao@cs.sjtu.edu.cn).

C. Zhang is with the School of Information Science and Technology, University of Science and Technology of China, Anhui, China (e-mail: chizhang@ustc.edu.cn).

This work was partially supported by the U.S. National Science Foundation under grant CNS-0916391 and the National Natural Science Foundation of China under grant No. 61003300. The work of X. Zhu was partially supported by the National Natural Science Foundation of China under grant 61003300, the Fundamental Research Funds for the Central Universities under grant K5051201041, and the China 111 Project under grant B08038. The work of Z. Cao was partially supported by the Key Program of the National Natural Science Foundation of China under grant 61033014, by the National Natural Science Foundation of China under grant 60972034, and by the National Natural Science Foundation of China A3 Foresight Program under grant 61161140320. The work of C. Zhang was partially supported by the National Natural Science Foundation of China under grant 61202140.

A preliminary version of this paper has been presented at IEEE Milcom[1].

Digital Object Identifier 10.1109/JSAC.2013.SUP.0513025

the range requirement $[0, R]$ in communication round t. The basic idea does yield a solution for the privacy preserving information sharing problem we raised before.

In [2], Srivatsa et. al. provide several variations of TBE schemes based on either the symmetric key or public key framework. However, as also pointed out in [2], TA is required to be online in the symmetric key framework in order to distribute fresh private keys to nodes whenever they wish to communicate with each other, inducing a great deal of communication burden to the system. On the other hand, all the three proposed public key TBE schemes [2] are based on identity based encryption (IBE) technique. The first scheme based on basic IBE techniques achieves a $\mathcal{O}(\log(u))$=$\mathcal{O}(\kappa)$ sized private key and $\mathcal{O}(\kappa)$ sized ciphertext. The receiver needs to obtain a fresh private key according to the current reputation rating value from TA in each communication round. Therefore, the communication traffic on the TA side is of size $\mathcal{O}(nT\kappa)$, where n is the number of the system users and T is the maximum communication rounds between any two communication parties in the system. Similar performance analysis results also apply to the second scheme, which is based on the ID-based multi-receiver key encapsulation mechanism (ID-MR-KEM). The third scheme is based on the hierarchical IBE scheme and achieves constant sized ciphertext and much larger private key size, which might be less favorable for most application scenarios. The receiver in both the second and third schemes is required to get his updated private key at each communication round.

As we can observe, the communication overhead on the TA side tends to be large in the existing TBE schemes. Besides, since the user reputation is essentially dynamic, the TA has to stay online most of the time in the current TBE schemes. This contradicts to the distributed nature of distributed collaborative networks.

This paper aims not only to improve the performance of collaborative networks by developing more efficient TBE schemes, but also to develop better tailored TBE schemes for distributed collaborative networks by reducing the interaction overhead between an individual user and the TA. In our first scheme, we propose a generic transformation approach to transforming a recently proposed identity based broadcast encryption (IBBE) scheme to a TBE scheme, in which both the ciphertext size and the private key size are reduced from logarithmic size of the number of users to constant size. It can significantly improve the performance of TBE scheme when static reputation value is considered. We also observe that the dynamic nature of reputation value is imperative to the practical reputation based systems where an individual is solely judged by its reputation. It is highly likely that the obsolete reputation values could be employed by malicious users to gain improper advantage in a collaborative network especially when their reputation drops. However, the existing scheme fails to serve an effective solution when dynamic reputation is considered due to a heavy traffic to the TA, which also further implies frequent user interactions with an online TA.

Our second TBE scheme, which intends to adjust to the dynamic nature of rating values, is based on the recently proposed revocable IBE system [3]. At the beginning of this scheme, the TA distributes a private key to an individual user. Then, the update information will be published periodically by the TA to revoke those whose rating scores have significantly changed during a prefixed time period. The size of published update information is dependent on the number of the revoked users. Thus, instead of obtaining a fresh private key from the TA in each communication round, a receiver can refresh his private key using the public update information without interacting with the TA when his rating score changes. Consequently, the communication overhead for the TA will now depend on the number of the revoked users. The TA can be kept offline and individual users do not need to interact with the TA most of the time when compared with the existing scheme [2].

The rest of the paper is organized as follows. We will first briefly introduce the original TBE scheme. After that, we will show how to improve the performance of the TBE scheme based on identity based broadcast encryption schemes, followed by another improved TBE scheme based on the revocable IBE scheme. Finally, we will conclude this paper in the last section.

II. Related Work

Identity based encryption has been a useful tool in designing secure distributed collaborative networks. In 2008, Srivatsa et al. [2] built a trust management paradigm for securing pan-organizational information flows, addressing the threat of information leakage. The TA here is assumed to be offline when the identity based encryption scheme is adopted. However, the fact that a user has to contact the TA whenever its reputation changes, basically renders an offline TA impossible. Since an offline or transparent TA is of paramount importance in a distributed network, such as P2P network, especially in military scenarios [2], where minimizing communication costs in battery powered mobile P2P networks is critical, how to provide a more flexible and offline TA in this paradigm remains a challenge, which is one of the major motivations of this paper.

Identity based cryptography (IBC) has been adopted as an underlying tool to provide a secure incentive scheme to stimulate users to forward packets in distributed collaborative networks such as the delay tolerant networks [4]–[6]. Most of those schemes assume an offline security manager (OSM), which can basically be considered as a TA in the traditional IBC. IBC has also been used for providing witness anonymity and robust communication under peer-to-peer networks [7]–[9]. An offline TA, i.e., offline group manager (OGM) is assumed in this setting [7], [9]. It was shown by Butler et al. [9] that IBC combined with symmetric cryptographic approach can be employed to design an effective decentralized architecture, which can serve as a practical solution to Sybil attack. Compared with those architectures based on traditional certificate authority-based PKI, it has been pointed out [9] that the IBC based system has the benefit of not requiring complicated certificate management. However, it is also noted that individual users have to obtain their private keys from the TA, which could add expensive communication and computation overhead to the system. Besides, this could lead to a constantly online running TA, which is against the distributive nature of

peer-to-peer systems. This issue is more prominent when it comes down to the case when the identity or key revocation is taken into consideration. It can be even more tricky when the IBC technique is applied to construct a trust based encryption scheme in the trust management paradigm [2]. Neither the existing architecture [9] nor the trust management paradigm [2] provides a good solution to this scenario. Our scheme provides a computation and communication efficient way to revoke reputation keys by systematically incorporating the revocable IBE technique with trust encryption scheme [2]. As a consequence, we can guarantee much less involved TA compared with what in the current trust management paradigm.

III. A Brief Introduction to Original TBE Scheme

In this section, we briefly review the basic idea of the original TBE scheme [2]. Suppose the sender Bob specifies a trust rating (or reputation score) R when encrypting a message for the receiver $Alice$. The decryption is successful if and only if the receiver has a secret key corresponding to a rating value r such that $r \leq R$. The secret keys are required to be dependent on temporal information related to the communication round, identities and rating value, so that keys for one communication round cannot be used for the next round. A secure channel is assumed to exist between the TA and each user to guarantee the secure delivery of user's secret key.

The TBE scheme is constructed on the identity based encryption (IBE) system ([10], [11]), in which there are three parties: the Private Key Generator (PKG), a TA holding a master key mk and responsible for initializing the system, publishing the system parameter pk and distributing a private key sk_{id} for a system user with identification (ID) id by running an extraction algorithm that takes mk and id as input; a message sender (or encryptor), who runs an encryption algorithm taking the message M, the receiver identity id and the public key pk as input to generate a ciphertext $C_{id}(M)$. The message receiver (or decryptor) id' will input the received ciphertext $C_{id}(M)$ and his private key $sk_{id'}$ to the decryption algorithm. The algorithm will output the original message M if and only if $id = id'$ and $\perp$ otherwise.

In the identity based TBE scheme[2], there is an online TA, from whom the receiver can obtain his private key according to his rating value r in the communication round t. The binary tree-based technique for range queries over the encrypted data [12] is adopted to generate the private keys with the desired property. The root of a binary tree with depth d will be labeled as $\top$ (which represents the string of length 0), a left-child at node s will be labeled as $s0$, and a right-child node will be labeled as $s1$ as shown in Fig. 1. Consequently, the leaves are labeled by d-bit strings from left-to-right, starting with $0\cdots0$ and ending with $1\cdots1$. Each binary string $b_0\cdots b_{d-1}$ uniquely corresponds to a real number $r = \sum_{i=0}^{\ell-1} b_i 2^{-(i+1)}$ in the interval $[0, 1)$. In the identity based TBE [2], the user with trust value r of form a/u is associated with an identity set S_r covering the interval $[a, u)$, i.e., a minimal set of subtrees covering the leave nodes of the range a to u. This identity set is denoted as ***rating set*** in the context. In order to generate a ciphertext for a range $[0, R]$ (representing the range requirement R), the sender first finds out all the nodes on the path from the root to the leaf node R, under which the message is encrypted. All the identity nodes on the path constitute the ***range set***. For instance, in Fig. 1 with $r = 1/8$ and $R = 1/4$, the rating set is $\{1, 01, 001\}$ and the range set is $\{\top, 0, 01, 010\}$. Thus, a message M is encrypted under the identity set $\{id||\top||t, id||0||t, id||01||t, id||010||t\}$, where id is the receiver identity, the respective rating value range is $[0, \frac{1}{4}]$, and t is the communication round. In other words, the respective ciphertext $C_{id,[0,R],t}(M)$ is composed of ciphertext $C_{id||\top||t}(M)$, $C_{id||0||t}(M)$, $C_{id||01||t}(M)$ and $C_{id||010||t}(M)$. The private key for a receiver id of the rating value $r = \frac{1}{8}$ will be assigned according to the identity set $\{id||1||t, id||01||t, id||001||t\}$ since the rating set for $\frac{1}{8}$ is $\{1, 01, 001\}$. In other words, this receiver will obtain a private key composed of $sk_{id||1||t}$, $sk_{id||01||t}$ and $sk_{id||001||t}$. The decryption is successful because there is an intersected identity $id||01||t$ between the ***rating set*** and ***range set***. The receiver can simply execute the decryption algorithm on the ciphertext $C_{id||01||t}(M)$ using his private key $sk_{id||01||t}$ to decrypt the message M.

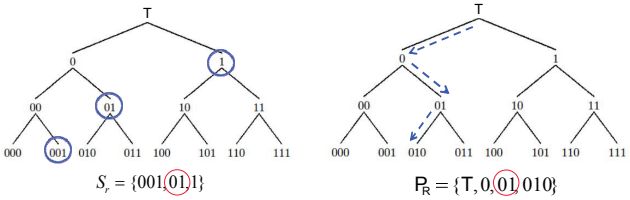


Fig. 1. Basic idea of the TBE in [2]: ***rating set*** r=$\frac{1}{8}$, ***range set*** for $[0, R]$=$[0, \frac{1}{4}]$, u=8.

IV. System Model and Design Goals

Our system model is similar to the original TBE system[2]. We also assume a scenario where a user wishes to share private information with other users over a collaborative distributed network, such as a P2P network. The sender and the receiver could be familiar with each other or they might even be complete strangers. In the first case, the receiver's identity is naturally known to the sender. In the second case, the receiver needs to notify the sender his identity when he asks for information sharing. Each user in the system has a reputation rating value r with a similar form as in the original TBE scheme, also assigned by the TA according to certain metrics. The design of the underlying rating system is out of scope of this paper though important. Just as in the original TBE system, we assume there have already existed a reputation rating system providing a fair and objective rating value for individual users. The TA, equipped with the reputation system, distributes secret keys to users according to their identities and rating values securely (we assume there is a secure channel for online private key distribution). Similar to the original TBE system, a message is encrypted under a reputation range requirement $[0, R]$ and the receiver's identity in our two proposed TBE systems. The receiver is only allowed to successfully decrypt the corresponding ciphertext when the rating value r belongs to the range $[0, R]$.

Our major focus is to improve the performance of the TBE systems, which is determined by the communication overhead and memory storage cost. The communication overhead is proportional to the size of the ciphertext from a sender to a receiver and the communication traffic between a user and the TA, which can also be dependent on the private keys size from TA to the user and the number of communication rounds between them. The memory space cost is mainly dependent on the storage requirement for a receiver, which depends on the size of decryption keys. Our first scheme is to reduce both the communication overhead and the memory space cost through the reduction of the ciphertext size and private key size while the target of our second scheme is to improve the communication overhead through reducing the number of the communication rounds (i.e., reducing the signaling traffic cost due to private key updates).

V. TBE Scheme from the Identity based Broadcast Encryption (IBBE)

In this section, we present our first TBE scheme. We will first provide a brief introduction to the IBBE system to be used, and then discuss how an efficient TBE scheme can be built upon this IBBE scheme.

A. Identity Based Broadcast Encryption (IBBE)

IBBE can be viewed as a generalization of traditional multicast group key management system [13], [14], where each user can join or leave a group dynamically. The traditional system [13], [14] adopts the logical key hierarchy for efficient key assignment. The parameters of these schemes are further improved in subsequent works [15], [16]. These traditional schemes are generally symmetric key based, which means that the TA is required to be online all the time. This contradicts to our requirement that the TA should be offline most of the time.

IBBE is the counterpart of the traditional group key management scheme in the identity based setting, on which the TBE is constructed. It considers the application scenario with n users, where each user has its own identity $\mathbf{ID}_i$. A sender chooses a receiver identity set $S = \{\mathrm{ID}_1, \cdots, \mathrm{ID}_s\}, s \leq n$, and encrypts a message M for this receiver set. If the receiver identity belongs to S, then the decryption would be successful, otherwise, the decryption fails. Even if all the users outside S collude with each other, they will not gain any useful information on the content of the broadcasted message. In IBBE, each user is identified with an arbitrary binary string, which gives us the room to adapt it in the scenario of TBE system.

The current most efficient IBBE scheme (See appendix for the concrete construction)[17] has constant sized private keys. The ciphertext contains only two group elements. The decryption is less efficient, which is dominated by s group element multiplications. Generally speaking, IBBE scheme consists of the following algorithms:

1) **BE-Setup** (λ, m): This algorithm is run by the TA, which takes as input the security parameter λ and $m = max(s)$, the maximal size of the set of receivers for one encryption, and outputs a master secret key **MSK** and a public key **PK**. The TA holds **MSK**, and makes **PK** public.
2) **BE-Extract**(**MSK**, $\mathbf{ID}_i$): The algorithm is also run by the TA. It takes as input the master key **MSK** and a user identity $\mathbf{ID}_i$ and outputs user private key $sk_{\mathbf{ID}_i}$.
3) **BE-Enc**(S, M, **PK**): This algorithm is run by the sender, which takes as input the public key **PK**, a message M and a set of included identities $S = \{\mathbf{ID}_1, \cdots, \mathbf{ID}_s\}$ with $s \leq m$, and outputs the ciphertext $C_S(M)$.
4) **BE-Dec**(S, $\mathbf{ID}_j$, $sk_{\mathbf{ID}_j}$, $C_S(M)$, **PK**): This algorithm is run by the receiver. It takes as input a subset $S = \{\mathbf{ID}_1, \cdots, \mathbf{ID}_s\}$ (with $s \leq m$), an identity $\mathbf{ID}_j$ and the corresponding private key $sk_{\mathbf{ID}_j}$, a ciphertext $C_S(M)$, and the public key **PK**. If $\mathbf{ID}_j \in S$, the algorithm outputs the message M. It will output $\perp$ otherwise.

B. TBE Scheme from IBBE Scheme: Simple Case

The original TBE scheme in [2] consists of four algorithms, **Setup**, **KeyDer**, **Encrypt**, and **Decrypt**. We can apply the IBBE scheme discussed in the previous subsection to develop our TBE scheme. It can be constructed in the following steps. At the beginning of the system operation, the **Setup** algorithm runs **BE-Setup** algorithm as its subroutine. **Setup** algorithm takes as input a security parameter λ and outputs system parameters, which include the master key **MSK** and the public key **PK** from the **BE-Setup** algorithm, and also the specifications of message, ciphertext, identity and private key memory space, and a granularity parameter $u = 2^\kappa$. The TA will run **KeyDer** algorithm to distribute private keys to a receiver *id*. This algorithm will take **BE-Extract**(**MSK**, $\mathbf{ID}_i$) as its sub-routine, where $\mathbf{ID}_i$=$id||ru||t$. r is the rating value of *id* at the communication round t. The output of **BE-Extract**(**MSK**, $id||ru||t$) is the private key $sk_{id||ru||t}$ for receiver *id*. **Encrypt** will run **BE-Enc**(S, **PK**) as its sub-routine. The input of **Encrypt** is a pair (id, R), system parameters, and a message M, which are interpreted as the following input to algorithm **BE-Enc**: the trust value range requirement $[0, R]$ and the receiver identity id will be synthetically represented as the following receiver set S=$\{id||0||t$, $id||u||t$, $id||2u||t$, $\cdots$, $id||Ru||t\}$. The output of **BE-Enc** is the respective ciphertext $C_{id,[0,R],t}(M)$=$C_S(M)$. The receiver *id* with a rating value $r \leq R$ can run the IBBE decryption algorithm **BE-Dec**(S, *id*, $sk_{id||ru||t}$, $C_{id,[0,R],t}(M)$, PK) to obtain message M. The decryption will be successful because the receiver identity $id||ru||t$ belongs to the receiver set S if $r \leq R$.

Complexity analysis: Since we use a generic method to transform an IBBE scheme into a TBE scheme, we can develop any efficient TBE scheme from the current most efficient IBBE scheme [17] (see Appendix). Moreover, the complexity for our TBE scheme can be analyzed from that of the underlying IBBE scheme. The private key contains only one group element, which is less than $\mathcal{O}(\log(u))$=$\mathcal{O}(\kappa)$ group elements in the original TBE. The communication cost is determined by the size of the ciphertext, which contains three group elements while the ciphertext in the original scheme also contains κ group elements.

Although IBBE is a cryptographic concept close to multi-receiver key encapsulation mechanism (MR-KEM) adopted in

the original TBE scheme [2], the different ways these two cryptographic tools are utilized results in significant performance gain in our TBE schemes. One of the major differences between our TBE scheme and the original ones is that we remove the binary tree framework from our construction. The minimal private key size of the original TBE scheme should be $\mathcal{O}(\kappa)$ due to the binary tree structure they used. However, the private key size could possibly reach constant only when we do not use binary tree method in the TBE scheme. Besides, although MR-KEM mechanism also considers the multi-receiver scenario, each receiver $\mathbf{ID}_i$ is still treated independently in the original TBE construction in the sense that an encapsulation C_i is generated for each $\mathbf{ID}_i$, and therefore the lower bound of ciphertext size for the binary tree structure based TBE scheme should be $\mathcal{O}(\kappa)$, which is exactly the ciphertext size of the original TBE scheme[2]. Apparently, the proposed IBBE based approach not only reaches the optimal memory cost for the constant sized private keys, but also reaches the optimal communication cost due to the constant sized ciphertext. Aside from the removal of binary tree structure, the reason for this performance gain can also be attributed to that we treat the receiver range set as a whole and the ciphertext of the underlying IBBE scheme is generated according to this range set.

C. Generalized TBE

We can also consider a more general case where the message is encrypted under a collection of ℓ reputation ranges $S = \bigcup_{i=1}^{\ell}[L_i, R_i]$ rather than a single range $[0, R]$, where L_i and R_i are the lower and upper bounds of $i-$th reputation range. This general case is useful because a sender might wish to send a message to a group of users falling into different reputation categories without even considering who the recipients really are. For instance, a sender with a rating value $\frac{3}{4}$ might want anyone who has a reputation close to his or has a very good reputation to decrypt his ciphertext. In reality, those with similar reputation could correspond to his close friends and those with good reputation might denote the strangers who he is willing to trust with his message. In this case, the range set might be $[\frac{1}{2}, 1] \bigcup [0, \frac{1}{4}]$. This generalized TBE scheme could be realized in a similar way compared with the basic construction because we only need to include more range sets in the receiver set S to represent the additional reputation range while the receiver identity id should be removed from S[1]. The rest algorithms work similarly as for the simple case except now the consistency condition is changed to be that any receiver with the rating value falling into either one of these reputation ranges can successfully decrypt the ciphertext.

Complexity analysis: The reduction of the communication cost is even more noticeable in this case because both of the ciphertext size and private key size of our generalized scheme remain constant[2]. The binary tree method introduced in Sec.III cannot directly represent multiple ranges since the nodes on the path from the root to the leaf node could only correspond to one single reputation range. If the orthogonal representation method is adopted, i.e., using a minimal node set covering multiple leaf nodes to represent multiple ranges and the nodes on the path from the root to the leaf node to represent receiver private key, then the ciphertext size of the original TBE scheme will increase to $\mathcal{O}(\ell\kappa)$, which is far less favorable compared with our constant size ciphertext.

Security analysis: Given the fact that we directly apply the IBBE scheme to the TBE system, the security for our TBE scheme is implied by that of the underlying IBBE scheme, which can be shown to be selectively chosen ciphertext attack secure.

Our TBE scheme can reach the same security level as that of the underlying IBBE scheme. Hence, the TBE scheme will be adaptively chosen ciphertext attack secure if the underlying IBBE scheme is replaced with the adaptively secure IBBE scheme [18]. In the adaptive model, the adversary does not need to submit the target identity at the beginning of the simulation in the proof. However, the efficiency of our TBE scheme based on the adaptively secure IBBE scheme [18] will not be that favorable compared with that based on selectively secure one [17] although the security level is indeed enhanced.

VI. TBE Scheme from R-IBE Scheme

In the above section, we adopt the IBBE scheme as the underlying tool to reduce the memory space and communication overhead of our TBE scheme in terms of the ciphertext size and the private key size. While in this section, the revocable identity based encryption (R-IBE) [3] will serve as an underlying tool to improve the communication overhead of the TBE system by reducing the communication traffic between users and the TA.

In what follows, we first provide a brief introduction to the R-IBE system. We then show how a direct application of R-IBE to design our TBE system can significantly reduce the communication rounds between users and the TA.

A. A Brief Introduction to the R-IBE

Revocable IBE scheme was proposed as a solution to realize efficient identity revocation in the IBE system. As users' private keys tend to be either stolen or expired in practice, a revocable IBE scheme can prevent these "corrupted" and thus illegal private keys from being employed to decrypt ciphertext. The scheme divides the system life time into time periods. At the beginning, each individual user will receive a private key from the TA for his identity. The sender encrypts a message under the receiver's identity id and the current time period t. In order to successfully decrypt the ciphertext, the receiver id is required to first derive the decryption key for the current time period t. Notice that the decryption key and the private key are different concepts in an R-IBE system. If one's identity is revoked in a certain time period, a decryption key cannot be derived from his private key for this time period. At the beginning of each time period, the TA publishes the update information only allowing the unrevoked users to update their private keys to derive the decryption keys corresponding to

[1]This is because we only focus on the reputation of the users rather their identities.

[2]We neglect the comparison of communication cost for the delivery of receiver set S contained in the ciphertext because both of our proposed schemes and the original TBE scheme needs to transmit the same receiver set.

the current time period. In this regard, the revoked users (or identities) are deprived of their decryption ability.

The R-IBE scheme is usually composed of the following seven algorithms:

1) **R-Setup**$(1^\lambda, n)$: The TA runs this algorithm, taking a security parameter λ and number n of the system users as input. It also publishes the public key pk and returns a master key msk and an initially empty revocation list rl for the TA.
2) **R-PriKeyGen**(msk, **id**): The TA also runs this algorithm, which takes as inputs an arbitrary identity string **id** and the master key msk, and outputs the user private key $sk_{\mathbf{id}}$ for the user with identity **id**.
3) **R-KeyUpdate**(pk, msk, t, rl): The TA runs this algorithm to publish the update information for the time period t. This algorithm takes as input the system parameters public key pk, master key msk, key update time t and revocation list rl, and then outputs the key update information ku_t. Here, the revocation list rl specifies the revoked user identity **id** and other related information. Although the key update information ku_t is publicly accessible, they are useless for the revoked identities.
4) **R-DecryKeyGen**$(sk_{\mathbf{id}}, ku_t)$: This decryption key generation algorithm is run by the unrevoked users each time after the TA publishes the update information ku_t. The unrevoked users run this algorithm by taking as the input the user private key $sk_{\mathbf{id}}$ and the key update information ku_t, and then outputs the decryption key $dk_{\mathbf{id},t}$. It outputs $\perp$ if a revoked user runs this algorithm.
5) **R-Enc**(pk, **id**$, t, M$): The encryption algorithm is run by a sender. It takes as the input the public key pk, the receiver identity **id**, the current time period t and the message M, and outputs the ciphertext $C_{\mathbf{id},t}(M)$.
6) **R-Dec**$(dk_{\mathbf{id},t}, C_{\mathbf{id},t}(M))$: The receiver runs this decryption algorithm by inputting the decryption key $dk_{\mathbf{id},t}$ and the ciphertext $C_{\mathbf{id},t}(M)$, and outputs a message M or a special symbol $\perp$. The correctness of the decryption is defined as: if the receiver identity **id** is unrevoked at the time period t, then the decryption algorithm will output the message M, and $\perp$ otherwise because the respective decryption key $dk_{\mathbf{id},t}$ cannot be derived by the revoked user.
7) **R-Revocation**: The revocation algorithm is run by the TA, which inputs the identity to be revoked **id** and the revocation list rl to the algorithm, which outputs an updated revocation list rl.

The basic idea of scheme [3] presented by Boldyreva et. al. is to combine the binary tree structure and the fuzzy identity based encryption. The R-IBE scheme (see Fig. 2) works as follows: for a system with n users, a binary tree with at least n leaf nodes is generated by the TA. Each user corresponds to one unique leaf node. The user private key is assigned according to a node set composed of all the nodes on the path from the root to its own leaf node. The update information is generated according to the minimal node set covering the unrevoked users, which is the reason why the update information is useless to those revoked users. Check the left sub-figure in Fig. 2, the key update information ku_t is generated corresponding to the big circle nodes covering the path nodes contained in the private key node set for the unrevoked users only, i.e. $\{id_2, id_3, id_4\}$. It is also observed that ku_t does not cover any of the path nodes in the private key node set for id_1, and hence is useless to id_1. The private key size is $\mathcal{O}(\log n)$ and the update information size is $\mathcal{O}(v \log(n/v))$, where v is the number of the revoked users. The individual decryption key size remains constant even after the key is updated. The concrete construction can be found in the appendix .

B. TBE Scheme from R-IBE

As a user's trust rating value is fluctuating with time, or a node, so the respective trust based private key, is subject to compromise, the TBE system should have a mechanism to revoke a user's reputation key whenever his reputation changes. Although a game theoretic mechanism [2] was proposed to ensure a rational user will honestly report his current rating value to the TA, this still cannot deter the irrational users from refusing to update their reputation keys and exploiting the obsolete reputation keys to act maliciously. Besides, reputation key revocation would be an even greater challenge when the trust rating mechanism depends on the collective opinions. This is the first reason why the reputation revocation approach has to be enforced in a TBE system.

In order to avoid the abuse of obsolete reputation based private key, both the encryption and decryption of the original TBE scheme is dependent on the communication round t. Therefore, a secure channel between a receiver and the TA must be established in order to guarantee the secure delivery of the fresh decryption key for every communication round. Whenever a receiver wishes to communicate with another node or access shared information encrypted with certain trust rating level, the receiver has to obtain a fresh private key from the TA, resulting in huge traffic burden to the TA (linearly dependent on the numbers of users and the communication rounds between each communication pair). As a result, the workload at the receiver side would also be heavy since each time when a receiver obtains the encrypted private decryption keys from the TA, they must decrypt the received message for the updated decryption keys before they could even proceed to run the TBE decryption algorithm.

Our TBE scheme adopts the revocable IBE as the underlying tool to mitigate the traffic between nodes and the TA for the private key delivery. In the proposed TBE with reputation revocation (TBE-RR) scheme, the system time is also divided into fixed time periods just as in the underlying R-IBE system. The length of time period is a system parameter, which can be dependent on the statistics for the dynamic range of the user reputation gathered from the reputation systems[2]. At the beginning of the TBE-RR system, each user obtains a trust based private key from the TA. Compared with the original TBE scheme, a message will not only be encrypted under the receiver's identity and the range requirement, but also the current time period. In one time period, two communication parties might have gone through several communication rounds and the receiver can use his decryption key for the

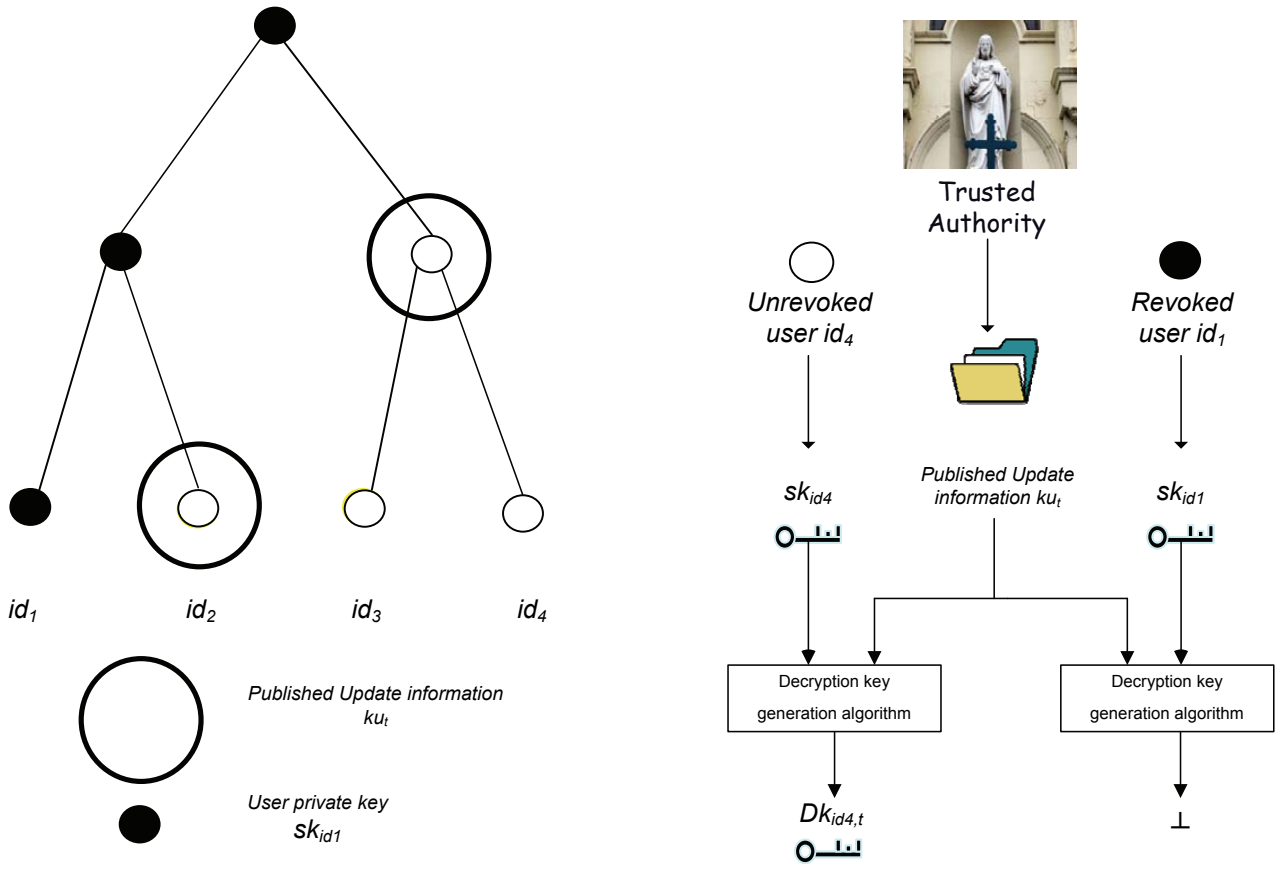


Fig. 2. Basic idea of an R-IBE.

current time period to decrypt all the received ciphertexts. The decryption key is also considered to be a different concept from the private key as in the revocable IBE scheme. A user with a valid private key might not be able to derive a decryption key for a certain time period unless he is unrevoked in this very time period. The TA periodically publishes update information solely for the unrevoked users to generate the updated decryption keys and deliver the updated private keys for the revoked users whenever necessary (for instance, when the delivery is requested by the revoked users) such that the cost of distributing the updated private keys (in terms of both communications and computation overhead) would be reduced from $\mathcal{O}(n)$ to $\mathcal{O}(v)$, where v denotes the number of the revoked users.

Technically, the proposed TBE-RR scheme is a combination of the R-IBE scheme and the original TBE scheme. At the initiation of the TBE-RR system, the TA runs **R-Setup** algorithm of the R-IBE scheme[3] and constructs a binary tree with at least N leaf nodes, where $N = n \times \kappa$ and n is the number of system users. κ and n are both assumed to be the power of 2. According to Sec.III, each user's rating value is represented by a rating node set composed of at most κ identities. Consequently, the binary tree covers all the rating sets S_{r_i} for each system user $id_i, i \in [1, n]$. The TA controls the system public key pk and the master key msk, and reserves the memory space for messages, identity, time period and the empty revocation list rl after running **R-Setup** algorithm. Each user will be assigned with a private key composed of all the identity based private keys for the respective trust rating set through running the **R-PriKeyGen**(msk, **id**) algorithm on each identity in the rating set. For example, for a system with four users id_1, id_2, id_3, id_4 with the rating values $\frac{1}{2}$, $\frac{1}{8}$, $\frac{1}{4}$, and $\frac{1}{4}$, respectively, the TA first constructs a binary tree covering all the rating set as shown in Fig. 3. To assign the private key for user id_2 with a rating value $\frac{1}{8}$, the TA runs **R-PriKeyGen**(msk, **id**) on each identity id in the rating set $\{id_2||1, id_2||01, id_2||001\}$ to output $sk_{id_2||1}$, $sk_{id_2||01}$, and $sk_{id_2||001}$, which constitute the user private key $sk_{id_2||r=\frac{1}{8}}$. In other words, the TA distributes each identity based private key according to the private key node set for all the leaf nodes. The original TBE system functions in a different manner because there is no temporal information contained in the original user private key as done in our TBE-RR scheme. When the sender encrypts a message for receiver id_2 with a reputation range requirement $[0, \frac{1}{4}]$ in time period t, the message will be encrypted under the range set $\{id_2||\top, id_2||0, id_2||01, id_2||010\}$ and time period t. Therefore, the sender runs the encryption algorithm in the revocable IBE scheme **R-Enc**(pk, id, t, M) on each identity id in the range set $\{id_2||\top, id_2||0, id_2||01, id_2||010\}$ to generate the ciphertext $\{C_{id_2||\top,t}(M), C_{id_2||0,t}(M), C_{id_2||01,t}(M), C_{id_2||010,t}(M)\}$, which constitute the final ciphertext $C_{id_2,[0,R],t}(M)$.

[3]Notice that all the algorithms containing a prefix **R-** in this section are referred to those in the R-IBE system introduced in Sec. VI-A

The update information ku_t is published by running the update algorithm **R-KeyUpdate**(pk, msk, t, rl). The update information can only be used by those with unrevoked reputation values. In other words, the receiver id_2 can successfully derive the decryption key in time period t only when its rating value is unrevoked[4]. The receiver id_2 runs **R-DecryKeyGen** algorithm, taking $sk_{id_2||r}$ and key update information ku_t as the input to output the respective decryption key $dk_{id_2||r,t}$. The decryption key is composed of all the decryption keys corresponding to its rating set, i.e., $dk_{id_2||1,t}$, $dk_{id_2||01,t}$, $dk_{id_2||001,t}$. Therefore, the receiver can execute the **R-Dec** algorithm, taking the ciphertext $C_{id_2||01,t}(M)$ (since $id_2||01$ is the intersection identity between the rating set and range set) and the respective decryption key $dk_{id_2||01,t}$ as the input in order to decrypt the respective message M.

Complexity analysis: The proposed scheme results in a user private key of size $\mathcal{O}(\log(\kappa N))$. However, the receiver, especially the one with constant reputation over time, is not required to communicate with the TA. The only thing to be done is to check out the published update information in order to derive his fresh decryption key for each time period. As a result, the communication traffic between users and the TA is significantly reduced. The ciphertext only contains an extra group element compared with the original TBE scheme if randomness reuse technique is used in the encryption algorithm [19]. If the proposed TBE-RR scheme employs the same underlying IBE technique as in the R-IBE system [3], then the sender in our TBE-RR system only needs to complete an additional modular exponential while generating the ciphertext compared with that of the original TBE system. The workload of the TA will mainly be determined by the task of distributing the update information and delivering the private keys for the revoked users. The computation and communication costs of both tasks depend on the number of the revoked users.

Security analysis: The security of our TBE-RR scheme can be reduced to the security of the underlying R-IBE scheme given the fact that the construction is a combination of the R-IBE system and the basic TBE scheme. The TBE scheme can be viewed as an IBE system where an individual user's identity is the concatenation of the original individual identity and its respective reputation value. Therefore, our proposed TBE-RR system can be viewed as a revocable IBE system where the individual identity is the concatenation. The R-IBE system [3] we adopt can be proven selective ID chosen ciphertext secure, therefore our proposed TBE-RR system can reach the same security level.

VII. Performance Evaluation

In this section, we conduct a more complete performance evaluation on our proposed schemes. In Table I, we present the comparison of the communication overhead and memory cost of our proposed schemes with that of the original TBE scheme. Let T denote the maximum communication rounds between two communication parties in the system, and τ denote the number of time periods which the lifetime of a TBE system is divided into. As we can observe from the table, our first scheme does improve the performance when the static reputation is considered. In our second proposed scheme, those with a steady reputation (corresponding to unrevoked users) will not generate traffic, which would be inevitable in the original TBE scheme, implying that these users are free from the decryption task after receiving the encryption of fresh private keys from the TA each communication round (since encryption is the only way to guarantee the secure delivery of those private keys), which would significantly reduce communication and computation overheads. The TA only needs to periodically publish some update information and deliver private keys for those whose reputations have changed if requested. Comparably, the TA in the original system has to deliver a fresh private key for each receiver in each communication round, which means it is forced to be online most of the time. Since one time period might contain many communication rounds between two communication parties, it is fair to say that the workload at the TA is also significantly reduced, which means the TA can sometimes be kept offline.

There is a factor of v in the workload of TA in our second scheme, which means the efficiency gain of the second scheme is more remarkable for those TBE systems where the reputations of most users remains relatively stable over time in terms of reputation dynamics. However, the second system might exhibit less superiority when the number of the revoked users is close to n because the TA will have to publish update information linearly dependent on the number of system users.

We also implement our proposed TBE-RR system and the existing TBE scheme[2] in C. Here, we adopt the Pairing-Based Cryptography (PBC) Library as the underlying tool. The curve we have used for our proposed scheme is type D. The curve of such type has the form of $y^2 = x^3 + ax + b$. We use MNT method [20] to generate this curve. The order of the curve is around 158 bits, as is $\mathbb{F}_q$, the base field. Our choice of parameters results in 79-bit brute force and 953-bit finite field MOV security levels [21]. We adopt the identity based encryption scheme proposed by Waters [22] as the underlying tool for implementing the original TBE scheme. The revocable IBE system proposed by Boldyreva et al. [3] is employed to implement our proposed TBE-RR scheme. We note that the revocable IBE system we adopt can be viewed as a generalization based on Waters' IBE scheme. They are both proven to be secure under the standard decisional bilinear Diffie-Hellman assumption, and thus have the same security level. We choose an identity of length 158 bits in both systems. For our experiments, we use a desktop machine with an Intel Celeron 530 1.73GHZ CPU and 1GB of RAM, running Linux/Ubuntu 6.10. All the timing reported below are averaged over 100 randomized runs. We assume all the individual users are communication active, which means each one at least receives one ciphertext from another user at least once in one time period. This is a reasonable assumption assuming the time period is properly set. For the ease of simulation, we show the performance comparison when there is only one communication round for each individual user in one time period. We note that our performance gain should be more remarkable if more individual communication rounds

[4]If the rating value r of this receiver is revoked in time period t', then the update information will only cover the leaf nodes but the rating set for $id_2||r$, i.e., all the transparent nodes.

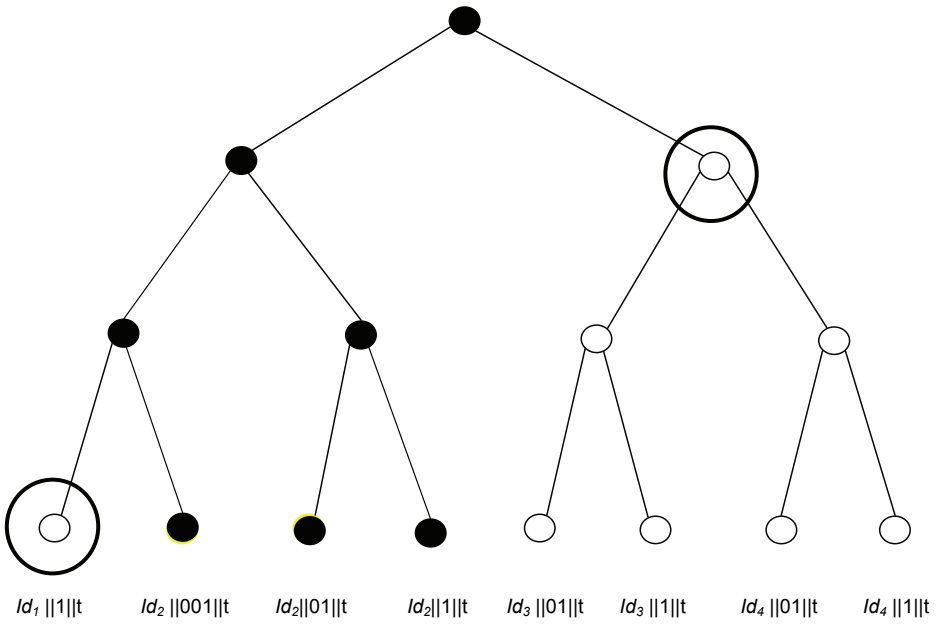


Fig. 3. Basic idea of our TBE-RR scheme.

TABLE I
EFFICIENCY COMPARISON

	original TBE	IBBE based-	R-IBE based-
Ciphertext size	$\mathcal{O}(\kappa)$	$\mathcal{O}(1)$	$\mathcal{O}(\kappa)$
Private Keys	$\mathcal{O}(\kappa)$	$\mathcal{O}(1)$	$\mathcal{O}(\log(\kappa n))$
Communication rounds (TA and unrevoked receiver) (After initialization)	$\mathcal{O}(T)$	$\mathcal{O}(T)$	none
Communication rounds (TA and revoked receiver) (After initialization)	$\mathcal{O}(T)$	$\mathcal{O}(T)$	$\mathcal{O}(\tau)$
workload of TA	$\mathcal{O}(nT\kappa)$	$\mathcal{O}(nT)$	$\mathcal{O}(\tau v \log(\kappa n))$

in one period are considered since the workload of both TA and individual users in the original scheme is dependent on the individual communication rounds while the performance of our proposed schemes is not.

We compare the performance of two systems under different choices of the number of system users n, the granularity of the reputation κ and the number of revoked users v. An individual user is assigned with a random reputation value in $[0, 2^{\kappa}]$, and we also choose a uniformly random revoked index set consisting of v revoked users. Fig. 4–Fig. 7 show the communication overhead and storage cost of an individual user in the two schemes under different parameter settings. The simulation results validate our performance analysis. Our IBBE based improvement significantly improves both the communication overhead and the storage requirement when the reputation value is static. We can also see that the revocable IBE based TBE scheme indeed reduces the communication overhead when the reputation value is dynamic. The private key size of revocable IBE based scheme is slightly larger than that in the IBBE based scheme and the original scheme. Hence, the revocable IBE based scheme is to find a tradeoff between the two performance parameters. However, the interaction times between an individual user and the TA are linearly proportional to the communication overhead. Hence, it is fair to say that the TA is least involved in the last improvement scheme.

VIII. CONCLUSION

In this paper, we have proposed to use two cryptographic techniques, the identity based broadcast encryption (IBBE) and revocable identity based encryption (R-IBE), to develop two novel trust based encryption (TBE) schemes used in information sharing and dissemination to significantly improve the efficiency in terms of memory storage requirements and communication overheads. We have shown that both TBE schemes perform much better than the previously known schemes and can be applied to peer-to-peer networks with reputation based mechanisms for information sharing and dissemination. One potential future research is to investigate how to employ the combination of IBBE and R-IBE [23] to further improve the TBE scheme.

IX. APPENDIX

A. IBBE[17]

The detailed procedure of IBBE is described as follows:

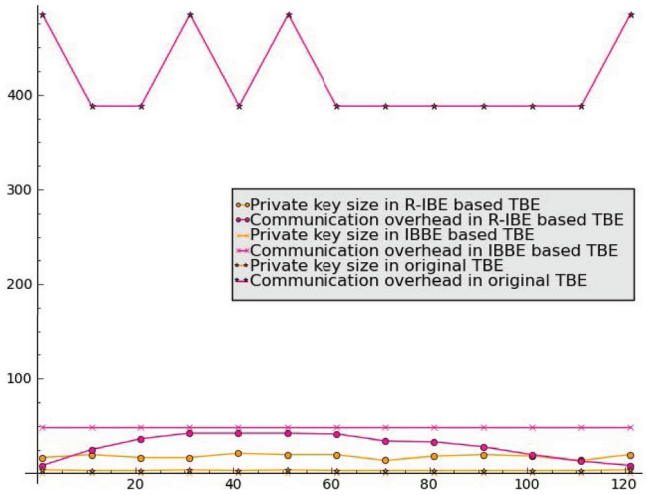


Fig. 4. Performance comparison when $\kappa = 4$ and $n = 128$.

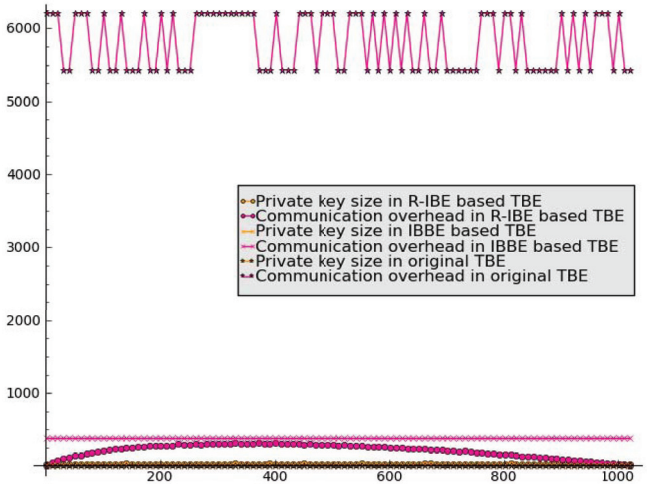


Fig. 5. Performance comparison when $\kappa = 4$ and $n = 1024$.

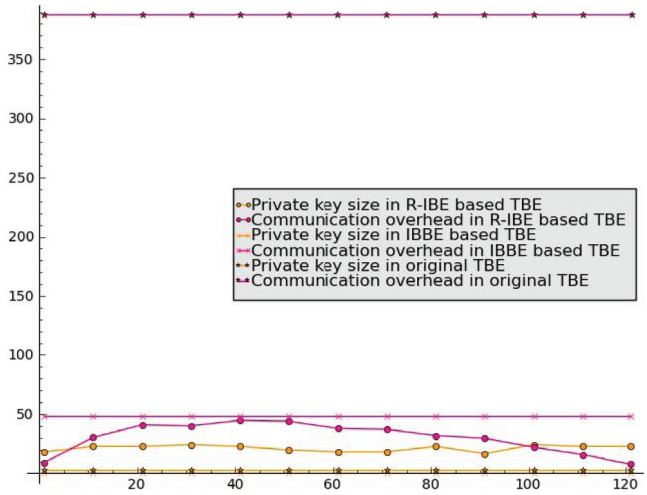


Fig. 6. Performance comparison when $\kappa = 5$ and $n = 128$.

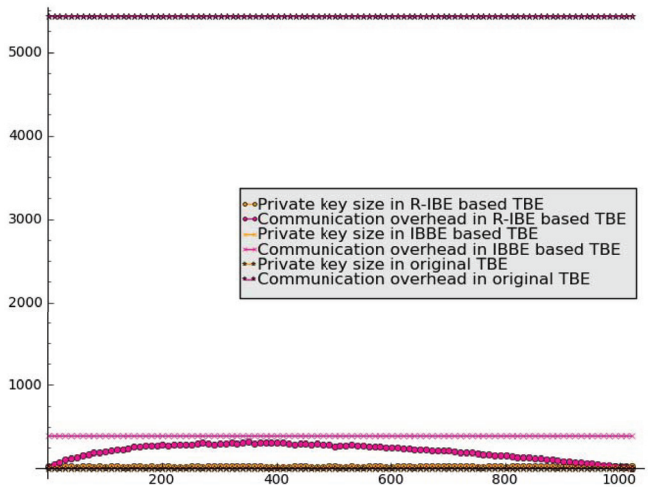


Fig. 7. Performance comparison when $\kappa = 5$ and $n = 1024$.

1) **Setup**(λ, M): Given the security parameter λ and an integer M, a bilinear map group system $\mathcal{B}$=(p, $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, $\hat{e}(\cdot,\cdot)$) is constructed such that $|p| = \lambda$. Also, two generators $g \in \mathbb{G}_1$ and $h \in \mathbb{G}_2$ are randomly selected as well as a secret value $\gamma \in \mathbb{Z}_p^\star$. Choose a cryptographic hash function $\mathcal{H} : \{0,1\}^\star \rightarrow \mathbb{Z}_p^\star$. The security analysis will view $\mathcal{H}$ as a random oracle. $\mathcal{B}$ and $\mathcal{H}$ constitute system public parameters. The master secret key is defined as MSK=(g, γ). The public key is PK=$(\omega, v, h, h^\gamma, \cdots, g^{\gamma^m})$ where $\omega = g^\gamma$, and $v = \hat{e}(g, h)$.
2) **Extract**(MSK, ID): Given MSK=(g, γ) and the identity ID, it outputs sk_{ID}=$g^{\frac{1}{\gamma+\mathcal{H}(\mathrm{ID})}}$.
3) **Encrypt**(S, PK, M). Assume for notational simplicity that S=$\{\mathrm{ID}_j\}_{j=1}^s$ with $s \leq m$. Given PK=$(\omega, v, h, h^\gamma, \cdots, h^{\gamma^m})$, and an message M, the broadcaster randomly picks $k \leftarrow \mathbb{Z}_p^\star$ and computes Hdr=(C_1, C_2) and C where C_1=ω^{-k}, C_2=$h^{k\cdot\prod_{i=1}^s(\gamma+\mathcal{H}(\mathrm{ID}_i))}$, $C = v^k \cdot M$. It outputs (Hdr, C).
4) **Decrypt**(S, ID_i, $\mathrm{sk}_{\mathrm{ID}_i}$, Hdr, PK): In order to retrieve the message encryption key K encapsulated in the header Hdr=(C_1, C_2), the user with the identity ID_i and the corresponding private key $\mathrm{sk}_{\mathrm{ID}_i}$=$g^{\frac{1}{\gamma+\mathcal{H}(\mathrm{ID}_i)}}$ (with $\mathrm{ID}_i \in S$) computes

$$K = \left(\hat{e}(C_1, h^{p_{i,S}(\gamma)}) \cdot \hat{e}(\mathrm{sk}_{\mathrm{ID}_i}, C_2)\right)^{\frac{1}{\prod_{j=1,j\neq i}^s \mathcal{H}(\mathrm{ID}_j)}}$$

$$p_{i,S}(\gamma) = \frac{1}{\gamma} \cdot \left(\prod_{j=1,j\neq i}^{s} (\gamma + \mathcal{H}(\mathrm{ID}_j)) - \prod_{j=1,j\neq i}^{s} (\mathcal{H}(\mathrm{ID}_j)) \right)$$

$$\begin{aligned} K' &:= \hat{e}(C_1, h^{p_{i,S}(\gamma)}) \cdot \hat{e}(C_2, \mathrm{sk}_{\mathrm{ID}_i}) \\ &= \hat{e}(g^{-k\gamma}, h^{p_{i,S}(\gamma)}) \cdot \hat{e}\left(g^{\frac{1}{\gamma+\mathcal{H}(ID_i)}}, h^{k\cdot\prod_{j=1}^{s}(\gamma+\mathcal{H}(\mathrm{ID}_j))}\right) \\ &= \hat{e}(g,h)^{-k\cdot\left(\prod_{j=1,j\neq i}^s(\gamma+\mathcal{H}(ID_j)) - \prod_{j=1,j\neq i}^s \mathcal{H}(ID_j)\right)} \\ &\cdot \hat{e}(g,h)^{k\cdot\prod_{j=1,j\neq i}^s(\gamma+\mathcal{H}(ID_j))} \\ &= \hat{e}(g,h)^{k\cdot\prod_{j=1,j\neq i}^s \mathcal{H}(ID_j)} \\ &= K^{\prod_{j=1,j\neq i}^s \mathcal{H}(ID_j)} \end{aligned}$$

B. R-IBE[3]

The detailed procedure of R-IBE is given below. Let $\mathcal{G}$ be a prime order bilinear group generator. Let J be $\{1, 2, 3\}$.

1) **R-Setup**$(1^\lambda, n)$: $(\hat{\mathbb{G}},\ p,\ g) \leftarrow \mathcal{G}(1^\lambda)$; $a \leftarrow \mathbb{Z}_p$; $g_1 \leftarrow g^a$; $g_2,\ h_1,\ h_2,\ h_3 \leftarrow \mathbb{G}$. Let rl be an empty set and T be a binary tree with at least n leaf nodes. Return pk=$(g, g_1, g_2, h_1, h_2, h_3)$, $m_k = a$; rl, st=T.
2) **R-PriKeyGen**$(pk,\ mk,\ \omega,\ st)$: Parse pk as $(g,\ g_1,\ g_2,\ h_1,\ h_2,\ h_3)$, mk as a, st as T. Pick an unassigned leaf node v from T and store ω in that node.
$\forall x \in \text{Path}(v)$ if a_x is undefined, then $a_x \leftarrow \mathbb{Z}_p$, store a_x in node x,

$$r_x \leftarrow \mathbb{Z}_p; D_x \leftarrow g_2^{a_x\omega+a} H_{g_2,\text{J},h_1,h_2,h_3}(\omega)^{r_x};$$
$$d_x \leftarrow g^{r_x}.$$

Return $sk_\omega = \{(x, D_x, d_x)\}_{x\in\text{Path(v)}}, st$.
Note that a_x above fixes first-degree polynomial $q_x(y) = a_x y + a$ corresponding to node x. The algorithm computes the $\omega-$ components of the decryption key using the polynomials of all the nodes on the path from leaf node corresponding to ω to the root node.
3) **R-KeyUpdate**$(pk,\ mk,\ t,\ rl,\ st)$: Parse pk as $(g,\ g_1,\ g_2,\ h_1,\ h_2,\ h_3)$, mk as a, st as T.
$\forall x \in KuNodes(\text{T}, rl, t)$

$$r_x \leftarrow \mathbb{Z}_p; E_x \leftarrow g_2^{a_x t+a} H_{g_2,\text{J},h_1,h_2,h_3}(t)^{r_x};$$
$$e_x \leftarrow g^{r_x}.$$

Return $ku_t = \{(x, E_x, e_x)\}_{x\in KuNodes(\text{T},rl,t)}$.
The algorithm first finds a minimal set of nodes which contains an ancestor (or, the node itself) of all the non-revoked nodes. Then it computes the $t-$ component of the decryption key using the polynomials of all the nodes in that set.
4) **R-DecryKeyGen**(sk_ω, ku_t): Parse sk_ω as $\{(i, D_i, d_i)\}_{i\in l}$, ku_t as $\{j, E_j, e_j\}_{j\in\text{J}}$ for some set nodes I, J.
$\forall (i, D_i, d_i) \in sk_\omega$, $(j, E_j, e_j) \in ku_t$. If $\exists (i, j)$ s.t. $i = j$ then $dk_{\omega,t} \leftarrow (D_i, E_j, d_i, e_j)$. Else (if sk_ω and ku_t do not have any node in common) then $dk_{\omega,t} \leftarrow \perp$.
Return $dk_{\omega,t}$.
// Above we can drop the subscripts i, j since they are equal, i.e., $dk_{\omega,t}$=(D, E, d, e).
The algorithm finds components of sk_ω and ku_t which were computed on the same polynomial.
5) **R-Enc**$(pk,\ \omega, t, M)$:
Parse pk as $(g, g_1, g_2, h_1, h_2, h_3)$.

$$z \leftarrow Z_p; c_1 \leftarrow M \cdot \hat{e}(g_1, g_2)^z; c_2 \leftarrow g^z;$$
$$c_\omega \leftarrow H_{g_2,\text{J},h_1,h_2,h_3}(\omega)^z; c_t \leftarrow H_{g_2,\text{J},h_1,h_2,h_3}(t)^z$$
$$c = (\omega, t, c_\omega, c_t, c_1, c_2).$$

The encryption algorithm is essentially the same as that of Fuzzy IBE.
6) **R-Dec**$(dk_{\omega,t}, c)$: Parse $dk_{\omega,t}$ as (D, E, d, e), c as $(\omega, t, c_\omega, c_t, c_1, c_2)$.

$$M \leftarrow c_1 \cdot \left(\frac{\hat{e}(d, c_\omega)}{\hat{e}(D, c_2)}\right)^{\frac{t}{t-\omega}} \left(\frac{\hat{e}(e, c_t)}{\hat{e}(E, c_2)}\right)^{\frac{\omega}{\omega-t}}$$

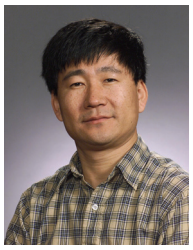
Return M.
The decryption algorithm is essentially the same as that of the Fuzzy IBE.
7) **Revocation** $R(\omega, t, rl, st)$: For all nodes v associated with identity ω add (v, t) to rl. Return rl.

REFERENCES

[1] H. Lin, X. Zhu, C. Zhang, Y. Fang, and Z. Cao, "Efficient trust based information sharing schemes over distributed collaborative networks," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Nov. 2011.
[2] M. Srivatsa, S. Balfe, K. G. Paterson, and P. Rohatgi, "Trust management for secure information flows," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 175–188.
[3] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.
[4] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proc. IEEE INFOCOM*, 2003.
[5] H. Zhu, X. Lin, R. Lu, X. Shen, D. Xing, and Z. Cao, "An opportunistic batch bundle authentication scheme for energy constrained DTNs," in *Proc. IEEE INFOCOM*, 2010, pp. 605–613.
[6] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in *Proc. ACM MobiHoc*, 2007, pp. 150–159.
[7] B. Zhu, S. Setia, S. Jajodia, and L. Wang, "Providing witness anonymity under peer-to-peer settings," *IEEE Trans. Inf. Forens. Security*, vol. 5, no. 2, pp. 324–336, 2010.
[8] M. Young, A. Kate, I. Goldberg, and M. Karsten, "Practical robust communication in DHTs tolerating a byzantine adversary," in *Proc. ICDCS*, 2010, pp. 263–272.
[9] K. R. B. Butler, S. Ryu, P. Traynor, and P. D. McDaniel, "Leveraging identity-based cryptography for node ID assignment in structured P2P systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 12, pp. 1803–1815, 2009.
[10] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. CRYPTO*, 2001, pp. 213–229.
[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO*, 1984, pp. 47–53.
[12] E. Shi, J. Bethencourt, H. T.-H. Chan, D. X. Song, and A. Perrig, "Multi-dimensional range query over encrypted data," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 350–364.
[13] C. K. Wong, M. G. Gouda, and S. S. Lam, "Secure group communications using key graphs," in *Proc. ACM SIGCOMM*, 1998, pp. 68–79.
[14] D.M.Wallner, E. Harder, and R. Agee, "Key management for multicast: Issues and architectures," IETF Draft Wallner-Key, 1997.
[15] R. Canetti, J. A. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: A taxonomy and some efficient constructions," in *Proc. IEEE INFOCOM*, 1999, pp. 708–716.
[16] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Trans. Softw. Eng.*, vol. 29, no. 5, pp. 444–458, 2003.
[17] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Proc. ASIACRYPT*, 2007, pp. 200–215.
[18] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," in *Proc. EUROCRYPT*, 2009, pp. 171–188.
[19] M. Bellare, A. Boldyreva, and J. Staddon, "Randomness re-use in multi-recipient encryption schemas," in *Proc. Public Key Cryptography (PKC)*, 2003, pp. 85–99.
[20] B. Lynn, "On the implementation of pairing-based cryptosystems," Ph.D thesis, 2008 [Online]. Available: http://crypto.stanford.edu/pbc/thesis.pdf
[21] A. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 1639–1646, 1993.
[22] B. Waters, "Efficient identity-based encryption without random oracles," in *Proc. EUROCRYPT*, 2005, pp. 114–127.
[23] N. Attrapadung and H. Imai, "Attribute-based encryption supporting direct/indirect revocation modes," in *Proc. IEEE Int. Conf. Image Process. (IMA)*, 2009, pp. 278–300.

Huang Lin received the M.S. degree in instrument science and technology from Harbin Institute of Technology, China, in 2006, and the Ph.D. degree in computer science from Shanghai Jiao Tong University in 2010. He is currently working towards his second Ph.D. degree at the University of Florida, USA. His research interests includes security, privacy, and cryptography.

Xiaoyan Zhu received her B.E. degree in information engineering from Xidian University, Xian, China, in 2000, and her M.E. degree and Ph.D. degree in information and communications engineering from Xidian University, Xian, China, in 2004 and 2009, respectively. She is now an Associate Professor with the School of Telecommunications Engineering at Xidian University. Her research interests include wireless security and network coding.

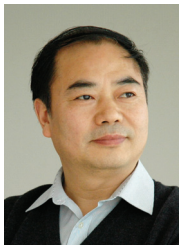


Yuguang "Michael" Fang (F'08) received a B.S./M.S. degree in mathematics from Qufu Normal University, Shandong, China, in July 1987; a Ph.D. degree in systems engineering from Case Western Reserve University in January 1994; and a Ph.D. degree in electrical engineering from Boston University in May 1997. He was an assistant professor in the Department of Electrical and Computer Engineering at the New Jersey Institute of Technology from July 1998 to May 2000. He then joined the Department of Electrical and Computer Engineering at the University of Florida in May 2000 as an assistant professor, got an early promotion to associate professor with tenure in August 2003, and became a full professor in August 2005. He held a University of Florida Research Foundation (UFRF) Professorship from 2006 to 2009, a Changjiang Scholar Chair Professorship with Xidian University, Xi'an, China, from 2008 to 2011, and a Guest Chair Professorship with Tsinghua University, China, from 2009 to 2012. He has published over 350 papers in refereed professional journals and conferences.

Dr. Fang received the National Science Foundation Faculty Early Career Award in 2001 and the Office of Naval Research Young Investigator Award in 2002, and is the recipient of the Best Paper Award in IEEE Globecom (2011), the IEEE International Conference on Network Protocols (ICNP, 2006), and is the recipient of the IEEE TCGN Best Paper Award in the IEEE High-Speed Networks Symposium, IEEE Globecom (2002). He has also received a 2010–2011 UF Doctoral Dissertation Advisor/Mentoring Award, a 2011 Florida Blue Key/UF Homecoming Distinguished Faculty Award, and the 2009 UF College of Engineering Faculty Mentoring Award. Dr. Fang is also active in professional activities. He has served as the Editor-in-Chief of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY since April 2013. He served as Editor-in-Chief for *IEEE Wireless Communications* (2009–2012) and serves/has served on several editorial boards of technical journals including the IEEE TRANSACTIONS ON MOBILE COMPUTING (2003–2008, 2011-present), IEEE NETWORK (2012–present), the IEEE TRANSACTIONS ON COMMUNICATIONS (2000-2011), the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS (2002–2009), the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (1999–2001), *IEEE Wireless Communications Magazine* (2003–2009), and *ACM Wireless Networks* (2001–present). He served on the Steering Committee for the IEEE TRANSACTIONS ON MOBILE COMPUTING (2008–2010). He has been actively participating in professional conference organizations such as serving as the Technical Program Co-Chair for IEEE INOFOCOM'2014, the Steering Committee Co-Chair for QShine (2004–2008), the Technical Program Vice-Chair for IEEE INFOCOM'2005, the Technical Program Area Chair for IEEE INFOCOM (2009–2013), Technical Program Symposium Co-Chair for IEEE Globecom'2004, and as member of the Technical Program Committee for IEEE INFOCOM (1998, 2000, 2003–2008). He is a fellow of the IEEE.

Dongsheng Xing received the M.S. degree in computer science from Shanghai Jiao Tong University, China, in 2012. He is currently interested in the implementation of cryptographic algorithms.

Chi Zhang received the B.E. and M.E. degrees in electrical and information engineering from Huazhong University of Science and Technology, China, in 1999 and 2002, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Florida in 2011. He joined the University of Science and Technology of China in September 2011 as an Associate Professor of the School of Information Science and Technology. His research interests are in the areas of network protocol design, network performance analysis, and network security guarantees, particularly for wireless networks and social networks. He has published over 60 papers in prestigious journals including the IEEE/ACM TRANSACTIONS ON NETWORKING, the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, and the IEEE TRANSACTIONS ON MOBILE COMPUTING, and in top networking conferences such as IEEE INFOCOM, ICNP, and ICDCS. He has served as Technical Program Committee (TPC) member for several international conferences including IEEE INFOCOM, ICC, GLOBECOM, WCNC, and PIMRC. He is the recipient of the 7th IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award.



Zhenfu Cao received the B.Sc. degree in computer science and technology and the Ph.D. degree in mathematics from Harbin Institute of Technology, Harbin, China, in 1983 and 1999, respectively. He was promoted to Associate Professor in 1987 and became a Full Professor in 1991. He is currently a Distinguished Professor and the Director of the Trusted Digital Technology Laboratory, Shanghai Jiao Tong University, China. He also serves as a member of the expert panel of the National Nature Science Fund of China. Prof. Cao is actively involved with the academic community, serving as Committee/Session Chair and program committee member for several international conferences, including the IEEE Global Communications Conference (since 2008), the IEEE International Conference on Communications (since 2008), the International Conference on Communications and Networking in China (since 2007), etc. He is an Associate Editor of *Computers and Security* (Elsevier), an Editorial Board member of *Fundamental Informaticae (IOS)* and *Peer-to-Peer Networking and Applications* (Springer-Verlag), and Guest Editor of the *Special Issue on Wireless Network Security*, *Wireless Communications and Mobile Computing* (Wiley), etc. He has received a number of awards, including the Youth Research Fund Award of the Chinese Academy of Science in 1986, the Ying-Tung Fok Young Teacher Award in 1989, the National Outstanding Youth Fund of China in 2002, the Special Allowance by the State Council in 2005, and is a co-recipient of the 2007 IEEE International Conference on Communications (Computer and Communications Security Symposium) Best Paper Award in 2007. He also received seven awards granted by the National Ministry and governments of provinces such as the first prize of the Natural Science Award from the Ministry of Education.