doi:10.3969/j.issn.1000-436x.2013.02.014

安全定位协议的 UC 模型

张俊伟，马建峰，杨超
（西安电子科技大学 计算机学院，陕西 西安 710071）

摘 要：研究了基于位置密码学中安全定位协议的可证明安全问题。在通用可组合安全框架下，提出了安全定位的可证安全模型。根据安全定位协议的需求，设计了安全定位的理想函数。同时，作为基于位置密码学的一种前提假设，设计了 BRM 模型的理想函数。此外，以 1-维空间的安全定位协议为例，证明了该协议在 BRM 模型下能够实现安全定位的理想函数。

关键词：基于位置密码学；安全定位；UC 安全
中图分类号：TP309 **文献标识码**：B **文章编号**：1000-436X(2013)02-0117-06

UC model of secure positioning protocols

ZHANG Jun-wei, MA Jian-feng, YANG Chao
(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: The provable security of secure positioning in position-based cryptography was investigated, and the provable secure model of secure positioning was established in the universally composable framework. According to the security requirements of secure positioning, the ideal functionality of secure positioning firstly was proposed. Then, the ideal functionality of bounded retrieval model was designed as one of the set-up assumptions in position-based cryptography. Lastly, the secure positioning protocol in 1-dimension space, as an example, could securely realize the functionality of secure positioning in the bounded retrieval model.

Key words: position-based cryptography; secure positioning; UC secure

1 引言

与传统的密码学不同，基于位置的密码学[1]将用户的物理位置信息作为该用户的唯一一个凭证信息。典型应用如基于位置的秘密通信、基于位置的认证/签名、基于位置的接入控制等。

目前，针对基于位置密码学的研究主要集中在安全定位方面。在无线安全领域，定位技术已经有了相当多的研究成果。定位技术的主要目标是测量并获得某个设备的物理地址。著名的全球定位系统（GPS）就是一种定位技术，雷达也是一种定位技术。除此之外，还有很多其他的定位技术，它们进行定位的实际方法是基于消息响应时间的技术。然而，之前的安全定位协议都不能抵御多个敌手的共谋攻击（collusion attack）。换句话说，这些定位方法都不是可证明安全的。文献[1]研究了安全定位中共谋攻击的问题，并在 Vanilla Model 下提出了一个安全定位协议，但该协议仅仅能够抵御 2 个敌手的共谋攻击，并不能抵御 3 个或者更多敌手的共谋攻击。

文献[2]首次在 BRM（bounded retrieval model）模型[3]下研究了安全定位和基于位置的密钥交换协议。设计的 2 个密钥交换协议中，一个是计算条件下安全的，另一个是信息论安全的。文献[4]研究了基于位置的量子密码学，利用量子密码学构造了基

收稿日期：2011-08-22；**修回日期**：2012-02-16
基金项目：国家科技重大专项基金资助项目（2011ZX03005-002）；国家自然科学基金资助项目（U1135002, 61100230, 61100233）；陕西省自然科学基础研究计划基金资助项目（2011JQ8003）；中央高校基本科研业务费基金资助项目
Foundation Items: The Major National S&T Program (2011ZX03005-002); The National Natural Science Foundation of China (U1135002, 61100230, 61100233); The Natural Science Basic Research Plan in Shaanxi Province of China(2011JQ8003); The Fundamental Research Funds for the Central Universities

于位置的安全定位、密钥交换以及认证协议。然而，这些研究并没有给出基于位置密码协议的组合安全模型，因此，设计的协议无法保证在组合环境下协议的安全性。

由 Canetti 提出的通用可组合框架（UC 框架，universally composable framework）[5]可以保证协议的通用可组合安全，即在 UC 框架下证明安全的协议，在与其他协议并发运行的情况下，或者作为一个系统的组件时，仍能保证协议的安全性。

理想函数是 UC 框架中非常重要的概念，它扮演着一个不可攻陷的可信第三方的角色，能够完成协议所执行的特定功能。目前，已经定义了多个最基本的理想函数，如认证消息传输 F_{AUTH}、密钥交换 F_{KE}、公钥加解密 F_{PKE}、签名 F_{SIG}、承诺 F_{COM}、零知识证明 F_{ZK}、不经意传输 F_{OT}[6]、基于一次签名（F_{OTS}）的广播认证（F_{BAUTH}）[7]和可信网络连接 F_{TNC}[8]等。

在UC框架下设计协议的困难所在和核心内容就在于形式化和抽象一个完美的并且可以安全实现的理想函数。然而，现有的UC框架没有基于位置密码学的理想函数，缺乏对基于位置密码学的支持，无法直接用于基于位置密码协议的分析与设计。

本文在 UC 框架下提出了安全定位协议的可证明安全模型。针对安全定位的安全需求，设计了安全定位的理想函数 F_{SP}。同时，针对基于位置密码学的前提假设模型——BRM 模型，提出了满足 BRM 模型性质的理想函数 F_{BRM}。针对安全定位理想函数的实现问题，以 Chandran 等设计的 1-维空间的安全定位协议为例，证明了该协议在 F_{BRM}-混合模型下能安全实现安全定位的理想函数 F_{SP}。

2 预备知识

2.1 UC 框架

UC 框架如图 1 所示。首先，UC 框架定义了现实环境。现实环境描述协议的真实运行情况，其中所有参与方在真实敌手攻击 A 存在的环境下运行真实协议。其次，UC 框架定义了理想环境用来描述密码协议的理想运行。在理想环境下，存在虚拟参与方，理想敌手 S 和理想函数 F。参与方之间以及敌手 S 与参与方不直接通信；所有参与方和敌手 S 均与理想函数交互。理想函数本质上是一个不可攻陷的可信角色，用来完成协议所需的理想运行和功能。在 UC 的安全框架中，环境 Z 模拟协议运行的整个外部环境（包括其他并行的协议、攻击者等等），Z 可以与所有的参与者以及攻击者 A 和 S 直接通信，Z 不允许直接访问理想函数 F。

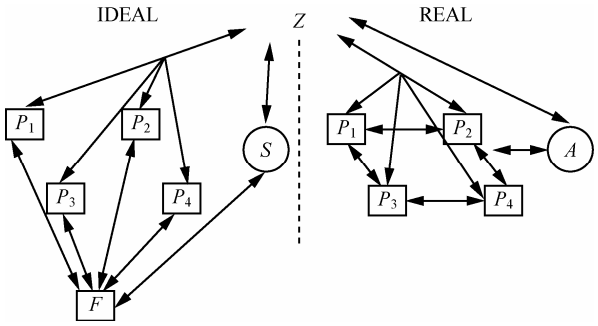


图 1 UC 框架

定义 1 UC 仿真[5]：协议 π 能够 UC 仿真理想函数 F 当且仅当对于任意真实敌手 A，存在理想敌手 S，使得任意环境 Z，至多以一个可忽略的概率来区分：存在 A 及协议 π 的现实环境和存在 S 及理想函数 F 的理想环境。如果协议 π 能够 UC 仿真理想函数 F，就称协议 π 在 UC 框架下安全实现了理想函数 F，也称协议 π 是 UC 安全的。

定理 1 组合定理[5]：如果协议 ρ 安全实现理想函数 F 且 π 是 F-混合模型[5]下的协议，那么协议 $\pi^{\rho/F}$（用协议 ρ 替换协议 π 中的理想函数 F 所得到的组合协议）UC 仿真 F-混合模型下的协议 π。特别地，如果协议 π 在 F-混合模型下安全实现理想函数 G，那么协议 $\pi^{\rho/F}$ 也安全实现理想函数 G。

通常，复杂的协议由多个子协议构成，每个子协议都可以实现某个安全任务。根据组合定理，利用 UC 安全的协议可以安全构建一个更为复杂的协议，从而实现指定的任务，并保证相应的安全属性。

2.2 BSM 模型和 BRM 模型

BSM 模型[9]（bounded storage model）假设参与方（包括敌手）能存储信息量存在一个上限。假设存在一个具有很高的最小熵（min-entropy）的信息串，那么敌手可以存储这个信息串的一个任意函数，只要这个函数输出的长度不超过敌手存储的上限。

BRM 模型[3]假设参与方可以存取具有很高最小熵的信息串，而敌手仅仅能提取这个信息串的一部分。在基于位置密码学中，假定验证者(verifiers)可以广播具有高的最小熵的信息串，那么当这些信息高速通过敌手的时候，敌手只能提取这些信息中有限的一部分。假设敌人不能提取全部信息主要从下面两方面考虑：1) 信息都是高速传输的(接近光

速)；2) 验证者可以有多个具有不同频率的消息源广播信息。

BRM 模型具有如下性质。

1) 验证者拥有一个可以生成具有高最小熵信息串的 reverse block entropy source。令最小熵为 $(\delta+\beta)n$, 其中 n 为信息串的长度。拥有 reverse block entropy source，意味着验证者自身可以生成并发送具有高最小熵的信息串。

2) 当这些信息串高速经过敌手时，敌手能够提取的信息量存在一个上限 βn。敌手可以提取这个信息串的任意函数，只要这个函数的输出长度$\leqslant\beta n$。提取上限 βn 可以是最小熵$(\delta+\beta)n$ 的任意部分。

2.3 BSM 熵生成器

定义 2 令存储率为 β，最小熵率为 α。EG: $\{0,1\}^n\times\{0,1\}^r\rightarrow\{0,1\}^t$ 是 (ε,ψ)-安全的BSM 熵生成器（BSM entropy generators），当且仅当, 对于$\{0,1\}^n$上任意的 αn-source 的 X，对于任意 A: $\{0,1\}^n\rightarrow\{0,1\}^{\beta n}$，随机变量$(\mathrm{EG}(X,K),A(X),K)$ 对$(W,A(X),K)$是 ε-close 的，其中 $K\xrightarrow{R}\{0,1\}^r$ 且 W 是 ψ-source 的。

根据(ε,ψ)-安全的 BSM EG 的定义[2]可得，对于任意算法 F，给定 $A(X)$和 K，算法 $F(A(X),K)$能正确计算出 $\mathrm{EG}(X,K)$的最大概率为 $\varepsilon+2^{-\psi}$。在安全参数为 κ 的情况下，如果 $r\geqslant(2/\delta)\kappa\log n$，那么 $\varepsilon+2^{-\psi}$ 是可忽略的。

关于 BSM 模型、BRM 模型、BSM EG 以及其中的 ψ-source 和 ε-close 等概念的详细内容，请参阅文献[2]。

3 理想函数

3.1 安全定位理想函数 F_{SP}

假设存在一个位于位置 p 证明者（prover）声称其位于 p'，当验证者（verifier）需要对证明者安全定位时，安全定位理想函数能够保证，证明者正确通过验证者的安全定位验证当且仅当 $p=p$'。理想函数 F_{SP}如下所示。

理想函数 F_{SP}

d−维空间。

验证者 $Ver=\{V_1,V_2,\cdots,V_n\}$分别在位置 $pos_1,pos_2,\cdots,pos_n$，其中 $pos_i=\mathrm{Pos}(V_i)$。

敌手 $Adv=\{A_1,A_2,\cdots,A_k\}$ 分别在位置 $apos_1,apos_2,\cdots,apos_k$，其中 $apos_i=\mathrm{Pos}(A_i)$。

Initial

当从 *Prov* 收到(Position Initialize, *sid*, *Prov*)：

令 Pos(*sid*, *Prov*) = ⊥，发送(Position Initialize, *sid*, *Prov*) 给敌手。

当从敌手收到(Position Initialize, *sid*, *Prov*, *p*)：

如果 $p=pos_i$ $(1\leqslant i\leqslant n)$ 或者 $p=apos_j$ $(1\leqslant j\leqslant k)$ 或者 p 不在 *Ver* 所构成的封闭空间内，发送 POSITION_INVALID 给敌手。

否则，令 p = Pos(*sid*, *Prov*)，并输出(Position Initialized, *sid*, *Prov*, *p*)。

Secure Positioning

当从 *Ver* 收到(Secure Position, *sid*, *Ver*, *Prov*, *p*)：

如果 $p=\mathrm{Pos}(sid, Prov)$, 发送(Secure Position, *sid*, *Ver*, *Prov*, *p*)给敌手。

否则，忽略这个消息。

当从敌手收到(Secure Positioned, *sid*, *Ver*, *Prov*, *p*', *f*)，其中 $f\in\{Accept, Reject\}$：

如果 Pos (*sid*, *Prov*)≠*p*'，那么输出(Secure Positioned, *sid*, *Ver*, *Prov*, *p*', *Reject*) 给 *Ver*；

否则，输出(Secure Positioned, *sid*, *Ver*, *Prov*, *p*', *Accept*) 给 *Ver*。

证明者位置的无关性：在理想函数 F_{SP} 初始化时，证明者的位置由敌手决定。这说明，安全定位协议的安全性不依赖证明者所处位置。

证明者位置的非机密性：由于证明者的位置在初始化时由敌手决定，因此，理想函数 F_{SP} 不能保证证明者位置信息的机密性。

敌手攻击行为：敌手可以得到无线信道中的消息，并伪装成合法用户发送虚假消息。但敌手不能完全阻止无线信道中的信息。

抗敌手共谋攻击：敌手 *Adv* 是多个敌手$\{A_1,A_2,\cdots,A_k\}$组成的集合，即理想函数 F_{SP} 是在多个敌手共谋情况下的运行。因此，理想函数 F_{SP} 能够抵御多个敌手共谋攻击。

定位的安全性：只有当 $p'=p=\mathrm{Pos}(sid, Prov)$ 时，理想函数 F_{SP} 才会输出(Secure Positioned, *sid*, *Ver*, *Prov*, *p*', *Accept*) 给 *Ver*。

3.2 BRM 理想函数 F_{BRM}

理想函数 F_{BRM} 保证：如果验证者（verifier）发送具有高的最小熵的信息串，那么当这些信息高速通过敌手的时候，敌手只能提取这些信息中有限的一部分。理想函数 F_{BRM} 如下所示。

理想函数 F_{BRM}

当从 P 收到(Broadcast BRMessage, *sid*, X)，如果 X 的最小熵为$(\delta+\beta)n$，则

1) 令 $X_i = X$，$i = i+1$；

2) 发送(Broadcasted BRMessage, *sid*, P, X)给所有参与方（除了敌手）；

3) 发送(Broadcasted BRMessage, *sid*, P, i)给敌手。

当从 P 收到(Send BRMessage, *sid*, Q, X)，如果 X 的最小熵为$(\delta+\beta)n$，则

1) 令 $X_i = X$，$i = i+1$；

2) 发送(Sent BRMessage, *sid*, P, Q, X)给 Q；

3) 发送(Sent BRMessage, *sid*, P, Q, i)给敌手。

当从敌手收到(Retrieve BRMessage, *sid*, i, F)：

1) 计算 $F(X_i)$；

2) 如果 $F(X_i)$的信息量没有超过上限(i.e.$\leqslant\beta n$)，则令 $f = F(X_i)$；否则，将 $F(X_i)$截短到适当的长度并将其设为 f；

3) 发送(Retrieved BRMessage, *sid*, i, f)给敌手。

消息序号 i：F_{BRM} 对每个要发送的最小熵为$(\delta+\beta)n$ 的信息串用 i 进行编号。敌手也可以通过编号使用(Retrieve BRMessage, *sid*, i, F)来提取该信息串的相关信息。

单播：F_{BRM} 使用(Send BRMessage, *sid*, Q, X)来发送信息串 X。

广播：F_{BRM} 使用(Broadcast BRMessage, *sid*, X)来广播信息串 X。

BRM：当敌手发送请求(Retrieve BRMessage, *sid*, i, F)来提取第 i 个信息串的信息时，仅能够提取出上限为 βn 的信息量。

4 实现理想函数 F_{SP}

本节以 1-维空间下的安全定位协议（记为 π_{SP1d}）[2]为例，证明协议 π_{SP1d} 在 F_{BRM}-混合模型下可以安全实现理想函数 F_{SP}。首先，给出在 F_{BRM}-混合模型下协议 π_{SP1d} 的形式化描述。其次，证明协议 π_{SP1d} 在 F_{BRM}-混合模型下满足 UC 安全性。

4.1 安全定位协议 π_{SP1d}

在 F_{BRM}-混合模型下，1-维空间的安全定位协议 π_{SP1d} 如下所示。

协议 π_{SP1d}

令 βn 为敌手提取信息的上限。验证者 V_1 拥有最小熵为$(\delta+\beta)n$ 的信息串 X_1, X_2, …, 其中 $X_i\in\{0,1\}^n$。(ε, ψ)-安全的 BSM 熵生成器 EG：$\{0,1\}^n\times\{0,1\}^l \to \{0,1\}^m$。令 $l\geqslant(2/\delta)\kappa\log(n)$，则 $\varepsilon+2^{-\psi}$ 在安全参数 κ 下是可忽略的。

Initial

当从 *Prov* 收到(Position Initialize, *sid*, *Prov*)：

1) 令 $p = \text{Pos}(sid, Prov)$；

2) 如果 $p = pos_i$ $(1\leqslant i\leqslant n)$ 或者 $p = apos_j$ $(1\leqslant j\leqslant k)$，那么令 $p = \text{POSITION\_INVALID}$；

3) 输出(Position Initialized, *sid*, *Prov*, p)。

Secure Positioning

当 *Ver* 收到(Secure Position, *sid*, *Ver*, *Prov*, p)：

1) V_1 从$\{0,1\}^l$ 中随机选择 K 并通过秘密信道发送(Send, *sid*, V_1, V_2, K)给 V_2；

2) 令 t 和 t'是无线电波分别从 V_1 和 V_2 到达 p 的时间，V_1 利用 reverse block entropy source 生成并在$(T-t)$时刻发送(Send, *sid*, V_1, *Prov*, X)给 F_{BRM}，其中，T 为 X 到达位置 p 的时刻，X 的最小熵为$(\alpha+\beta)n$。同时，V_1 计算 EG(X, K)；

3) 在$(T-t')$时刻，V_2 发送(Send, *sid*, V_2, *Prov*, K)给 *Prov*，使得 K 在 T 时刻在位置 p 与 X 相遇；

4) 在 T 时刻, Prov 收到(Sent, *sid*, V_2, *Prov*, K)，并从 F_{BRM} 收到(Sent, *sid*, V_1, *Prov*, X)，计算 $y = \text{EG}(X, K)$，并发送(Send, *sid*, *Prov*, V_1, y)给 V_1；

5) 当 V_1 从 p 收到(Send, *sid*, *Prov*, V_1, y')时，V_1 验证是否在$(T+t)$时刻收到 y'，且 y'是否等于 EG(X, K)。如果是，输出(Secure Positioned, *sid*, *Ver*, *Prov*, p, *Accept*)；否则，输出(Secure Positioned, *sid*, *Ver*, *Prov*, p, *Reject*)。

4.2 协议 π_{SP1d} 的安全性分析

定理 2 如果 X 的最小熵为$(\delta+\beta)n$，βn 为敌手提取信息的上限，EG 是(ε, ψ)-安全的 BSM 熵生成器，那么，协议 π_{SP1d} 在 F_{BRM}-混合模型下安全实现理想函数 F_{SP}。

证明 令 A 为现实敌手。构造理想敌手 S，使得对于任意环境 Z 只能以可忽略的概率区分：协议 π_{SP1d} 及 A 交互的现实环境（记为 *REAL*）和理想函数 F_{SP} 及 S 交互的理想环境(记为 *IDEAL*)，记为 $IDEAL\approx REAL$（表示 *REAL* 和 *IDEAL* 不可区分）。

1）构造 S

敌手 S 运行一个敌手 A 的仿真副本。因此，S 通常被称为仿真器（simulator）。S 将 Z 的所有输入发送给 A。A 的所有输出都作为 S 的输出。

敌手 S 运行如下。

①当从 F_{SP} 收到(Position Initialize, *sid*, *Prov*), *S* 将(Position Initialize, *sid*, *Prov*)作为输入为 *A* 运行 π_{SP1d} 的一个副本。然后将从 *A* 收到的响应(Position Initialized, *sid*, *Prov*, *p*)发送给 F_{SP}。

②当 *S* 从 F_{SP} 收到(Secure Position, *sid*, *Ver*, *Prov*, *p*), *S* 以(Secure Position, *sid*, *Ver*, *Prov*, *p*)为输入运行 π_{SP1d} 的副本。

③当 V_1 通过秘密信道发送(Send, *sid*, V_1, V_2, *K*)给 V_2 时，*S* 仿真从 V_1 到 V_2 通过秘密信道发送的消息(Send, *sid*, V_1, V_2, *K*)。

④当 V_1 在(*T*-*t*)时刻利用 F_{BRM} 发送(Send, *sid*, V_1, *Prov*, *X*)给 *Prov*，*S* 在(*T*-*t*)时刻利用 F_{BRM} 仿真从 V_1 到 *Prov* 的消息(Send, *sid*, V_1, *Prov*, *X*)。

⑤当 V_2 在(*T*-*t*') 时刻发送(Send, *sid*, V_2, *Prov*, *K*)给 *Prov*，*S* 在(*T*-*t*')时刻仿真从 V_2 到 *Prov* 的消息(Send, *sid*, V_2, *Prov*, *K*)。

⑥当 *Prov* 在 *T* 时刻发送(Send, *sid*, *Prov*, V_1, *y*)给 V_1，*S* 在 *T* 时刻仿真从 *Prov* 到 V_1 的消息(Send, *sid*, *Prov*, V_1, *y*)。

⑦当 π_{SP1d} 的副本输出(Secure Positioned, *sid*, *Ver*, *Prov*, *p*', *f*)，其中 $f \in \{Accept, Reject\}$，*S* 发送(Secure Positioned, *sid*, *Ver*, *Prov*, *p*', *f*)给 F_{SP}。

2) *IDEAL* 和 *REAL* 不可区分

事件 E_1：π_{SP1d} 的副本输出(Secure Positioned, *sid*, *Ver*, *Prov*, *p*', *Accept*), 其中 Pos (*sid*, *Prov*) ≠ *p*'。

事件 E_2：π_{SP1d} 的副本输出(Secure Positioned, *sid*, *Ver*, *Prov*, *p*', *Reject*), 其中 Pos (*sid*, *Prov*) = *p*'。

根据事件 E_1 和 E_2，按照下列 3 种情况分别讨论。

1) E_1 和 E_2 均不发生。当 E_1 和 E_2 事件都不发生的情况下，上述仿真是完美的，即 *IDEAL* ≈ *REAL*；

2) E_1 发生。E_1 事件发生的概率是可忽略的：假设事件 E_1 以不可忽略的概率发生，那么，就存在一个敌手（不在位置 *p*），它能够以不可忽略的概率在(*T*+*t*)时刻将正确的 *y* 发送给 V_1。在 *T* 时刻，*X* 和 *K* 在位置 *p*。假设存在 V_1 和 *p* 之间存在 *g* 个敌手，这些敌手从 *X* 中能分别提取 $S_1, S_2, \cdots, S_g$。令 $S = S_1 \cup S_2 \cup \cdots \cup S_g$，显然，$|S| \leqslant \beta n$。由于 *S* 是 V_1 和 *p* 之间信息的集合，敌手没有在位置 *p*，且在 *T* 时刻任何 *P* 和 V_2 之间关于 *X* 的信息也不能在(*t* + *T*)时刻到达 V_1，因此，如果敌手能够以不可忽略的概率在(*T*+*t*)时刻将正确的 *y* 发送给 V_1，那就意味着敌手存在一个算法 *A* 能够以不可忽略的概率正确计算 *y*=*A*(*S*, *K*)。但是，根据 BSM EG 的性质，给定 *S* 和 *K*，敌手能正确计算 *y* 的最大概率为 $\varepsilon+2^{-\psi}$，其中，$\varepsilon+2^{-\psi}$ 是可忽略的。因此，这与定义 2 相矛盾，假设不成立。即事件 E_1 只能以可忽略的概率发生。

3) E_2 发生。E_2 事件不会发生：由于敌手在无线环境下不具备阻止消息的能力，根据协议 π_{SP1d} 可知，如果 *Prov* 在位置 *p*，那么，*Prov* 在 *T* 时刻会收到 *X* 和 *K*，计算正确的 *y*，并将其发送给 V_1。V_1 会在(*T*+*t*)时刻收到正确的 *y* 并成功通过验证。即 E_2 事件不会发生。

综上，环境 *Z* 只能以可忽略的概率区分 *REAL* 和 *IDEAL*，即 *IDEAL* ≈ *REAL*。定理 2 得证。

5　安全定位协议 UC 模型的应用

本文提出的安全定位协议 UC 模型有以下 2 种应用方法。

1) 定位协议的安全性分析

利用安全定位协议 UC 模型，可以对定位的安全性进行形式化分析。如果一个定位协议可以安全实现理想函数 F_{SP}，那么该协议就满足 UC 安全，具有可组合安全性，即在任意环境下运行该协议，都能确保其安全性。

2) 定位协议的模块化设计

基于安全定位协议 UC 模型，结合 UC 组合安全理论，可以为协议的模块化设计提供理论支持。利用 UC 框架中混合模型，既可以借助其他子协议或理想函数（如 F_{BRM}），设计满足 UC 安全的定位协议，又可以将 UC 安全的定位协议作为子协议，与其他协议组合，实现组合协议的 UC 安全。

6　结束语

本文在 UC 框架下提出了安全定位的可组合安全模型。根据安全定位协议的特点，设计了安全定位的理想函数 F_{SP}。同时，设计了 BRM 模型的理想函数 F_{BRM}。最后，证明了 1-维空间的安全定位协议 π_{SP1d} 在 F_{BRM}-混合模型下可以安全实现理想函数 F_{SP}。

参考文献：

[1] CHIANG J T, HAAS J J, HU Y C. Secure and precise location verification using distance bounding and simultaneous multilateration[A]. WISEC, ACM[C]. 2009. 181-192.

[2] CHANDRAN N, GOYAL V, MORIARTY R, *et al*. Position-based cryptography[A]. Cryptology-CRYPTO 2009[C]. 2009. 391-407.

[3] DZIEMBOWSKI S, PIETRZAK K. Intrusion-resilient secret sharing[A]. FOCS '07: Proceedings of the 48th Annual IEEE Foundations of Computer Science[C]. 2007.

[4] BUHRMAN H, CHANDRAN N, FEHR S, *et al*. Position-based quantum cryptography: impossibility and constructions[EB/OL]. http://eprint.iacr.org/2010/275.pdf,2010.

[5] CANETTI R. Universally composable security: a new paradigm for cryptographic protocols[EB/OL]. http://eprint. iacr.org/2000/067,2000.

[6] 李凤华, 冯涛, 马建峰. 基于 VSPH 的 UC 不经意传输协议[J]. 通信学报, 2007, 28(7):28-34.
LI F H, FENG T, MA J F. Universally composable oblivious transfer protocol based on VSPH[J]. Journal on Communications, 2007, 28(7):28-34.

[7] 张俊伟, 马建峰, 杨力. UC 安全的基于一次签名的广播认证[J]. 通信学报, 2010, 31(5):31-36.
ZHANG J W, MA J F, YANG L. UC secure one-time signature based broadcast authentication[J]. Journal on Communications, 2010, 31(5): 31-36.

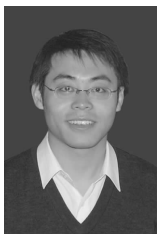
[8] ZHANG J W, MA J F, MOON S J. Universally composable secure TNC model and EAP-TNC protocol in IF-T[J]. Science China Information Sciences, 2010,53(3): 465-482.

[9] MAURER U M. Conditionally-perfect secrecy and a provebly-secure randomized cipher [J]. Journal of Cryptology, 1992, 5(1):53-66.

作者简介：

张俊伟（1982-），男，陕西西安人，博士，西安电子科技大学讲师，主要研究方向为密码学、网络安全。

马建峰（1963-），男，陕西西安人，教育部“长江学者”特聘教授，西安电子科技大学教授、博士生导师，主要研究方向为计算机安全、密码学。



杨超（1979-），男，陕西西安人，博士，西安电子科技大学副教授，硕士生导师，主要研究方向为无线网络安全、协议的安全性测试与仿真。