TABLE 2
Evidence Notations for our non-repudiation protocol with offline TA.

	No problem occurs	CSP launches **Abort protocol**	CSP or User launches **Recovery Protocol**
Evidences owned by CSP	EOR, $EOR_{K\|\|VO}$	Con_A	EOR, $Con_{K\|\|VO}$
Evidences owned by User	EOO, Sub, $EOO_{K\|\|VO}$	EOO, Sub, Con_A	EOO, Sub, $Con_{K\|\|VO}$

Algorithm 3 Verification

Input:
R: the query answer;
$Y = \{pk_1, pk_2, \ldots, pk_n\}$: a set of public keys;
VO: the verification object;
Output:
$accept$ or $reject$;
1: obtain the KN's signature and hash value from the VO, denoted as s=$(\tilde{x}, \tilde{y}, c_1, \ldots, c_n)$ and $hashvalue$, respectively;
2: compute $c_0 = H_2\left(Y \,\|hashvalue\,\|\, g^{\tilde{x}} h^{\tilde{y}} \prod_{j=1}^{n} pk_j^{c_j}\right)$;
3: **if** $\sum_{j=1}^{n} c_j \bmod p \neq c_0$ **then return** $reject$;
4: **end if**
5: reconstruct the KN's hash value, denoted as $hashvalue'$, according to R and VO;
6: **if** $hashvalue' = hashvalue$ **then return** $accept$;
7: **else return** $reject$;
8: **end if**

6 Security and Performance Analysis

In this section, we first prove the security of our scheme in terms of: the unforgeability and anonymity of the signature, the completeness, authenticity, and trustiness of the query answer, the interaction traceability between CSP and user. Then we present the performance analysis of our scheme.

6.1 Security Analysis

The security of our proposed scheme is mainly based on the discrete logarithm assumption(DLA) is hard.

Definition 6.1 (DLA). For any probabilistic polynomial time (PPT) algorithm A, the probability that $Pr[A(g, g^a) = a]$ is negligible, where g, $g^a \in_R G$.

This Computational Assumption is reasonable, since DLP in large number field is widely considered to be intractable [56], [57], [58]. Therefore a is not deducible from g^a even if g is publicly known. In this paper, the field G is large enough to ensure the security of our scheme.

Definition 6.2 (Unforgeability). A signature scheme is unforgeable if for all PPT adversary $\mathcal{A}$, the probability that he can construct a forged signature s_M which satisfies $V(Y, M, s_M)$=$accept$, denoted as $\mathbf{Adv}_{\mathcal{A}}^{unf} = \Pr[\mathcal{A}$ forges a valid signature$]$ is negligible, where M is a message, and s_M is the signature on M.

Definition 6.3 (Anonymity). A signature scheme is anonymous if for any PPT adversary $\mathcal{A}$, the probability that $\mathcal{A}$ can guess the signer, denoted as $\mathbf{Adv}_{\mathcal{A}}^{anon} = \Pr[\mathcal{A}$ infers the signer's public key$] - \frac{1}{n}$, is negligible.

Next we will analyze the security of our scheme from seven aspects, as shown in the following seven theorems.

Theorem 6.1 (Unforgeability). Our signature scheme is unforgeable.

Proof: Let's prove by contradiction. Assume a hash value hv, whose signature is denoted as $s = (\tilde{x}, \tilde{y}, c_1, \ldots, c_n)$, provided by DO_i. From Algorithm 3, we can get

$$c_0 = H_2\left(Y \,\|hv\,\|\, g^{\tilde{x}} h^{\tilde{y}} \prod_{j=1}^{n} pk_j^{c_j}\right)$$

where $\sum_{j=1}^{n} c_j \bmod p = c_0$. Now, an PPT adversary forges a signature, denoted as $s' = (\tilde{x}', \tilde{y}', c_1', \ldots, c_n')$, where there exists at least one element is not equal to the counterpart in s, i.e. $\tilde{x}' \neq \tilde{x}$, or $\tilde{y}' \neq \tilde{y}$, or $c_j' \neq c_j, j = 1, \ldots, n$. s' is assumed to satisfy the following equation:

$$c_0' = H_2\left(Y \,\|hv\,\|\, g^{\tilde{x}'} h^{\tilde{y}'} \prod_{j=1}^{n} pk_j^{c_j'}\right)$$

where $\sum_{j=1}^{n} c_j' \bmod p = c_0'$.

1) $c_0' = c_0$. Since the collision-resistance of hash function H_2, we can deduce

$$\begin{aligned}
& g^{\tilde{x}'} h^{\tilde{y}'} \prod_{j=1}^{n} pk_j^{c_j'} = g^{\tilde{x}} h^{\tilde{y}} \prod_{j=1}^{n} pk_j^{c_j} \\
\Rightarrow\ & g^{\tilde{x}' + \sum_{j=1}^{n} c_j' x_j} h^{\tilde{y}' + \sum_{j=1}^{n} c_j' y_j} = g^{\tilde{x} + \sum_{j=1}^{n} c_j x_j} h^{\tilde{y} + \sum_{j=1}^{n} c_j y_j} \\
\Rightarrow\ & \begin{cases} \tilde{x}' + \sum_{j=1}^{n} c_j' x_j = \tilde{x} + \sum_{j=1}^{n} c_j x_j \\ \tilde{y}' + \sum_{j=1}^{n} c_j' y_j = \tilde{y} + \sum_{j=1}^{n} c_j y_j \end{cases} \\
\Rightarrow\ & \begin{cases} (\tilde{x}' - \tilde{x}) + \sum_{j=1}^{n} \left(c_j' - c_j\right) x_j = 0 \\ (\tilde{y}' - \tilde{y}) + \sum_{j=1}^{n} \left(c_j' - c_j\right) y_j = 0 \end{cases}
\end{aligned}$$

   a) One obvious solution to the above equation is $\tilde{x}' = \tilde{x}, \tilde{y}' = \tilde{y}, c_j' = c_j, j = 1, \ldots, n$, which contradicts the assumption that $\tilde{x}' \neq \tilde{x}$, or $\tilde{y}' \neq \tilde{y}$, or $c_j' \neq c_j, j = 1, \ldots, n$.
   b) Other solutions are hard to calculate, since $x_j, y_j, j = 1, \ldots, n$ are kept secret.

2) $c' \neq c_0$. It is obviously hard to compute $\tilde{x}', \tilde{y}', c_1', \ldots, c_n'$ such that $\sum_{j=1}^{n} c_j' = H_2\left(Y \,\|hv\,\|\, g^{\tilde{x}'} h^{\tilde{y}'} \prod_{j=1}^{n} pk_j^{c_j'}\right) \bmod p$, since the one-way hash function and the hard DLP.

Hence, our signature algorithm proves unforgeable.

Theorem 6.2 (Anonymity). Our scheme can guarantee DO's identity anonymity.

Proof. Here we assume only public key pk_i can reveal the identity of DO_i. All the information the adversary can get is the signature $s = \{\tilde{x}, \tilde{y}, c_1, \ldots, c_n\}$, public key list Y, and public parameter PA. These information holds the following equation:

$$\sum_{j=1}^{n} c_j = H_2\left(Y \,\|hv\,\|\, g^{\tilde{x}} h^{\tilde{y}} \prod_{j=1}^{n} pk_j^{c_j}\right) \mod p$$

where the prefix $Y||hv$ can tell nothing about the identity of DO_i. We just consider the suffix, i.e., $g^{\tilde{x}} h^{\tilde{y}} \prod_{j=1}^{n} pk_j^{c_j}$. We denote $B = \prod_{j=1}^{n} pk_j^{c_j}$, and $A = g^{\tilde{x}} h^{\tilde{y}} B$. From Algorithm 1, we can obtain

$$\begin{array}{l} \tilde{x} = r_x - c_i x_i \mod p \\ \tilde{y} = r_y - c_i y_i \mod p \end{array}.$$

Hence the following equation holds:

$$\begin{array}{l} A = g^{r_x - c_i x_i} h^{r_y - c_i y_i} B = \frac{g^{r_x} h^{r_y} B}{pk_i^{c_i}} \\ \Rightarrow pk_i^{c_i} = \frac{B}{A} g^{r_x} h^{r_y} \end{array}$$

As described in Algorithm 1, r_x, r_y are random values and kept secret. Hence we can not compute the public key pk_i of DO_i.

Hence, our scheme can guarantee DO's anonymity.

Compared with the scheme in [9], the sign computation cost and verification computation cost are reduced from $E + 2M$ and $2M$ to $E + M$ and M respectively, where E represents an exponentiation, M represents a multi-bases exponentiation which is equal to the cost of approximate 1.3 exponentiation. We achieve this by discarding its linkability.

Theorem 6.3 (Completeness). If hash function is collision-resistant, the query answer and VO are all authentic, then our scheme can verify the completeness of query answer.

Proof. Assume the query answer is $\{a_k, a_{k+1}, \ldots, a_j\}$. In general, the first two elements of VO, as the output of Algorithm 2, are the left and right boundary data. When they are not null, we denote them as $a_{k'}$ and $a_{j'}$, respectively. $a_{k'}$ and $a_{j'}$ surely dissatisfy the query claims. If we can prove that $a_{k'}(a_{j'})$ is left (right) adjacent tightly to $a_k(a_j)$, then our scheme can verify the completeness of $\{a_k, a_{k+1}, \ldots, a_j\}$. Let's prove by contradiction. Assume that $a_{k'}(a_{j'})$ is not left (right) adjacent to $a_k(a_j)$. That is to say, there are other data records between $a_{k'}(a_{j'})$ and $a_k(a_j)$. When executing Algorithm 3, the verification result is $hashvalue' \neq hashvalue$ and failing, since hash function is collision-resistant. In consequence, only when $a_{k'}(a_{j'})$ is left (right) adjacent tightly to $a_k(a_j)$, will the authentication succeeds. So far the proof is completed. Our scheme can verify the completeness of query answer.

Theorem 6.4 (Authenticity). If hash function is collision-resistant, and the query answer is complete, our scheme can verify the authenticity of query answer.

Proof. Let's prove by contradiction. If the query answer is tamped or forged, hash value of the KN, reconstructed using unauthentic query answer and hash values of VO, will differ with the hash value computed from the signature of the same KN. Algorithm 3 will output *reject*. In consequence, only when $\{a_k, a_{k+1}, \ldots, a_j\}$ is authentic, will the verification succeed. The proof is completed. Our scheme can verify the authenticity of query answer.

Theorem 6.5 (Trustiness). If hash function is collision-resistant, our scheme can verify the trustiness of the query answer.

Proof. Theorems 6.3 and 6.4 have proven our scheme can verify the completeness and authenticity of query answer. As for the trustiness, it relies completely on the trustiness of the signature in VO. Assume the signature is denoted as s= $(\tilde{x}, \tilde{y}, c_1, \ldots, c_n)$. From the signing procedure in Algorithm 1, we can obtain

$$\begin{array}{l} c_1 + \ldots + c_n \mod p = H_2\left(Y \,\|hashvalue\,\|K\right) \\ = H_2\left(Y \,\|hashvalue\,\|\, g^{\tilde{x}+c_i x_i} h^{\tilde{y}+c_i y_i} \prod_{j=1, j\neq i}^{n} pk_j^{c_j}\right) \\ = H_2\left(Y \,\|hashvalue\,\|\, g^{\tilde{x}} h^{\tilde{y}} (g^{x_i} h^{y_i})^{c_i} \prod_{j=1, j\neq i}^{n} pk_j^{c_j}\right) \\ = H_2\left(Y \,\|hashvalue\,\|\, g^{\tilde{x}} h^{\tilde{y}} \prod_{j=1}^{n} pk_j^{c_j}\right). \end{array} \quad (1)$$

Algorithm 3 tells us that

$$c_0 = H_2\left(Y \,\|hashvalue\,\|\, g^{\tilde{x}} h^{\tilde{y}} \prod_{j=1}^{n} pk_j^{c_j}\right). \quad (2)$$

So $\sum_{j=1}^{n} c_j \mod p$=$c_0$ holds. Till now, the trustiness of the signature is proved. Hence, our scheme can verify the trustiness of the query answer.

Theorem 6.6 (Traceability). Our scheme can guarantee interaction traceability between CSP and user.

Proof. When the transaction between CSP and user is successful, either only the Main Protocol, or both the Main Protocol and Recovery Protocol, are launched. In each case, we can prove the interaction traceability of our scheme.

1. Only the Main Protocol is launched.

CSP has the evidence of non-repudiation receipt $\{EOR, EOR_{K||VO}\}$, and user has the evidence of non-repudiation origin $\{EOO, Sub, EOO_{K||VO}\}$.

After verifying R is correct through Algorithm 3, if user denies receipt of R, CSP can prove his receipt by presenting R, $E_K(R)$, K, VO, L and $\{EOR, EOR_{K||VO}\}$ to TA. TA executes three checks: 1) $EOR_{K||VO}$ is user's signature on $(f_{EOR_{K||VO}}, CSP, L, K, VO)$; 2) EOR is user's signature on $(f_{EOR}, CSP, TA, L, H_2(E_K(R)))$; 3) $R = D_K(E_K(R))$. If the above three checks are positive, TA will conclude user received R.

When CSP denies the origin of incorrect R, user has to present R, $E_K(R)$, K, VO, L and $\{EOO, Sub, EOO_{K||VO}\}$ to TA. Similarly, TA executes four checks: 1) $EOO_{K||VO}$ is CSP's signature on $(f_{EOO}, Cient, L, K, VO)$; 2) EOO is CSP's signature on $(f_{EOO}, User, TA, L, H_2(E_K(R)))$; 3) Sub is CSP's signature on $(f_{Sub}, User, L, E_{TA}(K||VO))$; 4)

$R = D_K(E_K(R))$. If the above four checks are all positive, TA claims that CSP is at the origin of incorrect R.

2. Both the Main and Recovery Protocol are launched.

CSP has the evidence of non-repudiation receipt $\{EOR, Con_{K||VO}\}$, and user has the evidence of non-repudiation origin $\{EOO, Sub, Con_{K||VO}\}$. As described in Section 4.2.4, $Con_{K||VO}$, the signature of TA on K, VO, is the substitution for $EOR_{K||VO}$ and $EOO_{K||VO}$, which has equal functions to $EOR_{K||VO}$ and $EOO_{K||VO}$. Hence we can prove the interaction traceability of our scheme in a similar way to the first case.

In all, we get the conclusion that our scheme can guarantee interaction traceability between CSP and user.

6.2 Performance Analysis

Theorem 6.7 (High Efficiency). The high efficiency of our scheme is mainly manifested in $ServiceVerify$ from two aspects: on the one hand, it reconstructs the subtree rooted in the KN of VO; on the other hand, it first checks the trustiness of signature in VO.

Proof. Even though one hashing operation is around 50 times faster than modular multiplication [11], the hashing computation cost is still high when facing the big data. To reduce the hashing computation overhead at user, our scheme improves the traditional MHT-based verification scheme from the following two aspects.

On the one hand, our scheme signs the hash values of the root node, as well as the nodes on level $\left\lfloor \log_2 \sqrt{N} + 0.5 \right\rfloor$. So if there is one KN on internal level covering the query answer and the two boundary values, our scheme just needs to reconstruct the subtree rooted in such a KN, while the traditional schemes always reconstruct the whole MHT.

On the other hand, when verifying query answer, previous schemes firstly reconstruct the hash value of the root node using a lot of hash computation, then compare it with the hash value computed from the signature. If the signature is not trusted, not only much hash computation is wasted, but also the query answer will prove to be false all the same even though it is correct. However, such problem can be avoided in our scheme by concatenating the hash values with their signatures, then checking trustiness before verifying the completeness and authenticity.

Next we will compare our scheme performance with those in [9] and [7]. Our scheme is improved from both [9] and [7]. The scheme proposed in [9] signs the values one by one. Chapter 3 in [7] describes an authentication scheme for selection queries on the basis of MHT. Assume the query answer R contains l data values. The comparison and analysis results are shown in Table 3. In Table 3, our scheme has two cases about verification computation cost and VO size, respectively. It is caused by the KN in VO. If the KN is the root node, both verification computation cost and VO size are the same as those in [7]. If the KN is an internal node, both verification computation cost and VO size are much smaller. In essence, our scheme sacrifices slightly higher sign computation cost to improve the verification efficiency and reduce the communication cost. Hence the sign computation cost is a little higher than that in [7], but far lower than that in [9], which will be proved by experiments in Section 7.

7 Experiment

All algorithms are implemented using Visual C++ 6.0 on a Windows 8.1 system with Intel CORE i7-4500U CPU @ 1.80GHz and 8.00G RAM. We implement the proposed scheme and evaluate the performance over multiple groups of random data. The selection queries are of the form as SELECT * FROM *stream* WHERE $l_i < A_i < u_i$.
In order to compare with other schemes fairly, there are different numbers of random data in each group. Moreover, 1000 random queries are processed. We compute averages of sign computation time, VO generation time, verification computation time, VO size and tamper detection time, respectively, as experimental results shown in Figs. 5–9.

Figs. 5–8 show the cost comparison results of sign computation, VO generation, verification computation and VO storage, respectively. Firstly, it is evident that all these cost, except the VO generation cost, as shown in the lines marked by circles, increase quickly. The scheme proposed in [9] signs all the data values one by one. As a consequence, the CSP need do nothing for VO generation, and just takes the signatures as the VO. In brief, the signature cost is proportional to the whole database size, and the VO generation cost is trivial. In our scenario, the volume of the data is very large. Hence the scheme [9] isn't applicable. By the way, the verification computation cost and VO size in [9] are experimentally proportional to the number of data in a query answer. But for simplicity, we present all these performance in one figure.

Next, let's see the comparison results between our scheme and the scheme proposed in [7], shown in lines marked by triangles and rectangles, respectively. We can see that our scheme has slightly higher sign computation cost, but the lower verification cost and the smaller VO size. Our scheme sacrifices slightly higher sign computation cost to improve the verification efficiency and reduce the communication cost, as analyzed in Theorem 6.7.

Finally, we compare the efficiency in detecting whether the signature is valid or not. Fig. 9 shows our scheme achieves the highest detection efficiency. The detection time cost of the schemes in [7], [9] is almost the same as the verification computation cost in Fig. 7. It is because that the signature tampering can not be detected until the whole verify process is completed. In our scheme, the signature is always companied with the corresponding signed hash value, which can help us to detect the signature tampering efficiently by Algorithm 3.

All the experimental results meet the theoretical analysis in Table 3.

8 Conclusion

Since there are multiple data providers and a wide range of users in cloud service systems, it is hard to take full advantage of cloud data to serve people well on the premise of not infringing upon the interests of others. In this paper, it is the first time to propose a cooperative query answer authentication scheme which applies to cloud. This scheme can not only verify the trustiness, completeness, authenticity of the query answers efficiently, but also satisfy DO's requirement for anonymity and guarantee non-repudiation service between CSP and user. Firstly, the proposed scheme

TABLE 3
Comparison and analysis

Scheme	Authenticity and completeness	High efficiency	Multi-DO supporting and DO's anonymity	Query non-repudiablility	Sign computation cost	Verification computation cost	VO size
[9]	×	×	√	×	$O(N)$	$O(l)$	$O(l)$
[7]	√	×	×	×	$O(log_2 N)$	$O(log_2 N)$	$O(log_2 N) + 2log_2 N$
Ours	√	√	√	√	$O\left(\log_2 N + \sqrt{N}\right)$	$O\left(\log_2 \sqrt{N}\right)$ or $O(\log_2 N)$	$O\left(\log_2 \sqrt{N}\right) + 2\log_2 N$ or $O(\log_2 N) + 2\log_2 N$

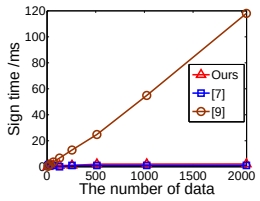

Fig. 5. Sign computation cost.

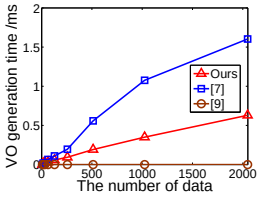

Fig. 6. VO generation cost.

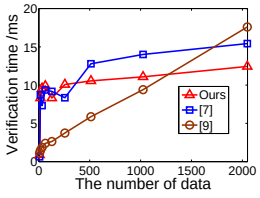

Fig. 7. Verification computation cost.

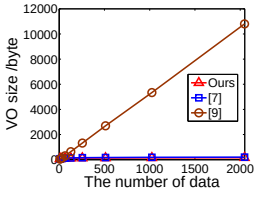

Fig. 8. VO size.

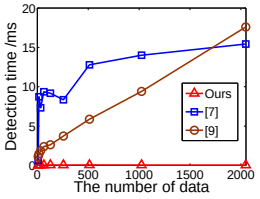

Fig. 9. Detection time cost for signature tampering.

chooses and signs the KN in the MHT based on the ring signature scheme, which can both verify the correct of query result when keeping DO anonymous, and supports multiple DOs. Secondly, we introduce a non-repudiation protocol based on VO to solve the repudiable behaviors of CSP and user. Finally, the experimental results show our proposed scheme is of higher efficiency and lower communication cost than others.

Acknowledgments

The work was supported by the National Natural Science Foundation of China (61472001, 61472283, U1405255), and the scientific research construction fee of Anhui University.

References

[1] D. Kwak, R. Liu, D. Kim, B. Nath, and L. Iftode, "Seeing is believing: Sharing real-time visual traffic information via vehicular clouds," *IEEE Access*, vol. 4, pp. 3617–3631, 2016.

[2] Q. Yang, B. Zhu, and S. Wu, "An architecture of cloud-assisted information dissemination in vehicular networks," *IEEE Access*, vol. 4, pp. 2764–2770, 2016.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on parallel and distributed systems*, vol. 25, no. 1, pp. 222–233, 2014.

[4] W. Zhang, Y. Lin, S. Xiao, J. Wu, and S. Zhou, "Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1566–1577, 2016.

[5] S. Tian, Y. Cai, and Z. Hu, "A parity-based data outsourcing model for query authentication and correction," in *IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2016, pp. 395–404.

[6] J. Li, A. Squicciarini, D. Lin, S. Sundareswaran, and C. Jia, "Mmbcloud-tree: Authenticated index for verifiable cloud service selection," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1–14, 2015.

[7] H. Pang and K.-L. Tan, "Query answer authentication," *Synthesis Lectures on Data Management*, vol. 4, no. 2, pp. 1–103, 2012.

[8] F. Li, K. Yi, M. Hadjieleftheriou, and G. Kollios, "Proof-infused streams: Enabling authentication of sliding window queries on streams," in *Proceedings of the 33rd international conference on Very large data bases*. VLDB Endowment, 2007, pp. 147–158.

[9] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Linkable ring signature with unconditional anonymity," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 1, pp. 157–165, 2014.

[10] R. C. Merkle, "A certified digital signature," in *Conference on the Theory and Application of Cryptology*. Springer, 1989, pp. 218–238.

[11] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*. ACM, 2006, pp. 121–132.

[12] ——, "Authenticated index structures for aggregation queries," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 4, p. 32, 2010.

[13] F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera, "Range query integrity in cloud data streams with efficient insertion," in *International Conference on Cryptology and Network Security*. Springer, 2016, pp. 719–724.

[14] Q. Chen, H. Hu, and J. Xu, "Authenticated online data integration services," in *Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data*. ACM, 2015, pp. 167–181.

[15] R. Vyas, A. Singh, J. Singh, G. Soni, and B. Purushothama, "Design of an efficient verification scheme for correctness of outsourced computations in cloud computing," in *International Symposium on Security in Computing and Communication*. Springer, 2015, pp. 66–77.

[16] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," Technical report, SRI International, Tech. Rep., 1998.

[17] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[18] ——, "Achieving k-anonymity privacy protection using generalization and suppression," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 571–588, 2002.

[19] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 1, no. 1, p. 3, 2007.

[20] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *2007 IEEE 23rd International Conference on Data Engineering*. IEEE, 2007, pp. 106–115.

[21] C. C. Aggarwal, "On unifying privacy and uncertain data models," in *2008 IEEE 24th International Conference on Data Engineering*. IEEE, 2008, pp. 386–395.

[22] X. M. Ren, J. Yang, J. P. Zhang, and Z. F. Jia, "Uncertain data privacy protection based on k-anonymity via anatomy," in *Advanced Engineering Forum*, vol. 6. Trans Tech Publ, 2012, pp. 64–69.

[23] G. Aggarwal, T. Feder, K. Kenthapadi, S. Khuller, R. Panigrahy, D. Thomas, and A. Zhu, "Achieving anonymity via clustering,"

in *Proceedings of the 25 ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*. ACM, 2006, pp. 153–162.

[24] J.-L. Lin, T.-H. Wen, J.-C. Hsieh, and P.-C. Chang, "Density-based microaggregation for statistical disclosure control," *Expert Systems with Applications*, vol. 37, no. 4, pp. 3256–3263, 2010.

[25] X. Xiao and Y. Tao, "Anatomy: Simple and effective privacy preservation," in *Proceedings of the 32nd international conference on Very large data bases*. VLDB Endowment, 2006, pp. 139–150.

[26] Q. Zhang, N. Koudas, D. Srivastava, and T. Yu, "Aggregate query answering on anonymized tables," in *2007 IEEE 23rd International Conference on Data Engineering*. IEEE, 2007, pp. 116–125.

[27] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2001, pp. 552–565.

[28] S. S. Chow, S.-M. Yiu, and L. C. Hui, "Efficient identity based ring signature," in *International Conference on Applied Cryptography and Network Security*. Springer, 2005, pp. 499–512.

[29] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous identification in ad hoc groups," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2004, pp. 609–626.

[30] F. Zhang and K. Kim, "Id-based blind signature and ring signature from pairings," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2002, pp. 533–547.

[31] X. Huang, J. K. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," *IEEE Transactions on Computers*, vol. 64, no. 4, pp. 971–983, 2015.

[32] X. Yang, W. Wu, J. K. Liu, and X. Chen, "Lightweight anonymous authentication for ad hoc group: A ring signature approach," in *International Conference on Provable Security*. Springer, 2015, pp. 215–226.

[33] P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong, "A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity," in *International Conference on Provable Security*. Springer, 2010, pp. 166–183.

[34] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in *Annual International Cryptology Conference*. Springer, 2002, pp. 465–480.

[35] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4833–4842, 2011.

[36] T. H. Yuen, J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Efficient linkable and/or threshold ring signature without random oracles," *The Computer Journal*, vol. 56, no. 4, pp. 407–421, 2013.

[37] H. Gan and L. Chen, "An efficient data integrity verification and fault-tolerant scheme," in *Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on*. IEEE, 2014, pp. 1157–1160.

[38] C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang, and J. Chen, "Mur-dpa: top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud," *IEEE Transactions on Computers*, vol. 64, no. 9, pp. 2609–2622, 2015.

[39] D. Wu, B. Choi, J. Xu, and C. S. Jensen, "Authentication of moving top-k spatial keyword queries," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 4, pp. 922–935, 2015.

[40] J. Zhou and D. Gollmann, "An efficient non-repudiation protocol," in *Computer Security Foundations Workshop, 1997. Proceedings., 10th*. IEEE, 1997, pp. 126–132.

[41] ——, "A fair non-repudiation protocol," in *IEEE symposium on security and privacy*. Citeseer, 1996, pp. 55–61.

[42] H. U. Yildiz, K. Bicakci, B. Tavli, H. Gultekin, and D. Incebacak, "Maximizing wireless sensor network lifetime by communication/computation energy optimization of non-repudiation security service: Node level versus network level strategies," *Ad Hoc Networks*, vol. 37, pp. 301–323, 2016.

[43] J. Li, H. Lu, and M. Guizani, "Acpn: a novel authentication framework with conditional privacy-preservation and non-repudiation for vanets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.

[44] C.-Y. Wu, Y. Xiong, W.-C. Huang, Q.-W. Lu, and X.-D. Gong, "A trusted fair non-repudiation protocol based on dynamic third party in mobile ad hoc networks," *Acta Electronica Sinica*, vol. 2, p. 004, 2013.

[45] J. Feng, Y. Chen, D. Summerville, W.-S. Ku, and Z. Su, "Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol," in *2011 IEEE Consumer Communications and Networking Conference (CCNC)*. IEEE, 2011, pp. 521–522.

[46] J. Feng, Y. Chen, W.-S. Ku, and P. Liu, "Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms," in *2010 39th International Conference on Parallel Processing Workshops*. IEEE, 2010, pp. 251–258.

[47] J.-Z. Luo, Z.-G. Han, and L.-m. Wang, "Trustworthy and controllable network architecture and protocol framework," *Chinese Journal of Computers*, vol. 32, no. 3, pp. 391–404, 2009.

[48] Z.-g. HAN and J.-z. LUO, "Analysis and improvement of timeliness of a multi-party non-repudiation protocol [j]," *Acta Electronica Sinica*, vol. 2, p. 025, 2009.

[49] S. Kremer, O. Markowitch, and J. Zhou, "An intensive survey of fair non-repudiation protocols," *Computer communications*, vol. 25, no. 17, pp. 1606–1621, 2002.

[50] T. Tedrick, "How to exchange half a bit," in *Advances in Cryptology*. Springer, 1984, pp. 147–151.

[51] ——, "Fair exchange of secrets," in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1984, pp. 434–438.

[52] Q. Wang, M. He, M. Du, S. S. Chow, R. W. Lai, and Q. Zou, "Searchable encryption over feature-rich data," *IEEE Transactions on Dependable and Secure Computing*, 2016.

[53] C. Bösch, P. Hartel, W. Jonker, and A. Peter, "A survey of provably secure searchable encryption," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, p. 18, 2015.

[54] K. Li, W. Zhang, C. Yang, and N. Yu, "Security analysis on one-to-many order preserving encryption-based cloud data search," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1918–1926, 2015.

[55] Z. Liu, X. Chen, J. Yang, C. Jia, and I. You, "New order preserving encryption model for outsourced databases in cloud environments," *Journal of Network and Computer Applications*, vol. 59, pp. 198–207, 2016.

[56] X.-Y. Li and T. Jung, "Search me if you can: privacy-preserving location query service," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2760–2768.

[57] T. Jung, X.-Y. Li, and M. Wan, "Collusion-tolerable privacy-preserving sum and product calculation without secure channel," *IEEE Transactions on Dependable and secure computing*, vol. 12, no. 1, pp. 45–57, 2015.

[58] T. Jung, X.-Y. Li, Z. Wan, and M. Wan, "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 190–199, 2015.

Liangmin Wang received his B. S. degree in Computational Mathematics in Jilin University, Changchun, China, in 1999, and the Ph.D degree in Cryptology from Xidian University, Xi'an, China, in 2007. He is a full professor in the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China. He has been honored as a "Wan-Jiang Scholar" of Anhui Province since Nov. 2013. Now his research interests include security protocols for wireless networks and Privacy & Security of Big Data.

He has published over 60 technical papers at premium international journals and conferences, like IEEE Transactions on Information Forensics and Security, IEEE Transactions on Vehicular Technology, IEEE GlobeCOM, IEEE WCNC. Dr WANG has been severed as the TPC of many IEEE conferences, such as IEEE ICC, IEEE HPCC, IEEE TrustCOM. Now he is an associate editor of Security and Communication Networks, a member of IEEE, ACM, and a senior member of Chinese Computer Federation.

Qingqing Xie received the B. Eng. degree in computer science and technology from Anhui University, PRC in 2012. She is currently a Ph.D. candidate in Department of Computer Science and Technology at Anhui University. She is also a research visitor in Department of Computer Science at Boise State University.

Her research interest includes data security, cloud computing, and applied cryptography.

Hong Zhong received her B. S. degree in applied mathematics in Anhui University, China, in 1986, and the Ph.D degree in computer science and technology from University of Science and Technology of China (USTC), China, in 2005. Now she is a professor and Phd Advisor of Anhui University.

Her research interests include security protocols and wireless sensor networks.