Multi-proxy Multi-signature Binding Positioning Protocol

Huafeng Chen[1], Qingshui Xue[1(✉)], Fengying Li[2], Huajun Zhang[1], Zhenfu Cao[1], and Jianwen Hou[3]

[1] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
chenhuafeng@sjtu.edu.cn, {xue-qsh,zfcao}@cs.sjtu.edu.cn, zhanghuajun.cn@gmail.com
[2] School of Continuous Education, Shanghai Jiao Tong University, Shanghai 201101, China
fyli@sjtu.edu.cn
[3] Shanghai Academy of Spaceflight Technology, Shanghai 201109, China
houjianwen0707@gmail.com

Abstract. Position-based cryptography has attracted lots of researchers' attentions. In mobile Internet, there are many position-based security applications. For the first time, one new conception, multi-proxy multi-signature (MPMS) binding positioning protocol is proposed. Based on one secure positioning protocol, one model of MPMS binding positioning protocol is proposed. In the model, positioning protocol is bound to MPMS tightly, not loosely. Further, we propose one scheme of MPMS binding positioning protocol. As far as we know, it is the first scheme of MPMS binding positioning protocol.

Keywords: Positioning protocol · Proxy signature · Multi-proxy multi-signature · Model · Scheme

1 Introduction

In the setting of mobile Internet, position services and position-binding security applications become one key requirement, especially the latter. Position services include position inquiring, secure positioning and so forth. Position inquiring consists of inquiring your own position and positioning of other entities. The technology of inquiring your own position has GPS (Global Positioning System) and other satellite service system. The technology of positioning of other entities has radar and so on [2–6]. As we all know, the positioning of other entities is more challenging one. Position-binding security applications such as position-based encryption and position-based signature and authentication are increasingly necessary for us. Take one application about position-based signature and authentication as an example. One mobile or fixed user signs messages at one place and sends them to another mobile user. The receiver can verify

K. Xu and J. Zhu (Eds.): WASA 2015, LNCS 9204, pp. 9–18, 2015.
DOI: 10.1007/978-3-319-21837-3_2

whether or not the received message is indeed signed at the place by the signer. Even if the signer moves to another address, it will not affect the receiving and verification of signed messages. On March 8, 2014, the missing Malaysian Airline MH370 can't be found till now, as reminds us of the significance of positioning and related security applications.

Currently, the research on position-based cryptography focuses on secure positioning about which some work had been proposed [1]. These positioning protocols are based on one-dimension, two-dimension or three-dimension spaces, including traditional wireless network settings [1], as well as quantum setting [7,8]. It seems to us that position-based cryptography should integrate secure positioning with cryptographic primitives. If only or too much concentrating on positioning protocols, perhaps we will be far away from position-based cryptography. In other words, nowadays positioning is bound loosely with related security applications, not tightly, as results in the slow progress of position-based cryptography and applications.

The proxy signature scheme [9], a variation of ordinary digital signature schemes, enables a proxy signer to sign messages on behalf of the original signer. Proxy signature schemes are very useful in many applications such as electronics transaction and mobile agent environment. Since the conception of the proxy signature was brought forward, a lot of proxy signature schemes have been proposed [10–12]. In 2001, Hwang et al. first proposed a MPMS scheme [13]. Till now, there is not any publication about MPMS scheme binding positioning protocol.

Relying on the thoughts, in the paper, our main contributions are as follows.

(1) We propose one model of MPMS binding positioning protocol. MPMS binding positioning protocol is one kind of MPMS, but a novel one. The definition is given and its model is constructed. In the meantime, we define its security properties.
(2) To realize the kind of MPMS, one secure-positioning-protocol-based MPMS scheme is proposed and its security is analyzed as well.

We organized the rest of the paper as follows. In Sect. 2, we introduced function of positioning and one secure positioning protocol. In Sect. 3, the model and definition of MPMS binding positioning protocol are given. We proposed one scheme of MPMS binding positioning protocol in Sect. 4. Finally, the conclusion is given.

2 Positioning Protocol

In the section, we will introduce the function of positioning protocols and one secure positioning protocol.

2.1 Function of Positioning Protocols

The goal of positioning protocol is to check whether one position claimer is really at the position claimed by it. Generally speaking, in the positioning protocol,

there are at least two participants including position claimers and verifiers, where the verifiers may be regarded as position infrastructure. According to destination of the positioning, there are two kinds of positioning protocol, i.e., your own position positioning protocol and others' position positioning protocol. As of now, lots of works on your own position positioning protocol have been done [2–6]. Nevertheless, research on others' positions positioning protocol is far less and there are still many open questions to resolve. In our model and scheme, we will make full use of the two varieties of positioning protocol.

2.2 One Secure Positioning Protocol [1]

Here, we will introduce one others' positions secure positioning protocol.

In the section, we will review N. Chandran et al.s secure positioning protocol in 3-dimensions [1], which can be used in mobile Internet.

In the protocol, 4 verifiers denoted by $V_1, \ldots, V_4$, which can output string X_i are used. The prover claims his/her position which is enclosed in the tetrahedron defined by the four verifiers. Let $t_1, \ldots, t_4$ be the time taken for radio waves to arrive at the point P from verifier $V_1, \ldots, V_4$ respectively. When we say that $V_1, \ldots, V_4$ broadcast messages such that they "meet" at P, we mean that they broadcast the messages at time $T-t_1, T-t_2, T-t_3$ and $T-t_4$ and respectively so that at time T all the messages are at position P in space. The protocol uses a pseudorandom generator namely an ε-secure $PRG : \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^m$. They select the parameters such that $\varepsilon + 2^{-m}$ is negligible in the security parameters. X_i denotes a string chosen randomly from a reverse block entropy source. The protocol is given as follows:

Step 1. $V_1, \ldots, V_4$ pick keys $K_1, \ldots, K_4$ selected randomly from $\{0,1\}^n$ and broadcast them through their private channel.

Step 2. For the purpose of enabling the device at P to calculate K_i for $1 \leqslant i \leqslant 4$, the verifiers do as follows. V_1 broadcasts key K_1 at time $T-t_1$. V_2 broadcasts X_1 at time $T-t_2$ and meanwhile broadcasts ${K_2}' = PRG(X_1, K_1) \oplus K_2$. Similarly, at time $T-t_3$, V_3 broadcasts $(X_2, {K_3}' = PRG(X_2, K_2) \oplus K_3)$, and V_4 broadcasts $(X_3, {K_4}' = PRG(X_3, K_3) \oplus K_4$ at time $T-t_4$.

Step 3. At time T, the prover at position P calculates messages $K_{i+1} = PRG(X_i, K_i) \oplus {K_{i+1}}'$ for $1 \leqslant i \leqslant 3$. Then it sends K_4 to all verifiers.

Step 4. All verifiers check that the string K_4 is received at time $(T+t_i)$ and that it equals K_4 that they pre-picked. If the verifications hold, the position claim of the prover is accepted. Otherwise, the position claim is invalid.

3 The Model of MPMS Binding Positioning Protocol

3.1 The Model

In the model, there are four kinds of participants including the original signer group (OSG) which consists of n original signers $OS_1, OS_2, \ldots, OS_n$, the proxy

signer group (PSG) which consists of m proxy signers $PS_1, PS_2, \ldots, PS_m$, the verifier (V) and position infrastructure (PI). All original signers (OSs) at individual positions cooperate to delegate their signing power to all proxy signers (PSs) at individual positions. All of PSs cooperate to sign one message at positions after their positions are confirmed by PI. V checks that the MPMS is generated by all of PSs at individual positions on behalf of all of OSs at the specified positions. PI, which is reckoned as one trusted third party, provides position services for all OSs and PSs.

3.2 Definition

MPMS Binding Positioning Protocol. Simply speaking, the kind of MPMS combines traditional MPMS and positioning protocols as one single scheme. It is mainly composed of three modules of multi-proxy multi-signing power delegation, multi-proxy multi-signing and multi-proxy multi-signature verifying. In the module of multi-proxy multi-signing power delegation, each of OSs first sends one request to PI for the purpose of cooperatively delegating signing power of theirs to all PSs. Then PI runs one positioning protocol to confirm the positions of all OSs and PSs. If all of their positions are valid, PI sends individual proxy delegation key package (*pdkp*) to each OS, and sends individual proxy signing key package (*pskp*) to each of PSs. Then all of OSs cooperates to produce multi-proxy multi-signing delegation warrant to all of PSs. In the module of multi-proxy multi-signing, each of PSs has to first check that his/her position is indeed at the designated position, which is specified in the multi-proxy multi-signing delegation warrant. If it holds, each of PSs can use his/her *pskp* to sign the message for only once and sends corresponding individual MPMS to signature collector. The signature collector checks the validity of individual MPMSs. If all are valid, the signature collector can generate the integrated signature, called MPMS binding position protocol, and sends it to V. In the module of MPMS verifying, V uses the identities and positions of all OSs and all PSs to check the validity of the MPMS binding positioning protocol.

Remark 1. During the module of multi-proxy multi-signing power delegation, if neither any OS nor PS can confirm its position, the OSG can't fulfill their delegation of signing power. In the module of multi-proxy multi-signing, each PSs have to confirm its position, before he/she is able to cooperate to generate the MPMS. During the module of MPMS verifying, it is unnecessary for the verifier to confirm the positions of all original signers and proxy signers.

In the model, it will be seen that we regard the three modules as three primitives. Therefore, the positioning protocol is bound tightly with the delegation of signing power and generation of the MPMS, instead loosely.

The MPMS binding positioning protocol is composed of four primitives: Initialization, PropMProxyMDelegate, PropMProxyMSign and PropMProxyMVerify. The model is illustrated in Fig. 1.

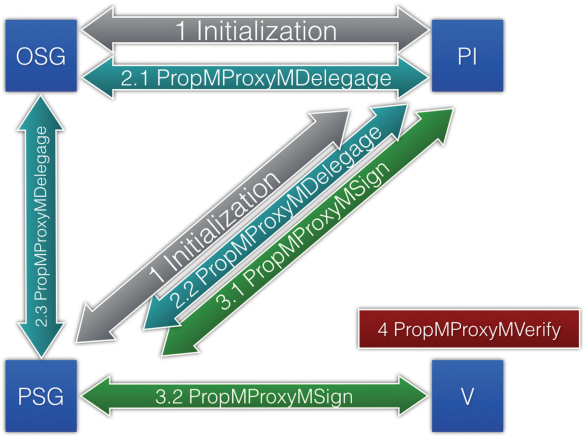

Fig. 1. Model of MPMS binding positioning protocol.

Initialization. PI takes as input secure parameter 1^k, generates system master key mk and outputs system public parameter pp, in the meantime, the system distributes users' identity ID_i for user i .

PropMProxyMDelegate. Each of OSs first sends his/her request to PI. PI confirms the positions $Pos_{OS_1}, Pos_{OS_2}, \ldots, Pos_{OS_n}$ of all OSs by running positioning protocol with each OS, and checks the validity of positions of all PSs. If all OSs is indeed at their position, and all PSs' positions are valid, PI generates and sends the acknowledgement along with $pdkp_{OS_i}(i = 1, 2, \ldots, n)$ to individual OSs by one public or safe channel. $pdkp_{OS_i}$ encapsulates positioning protocol, delegation key, the OS's identity ID_{OS_i} and position Pos_{OS_i}, delegation algorithm, etc. According to the acknowledgement fromPI, all of OSs cooperate to generate proxy delegation warrant dw and send it to each of PSs. PI generates the $pdkp_{PS_i}$ and sends it to $PS_i(i = 1, 2, \ldots, m)$. dw contains identities and positions of all OSs and PSs, message types to sign, expiry date and so on. $pskp_{PS_i}$ encapsulates positioning protocol, proxy signing key, the PS's identity ID_{PS_i} and position Pos_{PS_i}, signing algorithm, etc.

PropMProxyMSign. Each $PS_i(i = 1, 2, \ldots, m)$ first executes his/her $pskp_{PS_i}$ toconfirm his/her position Pos_{PS_i} with PI and check whether it is identical to the one in the proxy delegation warrant dw. If it holds,then he/she is able to use $pskp_{PS_i}$ to sign the message m for only once and sends corresponding individual proxy signature (m, s_i, dw, pp) to the signature collector which checks the validity of individual proxy signature s_i by using the identity ID_{PS_i} and position Pos_{PS_i} of PS_i and corresponding verification algorithm. If all the s_i are valid, the collector generates the final MPMS (m, s, dw, pp) and sends it to V.

PropMProxyMVerify. After receiving the MPMS (m, s, dw, pp) from the PSs, V takes as input the identities and positions of all the OSs and PSs as well as pp to check whether or not the proxy delegation warrant dw is valid, then V check whether or not s is the MPMS of the message m by using corresponding verification algorithm. If it holds, V can be sure that the message m was signed by all of PSs at individual position $Pos_{PS_i}(i = 1, 2, \ldots, m)$ on behalf of the OSG who cooperated to delegate their signing power to the PSG at individual position $Pos_{OS_i}(i = 1, 2, \ldots, n)$.

Remark 2. In the primitive of PropMProxyMDelegate, the Clerk can be any original signer. Similarly, in the primitive of PropMProxyMSign, the signature collector can be any proxy signer.

3.3 Security Properties of MPMS Binding Position Protocol

Positioning Protocol Binding. Besides security properties of MPMS, this kind of MPMS needs the security property of positioning-protocol-binding. In the module of PropMProxyMDelegate, the OSG is unable to finish their delegation of signing power without confirming of positions of all OSs and PSs with PI. In addition, the individual *pskp* of each PS generated by PI is tightly bound with positioning protocol. In the module of PropMProxyMSign, if the PSG need sign one message on behalf of the OSG, each PS has to make use of its *pskp* to run the positioning protocol with PI before he/she is able to sign one message.

Remark 3. One maybe think we should make use of one-time digital signing algorithm or one-time signing private key. Actually, in the model, using one-time signing key is optional. Since position-based applications are closely related with position instant authentication or confirmation, it seems to us that position-based cryptography should be deeply researched regarding online cryptography, which focuses on instant cryptographic algorithms and security processing.

3.4 Proxy Delegation Key Package (pdkg)

In the model, we make use of *pdkp* to fulfill the proxy delegation. *pdkp* is one type of executive modules such as .exe or .dll. It consists of delegation key, position localizing protocol, delegation generation algorithm, identities and positions of both OS and PS, and so on. Its structure is showed in Fig. 2.

3.5 Proxy Signing Key Package (pskg)

In the model, *pskp*s is also one kind of executive modules. It is composed of one position localizing protocol, one proxy signing algorithm, proxy signing private key and so forth. Its structure is showed in Fig. 3.

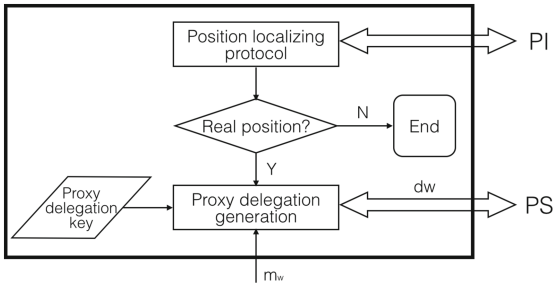

Fig. 2. Structure of proxy delegation key package.

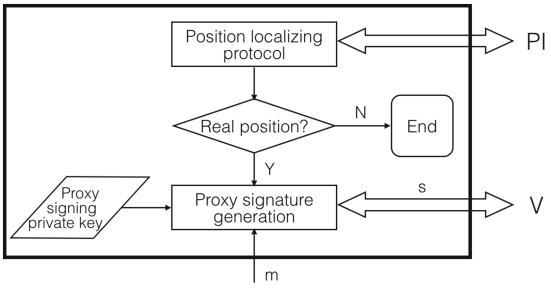

Fig. 3. Structure of proxy signing key package.

4 One MPMS Scheme Binding Secure Position Protocol

In this section, we proposed one MPMS scheme binding secure positioning protocol, in which there exist n original signers and m proxy signers. The scheme mainly includes four kinds of participants: the OSG which consists of $OS_1, OS_2, \ldots, OS_n$, the PSG which consists of $PS_1, PS_2, \ldots, PS_m$, the verifier (V) and PI. PI will make use of the secure positioning protocol mentioned in Sect. 2.2 to provide services of position for n OSs and m PSs. In addition, PI will be regarded as the trusted third party and system authority. The scheme is composed of four primitives: *Initialization*, *PropMProxyMDelegate*, *PropMProxyMSign* and *PropMProxyMVerify*. As primitives, they mean that they either fully run or do nothing. We will detail the four primitives as follows.

4.1 Initialization

PI takes as input secure parameter 1^k and outputs system master key mk and public parameter pp, at the same time, PI distributes user identity ID_i for user i. We can rewrite the primitive as Initialization (k, mk, pp) .

4.2 PropMProxyMDelegation

Step 1. When the original signer group wants to delegate their signing power to the proxy signer group, each of original signers $OS_i (i = 1, 2, \ldots, n)$ first sends requests $(ID_{OS_1}, Pos_{OS_1}, ID_{OS_2}, Pos_{OS_2}, \ldots, ID_{OS_n}, Pos_{OS_n}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, \ldots, ID_{PS_m}, Pos_{PS_m}, res_{dele})$ to PI.

Step 2. After PI gets each original signer's request, PI confirms the positions of each original signer by running positioning protocol with each original signer, and checks the validity of positions of all proxy signers. If each of original signers OS_i is indeed at its position $Pos_{OS_i} (i = 1, 2, \ldots, n)$, and all proxy signers' positions $Pos_{PS_i} (i = 1, 2, \ldots, m)$ are valid, PI sends the acknowledgement $(ID_{OS_1}, Pos_{OS_1}, ID_{OS_2}, Pos_{OS_2}, \ldots, ID_{OS_n}, Pos_{OS_n}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, \ldots, ID_{PS_m}, Pos_{PS_m}, ack_{dele})$ to each original signer, or the scheme fails to stop.

Step 3. PI generates and sends proxy delegation key packages $pdkp_{OS_i} (i = 1, 2, \ldots, n)$ to individual original signers OS_i by one public or safe channel. $pdkp_{OS_i}$ encapsulates positioning protocol, delegation key, and the original signer's identity ID_{OS_i} and position Pos_{OS_i}.

Step 4. Each of original signers OS_i uses its proxy delegation key packages $pdkp_{OS_i}$ to confirm the validity of its position and generates its individual proxy delegation $(ID_{OS_1}, Pos_{OS_1}, ID_{OS_2}, Pos_{OS_2}, \ldots, ID_{OS_n}, Pos_{OS_n}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, \ldots, ID_{PS_m}, Pos_{PS_m}, dw_i)$. OS_i sends it to the Clerk. dw_i is the signature generated by proxy delegation key packages $pdkp_{OS_i}$.

Step 5. The Clerk checks the individual proxy delegation dw_i is produced by OS_i, if the verification of all $dw_i (i = 1, 2, \ldots, n)$ holds, the Clerk generates the final proxy delegation warrant $(ID_{OS_1}, Pos_{OS_1}, ID_{OS_2}, Pos_{OS_2}, \ldots, ID_{OS_n}, Pos_{OS_n}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, \ldots, ID_{PS_m}, Pos_{PS_m}, dw)$. Here we can simply denote dw by $dw = \prod_{i=1}^{n} dw_i$

Step 6. The Clerk sends the final proxy delegation warrant to each of proxy signers. dw contains the identities and positions of all original signers and proxy signers, message types to sign, expiry date and so forth.

Step 7. PI generates the proxy signing key package $pskp_{PS_i} (i = 1, 2, \ldots, m)$ and sends it to each proxy signer. $pskp_{PS_i}$ encapsulates positioning protocol, individual proxy signing key, the proxy signer's identity ID_{PS_i} and position Pos_{PS_i}, signing algorithm, etc.

4.3 PropMProxyMSign

Step 1. When the proxy signer group wants to sign the message m on behalf of all original signers, each of proxy signers $PS_1, PS_2, \ldots, PS_m (i = 1, 2, \ldots, m)$ runs individual proxy signing key package $pskp_i$ for executing positioning protocol to confirm the validity of theposition Pos_{PS_i} withPI.

Step 2. If $PS_i's(i = 1, 2, \ldots, m)$ current position Pos_{PS_i} is identical to the one in the delegation warrant dw, proxy signing key package $pskp_i$ prompts PS_i to input the message m to $pskp_i$. Thus proxy signing key package $pskp_i$ produces the individual proxy signature s_i and sends it to the signature collector; if PS's current position Pos_{PS_i} is not identical to the one in the delegation warrant dw, PS_i is unable to perform the function of proxy signing and stops.

Step 3. After the signature collector receives the individual proxy signature $s_i(i = 1, 2, \ldots, m)$, he/she check s_i is the individual proxy signature by using verification algorithm,the identity and position of PS_i.

Step 4. if all $s_i's$ verification hold, the signature collector generates the final MPMS s by processing all individual proxy signature $s_i(i = 1, 2, \ldots, m)$. Here we can simply denote s as $s = \prod_{i=1}^{m} s_i$.

Step 5. The signature collector sends (m, s, dw, pp) to the proxy signature verifier V.

4.4 PropMProxyMVerify

Step1. After receiving the MPMS (m, s, dw, pp) from the proxy signers, V takes as input the identities $ID_{OS_1}, ID_{OS_2}, \ldots, ID_{OS_n}, ID_{PS_1}, ID_{PS_2}, \ldots, ID_{PS_m}$, positions $Pos_{OS_1}, Pos_{OS_2}, \ldots, Pos_{OS_n}, , Pos_{PS_1}, Pos_{PS_2}, \ldots, Pos_{PS_m}$, and pp to check whether or not dw is valid. If it is valid, the scheme continues, or fails to stop.

Step 2. V takes the same input as Step 1 to check whether or not s is the MPMS on the message m by using corresponding MPMS verification algorithm. If it holds, V can be sure that the message m was signed by all proxy signers at the position $Pos_{PS_i}(i = 1, 2, \ldots, m)$ on behalf of the original signer group who cooperated to delegate their signing power to all proxy signers at the individual position $Pos_{OS_i}(i = 1, 2, \ldots, n)$.

Remark 4. In the scheme, the signing algorithms which all original signers and proxy signers use for the sake of proxy delegation and multi-proxy multi-signing, can be any digital signature algorithms based on identity or attribute. As to the generation of the proxy signers' proxy signing key packages, in the scheme, it is produced by PI. Thus, the scheme is proxy-protected.

Due to the page constraints, we will detail correctness and security analysis of the proposed scheme in the full version.

5 Conclusions

In the paper, we construct a model of MPMS binding positioning protocol. Its definition, security properties and construction are given. As far as we know, it is the first model of combining positioning protocol, proxy signature and MPMS.

In the meantime, we also propose one secure-positioning-protocol-based MPMS scheme. We will further improve relevant models and schemes. We believed that the research on positioning-protocol-based cryptographic models or schemes will become one focus in the setting of mobile Internet.

Acknowledgments. This paper is supported by NSFC under Grant No. 61170227 and 61411146001, 973 Project under Grant No. 2012CB723401, Ministry of Education Fund under Grant No. 14YJA880033, and Shanghai Projects under Grant No. 2013BTQ001, XZ201301 and 2013001.

References

1. Chandran, N., Goyal, V., Moriarty, R., Ostrovsky, R.: Position based cryptography. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 391–407. Springer, Heidelberg (2009)
2. Naveen, S., Umesh, S., David, W.: Secure verification of location claims. In: Proceedings of the 2nd ACM Workshop on Wireless Security, pp. 1–10. ACM (2003)
3. Dave, S., Bart, P.: Location verification using secure distance bounding protocols. In: 2005 IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, p. 7. IEEE (2005)
4. Laurent, B.: Trust Establishment Protocols for Communicating Devices. Ph.D. thesis, Eurecom-ENST (2004)
5. Capkun, S., Hubaux, J.-P.: Secure positioning of wireless devices with application to sensor networks. In: Proceedings of IEEE INFOCOM 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1917–1928. IEEE (2005)
6. Capkun, S., Srivastava, M., Cagalj, M.: Secure localization with hidden and mobile base stations. In: IEEE Conference on Computer Communications (INFOCOM) (2006)
7. Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R., Schaffner, C.: Position-based quantum cryptography: impossibility and constructions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 429–446. Springer, Heidelberg (2011)
8. Harry, B., Serge, F., Christian, S., Florian, S.: The Garden-Hose Game: A New Model of Computation, and Application to Position-Based Quantum Cryptography (2011). arXiv: 1109.2563
9. Mambo, M., Usuda, K., Okamoto, E.: Proxy signature for delegating signing operation. In: Proceedings of the 3rd ACM Conference on Computer and Communications Security, New Dehli, pp. 48–57. ACM, New York (1996)
10. Li, J.G., Cao, Z.F., Zhang, Y.C.: Nonrepudiable proxy multi-signature scheme. J. Comput. Sci. Technol. **18**(3), 399–402 (2003)
11. Hwang, S.J., Chen, C.C.: Cryptanalysis of nonrepudiable threshold proxy signature scheme with known signers. Informatica **14**(2), 205–212 (2003)
12. Tsai, C.S., Tzeng, S.F., Hwang, M.S.: Improved nonrepudiable threshold proxy signature scheme with known signers. Informatica **14**(3), 393–402 (2003)
13. Hwang, S.J., Chen, C.C.: A new multi-proxy multi-signature scheme. In: 2001 National Computer Symposium on Information Security, pp. F019–F026, Taipei, Taiwan, ROC (2001)

http://www.springer.com/978-3-319-21836-6

Wireless Algorithms, Systems, and Applications
10th International Conference, WASA 2015, Qufu, China, August 10-12, 2015, Proceedings
Xu, K.; Zhu, H. (Eds.)
2015, XVII, 858 p. 345 illus., Softcover
ISBN: 978-3-319-21836-6