Threshold Proxy Signature Based on Position

Qingshui Xue
Dept. of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai, China
xue-qsh@cs.sjtu.edu.cn

Fengying Li
School of Continuous Education
Shanghai Jiao Tong University
Shanghai, China
fyli@sjtu.edu.cn
zfcao@cs.sjtu.edu.cn

Zhenfu Cao
Dept. of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai, China

Abstract—**Position-based cryptography has attracted lots of researchers' attention. In the mobile Internet, there are many position-based security applications. For the first time, one new conception, threshold proxy signature based on positions is proposed. Based on one secure positioning protocol, one model of threshold proxy signature based on positions is proposed. In the model, positioning protocols are bound to threshold proxy signature tightly, not loosely. Further, one position-based threshold proxy signature scheme is designed, its correctness is proved, and its security is analyzed. As far as we know, it is the first threshold proxy signature scheme based on positions.**

Keywords-position; threshold proxy signature; proxy signature; UC security; model; scheme.

I. 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 Global Positioning System (GPS) 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. For example, when one mobile user sends messages to one specific position, which is one either physical address or logical address (such as Internet Protocol address), it is desirable for us that only the user who is at that address or has been at that address can receive and decrypt messages encrypted. Even if other mobile users at that position receive messages, but they can't decrypt them. Or the specified receiver at that position due to some reasons temporarily leaves his/her position, it will not be able to receive or decrypt messages any more. In addition, if the specified receiver at that place moves to another place, and he/she hopes he/she can receive messages at the new place. 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 receive the signed message and verify whether or not received messaged 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.

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]-[9]. 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. Relying on the thoughts, in the paper, our main contributions are as follows.

(1)One model of threshold proxy signature based on positions is proposed. Position-based threshold proxy signature is one kind of threshold proxy signature, but a novel one. The definition is given and its model is constructed. In the meantime, its security properties are defined.

(2)To realize the kind of threshold proxy signature, one secure-positioning-protocol based threshold proxy signature scheme is proposed and its security is analyzed as well.

The rest of the paper is organized as follows. In Section 2, the function of positioning and one secure positioning protocol are introduced. In Section 3, the model and definition of threshold proxy signature based on positions are constructed. One position-based threshold proxy signature scheme is designed in Section 4. The correctness of the scheme is proved in Section 5. The security of the proposed scheme will be analyzed in Section 6. Finally, the conclusion is given.

 ISBN: 978-1-61208-376-6

II. POSITION PROTOCOLS

In this section, the function of positioning protocols and one secure positioning protocol are introduced.

A. 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 work 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.

B. One Secure Positioning Protocol

Here, one others' positions secure positioning protocol is introduced. Compared with your own position positioning protocol, others' positions positioning protocol is more complex.

In this section, N. Chandran et al.'s secure positioning protocol in 3-dimensions is reviewed [1], which can be used in mobile Internet.

In the protocol, 4 verifiers denoted by $V_1, V_2, ..., V_4$, which can output string X_i, are used. The prover claims his/her position, which is enclosed in the tetrahedron defined by the 4 verifiers. Let $t_1, ..., t_4$ be the time taken for radio waves to arrive at the point P from verifier $V_1, V_2, ..., V_4$ respectively. When we say that $V_1, V_2, ..., V_4$ 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 $T - t_4$ 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 $PRG: \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^m$. 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. $V_1, ..., V_3$ and V_4 pick keys $K_1, ..., K_3$ and K_4 selected randomly from $\{0,1\}^m$ and broadcast them through their private channel.

Step 2. For the purpose of enabling the device at P to calculate K_i for $1 \le i \le 4$, 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 $1 \le i \le 3$. 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 and it is supposed to be indeed at position P. Otherwise, the position claim is invalid.

III. THE MODEL OF POSITION-BASED THRESHOLD PROXY SIGNATURE

The model, definition and security properties are proposed in this section.

A. The model

In the model, there are four kinds of participants including the original signer (OS), the proxy signer group (PSG), which consists of n proxy signers $\{PS_1, PS_2, ..., PS_n\}$, the verifier (V) and position infrastructure (PI). OS takes responsibility of confirmation of position of his/her own and at one position delegates his/her signing power to the proxy signer group to sign messages at these proxy signers' positions on behalf of OS. $t(t \le n)$ or more proxy signers cooperate to sign one message at their individual positions after their positions are confirmed by PI and are the same as the ones in the proxy signing delegation warrant, whereas, less than t proxy signers can't. V checks that the proxy signature is generated by the actual proxy signers at their individual positions on behalf of OS. PI, which is one trusted third party, is used to provide position services for the related parties. The model is illustrated in Figure 1.

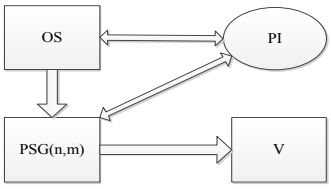

Figure 1. Model of position-based threshold proxy signature.

B. Definition

Position-based threshold proxy signature.

Simply speaking, the kind of proxy signature combines proxy signature, threshold proxy signature and positioning protocols as one single scheme. It is mainly composed of three modules of threshold proxy signing power delegation, threshold proxy signing and threshold proxy signature verifying. In the module of threshold proxy signing power delegation, OS first sends one request to PI for the purpose of delegating signing power to PSG. Then PI runs one positioning protocol to confirm OS and the proxy signers' positions. If their positions are valid, PI sends acknowledge to OS and the proxy signers. After that, PI produces proxy signing key packages for individual proxy signers and sends them to each proxy signer. OS produces proxy delegation warrant to all proxy signers. In the module of threshold proxy

 ISBN: 978-1-61208-376-6

signing, each proxy signer who wants to actually attend to sign has to first check that his/her position is at the designated position, which is specified in the proxy delegation warrant. If it holds, each actual proxy signer can use his/her proxy signing key package to sign the message for only once and sends individual proxy signature to one clerk who collects all individual signatures and generates final threshold proxy signature. In the module of threshold proxy signature verifying, V uses OS and all proxy signers' identities and positions to check the validity of threshold proxy signatures based on positions.

Remark 1. During the module of threshold proxy signing power delegation, if OS and all of proxy signers don't run positioning protocols with PI to confirm their own positions, OS is unable to delegate his/her signing power to the proxy signer group. Moreover, if neither OS nor each proxy signer can confirm its position with PI, OS can't fulfill his delegation of signing power. In the module of threshold proxy signing, if each of proxy signers doesn't perform positioning protocols to check the validity of his/her position, he/she is not able to generate individual proxy signature by individual proxy signature key package. That's to say, before the proxy signer group wants to sign one message on behalf of OS, each member has to confirm its position. Even if each proxy signer passes individual position's confirmation, he/she can sign one message for only once. During the module of threshold signature verifying, it is unnecessary for the verifier to confirm OS and all proxy signers' positions.

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

Thus, in the model, the positioning-based threshold proxy signature is composed of four primitives:Initialization, PropTProxyDelegate, PropTProxySign and PropTProxyVerify.

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

PropTProxyDelegate. When OS wants to delegate his/her signing power to the proxy signer group, OS first sends his/her requests to PI. After PI gets OS's request, PI checks the validity of positions $Pos_{OS}, Pos_{PS_1}, Pos_{PS_2}, ..., Pos_{PS_n}$ of OS and all proxy signers by running positioning protocol with OS and PS. If OS and all proxy signers' positions are valid, PI sends the acknowledgment to OS. According to the acknowledgment from PI, OS generates delegation warrant dw and sends it to each proxy signer PS_i $(i = 1, 2, ..., n)$. At the same time, PI produces proxy signing key package $pskp_i$ for PS_i $(i = 1, 2, ..., n)$. dw contains OS and all proxy signers' identities and positions, n, t (threshold value), message types to sign, expiry date and so forth. $pskp_i$ encapsulates positioning protocol, proxy signing key, the i^{th} proxy signer's identity ID_{PS_i} and position Pos_{PS_i}, signing algorithm, etc.

PropTProxySign. Before the proxy signer group wants to sign the message m on behalf of OS, actual proxy signer PS_i $(i = 1, 2, k. t\leq k\leq$ (here, assume that PS_i $(i = 1, 2, ..., k)$ are the proxy signers participating in the signing, denoted by aps)first executes individual proxy signing key package $pskp_i$ to run positioning protocol to confirm the validity of his/her position Pos_{PS_i} with PI. If his/her current position Pos_{PS_i} is identical to the one in the delegation warrant dw, he/she is able to use proxy signing key package $pskp_i$ to sign the message m for only once and sends corresponding individual proxy signature (m, s_i, dw, pp) to the Clerk, who collects and verifies individual signatures, and generates final threshold proxy signature. The Clerk checks the validity of individual signature s_i by using the identity ID_{PS_i} and position Pos_{PS_i} of PS_i and corresponding verification algorithm. If the number of the actual proxy signers k is equal to or more than t, and less than or equal to n, and k individual signatures are valid, the Clerk will generate the final threshold proxy signature (m, s, dw, asp, pp) and send it to V. Here, simply denote s by $s = \prod_{i=1}^{k} s_i$.

PropTProxyVerify. After receiving the threshold proxy signature (m, s, dw, asp, pp) from the proxy signer group, V takes as input the identities $ID_{OS}, ID_{PS_1}, ID_{PS_2}, ..., ID_{PS_n}$, positions $Pos_{OS}, Pos_{PS_1}, Pos_{PS_2}, ..., Pos_{PS_n}$, asp and pp to check whether or not s is the threshold proxy signature on the message m by using corresponding threshold proxy signature verification algorithm. If it holds, V can be sure that the message m was signed by actual proxy signers PS_i $(i = 1, 2, ..., k)$ at position Pos_{PS_i} $(i = 1, 2, ..., k)$ on behalf of OS who delegated his/her signing power to the proxy signer group at the position Pos_{OS}.

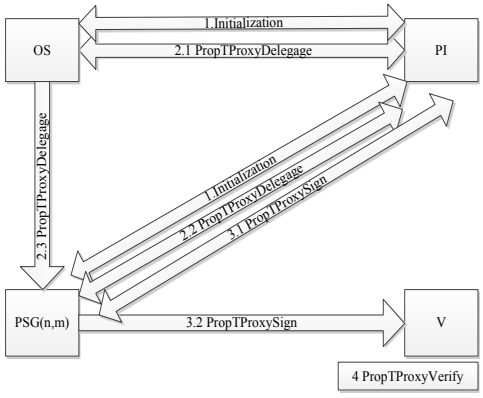

Figure 2. Position-based threshold proxy signature.

The model is illustrated in Figure 2.

C. Security Properties of Position-Based Threshold Proxy Signature

Besides security properties of threshold proxy signature, this kind of threshold proxy signature has the security properties as follows.

(1) Positioning protocol binding. In the module of PropTProxyDelegate, without confirming of positions of OS and all proxy signers by running positioning protocol with PI, OS is unable to fulfill his/her delegation of signing power. In addition, the proxy signing key package of each proxy signer produced by PI is tightly bound with positioning protocol, as means that if all of proxy signers want to use proxy signing key packages, each of them has to run positioning protocol with PI. In the module of PropTProxySign, if the proxy signer group needs to sign one message on behalf of OS, in order to get the proxy signing key (implicitly), each of proxy signers has to make use of individual proxy signing key package to run positioning protocol with PI. If each of proxy signers is indeed at the position specified in the delegation warrant dw, he/she will be able to obtain (implicitly) the proxy signing key to sign one message for once only. Actually, each of proxy signers can't get real individual proxy signing key, which is encapsulated in the proxy signing key package.

Remark 2. In the model, for each time, if the proxy signers want to cooperate to sign messages on behalf of OS, each of them has to run positioning protocol with PI to confirm the validity of individual positions. One maybe thinks we should make use of one-time digital signing algorithm or one-time signing private key. In fact, in the model, using one-time signing key is optional. On one hand, if the model uses fixed signed private key encapsulated in the proxy signing key package, each of proxy signers can't use it at will and can sign one message for only once. If the proxy signer group wants to sign another message, all of them still need to communicate with PI once again. In the sense, each of proxy signers actually has no the knowledge of its own proxy signing private key. On the other hand, if one-time signing private keys are used in the model, it is reasonable. That is to say, for each time, each proxy signing key package will release one random proxy signing key. In addition, because position-based applications are closely related with position instant authentication or confirmation, we think that position-based cryptography should be deeply researched with respect to online cryptography, which focuses on instant cryptographic algorithms and security processing. Of course, in the eyes of ours, it is one open question as well.

IV. ONE POSITION-BASED THRESHOLD PROXY SIGNATURE SCHEME

In this section, one position-based threshold proxy signature scheme, in which there exist one original signer and n proxy signers, is proposed. The scheme mainly includes four kinds of participants:the original signer (still denoted as OS), the proxy signer group (PSG) $PSG = \{PS_1, PS_2, ..., PS_n\}$, the verifier (V) and PI. PI will make use of the secure positioning protocol mentioned in Section 2.2 to provide services of position for the original signer and n proxy signers. In addition, PI will be regarded as the trusted third party and system authority. The scheme is composed of four primitives:Initialization, PropTProxyDelegate, PropTProxySign and PropTProxyVerify. As primitives, it means that they either fully run or do nothing. The four primitives are detailed as follows.

A. 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. Here, rewrite the primitive as Initialization (k, mk, pp).

B. PropTProxyDelegation

Step 1. The original signer sends his/her requests $(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, ..., ID_{PS_n}, Pos_{PS_n}, req_{deleg})$ of delegating signing power to the proxy signer group to PI.

Step 2. After PI gets OS's request, PI checks the validity of the positions $Pos_{OS}, Pos_{PS_1}, Pos_{PS_2}, ..., Pos_{PS_n}$ of OS and all proxy signers by running positioning protocol with OS and each proxy signer.

Step 3. If OS and all proxy signers' positions $Pos_{OS}, Pos_{PS_1}, Pos_{PS_2}, ..., Pos_{PS_n}$ are valid, as means that OS is indeed at the position Pos_{OS} and Pos_{PS_i} is one valid position of PS_i $(i = 1, 2, ..., n)$, PI sends the acknowledgement $(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, ..., ID_{PS_n}, Pos_{PS_n}, ack_{deleg})$ to OS; otherwise PI sends $(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, ..., ID_{PS_n}, Pos_{PS_n}, rej_{deleg})$ to OS.

Step 4. If OS receives $(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, ..., ID_{PS_n}, Pos_{PS_n}, ack_{deleg})$ from PI, he/she generates delegation warrant $dw(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, ..., ID_{PS_n}, Pos_{PS_n}, Sign_{OS}(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, ..., ID_{PS_n}, Pos_{PS_n}))$ where $Sign_{OS}(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, ..., ID_{PS_n}, Pos_{PS_n})$ is the digital signature on $(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2}, ..., ID_{PS_n}, Pos_{PS_n})$ generated by OS, and sends it to each proxy signer.

Step 5. PI produces proxy signing key package $pskp_i$ for each proxy signer and sends it to PS_i $(i = 1, 2, ..., n)$. $pskp_i$ encapsulates positioning protocol, proxy signing key, signing algorithm, the identity and position of PS_i, etc. Anyone wanting to use proxy signing key and signing algorithm in $pskp_i$ has to run the proxy signing key package $pskp_i$.

 ISBN: 978-1-61208-376-6

C. PropTProxySign

Step 1. When the proxy signer group wants to sign the message m on behalf of OS, each actual proxy signer PS_i $(i=1,2,...,k, t \le k \le n)$ (here, assume that PS_i $(i=1,2,...,k)$ are the actual proxy signers, denoted by asp)runs proxy signing key package $pskp_i$ for executing positioning protocol to confirm the validity of his/her position Pos_{PS_i} with PI.

Step 2. If $PS_i's$ 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 send it to the Clerk; 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 $(i=1,2,...,k)$.

Step 3. After the Clerk receives the individual proxy signature s_i , he/she checks s_i is the individual proxy signature by using verification algorithm, the identity and position of PS_i $(i=1,2,...,k)$.

Step 4. If all $s_i's$ verification hold, the Clerk generates the final threshold proxy signature s by processing all individual proxy signatures s_i $(i=1,2,...,k)$. Here, simply denote s by $s=\prod_{i=1}^{k} s_i$.

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

D. PropTProxyVerify

Step 1. After receiving the threshold proxy signature (m,s,dw,aps,pp) , V takes as input the identities $ID_{OS}, ID_{PS_1}, ID_{PS_2},..., ID_{PS_n}$, positions $Pos_{OS}, Pos_{PS_1}, Pos_{PS_2}$, $..., Pos_{PS_n}$ from dw and pp to check that the proxy delegation warrant dw is valid. If it is valid, the scheme continues, or V fails to stop.

Step 2. V takes as input the identities $ID_{OS}, ID_{PS_1}, ID_{PS_2},..., ID_{PS_n}$, positions $Pos_{OS}, Pos_{PS_1}, Pos_{PS_2}$, $..., Pos_{PS_n}$ from dw, aps and pp to check whether or not s is the threshold proxy signature on the message m , and $t \le k \le n$. If it holds, V can be sure that the message m was signed by actual proxy signers at individual position Pos_{PS_i} $(i=1,2,...,k)$ on behalf of OS who delegated his/her signing power to the all proxy signers at the position Pos_{PS_i} $(i=1,2,...,n)$, and all proxy signers.

V. CORRECTION OF THE ABOVE SCHEME

In fact, the proof of correctness of above scheme is simple. The following theorem about it is given.

Theorem 1:If the scheme accurately and sequentially runs according to the primitives above, the verifier V can confirm that the threshold proxy signature is generated by the actually proxy signers asp at individual position Pos_{PS_i} $(i=1,2,...,k)$ on behalf of the original signer OS who at the position Pos_{OS} delegates his/her signing power to the group of proxy signers, and all proxy signers.

Proof.

In the primitive of PropTProxyDelegation, PI checks the validity of positions $Pos_{OS}, Pos_{PS_1}, Pos_{PS_2},..., Pos_{PS_n}$ of OS and all proxy signers by running positioning protocol with OS and each proxy signer. If all of positions are valid, as means that OS is actually at the position Pos_{OS} and Pos_{PS_i} is one valid position of PS_i $(i=1,2,...,n)$, PI sends the acknowledgement $(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2}, Pos_{PS_2},$ $..., ID_{PS_n}, Pos_{PS_n}, ack_{deleg})$ to OS. Then OS can generates delegation warrant $dw(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1}, ID_{PS_2},$ $Pos_{PS_2},..., ID_{PS_n}, Pos_{PS_n}, Sign_{OS}(ID_{OS}, Pos_{OS}, ID_{PS_1}, Pos_{PS_1},$ $ID_{PS_2}, Pos_{PS_2},..., ID_{PS_n}, Pos_{PS_n}))$ and sends it to each proxy signer. At the same time, OS produces proxy signing key package $pskp_i$ for each proxy signer and sends it to $PS_i's$ $(i=1,2,...,n)$. In the primitive of PropTProxySign, when the proxy signer group wants to sign the message m on behalf of OS, the actual proxy signers PS_i $(i=1,2,...,k)$ runs proxy signing key package $pskp_i$ for executing positioning protocol to confirm the validity of his/her position Pos_{PS_i} with PI. If $PS_i's$ 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 Clerk. After the Clerk receives the individual proxy signatures s_i , he/she checks s_i is the individual proxy signature by using verification algorithms, the identities and positions of PS_i $(i=1,2,...,k)$. If all $s_i's$ verification hold, the Clerk generates the final threshold proxy signature s by processing all individual proxy signatures s_i $(i=1,2,...,k)$. Finally, the Clerk sends (m,s,dw,asp,pp) to the proxy signature verifier V. In the primitive of PropTProxyVerify, V takes as input the identities $ID_{OS}, ID_{PS_1}, ID_{PS_2},..., ID_{PS_n}$, positions $Pos_{OS}, Pos_{PS_1}, Pos_{PS_2}$, $..., Pos_{PS_n}$ from dw and pp to check that the proxy delegation

warrant dw is valid. Next, V takes as input the identities $ID_{OS}, ID_{PS_1}, ID_{PS_2}, ..., ID_{PS_n}$, positions $Pos_{OS}, Pos_{PS_1}, Pos_{PS_2}, ..., Pos_{PS_n}$ from dw, asp and pp to check whether or not s is the threshold proxy signature on the message m. If it holds, V can be sure that the message m was signed by the actual proxy signers at individual position Pos_{PS_i} $(i = 1, 2, ..., k)$ on behalf of OS who delegated his/her signing power to all proxy signers at the position Pos_{PS_i} $(i = 1, 2, ..., k)$, and all proxy signers. Thus, it is proved.

□

VI. Security Analysis of the Proposed Scheme

In the proposed scheme, three sorts of technology, i.e., secure positioning protocol including others' positions positioning protocol and your own position positioning, proxy signature and threshold proxy signature, are used. That means, the security of the proposed scheme depends on the security of used three kinds of technology. Because the proposed scheme or the model is one component framework, it is proper that its security is analyzed by the Universal Composition (UC) framework [10]. That is, by constructing the components of proxy signature model, digital signature model and positioning protocol model, and attack modeling from internal attackers, external attackers and conspiracy attackers, the security analysis of the above scheme can be made. The internal attackers are from the original signer and proxy signers; the external attackers can be any software systems or entities; the conspiracy attackers mainly are among proxy signers, partially between both the original signer and some malicious proxy signers. By adding these models into the idealistic environment in UC framework, if the security of the scheme in the idealistic environment can be proved secure, its security in the real environment can be proved as well. Its security analysis will be deeply done in the further study.

VII. Conclusion and Future Work

In the paper, according to security requirements of the mobile Internet, one model of position-based threshold proxy signature is constructed. Its definition, security properties and construction are given. As far as we know, it is the first model of combining positioning protocols, proxy signature and threshold proxy signature. In the meantime, one position-based threshold proxy signature scheme is proposed and analyze its security. We will further improve relevant models and schemes. It is believed by us that the research on positioning-protocol-based cryptographic models or schemes will become one focus in the setting of the mobile Internet.

Acknowledgment

I would like to thank so many anonymous reviewers for their advices of modification and improvements. In addition, this paper is supported by NSFC under Grant No. 61170227, Ministry of Education Fund under Grant No. 14YJA880033, and Shanghai Projects under Grant No. 2013BTQ001, XZ201301 and 2013001.

References

[1] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position Based Cryptography," CRYPTO 2009, Aug. 2009, pp. 391-407, doi: 10.1007/978-3-642-03356-8_23.

[2] S.M. Bilal, C.J. Bernardos, and C. Guerrero, "Position-based routing in vehicular networks: A survey," Journal of Network and Computer Applications, vol. 36, Feb. 2013, pp. 685-697, doi: doi: 10.1016/j.jnca.2012.12.023.

[3] D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," IEEE Conference on Mobile Adhoc and Sensor Systems Conference, Nov. 2005, pp. -840 doi: 10.1109/MAHSS.2005.1542879.

[4] A. Fonseca and T. Vazão, "Applicability of position-based routing for VANET in highways and urban environment," Journal of Network and Computer Applications, vol. 36, Mar. 2013, pp. 961-973, doi: 10.1016/j.jnca.2012.03.009.

[5] S. Capkun and J. P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," IEEE INFOCOM, Mar. 2005, pp. 1917-1928, doi: 10.1109/INFCOM.2005.1498470.

[6] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations," IEEE INFOCOM, Apr. 2006, pp. 1-10, doi: 10.1109/INFOCOM.2006.302.

[7] H. Buhrman et. al., "Position-Based Quantum Cryptography: Impossibility and Constructions," CRYPTO 2011, Aug. 2011, pp. 429-446, doi: 10.1007/978-3-642-22792-9_24.

[8] H. Buhrman et. al., "Position-Based Quantum Cryptography: Impossibility and Constructions," SIAM J. Comput., vol. 43, Jan. 2014, pp. 150–178, doi: 10.1137/130913687.

[9] T.Y. Wang and Z.L. Wei, "One-time proxy signature based on quantum cryptography," Quantum Information Processing, vol. 11, Feb. 2012, pp. 455-463, doi: 10.1007/s11128-011-0258-6.

[10] R. Canetti, "Universally composable security:a new paradigm for cryptographic protocols,"., 2001. Proceedings. 42nd IEEE Symposium on Foundations of Computer Science, Oct. 2001, pp. 136-145, doi: 10.1109/SFCS.2001.959888.

 ISBN: 978-1-61208-376-6