Position based key exchange: definitions and implementations

ZHANG Junwei, DU Fangqiong, MA Jianfeng, YANG Chao

School of Cyber Engineering, Xidian University, Xi'an 710071, China

Abstract: Chandran, et al. introduce the direction of position based cryptography at CRYPTO 2009. In position based cryptography, the position of a party is used to be its unique “credential” in order to realize the cryptographic tasks, such as position based encryption, position based signature, position based key exchange and so on. Position based key exchange, as a basic primitive in position based cryptography, can be used to establish a shared key based on the position of the participant. To begin with, this paper presents the notions of the prover-to-verifier mode and the prover-to-prover mode for position based key exchange. In the prover-to-verifier mode, a secret key can be shared between a prover and the verifiers according to the position of the prover. While in the prover-to-prover mode, two provers located at the valid positions can negotiate a shared key with the help of the verifiers and any other party whose position is illegal cannot obtain the shared key. At the same time, this paper formalizes two security definitions against colluding adversaries: position based prover-to-verifier key exchange and position based prover-to-prover key exchange. Then, this paper introduces the bounded retrieval model and the implementations of position based key exchange in two modes based on the bounded retrieval model. Finally, this paper discusses the position based key exchange protocols in two modes from both security and performance perspectives.

Key words: position based key exchange, position based cryptography, prover-to-verifier, prover-to-prover, bounded retrieval model

Citation: ZHANG J W, DU F Q, MA J F, et al. Position based key exchange: definitions and implementations[J]. Journal of communications and information networks, 2016, 1(4): 33-43.

1 Introduction

Location information about wireless devices is valuable due to its crucial role in data collection, reliable communications, resource management, emergency services/maintenance, and other important functions of wireless systems^[1]. At the same time, security issues in location based systems have received increasing attention^[2]. Thus, the method of

utilizing the location of a device to achieve security management in location based systems is becoming a focus nowadays.

It is well known that in classic cryptography a party holds some credentials so that its identity, access authority, etc. can be determined. Usually, the credentials consist of the following parts: a registered identity (e.g., an email address), secret knowledge (e.g., a pre-shared key or a password), authenticated

Manuscript received Sept. 06, 2016; accepted Nov. 22, 2016.

This work is supported by the National High Technology Research and Development Program of China (863 Program) (No. 2015AA016007), the National Natural Science Foundation of China (Nos. U1405255, 61472310, 61372075).

information (e.g., a certification issued by CA), a trusted computing base (e.g., a TPM^[3]), biometric data (e.g., a fingerprint) and so on. However, the location of a device or a user, which is an important piece of information, cannot be used as a credential and applied to realize cryptographic tasks in classic cryptography.

At CRYPTO 2009, Chandran, et al.^[4] first introduced the notion of position based cryptography, in which the credential of a party comes from its geographic location. At the same time, the design of secure cryptographic protocols using location as a credential such as secure positioning and position based key exchange, was also investigated. Unfortunately, as a vital primitive in position based cryptography, secure positioning has been proven to have no secure position protocol under collusion attacks without set-up assumptions. As a result, none of the position based cryptographic tasks, including position based key exchange, can be carried out without set-up assumptions. In the BRM (Bounded Retrieval Model), Chandran et al. propose secure positioning protocols resistant to collusion attacks. They also propose a secure position based key exchange protocol in the BRM^[4]. Subsequently, some position based cryptographic protocols have been proposed in the quantum model^[5-7]. Recently, the composition security of position based cryptography has also been investigated in universally composable security models^[8,9].

PbKE (Position based Key Exchange), which can establish a secret key between a prover located at a valid position and one verifier (or all of the verifiers), is one of the fundamental tasks in position based cryptography. The position based key exchange protocol proposed by Chandran^[4] can only realize key establishment between prover and verifier, which is called the p2v (Prover-to-Verifier) mode.

Besides the p2v mode, position based key exchange between two provers, called p2p (Prover-to-

Prover) mode, should also be considered one of the most important tasks in position based cryptography^[10].

This paper investigates the security definitions and the implementations of position based key exchange in two modes. Our contributions are shown below. In particular.

1) To begin with, we distinguish between the two modes of position based key exchange in position based cryptography: the p2v mode and the p2p mode.

2) Then we present the security definitions of position based key exchange. The p2v mode guarantees that one prover (located at one valid position) can share a secret key with the verifiers against the colluding adversaries. In contrast, the p2p mode guarantees that one prover (located at one valid position) can share a secret key with another prover (located at another valid position), while colluding adversaries cannot access any information about the shared key.

3) Under the BRM, we discuss the implementation of position based key exchange, which includes p2v key exchange protocols and p2p key exchange protocols.

4) Finally, we compare existing position based key exchange protocols from both security and performance perspectives.

The organization of the rest paper is as follows: Section 2 introduces the p2v mode and the p2p model and gives their security definitions. In Section 3, we present the position based p2v key exchange protocols in one dimension, while Section 4 presents the position based p2p key exchange protocols. We also present extensions of the PbKE protocols in Section 5. Section 6 compares the above protocols in three dimensions. Section 7 concludes our results.

2 The two modes and their security definitions

In this section, we introduce the adversary model, the

assumptions used in this paper and the two modes of key exchange in position based cryptography.

2.1 The adversary model

The colluding adversaries in PbKE protocols have the following capabilities:

- 1) Adversaries can access all messages (except high min-entropy information in the BRM) when they pass through the wireless communication channel.
- 2) Adversaries can send any forged message in the wireless communication channel.
- 3) An adversary can be located at any position except the target position when the prover located in that target position runs a PbKE protocol.

Note that corruption of a prover or a verifier is not considered in position based cryptography. One hand, a prover has no pre-sharing of cryptographic keys, and the unique credential of the prover is its position. the other hand, a secure position based key exchange protocol could not be realized without trusted verifiers.

2.2 The prover-to-verifier mode

In the p2v mode, a PbKE protocol in d -dimensions consists of a unique prover, some verifiers (at least $d+1$), and a group of colluding adversaries. At the end of a secure p2v key exchange protocol, the prover located at a valid position can securely share a key with verifiers against the colluding adversaries. For example, the p2v mode of key exchange in 2-dimensions is shown in Fig.1.

Formally, a position based p2v key exchange protocol π in d -dimensional space consists of two algorithms, i.e. $\pi = (Init, Key)$: the position initialization algorithm $Init(P)$ and the key exchange algorithm $Key(V, P, p)$. There is a set of verifiers $V = \{V_0, V_1, \dots, V_D\}$ at positions $pos_0, pos_1, \dots, pos_D$ respectively ($D \leq d$). At the same time, there are

colluding probabilistic polynomial time adversaries $A = \{A_1, A_2, \dots, A_K\}$ at positions $apos_1, apos_2, \dots, apos_K$ respectively. The $Init(P)$ algorithm initializes the location of prover P , i.e. if $Init(P) = p$, this means that the location of P is position p where p is in the tetrahedron enclosed by $pos_0, pos_1, \dots, pos_D$. The $Key(V, P, p)$ algorithm against colluding PPT (Probabilistic Polynomial Time) adversaries $A = \{A_1, A_2, \dots, A_K\}$ establishes a shared secret key $sk = Key(V, P, p)$ between uncorrupted P and V if P is located at p .

Figure 1 The p2v mode in 2-dimensions

Definition 1 (Position based p2v key exchange) A position based p2v key exchange protocol π is called a secure position based p2v key exchange protocol in security parameter k if for all sets of $A = \{A_1, A_2, \dots, A_K\}$, given $(V, P, p = Init(P))$, it is able to distinguish between $sk = Key(V, P, p)$ and a uniform string U (where $|U| = |sk|$) with a negligible function $\epsilon(k)$. Formally,

$$|\Pr[A^{V,P,p}(sk) = 1] - \Pr[A^{V,P,p}(U) = 1]| \leq \epsilon(k). \quad (1)$$

2.3 The prover-to-prover mode

As opposed to the p2v mode, the p2p mode deals with position based key exchange between two provers (with the help of verifiers). Fig.2 shows position based p2p key exchange in two dimensions.

Similar to the p2v mode, a position based p2p key exchange protocol π in d -dimensional space consists of two algorithms, i.e. $\pi = (Init, Key)$: the

position initialization algorithm $Init(P)$ and the key exchange algorithm $Key(V, P_1, p_1, P_2, p_2)$. A set of verifiers is denoted by $V = \{V_0, V_1, \dots, V_D\}$ at positions $pos_0, pos_1, \dots, pos_D$ respectively ($D \leq d$). The colluding probabilistic polynomial time adversaries are denoted by $A = \{A_1, A_2, \dots, A_K\}$ at positions $apos_1, apos_2, \dots, apos_K$ respectively. The $Init(P)$ algorithm can set the location of a prover P as position p where p is in the tetrahedron enclosed by $pos_0, pos_1, \dots, pos_D$. The $Key(V, P_1, p_1, P_2, p_2)$ algorithm against colluding PPT adversaries $A = \{A_1, A_2, \dots, A_K\}$ could establish a shared secret key $sk = Key(V, P_1, p_1, P_2, p_2)$ between uncorrupted P_1 and P_2 if P_1 is located at p_1 and P_2 is located at p_2 .

Figure 2 The p2p mode in 2-dimensions

Definition 2 (position based p2p key exchange) A position based prover-to-prover key exchange protocol π is called a secure position based p2p key exchange protocol in security parameter k if for all sets of $A = \{A_1, A_2, \dots, A_K\}$, given $(V, P_1, P_2, p_1 = Init(P_1), p_2 = Init(P_2))$, it is able to distinguish between $sk = Key(V, P_1, p_1, P_2, p_2)$ and a uniform string U (where $|U| = |sk|$) with a negligible function $\varepsilon(k)$. Formally,

$$|\Pr[A^{V, P_1, P_2, p_1, p_2}(sk) = 1] - \Pr[A^{V, P_1, P_2, p_1, p_2}(U) = 1]| \leq \varepsilon(k). \quad (2)$$

2.4 Assumptions

In this subsection, we present the assumptions used in this paper.

Assumption 1 (The BRM) As in the underlying model in Ref.[4], the protocols in this paper are based on the BRM. The bounded retrieval model assumes

that all adversaries can only retrieve part of high min-entropy information. More specifically, we have:

1) Verifiers can generate n -bit string X , where X has high min-entropy $(\delta + \beta)n$.

2) All adversaries can retrieve any part of X when X passes. However, the total retrieved information about X is no more than βn .

Assumption 2 (Private channel) We assume that there is a private channel among all of the verifiers in position based cryptography, i.e. that they can share any message securely.

Assumption 3 (Authenticated broadcast) In this paper, we assume that anyone of the verifiers has an authenticated broadcast channel in this paper. In other words, no adversary can modify or forge a message sent from a verifier in an authenticated channel.

It is also worth noting that there are some very efficient broadcast authentication protocols that can be used for position based cryptography, such as μ TESLA^[11], one-time signature^[12] and so on.

Assumption 4 (DDH assumption) Consider a cyclic group G with prime order q and generator g . If a and b are chosen randomly from Z_q , then any PPT adversary A can distinguish between $\{g^a, g^b, g^{ab}\}$ and $\{g^a, g^b, R\}$ with only negligible probability, where R is a uniform string and $|R| = |g^{ab}|$.

In addition, we use BSM PRG (BSM pseudorandom generators)^[4] and PRF (pseudorandom function family)^[13] to construct the PbKE protocols. Due to space limitations, we omit detailed description of BRM, BSM PRG, PRF and other cryptographic operations.

3 PbKE protocols in the p2v mode

In this section, we first present a position based p2v key exchange protocol in one dimension. Then, we present a generic version of the p2v key exchange protocol $p2pKE^d$ in d -dimensions ($d \in \{1, 2, 3\}$).

3.1 Protocol $p2vKE^1$ in one dimension

The position based $p2v$ key exchange protocol in one dimension, denoted by $p2vKE^1$, is shown in Fig.3. For one dimension, we employ two verifiers, denoted by V_0 and V_1 , which send messages at the speed of radio waves.

We assume that the position p being claimed by prover P is located between V_0 and V_1 .

Protocol $p2vKE^1$ is secure against an arbitrary number of adversaries colluding to establish a secret key between P and $V=\{V_1, V_2\}$ as long as the total information that these adversaries can retrieve during the protocol is bounded.

A detailed description of protocol $p2vKE^1$ in the BRM is as follows:

BSM PRG $F: \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^m$.

Initialization: Prover P runs the algorithm $Init(P)$ as follows:

- (1) Set $p = Init(P)$, i.e. P is located at p .
- (2) Set $s = (sid, p)$, where sid is session identity.

Let $t(V_i, p)$ be the time taken for a message from verifier V_i to reach position p .

Let T be the time at which the message sent by V_0 arrives at p .

Key Exchange: Prover P runs the algorithm $Key(V, P, p)$ as follows:

- 1) V_0 generates X_0 with min-entropy $(\delta+\beta)n$ and m -bit random string r , and V_1 generates X_1 with min-entropy $(\delta+\beta)n$. V_0 and V_1 can share X_0 , X_1 and r over a private channel.

2) V_0 computes $y_1 = F(X_1, r)$, $sk = F(X_0, y_1)$. V_0 sends (X_0, r, s) at time $T-t(V_0, p)$ over an authenticated broadcast channel.

3) V_1 also computes $y_1 = F(X_1, r)$, $s_k = F(X_0, y_1)$ and sends (X_1, s) at time $T-t(V_1, p)$ over an authenticated broadcast channel.

4) Upon receiving (X_0, r, s) and (X_1, s) at time T , P first computes $y_1 = F(X_1, r)$. Then, P computes $sk = F(X_0, y_1)$ as a shared key.

Theorem 1 If F is an ε -secure BSM PRG, X_0 and X_1 have min-entropy $(\delta+\beta)n$ and βn is the total retrieval bound, then protocol $p2vKE^1$ is a secure position based $p2v$ key exchange protocol in one dimension against an arbitrary number of colluding adversaries.

Outline of proof: Assuming that $p2vKE^1$ is not secure, we have that adversary G could distinguish between sk generated by $Key(V, P, p)$ and a random string U with a non-negligible probability.

Under the BRM, we know that the adversaries between V_1 and P can compute only $F(X_1, r)$, but that they does not have X_0 to compute sk . The adversaries between V_2 and P cannot compute $F(X_1, r)$, thus they cannot compute sk .

According to the Definition of BSM PRG, no adversary could distinguish between sk and U without adequate information. Thus, Theorem 1 holds.

3.2 Protocol $p2vKE^d$ in d -dimensions

Protocol $p2vKE^d$ in d -dimensions requires at least

Figure 3 Protocol $p2vKE^1$

$(d+1)$ verifiers to carry out position based p2v key exchange in d -dimensions.

The detailed description of protocol $p2vKE^d$ in the BRM is as follows:

BSM PRG $F: \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^m$.

Initialization: The Initialization phase is as same as that of protocol $p2vKE^1$.

Key Exchange:

1) V_0 generates X_0 with min-entropy $(\delta+\beta)n$ and m -bit random string r , and V_i generates X_i with min-entropy $(\delta+\beta)n$ ($1 \leq i \leq d$). V_i can share $X_0, \{X_i\}$ ($1 \leq i \leq d$) and r over a private channel.

2) V_0 computes the shared key $sk = F(X_0, r_0)$, where $r_{i-1} = F(X_i, r_i)$, $r_d = r$ ($1 \leq i \leq d$). V_0 sends (X_0, r, s) at time $T-t(V_0, p)$ over an authenticated channel, where $s=(sid, p)$.

3) V_i computes the shared key sk and sends (X_i, s) at time $T-t(V_i, p)$ over an authenticated channel. ($1 \leq i \leq d$)

4) Upon receiving (X_0, r, s) and $\{X_1, \dots, X_d\}$ at time T , P computes the shared key $sk=F(X_0, r_0)$, where $r_{i-1} = F(X_i, r_i)$, $r_d = r$ ($1 \leq i \leq d$).

Theorem 2 If F is ε -secure BSM PRG, $\{X_i\}$ have min-entropy $(\delta+\beta)n$ and βn is the total retrieval bound ($0 \leq i \leq d$), then protocol $p2vKE^d$ is a secure position based p2v key exchange protocol in d -dimensions.

The proof of Theorem 2 is similar to that of Theorem 1. Hence, it will not be discussed in this paper.

With regard to the region available for PbKE in two dimensions or three dimensions, Chandran et al. show that only a very small region near a verifier could not be used to realize secure PbKE, whether it be the p2v mode or the p2p mode^[4].

4 PbKE protocols in the p2p mode

In this section, we begin by presenting a position based p2p key exchange protocol in one dimension. Then, we show a generic version of the p2p key exchange protocol $p2pKE^d$ in d -dimensions ($d \in \{1, 2, 3\}$).

Intuitively, a prover P_1 could share a key k_1 with a verifier, and another prover P_2 could also share a key k_2 with a verifier using position based p2v key exchange. Then, prover P_1 and prover P_2 run a key exchange protocol, such as the Needham-Schroeder protocol^[14], involving a trusted third party (i.e. the above verifier) to carry out position based key exchange between prover P_1 and prover P_2 . However, a fatal shortcoming of this construction is that the verifier must maintain the correlation between a prover's current position and its key generated by the p2v mode. Otherwise, a prover may question that whether the position of the other prover during the p2v position based key exchange protocol is its current position or not. Obviously, maintaining this correlation is the construction's vulnerability and is too costly from the verifiers perspective. Furthermore, this construction demonstrates worse performance in terms of both efficiency and scalability.

Therefore, a construction based on the p2v mode would not be an effective way to realize p2p key exchange. In the following section, we discuss how to realize the position based p2p key exchange protocols.

4.1 Protocol $p2pKE^1$ in one dimension

The position based p2p key exchange protocol in one dimension, denoted by $p2pKE^1$, is shown in Fig.4. For one dimension, we employ two verifiers, denoted by V_0 and V_1 (which send messages at the speed of radio waves).

We assume that both position p_1 and position p_2 being claimed by prover P_1 and prover P_2 respectively are located between V_0 and V_1 .

Protocol $p2pKE^1$ is secure against an arbitrary number of adversaries, colluding to establish a secret key between P_1 and P_2 , as long as the total information that these adversaries can retrieve during the protocol is bounded.

A detailed description of protocol $p2pKE^1$ in the BRM is as follows:

BSM PRG $F: \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^m$.

PRF $f: \{0,1\}^{2m} \times \{0,1\}^l \rightarrow \{0,1\}^k$.

Initialization: P_1 and P_2 run the algorithm $Init(P_1)$ and $Init(P_2)$ as follows:

1) Set $p_1 = Init(P_1)$ and $p_2 = Init(P_2)$, i.e. P_1 is located at p_1 , and P_2 is located at p_2 .

2) Set $s = (sid, p_1, p_2)$ where sid is the session identity.

Let $t(V_i, p)$ be the time taken for a message from verifier V_i to reach position p . Let T_1 and T_2 be the times at which the message sent by V_0 arrive p_1 and p_2 respectively. Then, we have that $T_1 - T_2 = t(V_0, p_1) - t(V_0, p_2)$.

Key exchange: P_1 and P_2 run the algorithm $Key(V = \{V_1, V_2\}, P_1, p_1, P_2, p_2)$ as follows:

1) V_0 generates X_0 with min-entropy $(\delta + \beta)n$ and m -bit random string r , and V_1 generates X_1 and X_2 with min-entropy $(\delta + \beta)n$. V_0 and V_1 can share X_0, X_1, X_2 and r over a private channel.

2) V_0 computes $y_1 = F(X_1, r)$, $z_1 = F(X_0, y_1)$, $y_2 = F(X_2, r)$ and $z_2 = F(X_0, y_2)$, and sets $z = z_1 \oplus z_2$. V_0 sends (X_0, r, z, s) at time $T_1 - t(V_0, p_1)$ over an authenticated broadcast channel.

3) V_1 sends (X_1, s) and (X_2, s) at time $T_1 - t(V_1, p_1)$ and $T_2 - t(V_1, p_2)$ respectively over an authenticated broadcast channel.

4) Upon receiving (X_0, r, z, s) and (X_1, s) at time T_1 , P_1 computes $y_1 = F(X_1, r)$, $z_1 = F(X_0, y_1)$ and $z_2 = z \oplus z_1$. Then, P_1 computes $sk = f(z_1, z_2)$ as a shared key.

5) Upon receiving (X_0, r, z, s) and (X_2, s) at time T_2 , P_2 computes $y_2 = F(X_2, r)$, $z_2 = F(X_0, y_2)$ and $z_1 = z \oplus z_2$. Then, P_2 computes $sk = f(z_1, z_2)$ as a shared key.

Theorem 3 If F is an ε -secure BSM PRG, f is PRF, X_i has min-entropy $(\delta + \beta)n$ and βn is the total retrieval bound ($0 \leq i \leq 2$), then protocol $p2pKE^1$ is a secure position based p2p key exchange protocol in one dimension against an arbitrary number of colluding adversaries.

Outline of proof: Assuming that $p2pKE^1$ is not secure, an adversary G can distinguish between sk generated by $Key(V, P_1, p_1, P_2, p_2)$ and a random string U with a non-negligible probability.

Because the messages from the verifiers are broadcasted in an authenticated channel, no adversary can successfully launch an attack on the integrity of those messages. According to the protocol $p2pKE^1$, the session key sk should be equal to $f(z_1, z_2)$. If an adversary G were able to successfully attack the protocol $p2pKE^1$, there are two possible events:

Event 1 Adversary G could distinguish between sk and U without z_1 and z_2 . According to the Definition of PRF, Event 1 occurs with only a negligible probability.

Event 2 Adversary G could obtain the value of z_1 and z_2 . According to the BRM, Event 2 occurs with only a negligible probability. We know that the adversaries between V_1 and P_1 can compute $F(X_1, r)$ and $F(X_2, r)$ but do not have X_0 to compute z_1 and z_2 . The adversaries between P_1 and P_2 can only compute

Figure 4 Protocol $p2pKE^1$

$F(X_2, r)$ but do not have X_0 to compute z_1 . The adversaries between V_2 and P_2 cannot compute $F(X_1, r)$ and $F(X_2, r)$, thus they cannot obtain z_1 and z_2 .

Therefore, if f is a PRF and F is an ε -secure BSM PRG, then ε_f , ε_{F1} , ε_{F2} , ε_{F3} , and ε_{F4} are negligible, and ε_G is also negligible. Theorem 3 holds.

4.2 Protocol $p2pKE^d$ in d -dimensions

Protocol $p2pKE^d$ in d dimensions requires at least $(d+1)$ verifiers to realize position based p2p key exchange in d -dimensions.

A detailed description of protocol $p2pKE^d$ in the BRM is as follows:

BSM PRG $F: \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^m$.

PRF $f: \{0,1\}^{2m} \times \{0,1\}^l \rightarrow \{0,1\}^k$.

Initialization is the same as that of protocol $p2pKE^1$.

Key exchange:

1) V_0 generates X_0 with min-entropy $(\delta+\beta)n$ and m -bit random string r , and V_i generates $X_{(i,1)}$ and $X_{(i,2)}$ with min-entropy $(\delta+\beta)n$ ($1 \leq i \leq d$). V_i can share X_0 , $\{X_{(i,j)}\}$ ($1 \leq i \leq d$, $1 \leq j \leq 2$) and r over a private channel.

2) V_0 computes $z_1 = F(X_0, r_{(0,1)})$ and $z_2 = F(X_0, r_{(0,2)})$, where $r_{(i-1,j)} = F(X_{(i,j)}, r_{(i,j)})$, $r_{(d,j)} = r$ ($1 \leq i \leq d$, $1 \leq j \leq 2$), and sets $z = z_1 \oplus z_2$. V_0 sends (X_0, r, z, s) at time $T_1 - t(V_0, p_1)$ over an authenticated channel, where $s = (sid, p_1, p_2)$.

3) V_i sends $(X_{(i,1)}, s)$ and $(X_{(i,2)}, s)$ at time $T_1 - t(V_i, p_1)$ and $T_2 - t(V_i, p_2)$ respectively over an authenticated channel. ($1 \leq i \leq d$)

4) Upon receiving (X_0, r, z, s) and $\{X_{(1,1)}, \dots, X_{(d,1)}\}$ at time T_1 , P_1 computes $z_1 = F(X_0, r_{(0,1)})$ where $r_{(i-1,1)} = F(X_{(i,1)}, r_{(i,1)})$, $r_{(d,1)} = r$ ($1 \leq i \leq d$) and $z_2 = z \oplus z_1$. Then, P_1 computes $sk = f(z_1, z_2)$ as a shared key.

5) Upon receiving (X_0, r, z, s) and $\{X_{(1,2)}, \dots, X_{(d,2)}\}$ at time T_2 , P_2 computes $z_2 = F(X_0, r_{(0,2)})$ where $r_{(i-1,2)} = F(X_{(i,2)}, r_{(i,2)})$, $r_{(d,2)} = r$ ($1 \leq i \leq d$) and $z_1 = z \oplus z_2$. Then, P_2 computes $sk = f(z_1, z_2)$ as a shared key.

Theorem 4 If F is an ε -secure BSM PRG, f is a PRF,

X_0 and $\{X_{(i,j)}\}$ have min-entropy $(\delta+\beta)n$ and βn is the total retrieval bound ($1 \leq i \leq d$, $1 \leq j \leq 2$), then protocol $p2pKE^d$ is a secure p2p position based key exchange protocol in d -dimensions.

The proof of Theorem 4 is omitted due to space limitations.

5 Extensions

In this section, we extend the above protocols in order to establish some useful properties of key exchange, including key confirmation and without key escrow. Due to space limitations, we omit the detailed descriptions and security proofs of the extended protocols.

5.1 Protocols with key confirmation

A key exchange protocol between parties A and B satisfies mutual key confirmation if both of them are assured that the other party possesses the secret key. Obviously, protocol $p2vKE^d$ and $p2pKE^d$ do not have the key confirmation property. That is, a prover has no assurance that whether the verifiers (in the p2v mode) or the other prover (in the p2p mode) can obtain the shared key or not.

We can use message authentication code (MAC) to extend PbKE protocols for the key confirmation property as follows.

Assuming that g is a secure MAC algorithm, and f is a secure PRF, the prover P and the verifier V_i (in the p2v mode) or the other prover P' (in the p2p mode) have shared the secret key sk . First, the prover P and the verifier V_i (in the p2v mode) or the other prover P' (in the p2p mode) can compute the encryption key $ek = f(sk, 0)$ and the authentication key $ak = f(sk, 1)$ as a MAC key. Second, the prover P can compute $c_1 = g(ak, (P, s, r))$, and either the verifier V_i (in the p2v mode) can compute $c_2 = g(ak, (V_i, s, r))$ or the other prover P' (in the p2p mode) can compute $c_2 = g(ak,$

(P', s, r)). Finally, they exchange the MAC values c_1 and c_2 , and verify the validity of the MAC value from the other party. If both of the MAC values pass the verification, they can confirm that the other party must hold the same key.

5.2 Protocols without key escrow

In the above protocols, we assume that all of the verifiers are trusted. According to the logic of $p2pKE^d$ (or $p2pKE_C^d$), all verifiers can compute the shared key between provers P_1 and prover P_2 in the p2p mode, which implies the problem of key escrow^[15].

However, in some applications, there are only semi-trusted verifiers that provide the position-related services. Therefore, prover P_1 and prover P_2 maybe wish to keep their communication confidential from the semi-trusted verifiers in the p2p mode. In fact, a semi-trusted verifier can be treated as a passive attacker in the p2p mode.

Based on the DDH (Decision Diffie-Hellman) assumption^[16], we construct a position based p2p key exchange protocol $p2pKE_E^d$ without key escrow by adding a DH Exchange phase.

The protocol $p2pKE_E^d$ is shown as follows:

BSM PRG $F: \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^m$.

PRF $f: \{0,1\}^{2m} \times \{0,1\}^l \rightarrow \{0,1\}^k$.

MAC $g: \{0,1\}^l \times \{0,1\}^{2m} \rightarrow \{0,1\}^k$.

G : a cyclic group with prime order q and generator g .

Initialization & Key Exchange: Prover P_1 and prover P_2 run the Initialization and Key Exchange phases as in protocol $p2pKE^d$ and share a secret sk .

DH Exchange:

1) P_1 selects a random a from Z_q , and sends (P_1, s, g^a) to P_2 .

2) Upon receiving (P_1, s, g^a) , P_2 selects a random b from Z_q , computes $key = (g^a)^b$ and the authentication tag $c_2 = g(sk, (P_2, s, g^b, g^a))$, then it sends (P_2, s, g^b, c_2) to P_1 .

3) Upon receiving (P_2, s, g^b, c_2) , P_1 first verifies the

validity of the authentication tag c_2 , and if successful computes $key = (g^b)^a$ and the authentication tag $c_1 = g(sk, (P_1, s, g^a, g^b))$. Then, P_1 sends (P_1, s, c_1) to P_2 and outputs key as a shared key.

4) Upon receiving (P_1, s, c_1) , P_2 verifies the validity of c_1 . If successful, P_2 outputs key as a shared key.

Obviously, protocol $p2pKE_E^d$, like protocol $p2pKE_C^d$, has the property of key confirmation when using the message authentication code $g(sk, \bullet)$. At the same time, $p2pKE_E^d$ is also a secure position based p2p key exchange protocol if the DDH assumption holds.

6 Comparisons

In this section, we compare the PbKE protocols in three dimensions. Table 1 shows the comparison results.

Security: It is obvious that all of the position based key exchange protocols in this paper satisfy the Definition of a secure position based key exchange under Assumption 1, Assumption 2 and Assumption 3.

In addition, protocol $p2vKE_C^3$ and $p2pKE_C^3$ have the property of key confirmation, while protocol $p2pKE_E^3$ has the properties of key confirmation and being without key escrow by using Assumption 4 (i.e. the DDH assumption).

Performance: From the viewpoint of the verifiers in the p2p mode, the communication overhead and computation cost are the same. In other words, protocol $p2pKE_C^3$ and protocol $p2pKE_E^3$ would not generate additional cost for the verifiers, which helps the verifiers to provide reliable position-related services.

Protocols $p2vKE^3$ and $p2pKE^3$ are suitable for energy-limited applications, since the provers in protocol $p2vKE^3$ and $p2pKE^3$ have no communication overhead.

Compared to protocol $p2vKE^3$ and $p2pKE^3$, protocol $p2vKE_C^3$ and $p2pKE_C^3$ incur extra communication

overhead and computational cost to the prover for the key confirmation property. We note that the added operation cost of PRF or MAC is acceptable since there are some very efficient implementations of PRF and MAC for lowpower devices.

Note that position based cryptographic protocols using the TOA technique have a disadvantage in that they are not robust to round trip delays, which include propagation delays and processing delays. Therefore, the PbKE protocols in this paper as well as the protocols in Ref.[4] are all based on an assumption that there is no round trip delay: that is that all the participants can immediately send, receive and process data without delay.

7 Conclusion and future work

Position based key exchange is a basic primitive in position based cryptography. This paper distinguishes the prover-to-verifier mode and the prover-to-prover mode of position based key exchange. According to the different requirements of the two modes, this paper discusses the security definitions and the implementation of position based key exchange. Moreover, this paper extends position

based key exchange protocols in order to capture two meaningful properties of key exchange: key confirmation and without key escrow. Finally, this paper compares the position based key exchange protocols in two modes from both security and performance perspectives.

The next step will be to find new assumptions for position based cryptography and to construct new position based key exchange protocols that are more robust to round trip delays.

References

- [1] RAO B, MINAKAKIS L. Evolution of mobile location-based services[J]. Communications of the ACM, 2003, 46(12): 61-65.
- [2] BERESFORD A R, STAJANO F. Location privacy in pervasive computing[J]. IEEE pervasive computing, 2003, 2(1): 46-55.
- [3] ZHANG J W, MA J F, MOON S J. Universally composable secure TNC model and EAP-TNC protocol in IF-T[J]. Science china information sciences, 2010, 53(3): 465-482.
- [4] CHANDRAN N, GOYAL V, MORI-ARTY R, et al. Position based cryptography[C]//Advances in Cryptology-CRYPTO, Springer Berlin Heidelberg, 2009, 5677: 391-407.
- [5] BUHRMAN H, CHANDRAN N, FEHR S, et al. Position-based quantum cryptography: impossibility and constructions[J]. Siam Journal on Computing, 2010, 43(1): 150-178.
- [6] LAU H K, LO H K. Insecurity of position-based quantum-cryptography protocols against entanglement attacks[J]. Physical

Table 1 Comparison results

protocol	$p2vKE^3$	$p2vKE_C^3$	$p2pKE^3$	$p2pKE_C^3$	$p2pKE_E^3$
verifier computation	$4F$	$4F + 2F + 2g$	$8F$	$8F$	$8F$
verifier communication	$ r + 4 X $	$ r + 4 X + g $	$ r + 7 X $	$ r + 7 X $	$ r + 7 X $
prover computation	$4F$	$4F + 2f + 2g$	$4F + f$	$4F + 3f + 2g$	$4F + f + 2g + 2E$
prover communication	0	$ g $	0	$ g $	$ g + q $
mode	p2v	p2v	p2p	p2p	p2p
set-up assumptions	1,2,3	1,2,3	1,2,3	1,2,3	1,2,3,4
key confirmation	no	yes	no	yes	yes
without key escrow	—	—	no	no	yes

In Tab.1, f denotes the cost of one operation of PRF; g denotes the cost of one computation or verification of MAC; F denotes the cost of one operation of BSM PRG; E denotes the cost of one exponential operation in the DH exchange.

- review a, 2011, 83(1): 012322.
- [7] TOMAMICHEL M, FEHR S, KANIEWSKI J, et al. One-sided device-independent QKD and position-based cryptography from monogamy games[C]//Advances in Cryptology-EUROCRYPT, 2013, 7881: 609-625.
 - [8] ZHANG J W, MA J F, YANG C, et al. Universally composable secure positioning in the bounded retrieval model[J]. Science China information sciences, 2015, 58(11)110105: 1- 110105: 15.
 - [9] ZHANG J W, MA Z, MA J F, et al. UC security model of position based key exchange[J]. Journal of computer research and development, 2014, 51(2): 353-359.
 - [10] ZHANG J W, CHEN Z P, MA J F, et al. Provably secure position based prover-to-prover key exchange protocols[J]. Acta electronica sinica, 2016, 44(1): 353-359.
 - [11] PERRIG A, SZEWCZYK R, TYGAR J D, et al. SPINS: security protocols for sensor networks[J]. Wireless networks, 2002, 8(5): 521-534.
 - [12] ZHANG J W, MA J F, MOON S J. Universally composable one-time signature and broadcast authentication[J]. Science China information sciences, 2010, 53(3): 567-580.
 - [13] GOLDREICH O, GOLDWASSER S, MI-CALI S. How to construct random functions[J]. Journal of the ACM, 1986, 33(4): 792-807.
 - [14] ZHANG J W, MA J F, YANG C. Protocol derivation system for the Needham-Schroeder family[J]. Security and communication networks, 2015, 8: 2687-2703.
 - [15] CHEN L, KUDLA C. Identity based authenticated key agreement protocols from pairings[J]. International journal of information security, 2007, 20(4): 219-233.
 - [16] BONEH D. The decision Diffie-Hellman problem[J]. Algorithmic number theory, 1998, 23(2): 48-63.

About the authors

ZHANG Junwei [corresponding author] was born in 1982. He received a Ph.D. degree in computer architecture from Xidian University, where he is now an associate professor. His research interests include cryptography and information security. (Email: jwzhang@xidian.edu.cn)

MA Jianfeng was born in 1963. He received a Ph.D. degree from Xidian University, where he is now a professor. His research interests include network and information security. (Email: jfma@mail.xidian.edu.cn)

DU Fangqiong was born in 1993. She received a B.E. degree from Xidian University. She is now an M.S. candidate in computer architecture at Xidian University. Her research interests include protocol design and analysis. (Email: dufangqiong666@163.com)

YANG Chao was born in 1979. He received a Ph.D. degree in computer architecture from Xidian University, where he is now an associate professor. His research interests include system and information security. (Email: chaoyang@mail.xidian.edu.cn)