INTELLIGENT AUTOMATION & SOFT COMPUTING, 2017
http://dx.doi.org/10.1080/10798587.2016.1267239

Verifiable Outsourcing of High-degree Polynomials and its Application in Keyword Search

Jun Ye[a], Xianlin Zhou[b], Zheng Xu[c] and Yong Ding[d]

[a]Key Laboratory of Higher Education of Sichuan Province for Enterprise Informationalization and Internet of Things, Sichuan University of Science & Engineering, Guangxi Key Laboratory of Cryptography and Information Security, Lab of Security Insurance of Cyberspace, China; [b]College of Mathematics and Software Science, Sichuan Normal University, Sichuan, China; [c]The Third Research Institute of the Ministry of Public Security, Shanghai, China; [d]School of Computer Science and Information Security, Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guangxi, China

ABSTRACT

In big data era, people cannot afford more and more complex computation work due to the constrained computation resources. The high reliability, strong processing capacity, large storage space of cloud computing makes the resource-constrained clients remotely operate the heavy computation task with the help of cloud server. In this paper, a new algorithm for secure outsourcing of high degree polynomials is proposed. We introduce a camouflage technique, which the real polynomial will be disguised to the untrusted cloud server. In addition, the input and output will not be revealed in the computation process and the clients can easily verify the returned result. The application of the secure outsourcing algorithm in keyword search system is also studied. A verification technique for keyword search is generated based on the outsourcing algorithm. The client can easily verify whether the server faithfully implement the search work in the whole ciphertext space. If the server does not implement the search work and returns the client "null" to indicate there is no files with the query keyword, the client can easily verify whether there are some related files in the ciphertext database.

KEY WORDS

Secure outsourcing; verifiable; polynomial; keyword search

1. Introduction

With the rapid popularization of Internet and the extensive use of software applications, the data used in the field of social networking, medical, electricity and financial industry etc., is increasing explosively. The higher performance of the analysis, calculation, and storage of huge amounts of data is needed. However, the computation mode is different from the traditional mode, and the traditional computation mode cannot satisfy the requirement of data processing due to the limitation of computing power and storage resources in big data era. Google, Amazon and other companies put forward cloud computing services, which realized easy access to a shared resource at anytime and anywhere. This new model improves the service quality and reduces operating cost, which is widely used in IT industries.

In big data era, people cannot afford the complex computation work due to the constrained computation resources (Hu et al., 2014; Xu et al., 2016a,b,c,d). Outsourcing computation helps people to solve the heavy computation task. The resource-constrained clients outsourced large-scale computing tasks to the cloud server, which may not be trusted. Then the cloud server returns the computation results when it finishes the computing tasks. In this way, the client can use the large cloud computing resources to accomplish the costly computing. In the computing process, there is little cost for software and hardware in the process, and the efficiency is very high, the optimal allocation of resources can be achieved.

However, the cloud service provider is an untrusted third party, the privacy of the outsourced data and the correctness of the results cannot be guaranteed. It is significant to do some research on the protection of the inputs and outputs and the verification of the computing results. Verifiable computation can be used to test whether the outsourcing computation results is correct or not. The verification cost of this computation should be less than the cost of computing tasks.

Polynomials are widely used in the Engineering field, such as information security, image processing, financial data analysis, linear algebra, signal processing and so on. However, when facing with high degree polynomials, it cost much computation resources and working time of resource-constrained clients. It is necessary to study outsourcing polynomial computation.

Outsourcing computation of polynomials can be used in searchable encryption, which helps people retrieve the required files in a practicable way. However, in most of existing schemes, the cloud server is assumed to be honest, and the verification of the retrieved results is not considered. In the real world, it is hard to find a reliable cloud service provider in cloud computing. In order to get more benefits and save the resources, cloud server will probably return a "null" without searching.

There are also some researches on the verification of the returned results. The bloom filter is used in these schemes, and the clients can easily verify the results returned by the cloud server. However, there will be some mistakes due to the construction of bloom filter, it is inevitable. When some new keywords are generated, the bloom filter has to be reconstructed,

CONTACT Yong Ding stone_dingy@126.com
This article was originally published with an error. This version has been corrected. Please see Erratum (http://dx.doi.org/10.1080/10798587.2017.1299889).

and the misjudgment rate will increase. Polynomial is a good tool to deal with the above issue. There is no mistake, and the new polynomial can be easily reconstructed.

In this paper, we focus on the verifiable secure outsourcing of polynomials, and its application in verifiable keyword search. Our contribution is as follows:

- A disguising technique is proposed to blind the polynomial.
- A new algorithm for secure outsourcing of high degree polynomials is given based on the proposed disguising technique.
- The input and output can keep private in the computation process, and the clients can easily verify the returned result.
- A new verification technique for keyword search is generated with this verification technique. When cloud server returns "null", the clients can easily verify whether cloud server faithfully searched over the ciphertexts.

This paper is a revised and expanded version of the paper entitled "Secure Outsourcing Algorithm of Polynomials in Cloud Computing" presented at the 28th International Conference on Software Engineering and Knowledge Engineering, Redwood City, San Francisco Bay, California, USA (Zhou et al., 2016). We improve the secure outsourcing model and enhance the security. The application of the outsourcing algorithm is added, and a new verification technique for keyword search is proposed, with which the client can verify whether the server implement the search work or not.

The organization of this paper is as follows: The related work is given in Section 2. Some preliminaries are given in Section 3. The algorithm of secure outsourcing for polynomials is given in Section 4. In Section 5 we give the security analysis. The application of the outsourcing algorithm in keyword search is given in Section 6. Finally, the conclusion is made in Section 7.

2. Related Work

2.1. Outsourcing Computation

Outsourcing computation allows clients to do some computations with the help of the cloud, without disclosing the information about the inputs except possibly and the outputs. In 2002, secure outsourcing of scientific computing and numerical calculation were studied for the first time by Atallah, Pantazopoulos, Rice, and Spafford (2002), and they put forward a lot of suitable camouflage technologies for scientific computing, such as, matrix multiplication, inequality, linear equations, etc. However, verifiability of computing results was not studied. In 2005, Hohenberger and Lysyanskaya (2005) proposed the formal security definition of outsourcing. In 2008, Benjamin and Atallah (2008) used homomorphic encryption to construct a secure outsourcing scheme for linear algebraic computation, in which the client can verify the results. In 2010, Atallah and Frikken (2010) proposed a single server verifiable outsourcing scheme based on Shamir secret sharing scheme, and Gennaro, Gentry, and Parno (2010) proposed an outsourcing computation scheme for arbitrary function F with non-interactive verification based on fully homomorphic encryption. In 2016, Ye, Xu, and Ding (2016) proposed a secure outsourcing algorithm for modular exponentiation, which improves the efficiency of Hohenberger's scheme.

Polynomials are often used in many application fields, such as, signal processing, data analysis, etc. In 2011, Benabbas, Gennaro, and Vahlis (2011) proposed an algorithm of secure outsourcing for polynomials based on homomorphic encryption. In 2012, Fiore and Gennaro (2012) proposed a scheme for verifiable delegation of large polynomials. However, in these two schemes, the inputs would be revealed. In 2016, Ye, Zhang, and Fu (2016) proposed a scheme for secure outsourcing polynomials, in which an extra polynomial will be outsourced for verification.

2.2. Searchable Encryption

Searchable encryption allows a client to securely search the keyword and retrieve corresponding documents. The first searchable encryption scheme is proposed by Song, Wagner, and Perrig (2000) in 2000. However the queried keywords will be leaked. To improve the efficiency, Chang and Mitzenmacher (2005) proposed a similar index scheme; an encrypted hash table is built for the whole files. In the index table, each entry consists of the trapdoor of a keyword and an encrypted set of related file identifiers. Then the searchable encryption formal security notion is proposed by Curtmola, Garay, Kamara, and Ostrovsky (2006). Furthermore, (Fiore & Gennaro (2012) proposed a verifiable keyword search schemes. Though the keywords are secure in the symmetric key setting (Chai and Gong, 2012), it is resistless for the off-line keyword guessing attack in public key setting. However, the above schemes deal with symmetric encryptions.

Bao, Deng, Ding, and Yang (2008) proposed a searchable encryption scheme in multi-user setting. Clients in the group can search the encrypted files without sharing their secrets. However, the index generation should be interacted with the server, and server can identify the keyword if two clients search the same keyword. There are also some other works on searchable public key encryption (Ye, Wang, Zhao, Shen, and Li, 2016). Zhao, Nishide, and Sakurai (2011) proposed an attribute-based searchable encryption scheme. Zheng, Xu, and Ateniese (2014) used bloom filter to verify the search results.

3. Preliminaries

3.1. Outsource-security

An algorithm is said to be an outsource-secure algorithm if;

- Correctness: The result returned from the cloud server is the correct implementation of the algorithm.
- Security: For all probabilistic polynomial-time adversaries, the original computation cannot be obtained from the outsourced disguised computation.

3.2. Verifiable Outsourcing Computation

A verifiable outsourcing computation scheme is defined by the following algorithms:

- KeyGen(f,k) → (PK, SK): Based on the security parameter k, the key generation algorithm generates a key pair (PK, SK) for the function f. PK is provided to the server, and client keeps SK.
- ProGen (x) → (σ_x, V_x): The problem generation algorithm is run by client, who uses SK to encode the input x as σ_x, which is given to server, and a verification key V_x, which is kept private by client.
- Compute (σ_x) → (σ_y): The algorithm is run by the server to compute an encoded version of the output σ_y.

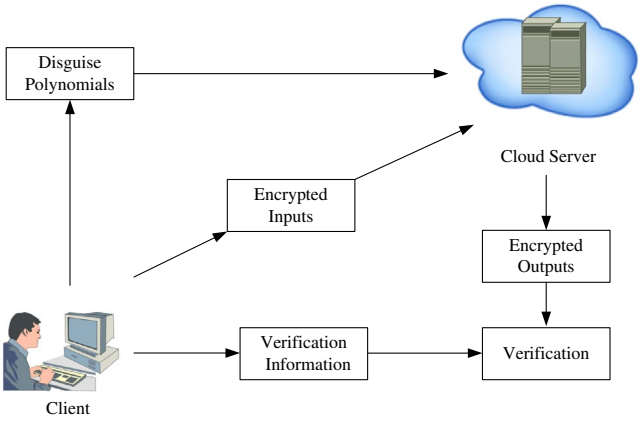

Figure 1. Outsourcing System Model.

- Verify $(V_x, \sigma_y) \rightarrow (y \cup \perp)$: The algorithm returns the value $y = f(x)$ or $\perp$, which indicates that σ_y is a false result of $f(x)$.

A verifiable computation scheme should be correct and secure.

- Correctness: A verifiable computation scheme is correct if the algorithms allow the honest server to output values that will pass the verification. That is, for any x and f and any

$$(PK,\ SK) \leftarrow \text{KeyGen}\,(f, k),$$

if

$$(\sigma_x, V_x) \leftarrow \text{ProGen}_{\text{SK}}(x)\,,\ (\sigma_y) \leftarrow \text{Compute}_{\text{PK}}(\sigma_x),$$

Then

$$f(x) \leftarrow \text{Verify}_{\text{SK}}(V_x, \sigma_y)$$

holds with all but negligible probability.

- Security: A verifiable computation scheme is secure if for any function f, and any PPT adversary A, that

$$\text{Adv}_A\left(V,\ f,\ k\right) \leq negl(k)$$

Where $negl(\cdot)$ is a negligible function.

In the verifiable computation scheme the time for verifying the output must be much smaller than the time to compute the function.

- Efficiency: A verifiable computation scheme is efficient, if the time required for Verify (V_x, σ_y) is $O(T)$, where T is the time required to compute $f(x)$.

3.3. Verifiable Keyword Search

The process of verifiable keyword search can be described as follows:

- Setup: A probabilistic algorithm executed by Authority (AU) to set up the system and to initialize system parameters. The algorithm outputs the public keys PK and secret keys SK for AU.
- Enroll: Executed by AU to enroll client to the system. Taking as input SK, it outputs client's ID and query key.
- GenIndex: Client generates $I(w)$ with PK and the desired keyword w.
- Write: Client invokes GenIndex to generate search token $I(d{\cdot}w)$.
- ConstructQ: Run by a client to construct a query, which takes the public key PK, the secret key and a chosen keyword was inputs and outputs a query $Q(w)$.
- Search: Run by server to search in the ciphertexts database for the records associated with w. If some records exist, it returns the records, or returns "null" if there is no record associated with w.
- Verify: Run by a client to verify the search result. When the server returns "null", client checks the correctness by using the verification algorithm. If there is no record associated with w, it outputs1, else, outputs 0.

4. Secure Outsourcing of Polynomials

A resource-constrained client wants to outsource a high degree polynomial with fixed coefficients. This polynomial will be used latter for some applications frequently. We focus on the outsourcing of the fixed polynomials without homomorphic encryption, which will be used in the verification of keyword search work. In the outsourcing process, the inputs and the outputs should be blind to cloud server and the client should verify the correctness of the result efficiently.

4.1. Design Goals

To securely outsourcing the computation of polynomials efficiently, there are four design goals.

- Camouflage: Design a camouflage method to disguise the real computing polynomials, so that the cloud server cannot get the information of original polynomials.
- Security: Prevent the cloud server from learning any information of the inputs and outputs.
- Verification: The algorithm should be guaranteed that the server returns the correct computing results.
- Efficiency: The computation cost in the verification phase should be greatly less than that of polynomial computation.

4.2. System Model

The secure outsourcing model with the resource-constrained client and the untrusted powerful cloud server is shown in Figure 1.

Client firstly camouflages the original polynomial into a disguised polynomial, which will be outsourced to the cloud server. When client wants to do some computations on the outsourced polynomial, he/she encrypts the inputs and sends to the cloud server. When finishes the computations, the cloud server returns the computation results to the client. Then client verify the computation results by using the verification information. If the returned results are correct, client will transform the encrypted outputs into the real computation results.

4.3. Camouflage Technique

In the following we give the camouflage technique for secure outsourcing of polynomials.

The polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

Table 1. Comparisons.

	Input Privacy	Output Privacy	Homomorphic Encryption
Benabbas et al. (2011)	No	No	Yes
Fiore and Gennaro (2012)	No	No	Yes
Ours	Yes	Yes	No

Where $a_i \in Z_p$, $0 \le i \le n$, is a high degree polynomial, which will be outsourced to the cloud server and the client wants to compute the function on the value of x.

For the secure outsourcing and efficient verification, a disguised polynomial $F(\sigma_x)$ is constructed, which should satisfy the following requirements.

- Server cannot get any information about coefficients a_i of $f(x)$ from the outsourcing polynomial $F(\sigma_x)$.
- Server cannot get any information about the input x of $f(x)$ from the outsourcing input $F(\sigma_x)$.
- Server cannot get any information about the output $f(x)$ from the output $F(\sigma_x)$.

We use the following technique to achieve the requirements. Client randomly selects $r, c, d \in Z_p$, and computes $b_0 = c + a_0$. The coefficients of the disguised polynomial

$$F(\sigma_x) = b_n\sigma_x^n + b_{n-1}\sigma_x^{n-1} + \cdots + b_1\sigma_x + b_0$$

is generated as $b_i = a_i r^i - d^i$, where $0 \le i \le n$.

$F(\sigma_x)$ will be outsourced to cloud server.

4.4. Outsourcing Algorithm

We assume σ_x is an encoded input and σ_y is an encoded output, the polynomial F is a disguised polynomial and we denote g is a generator of the finite field Z_p.

Client wants to computes

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mod p$$

where $f(x)$ is a high degree polynomial.

He/she firstly transforms $f(x)$ into $F(\sigma_x)$ by using the above camouflage technique, and then delegates it to the cloud server. Furthermore, the client can verify the correctness of the result.

Initialization: Client randomly selects six numbers $r, c, d, R, k_0, k_1 \in Z_p$, and then sets $\sigma_x = \frac{x}{r}$. Finally, client generates

$$F(\sigma_x) = b_n\sigma_x^n + b_{n-1}\sigma_x^{n-1} + \cdots + b_1\sigma_x + b_0$$

where

$$b_0 = c + a_0,\ b_1 = a_1 r - d,\ b_2 = a_2 r^2 - d^2, \ldots, b_n = a_n r^n - d^n$$

Then client computes

$$t_0 = g^{k_0 k_1^0 + Rb_0},\ t_1 = g^{k_0 k_1^1 + Rb_1},\ t_2 = g^{k_0 k_1^2 + Rb_2},\ \ldots,\ t_n = g^{k_0 k_1^n + Rb_n}$$

Delegation: We denote $t = (t_0, t_1, \cdots, t_n)$, and $g_i = g^{k_0 k_1^i}$, $0 \le i \le n$. Client sends the polynomial

$$F(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

And

$$t = (t_0, t_1, \ldots, t_n)$$

to the cloud server.

When client wants to compute $f(x)$, client computes $\sigma_x = \frac{x}{r}$ and sends σ_x to cloud server. Then client computes

$$Z = \prod_{i=0}^{n} g_i^{\sigma_x^i} = g^{k_0 \frac{1-(k_1\sigma_x)^{n+1}}{1-k_1\sigma_x}}.$$

Computation: Cloud server computers $\sigma_y = F(\sigma_x)$ and $T = \prod_{i=0}^{n} t_i^{\sigma_x^i}$.

Then cloud server sends (σ_y, T) to the client.

Verification: Client verifies whether following equation holds

$$T = Zg^{R\sigma_y}.$$

If not, the server gives the wrong answer, σ_y is not correct. If the equation holds, client can get the final result by computing

$$y = \sigma_y - \tilde{y}$$

Where

$$\tilde{y} = \sum_{i=1}^{n} d^i \sigma_x^i = \frac{d\sigma_x - (d\sigma_x)^{n+1}}{1 - d\sigma_x} - c$$

5. Security Analysis

Theorem 1. Server cannot get any information about a_i from b_i.

For b_i is generated by a_i, r and d, i.e. $b_i = a_i r^i - d^i$.

Only the value of b_i, $0 \le i \le n$ can be obtained by cloud server.a_i, r and d are unknown to server. If server can get a_i from the following n equations

$$b_0 = c + a_0,\ b_1 = a_1 r - d,\ b_2 = a_2 r^2 - d^2,\ \ldots, b_n = a_n r^n - d^n$$

However, there are only n+1 equations with n+3 unknown variables; the server cannot get a_i from the equations. Thus, server cannot get any information about coefficients a_i of f from the outsourcing polynomial F.

Theorem 2. The input and output of the polynomial are secure.

The real input is x, however, the encrypted input is σ_x, where $\sigma_x = \frac{x}{r}$.

For r is randomly chosen, the input x is keeping privacy.

The output client needs is $y = \sigma_y - \tilde{y}$. Cloud server can get σ_y, however, it cannot get $\tilde{y}$.

For

$$\tilde{y} = \frac{d\sigma_x - (d\sigma_x)^{n+1}}{1 - d\sigma_x} - c$$

where d and c are randomly chosen by the client.

Cloud server can just get σ_x and in the computation process, cloud server cannot get the private parameters d and c from the outsourced polynomial.

Hence, the input and output would not be revealed.

6. Comparison

Our algorithm is the improvement of the algorithm in Benabbas et al. (2011), and we enhanced the security of the input and output privacy. The comparisons between our scheme and some recent schemes are listed in Table 1.

7. Application

In keyword search system, client generates a keyword search token, and sends to the server. The server searches over the

ciphertext database. If there is no corresponding information, the server will return "null" to the client. In most of the existing schemes, the server is assumed to be honest. However, in real word, the server is usually dishonest. So the client has to verify the search results. Verifiable outsourcing of polynomial is a useful technique to verify whether the server searches over the database or just returns "null" without searching. The client can deal with this issue as follows:

We assume there are three parties in the keyword search system, client, Server 1 (verify the search result when Server 2 returns "null") and Server 2 (implement the search work for client).

Client constructs a polynomial with the keywords extracted from the files, which is stored in a database in the form of ciphertexts.

$$f(w) = (w - w_1)(w - w_2)\cdots(w - w_n)$$
$$= a_n w^n + a_{n-1} w^{n-1} + \cdots + a_1 w + a_0 \mod p$$

Then Client randomly selects six numbers $r, c, d, R, k_0, k_1 \in Z_p$, and a generator of the finite field Z_p, g, and then disguises the $f(w)$ as $F(\sigma_w)$

$$F(\sigma_w) = b_n \sigma_w^n + b_{n-1} \sigma_w^{n-1} + \cdots + b_1 \sigma_w + b_0$$

where $b_0 = c + a_0, b_1 = a_1 r - d, b_2 = a_2 r^2 - d^2, \ldots, b_n = a_n r^n - d^n$.

Client computes $t_0 = g^{k_0 k_1^0 + R b_0}, t_1 = g^{k_0 k_1^1 + R b_1}, t_2 = g^{k_0 k_1^2 + R b_2}, \ldots, t_n = g^{k_0 k_1^n + R b_n}$.

And then, the client sends $F(\sigma_w)$ and $t = (t_0, t_1, \cdots, t_n)$ to Server 1 for verification.

Client selects a keyword w_0, and generates the query $Q(w_0)$ and sends to Server 2. Server 2 searches the related files in the database. If there is no related file in the database, it returns "null".

Client then verifies the result. He/she computes $\sigma_w = \frac{w_0}{r}$, and

$$Z = \prod_{i=0}^{n} g_i^{\sigma_w^i} = g^{k_0 \frac{1-(k_1\sigma_w)^{n+1}}{1-k_1\sigma_w}},$$

$$\tilde{y} = \frac{d\sigma_w - (d\sigma_w)^{n+1}}{1 - d\sigma_w} - c$$

And the client sends σ_w to Server 1.

Server 1 computes the outsourced polynomial with σ_w, and returns (σ_y, T) to the client.

Client verifies whether the equation $T = Zg^{R\sigma_y}$ holds or not. If the equation holds, then the client computes $y = \sigma_y - \tilde{y}$.

If $y = 0$, this indicates there is no file related with the keyword w_0. Else, that means Server 2 did not search over the whole ciphertexts.

8. Conclusion

In the era of information explosion, people have to deal with huge amounts of data. It is a great computation burden for the resource-constrained clients. Cloud servers provide a lot of convenience for the resource-constrained clients by sharing the computing resources. Clients can outsource the complex computation task to the powerful cloud servers. In this way, the computation burden of clients can be greatly reduced. In this paper a new algorithm of secure outsourcing for polynomials is proposed. In the computation process, the computation polynomial is disguised to the cloud server, and the inputs and outputs of polynomials will not be revealed. In addition, clients can efficiently verify the computation result. We also give the application of the secure outsourcing algorithm. In the keyword search system, the server who implements the search work is usually assumed to be honest in most of the existing researches. However, it is hard to find an honest cloud server in real word. Thus, we consider the weak scenario. In order to save the computation resource, the cloud server does not implement the search work, and returns the client "null" to show that there is no related file according to the search query. Our application focus on this issue and an efficient verification algorithm is given. The client can easily verify whether the cloud server faithfully implement the search work. Our scheme is practical.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the Fund of Lab of Security Insurance of Cyberspace, Sichuan Province (szjj2016-091); the key laboratory of higher education of Sichuan Province for enterprise informationalization and Internet of things (No.2014WYJ03); the Scientific Research Fund Project of Sichuan Normal University (15YB008) Guangxi Key Laboratory of Cryptography and Information Security (No. GCIS201607).

Notes on Contributors

Jun Ye received a B.S. degree in Applied Mathematics at Chongqing University and an M.S. degree in Cryptography at Guilin University of Electronic Technology. He is a Lecturer in the School of Science, Sichuan University of Science & Engineering. His current research interests include cryptography and information security.

Xianlin Zhou received a B.S. degree in Information and Computing Science at Chongqing University and an M.S. degree in Computer Science at Chongqing University. She is a Lecturer in Collage of Mathematics and Software Science, Sichuan Normal University. Her current research interests include cryptography and information security.

Zheng Xu was born in Shanghai, China. He received diploma and a Ph.D. degree from the School of Computing Engineering and Science, Shanghai University, Shanghai, in 2007 and 2012, respectively. He is currently working in the Third Research Institute of Ministry of Public Security and the postdoctoral in Tsinghua University, China. His current research interests include topic detection and tracking, semantic Web and Web mining. He has authored or co-authored more than 70 publications including IEEE Trans. On Fuzzy Systems, IEEE Trans. On Automation Science and Engineering, IEEE Trans. On Cloud Computing, IEEE Trans. On Emerging Topics in Computing, IEEE Transactions on Systems, Man, and Cybernetics: Systems, etc.

Yong Ding was born in Chongqing, China. He received a Ph.D. degree from the School of Communication Engineering, Xidian University, Shaanxi, in 2005. He is currently professor in Guilin University of Electronic Technology, China. His current research interests include cryptography and information security.

References

Atallah, M.J., & Frikken, K.B. (2010, April). Securely outsourcing linear algebra computations. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security* (pp. 48–59). ACM. DOI:10.1145/1755688.1755695

Atallah, M.J., Pantazopoulos, K.N., Rice, J.R., & Spafford, E.E. (2002). Secure outsourcing of scientific computations. *Advances in Computers, 54*, 215–272. DOI:10.1016/S0065-2458(01)80019-X

Bao, F., Deng, R.H., Ding, X., & Yang, Y. (2008, April). Private query on encrypted data in multi-user settings. In *International Conference on Information Security Practice and Experience* (pp. 71–85). Springer Berlin Heidelberg. DOI:10.1007/978-3-540-79104-1_6

Benabbas, S., Gennaro, R., & Vahlis, Y. (2011, August). Verifiable delegation of computation over large datasets. In *Annual Cryptology Conference* (pp. 111–131). Springer Berlin Heidelberg. DOI:10.1007/978-3-642-22792-9_7

Benjamin, D., & Atallah, M.J. (2008, October). Private and cheating-free outsourcing of algebraic computations. In *Privacy, Security and Trust, 2008. PST'08. Sixth Annual Conference on* (pp. 240–245). IEEE. DOI:10.1109/PST.2008.12

Chai, Q., & Gong, G. (2012, June). Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers. In *2012 IEEE International Conference on Communications (ICC)* (pp. 917–922). IEEE. DOI:10.1109/ICC.2012.6364125

Chang, Y.C., & Mitzenmacher, M. (2005, June). Privacy preserving keyword searches on remote encrypted data. In *International Conference on Applied Cryptography and Network Security* (pp. 442–455). Springer Berlin Heidelberg. DOI:10.1007/11496137_30

Curtmola, R., Garay, J., Kamara, S., & Ostrovsky, R. (2006, November). Searchable symmetric encryption: Improved definitions and efficient constructions. *Proceedings of the 13th ACM conference on Computer and communications security, CCS '06, ACM* (pp. 79–88). DOI:10.1145/1180405.1180417

Fiore, D., & Gennaro, R. (2012, October). Publicly verifiable delegation of large polynomials and matrix computations, with applications. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 501–512). ACM. DOI:10.1145/2382196.2382250

Gennaro, R., Gentry, C., & Parno, B. (2010, August). Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In *Annual Cryptology Conference* (pp. 465–482). Springer Berlin Heidelberg. DOI:10.1007/978-3-642-14623-7_25

Hohenberger, S., & Lysyanskaya, A. (2005, February). How to securely outsource cryptographic computations. In *Theory of Cryptography Conference* (pp. 264–282). Springer Berlin Heidelberg. DOI:10.1007/978-3-540-30576-7_15

Hu, C., Xu, Z., Liu, Y., Mei, L., Chen, L., & Luo, X. (2014). Semantic link network-based model for organizing multimedia big data. *IEEE Transactions on Emerging Topics in Computing, 2*, 376–387. DOI:10.1109/TETC.2014.2316525

Song, D.X., Wagner, D., & Perrig, A. (2000). Practical techniques for searches on encrypted data. In *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on* (pp. 44–55). IEEE. DOI:10.1109/SECPRI.2000.848445

Xu, Z., Liu, Y., Yen, N., Mei, L., Luo, X., Wei, X., & Hu, C. (2016a). Crowdsourcing based description of urban emergency events using social media big data. *IEEE Transactions on Cloud Computing, 2016*, DOI:10.1109/TCC.2016.2517638

Xu, Z., Zhang, H., Hu, C., Mei, L., Xuan, J., Raymond Choo, K.-K., ... Zhu, Y. (2016b). Building knowledge base of urban emergency events based on crowdsourcing of social media. *Concurrency and Computation: Practice and Experience, 28*, 4038–4052. DOI:10.1002/cpe.3780

Xu, Z., Zhang, H., Sugumaran, V., Raymond Choo, K.-K., Mei, L., & Zhu, Y. (2016c). Participatory sensing-based semantic and spatial analysis of urban emergency events using mobile social media. *EURASIP J. Wireless Comm. and Networking, 2016*, 44. DOI:10.1186/s13638-016-0553-0

Xu, Z., Wei, X., Liu, Y., Mei, L., Hu, C., Raymond Choo, K.-K., ... Sugumaran, V. (2016d). Building the search pattern of web users using conceptual semantic space model. *International Journal of Web and Grid Services, 12*, 328–347. DOI: 10.1504/IJWGS.2016.079158

Ye, J., Wang, J., Zhao, J., Shen, J., & Li, K.C. (2016). Fine-grained searchable encryption in multi-user setting. *Soft Computing*, 1–12. DOI:10.1007/s00500-016-2179-x

Ye, J., Xu, Z., & Ding, Y. (2016). Secure outsourcing of modular exponentiations in cloud and cluster computing. *Cluster Computing, 19*, 811–820. DOI:10.1007/s10586-016-0571-z

Ye, J., Zhang, H., & Fu, C. (2016). Verifiable delegation of polynomials. *Int. J. Netw. Secur, 18*, 283–290.Retrieved from http://ijns.jalaxy.com.tw/contents/ijns-v18-n2/ijns-2016-v18-n2-p283-290.pdf

Zhao, F., Nishide, T., & Sakurai, K. (2011, November). Multi-user keyword search scheme for secure data sharing with fine-grained access control. In *International Conference on Information Security and Cryptology* (pp. 406–418). Springer Berlin Heidelberg. DOI:10.1007/978-3-642-31912-9_27

Zheng, Q., Xu, S., & Ateniese, G. (2014, April). VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications* (pp. 522–530). IEEE. DOI:10.1109/INFOCOM.2014.6847976

Zhou, X., Ding, Y., Wang, Z., Li, X., Xu, Z., & Ye, J. (2016, July). Secure Outsourcing Algorithm of Polynomials in Cloud Computing. *Proc. of 28th International Conference on Software Engineering and Knowledge Engineering, July 1-3, Redwood City, San Francisco Bay, California, USA*. DOI:10.18293/SEKE2016-022