International Journal of Future Generation Communication and Networking
Vol. 9, No. 7 (2016), pp. 269-278
http://dx.doi.org/10.14257/ijfgcn.2016.9.7.25

Towards an Analysis of Verifiable Mix Network Properties

Tianbo Lu[1] , Jiaxi Lin[1], Xiaofeng Du[2], Yang Li[1]

[1]*School of Software Engineering, Beijing University of Posts and Telecommunications, 100876, Beijing, China*
[2]*School of Computer Science, Beijing University of Posts and Telecommunications, 100876, Beijing, China*
lutb@bupt.edu.cn, linjx0515@gmail.com

Abstract

With the development of mix-net, the basic properties of mix-net cannot satisfy all the requirements of people. The verifiable mix-net raised in response to the proper time and conditions. In this paper, we study the problem of simultaneously achieving several security properties, for mix-nets and verifiability mix-nets. More precisely, under different assumptions and requirements, verifiability mix-nets have more extra security properties than mix-nets. The basic properties of mix-nets contain correctness, privacy, robustness, availability and efficient. The extra properties of verifiability mix-nets contain universal verifiability, unconditional anonymous, receipt-freeness. This paper summarizes all of the security properties, and defines them explicitly and systematically.

Keywords*: verifiability; mix-nets; security properties*

1. Introduction

In 1981, in order to achieve anonymous, Chaum introduced the concept of a mix-net [Chaum]. A mix-net consists of a sequence of servers, called mixes. Each server receives a batch of input messages and produces as output the batch in mixed order. Such mix-nets are sometimes called mix cascades or shuffle networks. In the mix-nets, the correspondences between the items in its input and those in its output are hidden. In Chaum's original proposal, before a message is sent through the mix-nets, it is first successively encrypted with the public keys of the mixes it will traverse in reverse order; each mix then decrypts each message before sending it on the next mix.

Informally the basic properties of mix-net require: correctness, privacy, robustness, availability and efficiency. Correctness means that the mix result is correct due to all honest mix-centers. Privacy means that if some conditions are fulfilled, anonymity of the sender of a message is ensured. Robustness means that if some conditions are fulfilled, any attempt to cheat is detect and defeated. Availability and efficiency are the general requirement on any system run on an open network.

Apart from these properties, verifiability mix-net possesses some other extra properties: universal verifiability, unconditional anonymous, receipt-freeness. Universal verifiability means universally checking the validity and the correction of the result of mix. Unconditional anonymous means that after mix, nobody can learn any additional information. Receipt-freeness means that one cannot provide a proof of its mix to a third party.

In this paper, we address this question: can we summarize these properties and define them in a systematical way? More precisely, on the one hand each of properties has a variety of relationships. On the other hand, some of properties condition each other. In both case, obviously, properties of mix-net should not been merely introduced. However, we have to systematically define them in the view of relations of each other's.

ISSN: 2233-7857 IJFGCN

The organization of the paper is as follows. In section 2, we recall Chaum's work. Section 3 gives definitions of the properties of mix-net. The next section shows the relationships of them. Section 5 concludes the paper.

2. Background

In 1981, Chaum first formally put forward the concept of mix, a cryptographic laundering technique for preventing traffic analysis of electronic mail, providing unlink ability between sender and receiver. Nowadays, mix has been used as a universal anonymous technology of communication.

The basic idea of mix is the permutation and the shuffle of messages from multi participants by using mix server. In this way, eavesdropper cannot determine input/output relations so that is not able to trace entire path of the message.

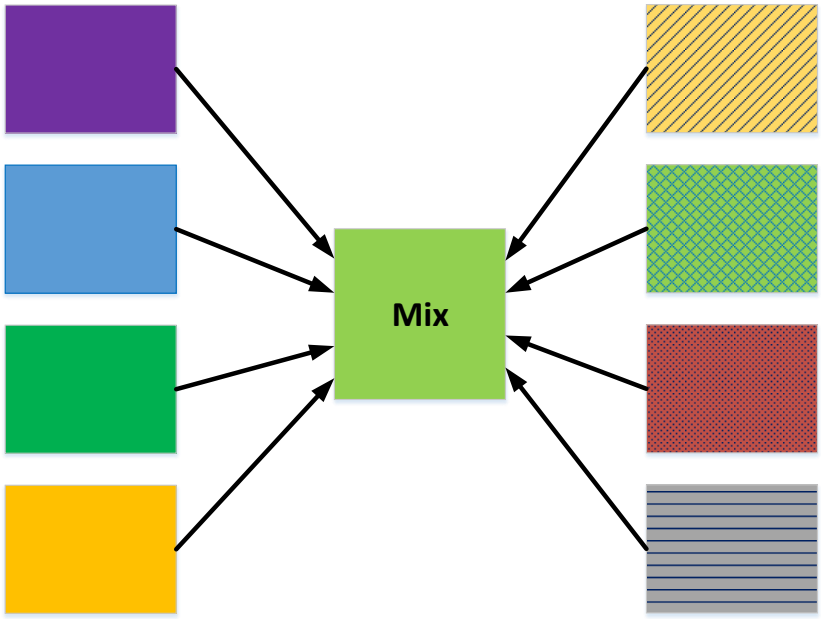


Figure 1. A Mix Server

A mix server is a computer which is used for storing and forwarding messages, as shown in figure 1. It accepts fixed-length message from different sources then encrypts, permutes and transmits them for the purpose of hiding the relations between inputs and outputs. A mix server makes attackers difficult to trace any specific messages only based on the coding, size or sorting of the message. If messages are transmitted through several mix servers in the mix net (as shown in Figure 2), the anonymity is satisfied with one or more mix server being honest. Let's simply introduce the principles of mix.

Participants should determine a path before transmitting message, and obtain the public keys of the entire mix server in the path. Then construct:

$M_0=K_0(R_0,M)$;

$M_1=K_1(R_1,M_0,A_0)$;

$M_2=K_2(R_2,M_1,A_1)$;

……

$M_n=K_n(R_n,M_{n-1},A_{n-1};)$;

Here, K_n to K_1 are the public keys of mix servers in the path of participant to receiver, and A_i is an address, R_i is a random filter, subscript represents the final receiver.

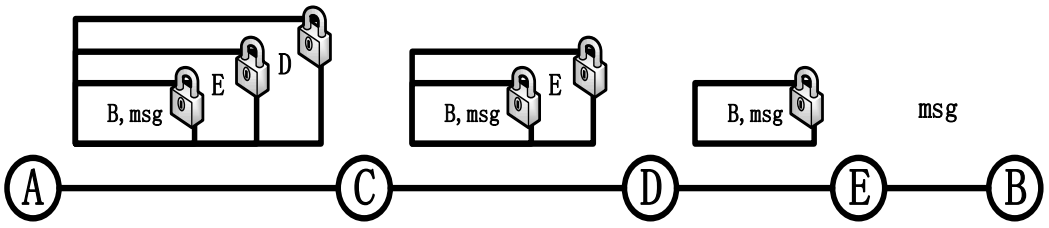


Figure 2. Messages are transmitted through Several Mix Servers in the Mix Net

Message M_n is posted to the first mix server, which uses private key to encrypt it and send message $M_{n-1}$to the mix server A_{n-1} signed to; this process is performed by mix servers which receive message, until receiver A_0 obtains message M. This kind of encryption (decryption) method in mix is called multi-layer encryption (decryption). Obviously, without obtaining Ki, people cannot discover the relations between M_i and M_{i-1}.

As we known, after that, the technology of mix develops very rapidly in the following years. In the meantime, more and more requirements of properties are put forward for the purpose of improving the performance of mix. In the following, we will discuss all the properties in the mix-net and the verifiable mix-net.

3. Basic Properties

The mixnet properties are determined by the requirements of the applications of various schemes. However, no matter what kind of schemes, basic properties of mix must to be provided. The basic properties can be listed as follows.

3.1. Correctness

Jun Furukawa and Kazue Sako in [1] considered the correctness that the result is correct given that all mix-center are honest.

Jakobsson M, Juels A, Rivest R L thought that in the mix-net, the output should correspond to a permutation of the input [2].

Golle P, Jakobsson M, Juels A considered mix-net is correct if the set of outputs it produces is a permutation of the set of inputs [3].

Golle P, Wang X F, Jakobsson M held the view that a mix server mixes a batch of inputs correctly, which is correctness [4].

Peng K, Boyd C, Dawson E D, *et al* thought that if the outputs are a permutation of the plaintexts of the inputs, the property is correctness [5].

For proving correctness, it is necessary to show that the mixes did not change any of the messages [10].

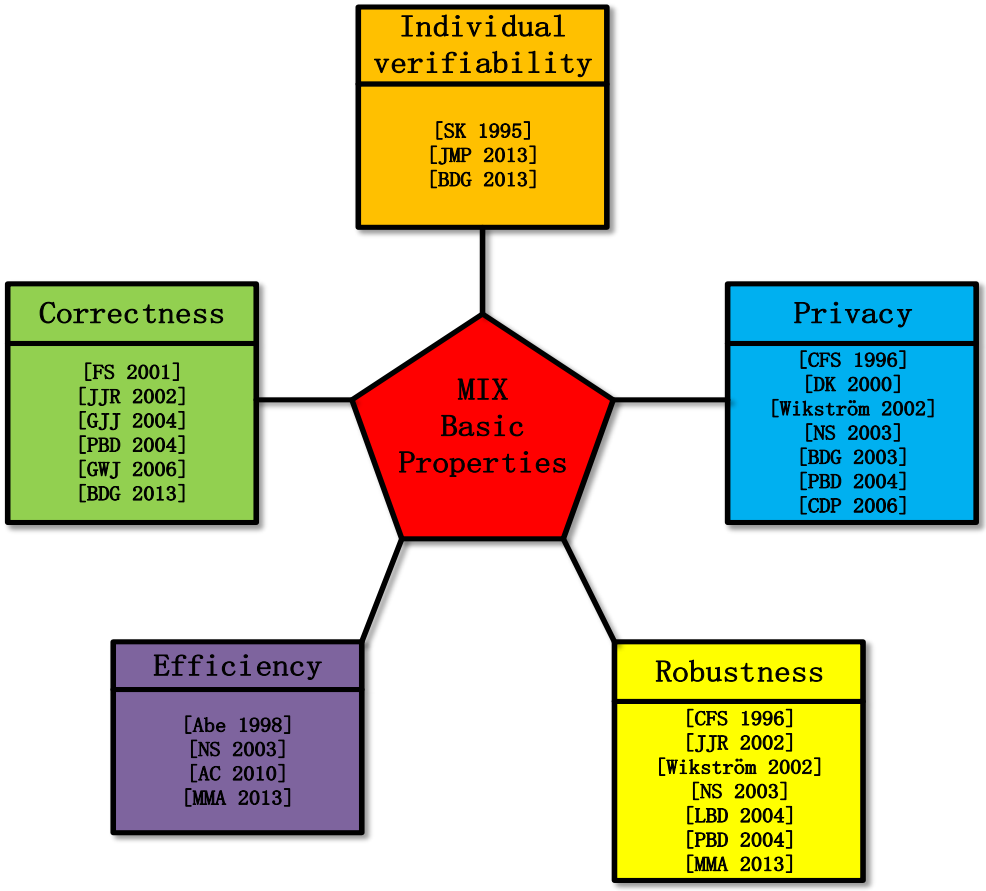


Figure 3. Main Universities and Institutes Studying of Mix Basic Properties

3.2. Privacy

Privacy ensures that an individual participant will be kept secret from any (reasonably sized) coalition of parties that does not include the participant herself [17].

Desmedt Y, Kurosawa K thought privacy is satisfied if the relationship between outputs and inputs is kept secret [7].

Jakobsson M, Juels A, Rivest R L [2] considered privacy is provided if an observer should not be able to determine which input element corresponds to a given output element (and vice versa) in any way better than guessing.

In [9], Privacy implies that if a fixed minimum number of mix-centers are honest anonymity of the sender of a message is ensured.

In [6], privacy means that it is infeasible for the adversary to output a pair of input and the corresponding output of an honest user with probability significantly greater than random guess.

Peng K, Boyd C, Dawson E D, *et al*thought that the privacy is the permutation between the outputs and the inputs being unknown [5].

In [29], privacy means that nobody should learn more information than what is leaked by the tally.

If at least one mix is honest and keeps the used permutation secret, then privacy follows from the fact that the output batch is an unknown permutation of the input batch [10].

3.3. Robustness

Robustness ensures that the system can recover from the faulty behavior of any (reasonably sized) coalition of parties [17].

Robustness implies that if a fixed number of mix-centers are honest, then any attempt to cheat is detected and defeated [9].

In [2], robust is providing a proof or at least strong evidence that it has operated correctly.

In [6], robustness is ensuring that the probability of producing incorrect output is negligibly less than 1. Robustness also means that the mix-net is able to operate correctly regardless of component failure.

Peng K, Boyd C, Dawson E D, *et al* [5] considered that a mix network achieves robustness if it can still work properly in abnormal situations, such as failure of one or more switching nodes in mix-net.

Robustness ensures that the system can tolerate a certain number of faulty participants [12].

Golle P, Wang X F, Jakobsson M, et [4] al hold the view that robustness primarily refers to systems in which each mix is asked to provide a proof or strong evidence for its honest behavior.

Mursi M F M, Assassa G M R, Abdelhafez A, *et al* [11] thought that being successful regardless of partial failure of the system is robustness

3.4. Individual Verifiability

Before [16], many schemes have been proposed based on Chaum's work have only individual verifiability. Individual verifiability ensures that a participant can verify that her mix result correctly.

In [13], individual verifiability is defined that a participant can verify that the result containing her deed is in the published set of "all" (as claimed by the system).

Individual verifiability follows, simply because the fact that the users can check that their input is published [10].

3.5. Efficiency

Abe M considered efficiency is based on computational cost, throughput, and communication complexity [14].

In other words, the work done by a verifier is independent of the number of the number of mix servers. The computation work done by each server is independent of the number of servers except some negligible ones like addition [14].

Nguyen L and Safavi-Naini R considered that efficiency is measured in terms of the computation and communication costs of participants [6].

Allepuz J P, Castelló S G held the view that efficiency is reducing the amount of cryptographic operations required to generate and verify the cryptographic proofs [15].

Mursi M F M, Assassa G M R and Abdelhafez A thought that efficiency focuses on avoiding too many steps to reach mix efficiency for participants [28]. The definition of efficiency is that the whole mix can be held in a timely manner, for instance, all computations are done in a reasonable amount of time and participants are not required to wait for others to complete the process.

4. Extra Properties in Verifiable Mix

The verifiable mix used to address the more higher-requirement properties in the mixnet determine the performance of the mixnet. The extra properties in verifiable can be listed as follows.

4.1. Universal Verifiability

Universal verifiability was first proposed by Sako K and Kilian J [16]. By universally verifiable they mean that in the course of the protocol the participants broadcast information that allows interested third party to at a later time verify that the mix result was properly performed.

Universal verifiability (first recognised explicit by Sako and Kilian [16]) ensures that any observer (who may be a participant) can verify that the result is a correct reflection of the set of mix.

Universal verifiability ensures that any party, including a passive observer, can convince herself that the mix result is correct, i.e., that the published final result is performed correctly [17].

Abe thought that universal verifiability means that correctness of the result of mix is verifiable for any verifiers [14].

Nguyen L, Safavi-Naini R [6] said that verifiability means that the correctness of mix-net operation can be verified by any system participant. If a set of participating mix servers produce an output different from the one prescribed by the protocol, then the verification will be able to establish this fact and reveal the identities of the cheating servers. If verification only uses publicly available information of the mix-net, the mixnet is called universally verifiable.

Universal verifiability is focused on providing means for any auditor or observer to verify the correct decryption of the votes, using cryptographic proofs that are generated by the decryption process [15].

In [13], universal verifiability is defined that anyone can verify that the result corresponds with the published set of "all".

4.2. Unconditional Anonymity

By unconditional anonymity, Chevallier-Mames B, Fouque P A, Pointcheval D, *et al* meant that nobody should be able to learn any additional information even several centuries after the mix process [8].

Buchmann J, Demirel D, van de Graaf J thought that a computationally unbounded attacker cannot obtain any additional information, since the commitments used to encode the messages are unconditional and all used proofs provide perfect zero-knowledge, which satisfied unconditional anonymity [10].

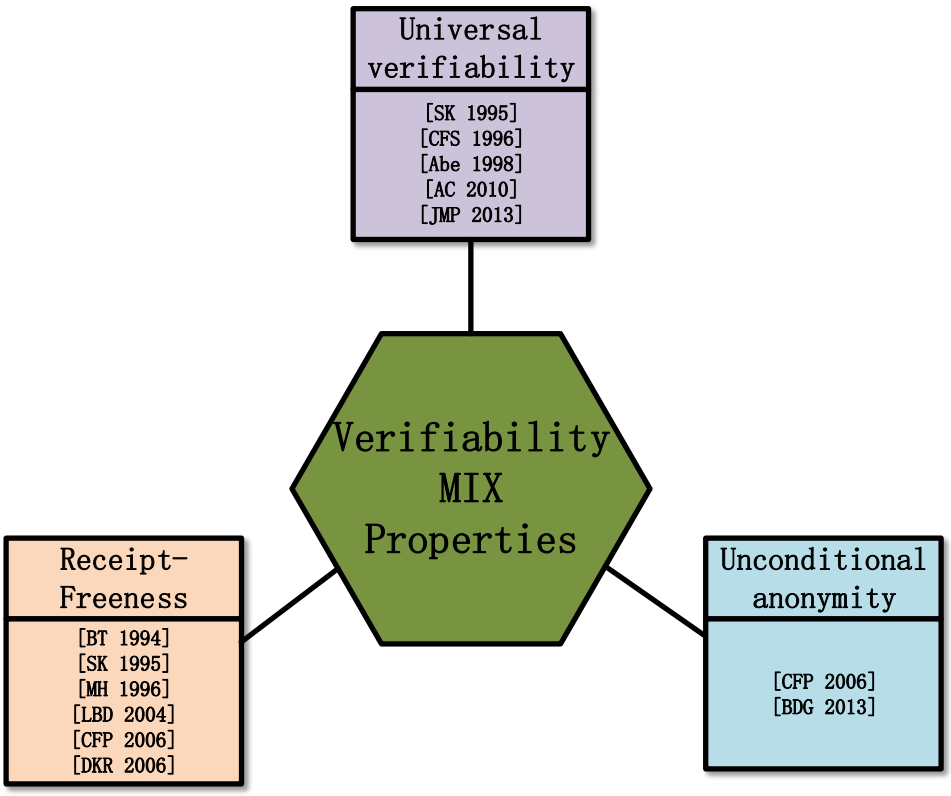


Figure 4. Main Universities and Institutes Studying of Verifiability Mix Properties

4.3. Receipt-Freeness

Benaloh and Tuinstra [18] observed that, nearly all electronic protocols give the participants a receipt by which they can prove how they participated. Such receipts provide a ready means by which participants can sell their participation right or another party can coerce a participant.

[16] presented a receipt-free scheme based on a mix-type anonymous channel [Chaum]. The receipt-freeness property enables participants to hide how they participated even from a powerful adversary who is trying to coerce him.

Michels M and Horster P thought that a participant can't prove to a coercer how he participated, which is receipt-freeness. As a result, verifiable vote buy is impossible [19].

Ensures that a participant neither obtains nor is able to construct a receipt which can prove the content of his perform [12].

In [8], the receipt-freeness property means that a participant cannot produce a proof of his participation to a third party.

A participant does not gain any information (a receipt) which can be used to prove to a coercer that she performed in a certain way [25].

5. Relationship among the Properties

5.1. Resilience

A mix-net that provides privacy, robustness and verifiability is called resilient [26], which is resilient if it satisfies privacy, robustness and verifiability [6].

Amongst these is the concept of resilience which involves the properties of verifiability, privacy, and robustness [27].

5.2. Universal Resilience

A resilient mix-net is universally resilient if it is universally verifiable [6].

5.3. Privacy and unconditional anonymity

In some literatures [8] [23] [20] [21] [22], privacy is often regarded as anonymous. Some others distinguished privacy and anonymity without presented each of their definitions and differences. And even the other literatures anonymity is owned to privacy [24].

In general, we think that both of privacy and anonymous are extremely similar, even actually same. We are not able to distinguish them due to their definitions.

However, the property of unconditional anonymity is on the deeper level than privacy.

5.4. Correctness and Verifiability

No matter individual verifiability or universal verifiability, the purpose of the both properties is to verify the correctness of the mix result. [16][17][14][15] obviously refer to this kind of relationship.

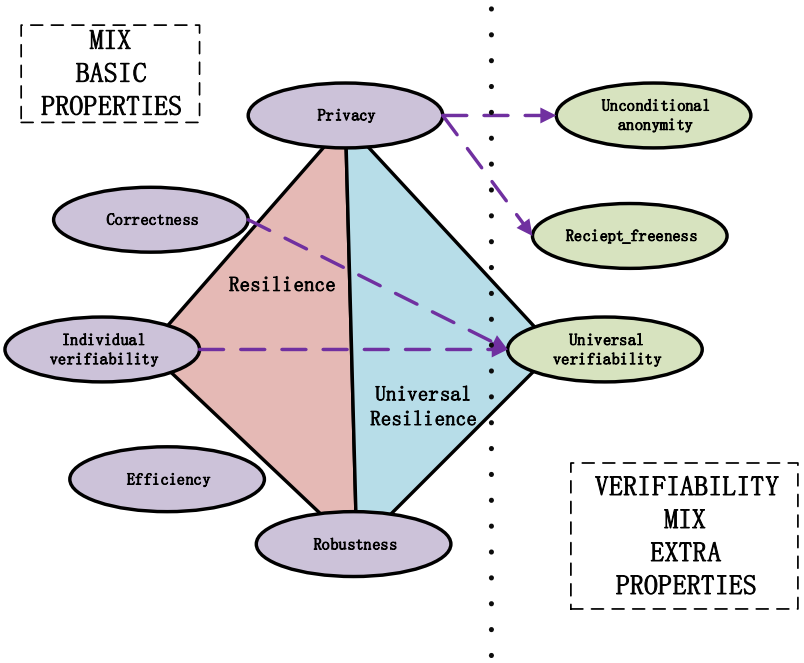


Figure 5. Relationship among the Properties

5.4. Individual Verifiability and Universal Verifiability

In terms of the definitions of verifiability, individual verifiability and universal verifiability have different subjects. By individual verifiability, the participant should be the only one who can check the correctness of her result. But by the universal verifiability, any participants or interested third parties are able to verify the result correctly. In fact, universal verifiability requires higher technique than individual.

5.5. Privacy and Reciept-freeness

The privacy property guarantees that the link between a participant and her perform remains secret. Receipt-freeness guarantees that anyone cannot become

convinced of how a participant deed in a certain way in the process of mix, even if the participant cooperates with him. It is intuitively that receipt-freeness is stronger than privacy, since that privacy is very possible for the participants' cooperation.

6. Conclusion

With the rapid development, mix has been an efficient anonymous technology of communications. As a means of protecting privacy of users, it hides relations between sender and receiver in communications, which makes attackers cannot obtain the relation and the identifications of either sender or receiver. In the past, some basic properties, such as correctness, privacy, robustness, individual verifiability and efficiency, can satisfy people's requirements. However, people's requirements will become more and more, then universal verifiability mix rises in response to the proper time and conditions, which can afford more excellent properties which contain universal verifiability, unconditional anonymity and receipt-freeness. Our paper also presents the relations in all the properties.

Acknowledgements

This work is supported by the following programs: the National Natural Science Foundation of China under Grant No.61170273; 2010 Information Security Program of China National Development and Reform Commission with the title "Testing Usability and Security of Network Service Software".

References

[1] J. Furukawa and K. Sako, "An efficient scheme for proving a shuffle", Advances in Cryptology—CRYPTO 2001, Springer Berlin Heidelberg, **(2001)**, pp. 368-387.
[2] M. Jakobsson, A. Juels and R. L. Rivest, "Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking", USENIX security symposium, **(2002)**, pp. 339-353.
[3] P. Golle, M. Jakobsson and A. Juels, "Universal re-encryption for mixnets", Topics in Cryptology–CT-RSA 2004, Springer Berlin Heidelberg, **(2004)**, pp. 163-178.
[4] P. Golle, X. F. Wang and M. Jakobsson, "Deterring voluntary trace disclosure in re-encryption mix networks", Security and Privacy, 2006 IEEE Symposium on. IEEE, **(2006)**, 11 pp. 11-131.
[5] K. Peng, C. Boyd and E. D. Dawson, "A correct, private, and efficient mix network", Public Key Cryptography–PKC 2004, Springer Berlin Heidelberg, **(2004)**, pp. 439-454.
[6] L. Nguyen and R. S. Naini, "Breaking and mending resilient mix-nets", Privacy Enhancing Technologies, Springer Berlin Heidelberg, **(2003)**, pp. 66-80.
[7] Y. Desmedt and K. Kurosawa, "How to break a practical mix and design a new one", Advances in Cryptology—EUROCRYPT 2000. Springer Berlin Heidelberg, **(2000)**, pp. 557-572.
[8] B. C. Mames, P. A. Fouque and D. Pointcheval, "On some incompatible properties of voting schemes", In IAVoSS Workshop On Trustworthy Elections, WOTE'06, **(2006)**.
[9] D. Wikström, "The security of a mix-center based on a semantically secure cryptosystem", Progress in Cryptology—INDOCRYPT 2002, Springer Berlin Heidelberg, **(2002)**, pp. 36-31.
[10] J. Buchmann, D. Demirel, J. V. D. Graaf, "Towards a publicly-verifiable mix-net providing everlasting privacy", Financial Cryptography and Data Security, Springer Berlin Heidelberg, **(2003)**, pp. 197-204.
[11] M. F. M. Mursi, G. M. R. Assassa, A. Abdelhafez, "On the Development of Electronic Voting: A Survey", International Journal of Computer Applications, vol. 61, no. 16, **(2013)**, pp. 1-11.
[12] B. Lee, C. Boyd and E. Dawson, "Providing receipt-freeness in mixnet-based voting protocols", Information Security and Cryptology-ICISC 2003, Springer Berlin Heidelberg, **(2004)**, pp. 245-25.
[13] H. Jonker, S. Mauw and J. Pang, "Privacy and verifiability in voting systems: Methods, developments and trends", Computer Science Review, vol. 10, **(2013)**, pp. 1-30.
[14] M. Abe, "Universally verifiable mix-net with verification work independent of the number of mix-servers", Advances in Cryptology—EUROCRYPT'99, Springer Berlin Heidelberg, vol. 199, pp. 437-447.
[15] J. P. Allepuz and S. G. Castelló, "Universally verifiable efficient re-encryption mixnet", Electronic Voting, vol. 167, **(2010)**, 241-254.
[16] K. Sako and J. Kilian, "Receipt-free mix-type voting scheme", Advances in Cryptology—EUROCRYPT'95, Springer Berlin Heidelberg, **(1995)**, pp. 393-403.
[17] R. Cramer, M. Franklin and B. Schoenmakers, "Multi-authority secret-ballot elections with linear work", Advances in Cryptology—EUROCRYPT'96, Springer Berlin Heidelberg, **(1996)**, pp. 72-3.

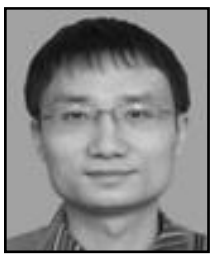
[18] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections", Proceedings of the twenty-sixth annual ACM symposium on Theory of computing, ACM, **(1994)**, pp. 544-553.
[19] M. Michels and P. Horster, "Some remarks on a receipt-free and universally verifiable mix-type voting scheme", Advances in Cryptology—ASIACRYPT'96, Springer Berlin Heidelberg, **(1996)**, pp. 125-132.
[20] M. Smart and E. Ritter, "Remote electronic voting with revocable anonymity", Information Systems Security, Springer Berlin Heidelberg, **(2009)**, pp. 39-54.
[21] J. Crowcroft and I. Pratt, "Peer to Peer: peering into the future", Advanced lectures on networking, Springer Berlin Heidelberg, **(2002)**, pp. 1-19.
[22] S. Valsamidis, A. Mandilas and S. Kontogiannis, "ELAN, an alternative approach to e-voting systems, focused on elections data analysis", MIBES) 2011 International Conference, **(2011)**, pp. 1-21.
[23] D. Kesdogan and C. Palmer, "Technical challenges of network anonymity", Computer Communications, vol. 29, no. 3, **(2006)**, pp. 306-324.
[24] A. F. N. A. Shammari and A. Villafiorita, "A Synthesis of Vote Verification Methods in Electronic Voting Systems", Design, Development, and Use of Secure Electronic Voting Systems, **(2014)**, p. 92.
[25] S. Delaune, S. Kremer and M. Ryan, "Coercion-resistance and receipt-freeness in electronic voting", Computer Security Foundations Workshop, 19th IEEE, **(2006)**, pp. 12-42.
[26] Y. Desmedt and K. Kurosawa, "How to break a practical mix and design a new one", Advances in Cryptology—EUROCRYPT 2000, Springer Berlin Heidelberg, **(2000)**, pp. 557-572.
[27] J. A. Vaccaro, J. Spring and A. Chefles, "Quantum protocols for anonymous voting and surveying", Physical Review A, vol. 75, no. 1, **(2007)**.
[28] M. F. M. Mursi, G. M. R. Assassa and A. Abdelhafez, "On the Development of Electronic Voting: A Survey", International Journal of Computer Applications, vol. 61, no. 16, **(2013)**, pp. 1-11.
[29] B. C. Mames, P. A. Fouque and D. Pointcheval, "On some incompatible properties of voting schemes", In IAVoSS Workshop On Trustworthy Elections, WOTE'06, **(2006)**.

Authors

Tian-Bo Lu, he was born in Guizhou Province, China, 1977. He is an Associate professor in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information security and computer network.

Jia-Xi Lin, he was born in Inner Mongolia, China, 1989. He is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information and network security, anonymous communication.

Xiao-feng Du, he was born in Shaanxi Province, China, 1973.He is a Lecturer in School of Computer, Beijing University of Posts and Telecommunications, China. His technical interests include information security and computer network.



Yang Li, he was born in Hunan Province, China, 1978. He is a PhD and his technical interests include information security, distributed computing and P2P network.

