pISSN 1976-913X
eISSN 2092-805X

A Secure Network for Mobile Wireless Service

Kun Peng*

Abstract—A new secure network communication technique that has been designed for mobile wireless services, is presented in this paper. Its network services are mobile, distributed, seamless, and secure. We focus on the security of the scheme and achieve anonymity and reliability by using cryptographic techniques like blind signature and the electronic coin. The question we address in this paper is, "What is the best way to protect the privacy and anonymity of users of mobile wireless networks, especially in practical applications like e-commerce?" The new scheme is a flexible solution that answers this question. It efficiently protects user's privacy and anonymity in mobile wireless networks and supports various applications. It is employed to implement a secure e-auction as an example, in order to show its advantages in practical network applications.

Keywords—Mobile Wireless Network, Security

1. INTRODUCTION

The mobile wireless network is becoming more and more popular nowdays. We are especially interested in a special kind of wireless network—an ad hoc network. As demonstrated in [3], an ad hoc network has its advantages and we will demonstrate that it is suitable for network applications with security requirements like e-auctions and e-finance. In these applications, the users want to be anonymous and the services should be reliable. The properties listed below are usually desired in the applications for mobile wireless networks.

- Mobility: the network services are not limited to fixed locations, but are instead provided dynamically.
- Distribution: there is not a service center and distributed network structure like an ad-hoc network.
- Reliability: the users can be guaranteed with a large probability that the network providers will properly handle their applications.
- Anonymity: unlinkability between the users and their activities is guaranteed.
- Flexibility: various applications are supported.

Our motivation in this paper is to design a network scheme to satisfy these properties. We are especially interested in how to protect the privacy and anonymity of the users of mobile wireless networks, especially in practical applications like e-commerce. To achieve anonymity, the users' communication should be sealed and transferred in a random path that is difficult to trace. This

Manuscript received October 29, 2012; first revision January 28, 2013; accepted March 11, 2013.
Corresponding Author: Kun Peng
* Institute for Inforcomm Research, Singapore (dr.kun.peng@gmail.com)

method is general and flexible, but it also has its own issue in that the implementation of the anonymous communication network in a static network is inefficient. As it is easy to trace a message and find the IP address of a sender in a static communication network like the Internet and since universal verifiability is required for this method, costly operations like a mix network [1, 14, 17, 18, 23, 24, 26, 28, 30] or onion routing [5, 13, 15, 16] must be performed to implement anonymous communication.

Kesdogana and Palme [19] defined and classified privacy and anonymity from a technical angle as follows:

- Anonymity is the state of not being identifiable within a set of subjects that are known as the anonymity set. Anonymity in communications can be further distinguished as sender and recipient anonymity.
- Unobservability is the state of an item of interest being indistinguishable from any other item of interest.
- Unlinkability of two or more items or actions means that these items are no more and no less related than they were previously (attacker gains no information).

Unobservability can be reduced to a set of data items, senders, or receivers. For example, a concrete requirement for messages is that each message cannot be linked to any potential sender or receiver from the set. At a higher level, relationship unobservability requires that it is not discernable whether anything is being sent from a set of potential senders to a set of potential recipients. The definition of anonymity is incomplete if an attacker model (opponent model) is not specified. The attacker model describes the demands placed on the anonymity techniques and is also for the evaluation and comparison of the proposed solutions. In general, a direct relationship exists between the strength of the attacker model and the quality of the protection provided by a given solution. To guarantee formal and reliable anonymity, it is necessary to assume that anonymity is to be provided in the presence of a powerful attacker. Thus, the capabilities of attacker ***A*** may vary. For the sake of simplicity, it is assumed here that the cryptography used is unbreakable. However, it is good to keep in mind that it is inappropriate to provide or demand more anonymity protection than the underlying cryptography can provide. Attackers may be classified as described below, according to [19].

- A1. Passive attacker. An attacker who can observe all communication links.
- A2. A passive attacker with sending capabilities. The A2 attacker is not much stronger than A1, yet the A2 attacker poses a bigger threat than A3 because they are by definition—undetectable. An attacker may take part in the anonymity technique (i.e., the attacker can send a messages) if participation has not been explicitly forbidden to him.
- A3. Active attacker. This is an attacker who can control all communication links, switches, etc. and can attack all messages with delete, replay, and send, or delay actions.

We believe that a better method to implement anonymity in the security model defined above is to replace the static network with a mobile wireless ad hoc network. We adopted an attacker model between A2 and A3, where an attacker can only at most compromise the *n-1* of all the *n* routing nodes in our network. The proposed scheme employs an anonymous mobile communication network. More precisely, its anonymous communication network is a mobile ad hoc network instead of a static network in most other solutions. In a mobile ad hoc network, the participants (nodes in the network) are moving and the connections are dynamic, so it is impossible to identify a sender by tracing their message to their location. Therefore, anonymous communication is implemented if the participants use pseudonyms and conceals their identities. Costly operations like shuffling [1, 14, 17, 18, 23, 24, 26, 28, 30] or onion routing [5, 13, 15, 16] are not needed and higher efficiency can be achieved. The users' pseudonyms are authorised by a registration authority using blind signature techniques such that the users can sign their messages to protect the messages' integrity while their identities are not revealed from their signatures.

It should be noted that using blind-signature-based pseudonyms to implement anonymity is not a new idea and has been employed in schemes like [10]. However, its application in static networks is complex and inefficient. In a static network, the users are identified if their messages are traced and their static locations are found. So, in a static network, even if the users use pseudonyms, an anonymous communication channel still must be employed to prevent tracing and to protect the users' anonymity. Therefore, an inefficient anonymous communication network is still needed for anonymity in static networks. Normally, operations in an anonymous communication network must be publicly and instantly verified. As a result, it becomes very costly for computation and communication. In contrast, when applied to mobile ad hoc network, this technique does not have any additional requirements in network communication and thus, is very efficient.

Although anonymity is efficiently achieved in the mobile ad hoc network, there is another challenge of how to guarantee that no message is discarded in the mobile ad hoc network. Namely, the reliability of network services must be guaranteed. Our solution to this new challenge is the electronic coin. An electronic coin based stimulation mechanism is employed to award the nodes for their work in the mobile ad hoc network and to guarantee that the nodes will not discard the messages.

Our contribution is clear, which is that a new communication network has been designed based on an ad hoc network to efficiently achieve security properties like privacy and anonymity. At the end of this paper, the new mobile wireless network scheme is employed in an e-auction. This example demonstrates its advantages in practical network applications.

2. Symbols and Preliminary Primitives

The following symbols are used in this paper:

- $E_k(m)$ stands for the encryption of message m using key k.
- $D_k(c)$ stands for the decryption of ciphertext c using key k.
- $S_k(m)$ stands for the signature on message m using key k. It includes the message and the signature on it.

Preliminary primitives to be employed in the new mobile wireless network scheme are described in the sections below.

2.1 Blind Signature

In a blind signature scheme [6-8], a signer signs an unknown message. Even after the signature is generated, the signer still has no idea about the message he has signed. A well-known RSA based blind signature [7] is described below as an example. In the example, the signer signs m for a message he does not know.

1. p and q are large primes with similar size. $N = pq$ is published while p and q are kept secret. The public key is e in Z_N and the private key is d such that $ed = 1 \bmod \phi(N)$.
2. The message m is supposed to be signed. The random integer r is chosen from Z_N and $m' = mr^e \bmod N$ is sent to the signer, who holds d.
3. The signer feeds back $s' = m'^d \bmod N$.
4. From the s' signature on m: $s = s'/r \bmod N$ can be extracted.

In this paper, each user chooses a private key and makes an authority to blindly sign a public key certificate, which includes the corresponding public key but does not include the identity of the user. Therefore, the user can sign his message as a party authenticated by the authority, while his identity is not revealed from his signature. In other words, the blindly signed public key certificate is just like an authorised pseudonym of the user. The public key certificate is called a ‘pseudonym public key certificate’ and the embedded public key is called a ‘pseudonym public key’ in this paper.

2.2 Electronic Coin

An electronic coin is used as a stimulating and awarding measure in this paper. An e-coin is a digital payment, by which a payer can transfer a certain amount of money to a payee. In our design, the idea in [9] is developped and extended such that payer A can pay the amount m to payee B by e-coin as shown below, where A and B have accounts in the two banks of C_1 and C_2 respectively.

1. A publishes his public key pk_A and holds the corresponding private key sk_A
2. A generates an e-coin $s = S_{sk_A}(A, m, C_1, c, \tau)$ where c is A's account number and τ is a random number (e.g., the time of transaction).
3. A sends s to B.
4. B sends s to C_2 for payment.
5. C_2 sends s to C_1.
6. C_1 verifies the validity of signature s using pk_A.
7. If the signature verification succeeds, C_1 takes the designated amount of money from A's account and transfers the money to C_2, which then puts the money into B's account.
8. C_1 records s so that it cannot be re-used.

In this paper, to encourage the nodes in a network to transfer the messages, an e-coin is used to pay a node for transferring a message. So although transfer in the mobile ad hoc network is not publicly verifiable, the nodes will not discard the messages.

3. The Network Communication Scheme

The network communication scheme consists of the following four stages: registration, submission, processing, and payment. In the registration phase, each user chooses a private key and generates a corresponding public key certificate as his pseudonym. Then, he registers at a registration authority, who blindly signs the users' pseudonym public key certificates. In the submission phase, one or more application providers set up a private (decryption) key and publishes the public (encryption) key, while the users submit their messages to the application providers through the mobile wireless network. Each user encrypts his message using the encryption key, signs his encrypted message using his pseudonym private key, and sends the encrypted and signed message to the application provider through the mobile wireless network. In the processing phase, the application provider decrypts the received ciphertext and verifies the validity of the decryption result. In the payment phase, the nodes in the network get their payment in the form electronic coins for their contribution in transferring the messages.

We need to emphasize that in terms of security we focused on communication security and did not cover server security. Server security topics like server invasion and hijacking, or the fishing or spoofing of servers all fall into the field of server attack-and-defense and intersted readers should refer to the literature in that field.

3.1 Registration Phase

The registration authority R is set up and its public key k_R is published. Suppose there is a user U . The registration operation is as follows:

1. U chooses his private key sk and generates a corresponding certificate S , which contains his public key pk and some application information like an identifier and validity period.
2. U contacts R and proves his identity. For example, U can prove his knowledge of his private key corresponding to his public key in PKI using zero knowledge proof. (Note that this key pair is not the pseudonym key pair sk and pk .)
3. After being identified, U makes R blindly sign S using a blind signature algorithm. The signed certificate (including the certificate and the signature on it) is denoted as S' , which is the user's pseudonym certificate.

The deployment of R can be flexible. Depending on the concrete application, it can be implemented in a single central server or may have multiple mirror servers holding the same key. In either case, security is not compromised as:

- The blind signature technique guarantees that the signatures are not traceable,
- R only participates in the registration phase.

3.2 Submission Phase

Suppose there is an application provider (e.g., a bank or auctioneer), whose application service (e.g., e-banking or e-auction) is needed by the user. The application provider chooses a private key SK and publishes the corresponding public key PK . For stronger security, multiple parties can be employed by it such that SK is shared by them and decryption is only possible if the number of cooperating parties exceed the threshold. Suppose that the user has a computing device (e.g., laptop, PDA, or mobile phone) to dynamically communicate with the mobile wireless network and to perform computations like-encryption and signature generation. The user will communicate with the mobile wireless network as follows:

1. U chooses the user's application information u, whose content depends on the concrete application service (e.g., a bid in an e-auction system).
2. U encrypts u into $u' = E_{PK}(u)$. The user then signs it and obtains $u'' = S_{sk}(u')$.
3. U tries to connect the mobile wireless network. Suppose it finds the nearest network node, which is denoted as N_1.
4. N_1 authenticates itself to U, who verifies the user's authentication (e.g., in the form of a signature or ZK proof).
5. U sends their application packet u_1 to N_1. u_1 contains two parts: application information a_1 and routing information b_1 where $b_1 = (S', S_{sk}(pk_1))$ and pk_1 is the publicly key of N_1.
6. N_1 receives u_1 and verifies that their pseudonym public key is signed by U and attached in the packet. Then the user finds the next router and continues routing the application packet.
7. The routing of u'' continues and the j^{th} router N_j receives $u_j = (a_j, b_j)$, finds the next router N_{j+1} and sends $u_{j+1} = (a_{j+1}, b_{j+1})$ to N_{j+1} where $a_{j+1} = a_j$, $b_{j+1} = (b_j, S_{sk_j}(pk_{j+1}))$ and pk_{j+1} is the public key of N_{j+1} issued by R.
8. Finally, the application packet arrives at the application server.

We need to emphasize that the public key of an application provider is not a pseudonym public key. This is because the bank needs to know which account the money needs to be withdrawn from, as shown later.

3.3 Processing Phase

The application provider receives $u_m = (a_m, b_m)$ from his server where $b_m = (b_{m,0}, b_{m,1}, \ldots b_{m,m})$ is the routing path. He acts as follows.

1. The application provider verifies that $b_{m,0}$ is a pseudonym public key certificate signed by R.
2. The application provider extracts the pseudonym public key from $b_{m,0}$, which is denoted as k.
3. The application provider uses k to verify that a_m is correctly signed with the corresponding private key.
4. The application provider decrypts a_m and obtains $s = D_{SK}(a_m)$ if a key that has been certified by R correctly signs it. Otherwise, s is discarded.
5. The application provider processes the application request in s. If multiple parties sharing the private key perform the decryption, they use a zero knowledge proof to demonstrate the validity of their decryption operations. (For example, the validity of the ElGamal decryption can be demonstrated by a zero knowledge proof of equality of logarithms [11].)

6. The application provider uses k to verify that $b_{m,1}$ is correctly signed with the corresponding private key.
7. After the validity of $b_{m,1}$ is verified, the pseudonym public key in it is extracted and used to verify the validity of $b_{m,2}$ in the same way.
8. In general, the application provider extracts the pseudonym public key from $b_{m,j}$ and verifies that the corresponding private key is being used to generate signature $b_{m,j+1}$ for $j = 0,1,\ldots,m-1$.
9. After $b_{m,1},\ldots b_{m,m}$ are verified to be valid, each pseudonym public key in them is used to encrypt an electronic coin. The electronic coin includes the sum of payment for transferring one application packet as a router, the application provider's account number, the name of his bank, and his signature on them. All of the encrypted e-coins are published on the application server together with the pseudonym public key used to encrypt it.

To achieve stronger security, multiple parties can play the role of the application provider. They share SK using threshold secret sharing and cooperate to decrypt the encrypted messages, which is feasible only when the number of cooperating application providers is over a threshold. Moreover, multiple payments to the same pseudonym key holder can be combined into a single e-coin for higher efficiency.

3.4 Payment Phase

Each router working in the mobile wireless network collects their payments as follows:

1. The router finds the user’s pseudonym public key on the application provider's server.
2. The router finds the encrypted e-coins put together with the user’s pseudonym public key.
3. The router decrypts the encrypted e-coins.
4. The router sends the e-coins to the user’s bank, which forwards them to the application provider's bank.
5. After verifying the application provider's signature on the e-coins, the provider's bank transfers the money from its account to the router's bank, which puts the money into the router's account.
6. The application provider's bank records that the e-coin has expired and will not be accepted again in the future.

If the application provider combines the payments to the same key holder into a single e-coin, each router only needs to use one e-coin to claim all of their payments. We need to emphasize that when a router sends the e-coin to his own bank, the router needs to tell the bank his own real identity instead of his pseudonym public key. This is because the bank does not know the correspondence between the account and the pseudonym public key. That implies that a bank may know the relationship between the pseudonym public key and the real identity of some of its customers. However, we noticed that usually a routing path consists of multiple hops and that there are usually many routers using different banks and the application provider and the user do not usually know which bank every router uses. So privacy and anonymity can still be maintained in the network.

Note that an ad hoc network connection is not necessary in the payment phase, which is not actually a real time operation of our mobile wireless service system. First, the application provider's server is usually fixed in a position and can be accessed more conveniently via other networks like the Internet. Second, as we just emphasized, no anonymity requirement is needed or is even possible between a claimer and his bank and thus the advantage of an ad hoc network for anonymity is not useful. In short, an appropriate network connection can be employed according to the concrete application.

4. ANALYSIS

Reliability is achieved in the proposed mobile wireless network scheme due to the following reasons:

- The routers can get paid for transferring the information, so they are motivated to route the information and will not discard it. Even if some of them want to cheat in the application, this target cannot be achieved by discarding any application packet as the packets are encrypted. Before deciding whether to discard a packet, a router has to know its content, which is impossible unless the router obtains collusion from the application providers and the number of the colluding application providers is over the sharing threshold.
- As the application information is signed by the users, it cannot be tampered with. As the users' pseudonym signatures on their messages are verifiable, the validity of the communication can be checked.

Privacy is achieved in the proposed mobile wireless network scheme due to the following reasons:

- A blind signature is employed to issue a pseudonym public key certificate to the users. So the users' signatures on their messages do not reveal their identities.
- In a mobile ad hoc network, no node has a constant location, so the users' identities cannot be found by tracing their messages or locating them.

There is not any limitation to message format in the proposed mobile wireless network scheme, except that a maximum value may need to be set for the number of routers to avoid heavy overload in some applications. Consequently, any application is supported and flexibility is achieved. There is not a costly message shuffling in the proposed mobile wireless network scheme, and thus, a high efficiency is achieved.

The routers can obtain their payments and only their payments due to the following reasons:

- As each router's payment depends on a signature chain containing the signatures of all the routers before him, for he will not remove those routers' signatures his own interest. Moreover, if any router removes any previous router's signature from any routing packet, the signature chain starting from the user will be broken and thus, the attack will be detected.
- To remove a router's signature from an application packet without being detected, multiple other routers (at least one before the removed router and one behind it in the route) are

needed to cooperate to re-build the application packet. This is a costly attack without any interest, so it usually will not happen.

- To add some routers' signatures into an application packet, the added routers must cooperate and provide their signatures. The computation and communication costs for this operation is no lower than the additional payment that they can obtain. Therefore, there is no motivation for this attack.
- Each e-coin is encrypted using its owner's public key, so no other person can steal it.
- Every used e-coin is recorded and so they cannot be re-used.

Reliability in the proposed mobile wireless network scheme is not absolutely guaranteed. However, there is the assumption that people usually do not go through the trouble to break the rules when they cannot gain interest and may even lose income. So, from a statistical point of view, the proposed scheme can guarantee the correctness of any single packet with a very large probability. Although the achieved correctness is not absolute, it is enough in many applications.

5. APPLICATION AND EFFICIENCY COMPARISON

To convincingly show the high efficiency of the new mobile wireless network, we took the example of an e-auction as its application. An efficiency comparison between the new e-auction solution and the existing two methods in an e-auction design (a homomorphic auction and an auction using static anonymous communication) is made in Table 1. In the two existing methods we do not choose any specific scheme as an example because some of them are more efficient but still fail to satisfy some desired property and some of them satisfy all of the desired properties but do not employ the most efficient design. Instead, we used the most advanced and efficient technique in each method on the condition that the desired properties in the e-auction were satisfied. For example, all the bids are signed and their signatures are verified. The bid validity must be proved and verified in a homomorphic auction and universal and instant verification must be guaranteed in a static anonymous communication based auction. In the new solution, we supposed that the new mobile wireless network was employed and that the bidders formed an ad-hoc mobile network and acted as users and routers. The cost of registration is not included in Table 1 for two reasons. First, it is much more efficient than an auction and doing an opening bid. Second, the registration is similar in all of the three solutions (including the authentication and authorization in each of them). Although authorization in the new auction scheme has a special requirement (blindness), its cost is similar to authorization in the other two solutions.

It is assumed that the ElGamal encryption, RSA signature, and RSA-based blind signature are employed when necessary in the solutions. In the comparison of the computational cost, exponentiations are counted. In the comparison of the communicational cost, transmission of integers with large length are counted. For the sake of simplicity, a simple and very common election rule is used in the comparison where one winner is elected from ten candidates. In all the three methods it is assumed that there are n bidders and 3 auctioneers and in the static anonymous communication based auction and mobile ad hoc auction it is assumed that there are 3 routers.

Table 1 illustrates that in a mobile ad hoc network a secure e-auction can be more efficiently implemented. The low efficiency of the homomorphic auction lies in that each bidder has to submit n ciphertexts and prove that all of them are valid, while the auctioneers have to verify

Table 1. Efficiency Comparison in the Example of an E-Auction

Method	Computation		Communication
	Generating a bid	Transferring and opening the bids	Total cost
Homomorphic auction [2, 4, 12, 20, 21, 22, 25, 27, 29, 33]	41	41n+10	101
An auction using the static anonymous communication [31, 32]	3	29n	52
An auction in a mobile wireless network	3	11n	40

the validity of all the n ciphertexts. The low efficiency of the static anonymous communication based auction lies in that each auctioneer has to shuffle the bids and publicly prove that the shuffling is valid.

6. Conclusion

A new mobile wireless network has been designed. It employs a mobile ad hoc network to transfer the messages so that the privacy of the messages can be more efficiently achieved. In the mobile ad hoc environment, only a blind signature based pseudonym mechanism is needed to guarantee the anonymity of the users. An e-coin based awarding mechanism is employed to guarantee the reliability of the applications. The proposed mobile wireless network scheme is both flexible and efficient.

References

[1] M Abe and F Hoshino. Remarks on mix-network based on permutation networks. In PKC '01, pp.317-324.

[2] M Abe, M Ohkubo, and K Suzuki. 1-out-of-n signatures from a variety of keys. In ASIACRYPT '02, pp.415-432.

[3] L Buttyan and J Hubaux. Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks. Technical report, Swiss Federal Institute of Technology Lausanne, 2001.

[4] F Brandt. Cryptographic protocols for secure second-price auctions. 2001. Available at http://www.brauer.in.tum.de/ brandtf/papers/cia2001.pdf

[5] J Camenisch and A Mityagin. A formal treatment of onion routing. In CRYPTO '05, Vol.3089 of Lecture Notes in Computer Science, pp.169-187, Berlin, 2005. Springer-Verlag.

[6] D Chaum. Blind signatures for untraceable payments. In CRYPTO '82, pp.199-204.

[7] D Chaum. Security without identification: transaction systems to make big brother obsolete. In Communications of the ACM, 28 (1985), pp.1030-1044.

[8] D Chaum. Blinding for unanticipated signatures. In EUROCRYPT '87, pp.227-236.

[9] D Chaum, A Fiat and M Naor. Untraceable electronic cash. In Crypto '88, pp.319-327.

[10] D Chaum. Elections with unconditionally-secret ballots and disruption equivalent to breaking rsa. In Eurocrypt '88, pp.177-182.

[11] D Chaum and T Pedersen. Wallet databases with observers. In CRYPTO '92, pp.89-105.

[12] K Chida, K Kobayashi, and H Morita. Efficient sealed-bid auctions for massive numbers of bidders with lump comparison. In Information Security, 4th International Conference, ISC 2001, pp.408-419.

[13] R. Dingledine, N. Mathewson, and P. F. Syverson. Tor: The second-generation onion router. In USENIX Security Symposium, pp.303-320, 2004.

[14] J Furukawa and K Sako. An efficient scheme for proving a shuffle. In CRYPTO '01, pp.368-387.

[15] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, STOC 1987, pp.218-229, 1987.

[16] D. M. Goldschlag, M. G. Reed, and P. F. Syverson. Onion routing for anonymous and private internet connections. Comm. of the ACM, 42(2), pp.84-88, 1999.

[17] J Groth. A verifiable secret shuffle of homomorphic encryptions. In Public Key Cryptography 2003, pp.145-160.

[18] J Furukawa. Efficient and verifiable shuffling and shuffle-decryption. In IEICE Transactions 88-A(1), pp.172-188, 2005.

[19] D Kesdogana and C Palme. Technical challenges of network anonymity. In Computer Communications, Vol.29, Issue 3, 1 February 2006, pp.306-324.

[20] H Kikuchi, M Harkavy, and J Tygar. Multi-round anonymous auction. In IEEE Workshop on Dependable and Real-Time E-Commerce Systems 1998, pp.62-69.

[21] H Kikuchi. (m+1)st-price auction. In FC '01, 291-298.

[22] H Kikuchi, S Hotta, K Abe, and S Nakanishi. Distributed auction servers resolving winner and winning bid without revealing privacy of bids. In NGITA '00, pp.307-312.

[23] C Neff. A verifiable secret shuffle and its application to e-voting. In ACM CCS '01, pp.116-125, 2001.

[24] C Neff. Verifiable mixing (shuffling) of elgamal pairs. 2004. Available as http://theory.lcs.mit.edu/rivest/voting/papers/Neff-2004-04-21-ElGamalShuffles.pdf.

[25] K Omote and A Miyaji. A second-price sealed-bid auction with the discriminant of the p-th root. In FC '02, pp.57-71.

[26] K Peng, C Boyd, and E Dawson. Simple and efficient shuffling with provable correctness and ZK privacy. In CRYPTO '05, pp.188-204.

[27] K Peng, C Boyd, E Dawson, and K Viswanathan. Robust, privacy protecting and publicly verifiable sealed-bid auction. In ICICS '02, pp.147-159.

[28] K Peng, C Boyd, E Dawson, and K Viswanathan. A correct, private and efficient mix network. In PKC '04, pp.439-454.

[29] K Peng and F Bao. Efficiency improvement of homomorphic e-auction. In TRUSTBUS '10, pp.238-249.

[30] K Peng, E Dawson, and F Bao. Modification and optimisation of a shuffling scheme: stronger security, formal analysis and higher efficiency. In International Journal of Information Security, 2011 Vol.10, No.1, pp.33-47.

[31] K Peng. Secure E-auction for mobile users with low-capability devices in wireless network. In WISTP '11, pp.351-360.

[32] K Peng and Y Zhang. A Secure Mix Network with an Efficient Validity Verification Mechanism. In IDCS '12, pp.85-96.

[33] K Peng. Efficient homomorphic sealed-bid auction free of bid validity check and equality test. In Security and Communication Networks. Available online MAY 2012 at DOI: 10.1002/sec.549.

KUN PENG

Dr. Kun Peng received his Bachelor's degree in Software Engineering and his Master degree's in Computer Security from Huazhong University of Science and Technology in China. He obtained his PhD in information security from the Information Security Institute at the Queensland University of Technology in Australia in 2004. His main research interest is in applied public key cryptology. His main research interests include applied cryptology, network security, and secure e-commerce, and e-government. He is now a scientist at the Institute for Infocomm Research in Singapore.