协议组合逻辑安全的 4G 无线网络接入认证方案

王丽丽[1]，冯涛[1,2,3]，马建峰[3]

(1. 兰州理工大学 计算机与通信学院，甘肃 兰州 730050;

2. 福建师范大学 网络安全与密码技术重点实验室，福建 福州 350007;

3. 西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071)

摘 要：针对 4G 无线网络中移动终端的接入认证问题，基于自证实公钥系统设计了新的安全接入认证方案，并运用协议演绎系统演示了该方案形成的过程和步骤，用协议组合逻辑对该方案的安全属性进行了形式化证明。通过安全性证明和综合分析，表明该方案具有会话认证性和密钥机密性，能抵御伪基站攻击和重放攻击，并能提供不可否认服务和身份隐私性，同时提高了移动终端的接入效率。

关键词：自证实公钥；协议组合逻辑；协议演绎系统；认证协议；4G

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2012)04-0077-08

Secure access authentication scheme for 4G wireless network based on PCL

WANG Li-li[1], FENG Tao[1,2,3], MA Jian-feng[3]

(1.School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China;

2. Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China;

3. Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an 710071, China)

Abstract: Considering the access authentication for mobile terminals in the 4G wireless network, a new secure access authentication scheme based on the self-certified public key system was designed. Then the deductive process of the scheme was derived with the protocol derivation system and its security attributes was formally proofed with protocol composition logic. By the security proof and comprehensive analysis, it is showed that the proposed scheme not only has session authentication and key confidentiality, but also can defend pseudo-base station attack and reply attack, provide the undeniable service and identity privacy. Moreover, the scheme can improve the access efficiency of the mobile terminals.

Key words: self-certified public key; protocol composition logic; protocol derivation system; authentication protocol; 4G

收稿日期：2010-08-23；**修回日期**：2010-12-15

基金项目：国家高技术研究发展计划(“863”计划)基金资助项目(2007AA01Z429)；国家自然科学基金资助项目(60972078)；甘肃省高等学校基本科研业务费基金资助项目(0914ZTB186)；甘肃省自然科学基金资助项目(2007GS04823)；兰州理工大学博士基金资助项目(BS14200901)；网络安全与密码技术福建省高校重点实验室开放课题基金资助项目(09A006)

Foundation Items: The National High Technology Research and Development Program of China (863 Program)(2007AA01Z429) The National Natural Science Foundation of China(60972078); The Universities Basic Scientific Research Foundation of Gansu Province in China(0914ZTB186); The Natural Science Foundation of Gansu Province(2007GS04823); The Lanzhou University of Technology Ph.D. Programs of China(BS14200901); Funds of Key Lab of Fujian Province University Network Security and Cryptology (09A006)

1 引言

在多种无线通信技术及异构网络共存、融合的趋势下，4G无线网络移动终端的安全接入问题变得更加复杂和重要[1]。2009年，ITU-R确立了两大4G候选标准：LTE-Advanced和IEEE 802.16m。文献[2,3]中介绍了关于LTE RAN(radio access network)的安全决策，但没有给出具体的接入认证协议。文献[4]中，IEEE 802.16m工作组针对4G网络的安全机制提出了PKMv3(privacy key management version 3)协议，但也没有给出具体的接入认证过程。

1991年，Girault首次提出自证实公钥系统[5]。同基于证书的公钥密码体制相比，自证实公钥系统更适用于移动环境。首先，AN(access network)和ME(mobile equipment)的认证参数中不包含公钥证书，协议交互之前，不需要存储和传送自己的公钥证书，不需要验证彼此公钥证书的合法性和有效性，节省了存储空间和通信带宽，减轻了网络负载和传输时延，减少了移动终端的计算负担；此外，对公钥的验证隐藏在签名验证或加密过程中，当网络存在阶层关系时也不需要通过其他网络实体转发认证信息，提高了公钥验证效率和认证效率。

Zheng等人[6]基于自证实公钥系统提出了一个4G网络用户认证方案，但方案还存在不足之处。第一，方案中，网络端的公钥并不是基于自证实公钥系统构建的，对该公钥的验证是利用基站联合广播，并在ME中设立缓冲区，通过概率统计方法实现的。但是验证结果存在风险，如局部出现伪基站密度超过合法基站的可能等。而且，方案中没有明确指出如何确定终端缓冲区的长度、如何确定伪基站与合法基站的数量同识别成功的概率之间的关系。第二，该方案的首次接入认证和切换认证协议中，用户的归属环境和访问网络之间需要交互部分认证信息，接入时延会增加，对实时应用很不利。第三，Zheng没有对该方案的安全属性进行形式化分析和证明。

考虑到4G网络中ME的安全接入问题，以及ME的移动性和漫游性，本文基于自证实公钥设计了一个新的4G无线网络终端接入方案，方案包括首次/切换接入认证协议和再次接入认证协议。由于安全协议的分析和证明对于现代安全网络系统至关重要，通过运用DDMP理论[7]，本文给出新方案的演绎推导，并对其安全属性进行了形式化证明和分析。DDMP理论由A.Datta等人[7]提出，它包括协议演绎系统PDS和协议组合逻辑PCL，该理论既可以作为协议设计的新方法，又为协议的安全性证明和分析提供了一种全新的形式化方法。

2 预备知识

2.1 自证实公钥系统

TA(trust authority)公开模数 n 及其公钥 e，秘密保留私钥 d，用户的注册过程如下[5,8]。

1) 用户选定长度为160bit以上的私钥 x，并计算出 $V = g^{-x} \bmod n$，n 是长度为1 024bit以上的模数，然后将 V 和自己身份ID传给TA。

2) TA计算用户的公钥 Y，$Y = (V - ID)^d \bmod n$，并将 Y 传给用户。

3) 用户验证 $V = (Y^e + ID) \bmod n$，若等式成立，则用户的公钥为 Y，私钥为 x。

在自证实公钥系统中，用户的身份、公钥和私钥满足一种计算上不可伪造的数学关系，在利用密钥执行加解密、签名验证、密钥协商或其他密码操作的同时，就可以验证该数学关系，从而验证公钥的合法性和有效性。用户的私钥是自己选定的，其安全性基于解离散对数困难问题，TA无法从传送过来的数据中得到用户的私钥，不能冒充用户伪造他们的签名，相比于基于身份的公钥密码体制，具有更高的安全性，更适合于开放系统环境中的应用。此外，TA无法完全掌握公钥的产生和验证，即使TA伪造出相同用户的另一个公钥也会被检测出来。

2.2 协议演绎系统和协议组合逻辑

协议演绎系统(PDS)由构件集合和操作集合组成，构件是用于构造复杂协议的简单协议，操作集合包含3类不同的演绎操作：组合、求精和转换。组合操作用于2个协议的组合，包括并行组合和串行组合。求精操作用于一个简单协议构件上，为协议添加必要的安全属性，且不会改变协议的消息数或协议的基础结构，例如用加密的随机数代替原来没有加密的随机数。转换操作则是通过移动消息、组合协议步骤、插入一个或多个协议步骤等操作完成对协议的修改，例如将数据从一个消息移动到另外一个较早的消息中。本文中主要使用的演绎操作包括串行组合操作、转换操作T1以及求精操作R3、R4和R6(具体含义在本文设计的安全协议演绎过程

中说明)。

协议组合逻辑(PCL)可用于安全协议的形式化证明和分析，同 BAN 逻辑及其他的逻辑方法相比，PCL 支持安全协议的组合证明；由于包含了协议的执行过程，PCL 不需要对协议进行抽象；PCL 采用的是标准逻辑概念，而不需要使用“管辖(jurisdiction)”和“信念(belief)”等不清晰规则。此外，PCL 加入了密码学原语，并重点刻画了消息的发送和接收，这些概念体现了安全协议的基本要素。目前，PCL 已经被成功用于形式化证明多个协议的正确性，如 SSL/TLS 协议[7]、IEEE 802.11i 协议[9]、Kerberos V5 协议[10]等。

PCL 的基本语法元素是前置断言—后置断言表达式，即几乎所有的安全协议证明步骤都遵循 $\theta[P]_X\phi$ 规则，该规则表明协议的执行实例 X 执行动作序列 P 以后，状态由 θ 转变为 ϕ。本文用到的部分公理和法则如下[7,11,12]。

Contains(t_1,t_2)：表示 t_1 包含 t_2。

Fresh(X,t)：表示在实例 X 中产生的 t 是新鲜的。

Has(X, t)：秘密属性的一种描述，表示实体 $\hat{X}$ 在实例 X 中拥有信息 t。

Honest($\hat{X}$)：表示实体 $\hat{X}$ 在当前轮中是诚实的，其执行的所有动作都是协议所规定的。

Send(X, t)/New(X,t)/Sign(X,t)/Encrypt(X,t)：分别表示发生了发送、生成随机数、签名和加密动作。

AN2　$\top[\text{new } t]_X \text{Has}(Y,t) \supset (Y = X)$

ENC4　$\text{SymDec}(X,\text{ENC}_k\{|t|\}) \supset \exists Y.\text{SymEnc}(Y,t,k)$

SEC　$\text{Honest}(\hat{X}) \wedge \text{Decrypt}(Y,\text{ENC}_{\hat{X}}\{|x|\}) \supset (\hat{Y} = \hat{X})$

VER　$\text{Honest}(\hat{X}) \wedge \text{Verify}(Y,\text{SIG}_{\hat{X}}\{|x|\}) \wedge \hat{X} \neq \hat{Y} \supset \exists X,t.\text{Send}(X,t) \wedge \text{Contains}(t,\text{SIG}_{\hat{X}}\{|x|\})$

FS2　$\text{FirstSent}(X,t,t') \wedge \text{a}(Y,t'') \supset \text{Send}(X,t') < \text{a}(Y,t'')$ where $X \neq Y$ and $t \subseteq t''$

$\text{HasAlone}(X,t) \equiv \text{Has}(X,t) \wedge (\text{Has}(Y,X) \supset (Y = X))$

P3　$\text{HasAlone}(X,t)[\alpha]_X \text{HasAlone}(X,t)$ where $t \not\subset \alpha$

DH2　$\text{Has}(X,g(ab)) \supset (\text{Computes}(X,g(ab)) \vee \exists t.(\text{Receive}(X,t) \wedge \text{Contains}(t,g(ab))))$

DH3　$(\text{Receive}(X,t) \wedge \text{Contains}(t,g(ab))) \supset \exists Y,t'.((\text{Computes}(X,g(ab))) \wedge \text{Send}(X,t') \wedge \text{Contains}(t',g(ab)))$

$$\text{HON}_Q\ \frac{\text{Start}(X)[\ ]_X\phi \quad (\forall\rho\in Q.\forall P\in \text{BS}(\rho).\phi[P]_X\phi)}{\text{Honest}(\hat{X}) \supset \phi}$$

3　4G 无线网络接入认证新方案

3.1　参数描述

相关参数要求[5,8]：$|x|$表示 x 的长度，整数 A、B、S 满足 $|B| \geqslant 32$，$|S| \geqslant 160$，$|A| \geqslant |B| + |S| + 80$，其中，$|S|$表示私钥长度。TA 为 ME 产生自证实公钥的过程如下。

1) ME 选定私钥 x_{ME}，计算 $V_{\text{ME}} = g^{-x_{\text{ME}}} \bmod n$，并将 ID_{ME}、ID_{HE} 和 V_{ME} 发送给 TA，其中，ID_{ME} 是 ME 的身份标识符(IMSI)，ID_{HE} 是 ME 的归属环境 HE(home environment)的标识符。

2) TA 根据 $Y_{\text{ME}} = (V_{\text{ME}} - ID_{\text{ME}} - ID_{\text{HE}})^d \bmod n$ 计算出 ME 的公钥 Y_{ME}，并将其发送给 ME。

3) ME 验证等式 $Y_{\text{ME}}^e + ID_{\text{ME}} + ID_{\text{HE}} = V_{\text{ME}}$。若验证成功，则移动终端获得公钥 Y_{ME}，私钥 x_{ME}。

同理，AN 通过 TA 获得公钥 Y_{AN}，私钥 x_{AN}。

3.2　移动终端的首次/切换接入认证协议

为了满足移动网络的需求和特性，针对用户在首次接入、再次接入和漫游切换等不同场景，本文基于自证实公钥系统提出了首次/切换接入场景下的认证与密钥交换协议(AKEBSP,authentication and key exchange protocol based on self-certified public key)和再次接入场景下的认证协议，在确保安全接入的前提下，提高了认证效率。首次/切换接入场景下的认证过程如图 1 所示。

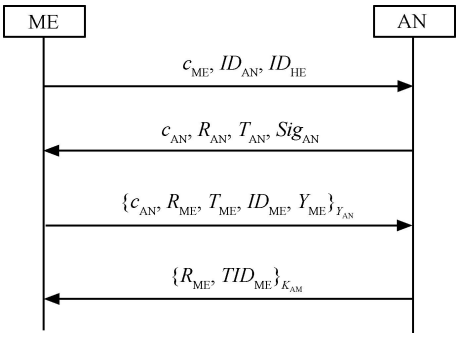

图 1　首次/切换接入认证过程

此过程说明如下。

1) ME 收到 AN 广播的 ID_{AN} 和公钥 Y_{AN} 后，选

择随机数 $c_{\mathrm{ME}} \in [0, B]$，并将 c_{ME}、ID_{AN}、ID_{HE} 发送给 AN。

2) AN 验证 ID_{AN} 后，选择随机数 $r_{\mathrm{AN}} \in [0, A]$ 和 $c_{\mathrm{AN}} \in [0, B]$，分别计算 $T_{\mathrm{AN}} = r_{\mathrm{AN}} + x_{\mathrm{AN}} c_{\mathrm{ME}}$ 和 $R_{\mathrm{AN}} = g^{r_{\mathrm{AN}}} \bmod n$，并将消息 c_{AN}、R_{AN}、R_{AN}、Sig_{AN} 发送给 ME，其中 $Sig_{\mathrm{AN}} = \{c_{\mathrm{ME}}, c_{\mathrm{AN}}, R_{\mathrm{AN}}, T_{\mathrm{AN}}\}_{x_{\mathrm{AN}}}$。

3) ME 首先验证 Sig_{AN}，如果正确，则验证下面式子是否成立：$g^{T_{\mathrm{AN}}} (Y_{\mathrm{AN}}^{e} + ID_{\mathrm{AN}})^{c_{\mathrm{ME}}} \bmod n = R_{\mathrm{AN}}$ 和 $T_{\mathrm{AN}} \in [0, A + (B-1)(S-1)]$。如果成立，则选择随机数 $r_{\mathrm{ME}} \in [0, B]$，并计算 $T_{\mathrm{ME}} = r_{\mathrm{ME}} + x_{\mathrm{ME}} c_{\mathrm{AN}}$，$K_{\mathrm{AM}} = R_{\mathrm{AN}}^{r_{\mathrm{ME}}} \bmod n$ 和 $R_{\mathrm{ME}} = g^{r_{\mathrm{ME}}} \bmod n$，然后将消息 $\{c_{\mathrm{AN}}, R_{\mathrm{ME}}, T_{\mathrm{ME}}, ID_{\mathrm{ME}}, Y_{\mathrm{ME}}\}_{Y_{\mathrm{AN}}}$ 发送给 AN。

4) AN 收到并解密该消息之后，验证下面式子是否成立：$g^{T_{\mathrm{ME}}} (Y_{\mathrm{ME}}^{e} + ID_{\mathrm{ME}} + ID_{\mathrm{HE}})^{c_{\mathrm{AN}}} \bmod n = R_{\mathrm{ME}}$ 和 $T_{\mathrm{ME}} \in [0, A + (B-1)(S-1)]$，如果成立则计算 $K_{\mathrm{AM}} = R_{\mathrm{ME}}^{r_{\mathrm{AN}}} \bmod n$，并生成 ME 的临时身份 TID_{ME}，将消息 $\{R_{\mathrm{ME}}, TID_{\mathrm{ME}}\}_{K_{\mathrm{AM}}}$ 发送给 ME。

5) ME 收到消息并解密，获得了自己的临时身份 TID_{ME}，供再次接入该网络使用。

认证结束后，AN 会在数据库中存储 TID_{ME} 和（ID_{ME}, Y_{ME}, K_{AM}）的对应关系，向 ME 提供服务后可以将 $\{R_{\mathrm{AN}}, T_{\mathrm{ME}}, c_{\mathrm{AN}}, bill, Sig'_{\mathrm{AN}}\}$ 作为不可否认凭证发送给 ME 的归属环境 HE。其中，*bill* 为计费信息，$Sig'_{\mathrm{AN}} = \{R_{\mathrm{AN}}, T_{\mathrm{ME}}, c_{\mathrm{AN}}, bill\}_{x_{\mathrm{AN}}}$。

3.3 移动终端再次接入认证协议

首次/切换接入认证通过后，ME 需要再次接入到同一网络时，可以利用 TID_{ME} 代替协议中的 ID_{ME} 进行再次接入认证，保护了 ME 的身份隐私，其认证交互过程如图 2 所示。其中，TID_{ME}'是 AN 为 ME 生成的新的临时身份，K_{AM}'是 AN 生成的新的会话密钥，作为 ME 和 AN 下次交互使用，减少了攻击者通过已攻陷的会话密钥同网络交互的风险。

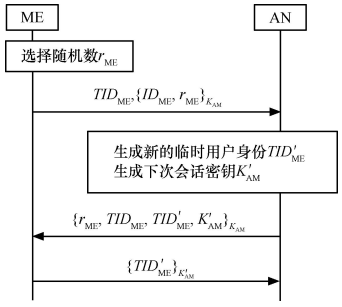

图 2 再次接入认证过程

4 新协议的演绎

由于篇幅限制，本文仅对首次/切换接入场景下的认证与密钥交换协议 AKEBSP 进行演绎推导和形式化证明。在新协议的演绎过程和步骤中，为了简洁和清晰，分别用 $\hat{X}$ 和 $\hat{Y}$ 表示协议的 2 个参与方：移动终端 ME 和接入网络 AN，其相应的实体分别用 X 和 Y 表示。此外，AN 的公钥也可用 $\hat{Y}$ 表示，终端的归属环境标识符用 ID_H 表示。

首先，选取 3 个简单的基本协议，一个是基于签名的挑战应答协议 P1，另外 2 个是基于加密的挑战应答协议 P2 和 P3（其中，$\hat{Y}$ 是 AN 的公钥，密钥 K 是 ME 通过 R_Y 计算得到的）。

$$\mathrm{P1}: X \to Y: c_X$$
$$Y \to X: SIG_{\hat{Y}}(c_X)$$
$$\mathrm{P2}: Y \to X: c_Y$$
$$X \to Y: ENC_{\hat{Y}}(c_Y)$$
$$\mathrm{P3}: X \to Y: R_X$$
$$Y \to X: ENC_K(R_X)$$

对协议 P1 和 P2 进行串行组合（串行组合操作是通过适当的替代步骤，使前一协议模块的输出代替后一协议模块的输入来完成协议的组合），用协议 P1 的输出代替 P2 的输入，从而得到协议 P4。

$$\mathrm{P4}: X \to Y: c_X$$
$$Y \to X: SIG_{\hat{Y}}(c_X)$$
$$Y \to X: c_Y$$
$$X \to Y: ENC_{\hat{Y}}(c_Y)$$

对协议 P4 应用转换操作 T1（通过将数据从一个消息移动到另外一个较早的消息中），将 c_Y 移动到较早的消息中，从而得到协议 P5，其主要目的是减少消息数量。

$$\mathrm{P5}: X \to Y: c_X$$
$$Y \to X: c_Y, SIG_{\hat{Y}}(c_X)$$
$$X \to Y: ENC_{\hat{Y}}(c_Y)$$

由于 ME 验证 AN 时需要使用 2 个参数，分别是由 $R_{\mathrm{AN}}=g^{r_{\mathrm{AN}}} \bmod n$ 和 $T_{\mathrm{AN}}=r_{\mathrm{AN}}+x_{\mathrm{AN}}c_{\mathrm{ME}}$ 计算得到的 R_{AN} 和 T_{AN}，但协议 P5 中并未给出，根据转换操作的定义，这里可以应用转换操作在协议第二步中加入 R_{AN} 和 T_{AN}，从而得到协议 P6。

$$\mathrm{P6}: X \to Y: c_X$$
$$Y \to X: c_Y, R_Y, T_Y, SIG_{\hat{Y}}(c_X)$$
$$X \to Y: ENC_{\hat{Y}}(c_Y)$$

为了让 X 确信消息是由 Y 新鲜生成的，对协议 P6 应用转换操作 T2，得到协议 P7，其主要目的是为了防止重放攻击。

$$\begin{aligned}&\text{P7}: X \to Y : c_X\\ &\quad Y \to X : c_Y, R_Y, T_Y, SIG_{\hat{Y}}(c_X, c_Y, R_Y, T_Y)\\ &\quad X \to Y : ENC_{\hat{Y}}(c_Y)\end{aligned}$$

由于 ME 要明确接收消息的 AN，并需要同归属环境进行交互，根据转换操作的定义，在协议第一步中加入 ID_Y 和 TID_H，从而得到协议 P8。

$$\begin{aligned}&\text{P8}: X \to Y : c_X, ID_Y, ID_H\\ &\quad Y \to X : c_Y, R_Y, T_Y, SIG_{\hat{Y}}(c_X, c_Y, R_Y, T_Y)\\ &\quad X \to Y : ENC_{\hat{Y}}(c_Y)\end{aligned}$$

对协议 P8 和 P3 进行串行组合，用协议 P8 输出代替协议 P3 的输入，从而得到协议 P9。

$$\begin{aligned}&\text{P9}: X \to Y : c_X, ID_Y, ID_H\\ &\quad Y \to X : c_Y, R_Y, T_Y, SIG_{\hat{Y}}(c_X, C_Y, R_Y, T_Y)\\ &\quad X \to Y : ENC_{\hat{Y}}(c_Y)\\ &\quad X \to Y : R_X\\ &\quad Y \to X : ENC_K(R_X)\end{aligned}$$

对协议 P9 应用转换操作 T1，将消息 R_X 移动到较早的消息中，从而得到协议 P10，其主要目的也是减少消息数量。

$$\begin{aligned}&\text{P10}: X \to Y : c_X, ID_Y, ID_H\\ &\quad Y \to X : c_Y, R_Y, T_Y, SIG_{\hat{Y}}(c_X, c_Y, R_Y, T_Y)\\ &\quad X \to Y : ENC_{\hat{Y}}(c_Y, R_X)\\ &\quad Y \to X : ENC_K(R_X)\end{aligned}$$

由于 AN 验证 ME 时还需要参数 T_X、X 的身份标识 ID_X 以及 X 的公钥 Y_X，但协议 P10 中并未给出，根据转换操作的定义，这里可以应用转换操作在协议第 3 步中加入 T_X、ID_X 和 Y_X，从而得到协议 P11。

$$\begin{aligned}&\text{P11}: X \to Y : c_X, ID_Y, ID_H\\ &\quad Y \to X : c_Y, R_Y, T_Y, SIG_{\hat{Y}}(c_X, c_Y, R_Y, T_Y)\\ &\quad X \to Y : ENC_{\hat{Y}}(c_Y, R_X, T_X, ID_X, \hat{X})\\ &\quad Y \to X : ENC_K(R_X)\end{aligned}$$

为了保护用户的身份隐私，首次认证或切换认证之后，用户再次接入该网络时是借助一个临时身份 TID_X，但协议 P11 中并未给出，根据转换操作的定义，这里可以应用转换操作在协议第 4 步中加入 TID_X，从而得到协议 P12。

$$\begin{aligned}&\text{P12}: X \to Y : c_X, ID_Y, ID_H\\ &\quad Y \to X : c_Y, R_Y, T_Y, SIG_{\hat{Y}}(c_X, c_Y, R_Y, T_Y)\\ &\quad X \to Y : ENC_{\hat{Y}}(c_Y, R_X, T_X, ID_X, \hat{X})\\ &\quad Y \to X : ENC_K(R_X, TID_X)\end{aligned}$$

到此为止，通过协议演绎系统(PDS)演绎得到了新协议 AKEBSP。

5　新协议安全性的形式化证明和分析

5.1　协议流程表示

PCL 标记法表示的协议角色如下。

$$\begin{aligned}&\text{Init}_{\text{AKEBSP}} \equiv (\hat{Y})[\\ &\qquad \text{new } n_{X1};\ \ \text{send } \hat{X}, \hat{Y}, n_{X1}, ID_Y, ID_H;\\ &\qquad \text{receive } \hat{Y}, \hat{X}, n_{Y2}, R_Y, T_Y, r_1;\\ &\qquad \text{verify } r_1, (n_{X1}, n_{Y2}, R_Y, T_Y), \hat{Y};\\ &\qquad \text{new } n_{X2};\ \ \ \text{match } g(n_{X2})/R_X;\\ &\qquad \text{match } (n_{X2} + \hat{X} n_{Y2})/T_X;\\ &\qquad \text{match } R_Y(n_{X2})/K;\\ &\qquad r_2 := \text{enc } (n_{Y2}, R_X, T_X, ID_X, \hat{X}), \hat{Y};\\ &\qquad \text{send } \hat{X}, \hat{Y}, r_2;\ \ \ \text{receive } \hat{Y}, \hat{X}, r_3;\\ &\qquad s_2 := \text{dec } r_3, K;\ \ \text{match } s_2/(R_X, TID_X);\\ &\qquad]_X()\\ &\text{Resp}_{\text{AKEBSP}} \equiv ()[\\ &\qquad \text{receive } \hat{X}, \hat{Y}, n_{X1}, ID_Y, ID_H;\\ &\qquad \text{new } n_{Y1};\ \ \ \text{match } g(n_{Y1})/R_Y;\\ &\qquad \text{match } (n_{Y1} + \hat{Y} n_{X1})/T_Y; \text{new } n_{Y2};\\ &\qquad r_1 = \text{sign } (n_{X1}, n_{Y2}, R_Y, T_Y), \hat{Y};\\ &\qquad \text{send } \hat{Y}, \hat{X}, n_{Y2}, R_Y, T_Y, r_1;\\ &\qquad \text{receive } \hat{X}, \hat{Y}, r_2;\ \ \ s_1 := \text{dec } r_2, \hat{Y};\\ &\qquad \text{match } s_1/(n_{Y2}, R_X, T_X, ID_X, \hat{X});\\ &\qquad \text{match } R_X(n_{Y1})/K;\ \ \text{new } TID_X;\\ &\qquad r_3 := \text{enc } (R_X, TID_X), K;\\ &\qquad \text{send } \hat{Y}, \hat{X}, r_3;\\ &\qquad]_Y()\end{aligned}$$

其中，$\text{Init}_{\text{AKEBSP}}$ 是发起者角色(对应于 ME)的动作序列，$\text{Resp}_{\text{AKEBSP}}$ 是响应者角色(对应于 AN)的动作序列。

5.2　安全属性的形式化证明

定理 1　AKEBSP 安全认证协议具有会话认证性。

根据协议组合逻辑 PCL，需要证明的发起者角色会话认证性的形式化表示为

$$\vdash Q_{\text{AKEBSP}} \top [\text{Init}_{\text{AKEBSP}}]_X \text{Honest}(\hat{Y}) \wedge \hat{Y} \neq \hat{X} \supset \phi_{\text{auth}}$$

其中，

$$\begin{aligned}\phi_{\text{auth}} \equiv \exists Y.((&\text{Send}(X, msg_1) < \text{Receive}(Y, msg_1)) \\ &\wedge (\text{Receive}(Y, msg_1) < \text{Send}(Y, msg_2)) \\ &\wedge (\text{Send}(Y, msg_2) < \text{Receive}(X, msg_2)) \\ &\wedge (\text{Receive}(X, msg_2) < \text{Send}(X, msg_3)) \\ &\wedge (\text{Send}(X, msg_3) < \text{Receive}(Y, msg_3)) \\ &\wedge (\text{Receive}(Y, msg_3) < \text{Send}(Y, msg_4))) \\ &(\text{Send}(Y, msg_4) < \text{Receive}(X, msg_4)))\end{aligned}$$

$$msg_1 \equiv (\hat{X}, \hat{Y}, n_{X1}, ID_Y, ID_H)$$

$$msg_2 \equiv (\hat{Y}, \hat{X}, n_{Y2}, R_Y, T_Y, SIG_{\hat{Y}}\{|\, n_{X1}, n_{Y2}, R_Y, T_Y \,|\})$$

$$msg_3 \equiv (\hat{X}, \hat{Y}, ENC_{\hat{Y}}\{|\, n_{Y2}, R_X, T_X, ID_X, \hat{X} \,|\})$$

$$msg_4 \equiv (\hat{Y}, \hat{X}, ENC_K\{|\, R_X, TID_X \,|\})$$

当上式成立时，AKEBSP 协议的发起者角色能够保证会话认证性。这里仅给出 ME 端的证明情况，AN 端的证明情况类似。

证明

1) AN3 $\top [\text{new } n_{X1}]_X \text{Fresh}(X, n_{X1})$

2) FS1 $\text{Fresh}(X, n_{X1})$
$[\text{send } \hat{X}, \hat{Y}, n_{X1}, ID_Y, ID_H]_X$
$\text{FirstSend}(X, n_{X1}, msg_1)$

3) 1),2),SEQ,P1 $\top [\text{Init}_{\text{AKEBSP}}]_X \text{FirstSend}(X, n_{X1}, msg_1)$

4) 3),FS2 $\top [\text{Init}_{\text{AKEBSP}}]_X \text{Receive}(Y, msg_1) \wedge \hat{Y} \neq \hat{X} \supset (\text{Send}(X, msg_1) < \text{Receive}(Y, msg_1))$

5) AA1 $\top [\text{verify } r_1, (n_{X1}, n_{Y2}, R_Y, T_Y), \hat{Y}]_X \text{Verify}(X, SIG_{\hat{Y}}\{|n_{X1}, n_{Y2}, R_Y, T_Y|\})$

6) 5),P1,SEQ $\top [\text{Init}_{\text{AKEBSP}}]_X \text{Verify}(X, SIG_{\hat{Y}}\{|n_{X1}, n_{Y2}, R_Y, T_Y|\})$

7) 6),VER $\top [\text{Init}_{\text{AKEBSP}}]_X \exists Y, t.\text{Send}(Y, t) \wedge \text{Contains}(t, SIG_{\hat{Y}}\{|n_{X1}, n_{Y2}, R_Y, T_Y|\})$

8) $\text{HON}_{Q_{\text{AKEBSP}}}$ $(\text{Honest}(\hat{Y}) \wedge \text{Send}(Y, t) \wedge \text{Contains}(t, SIG_{\hat{Y}}\{|n_{X1}, n_{Y2}, R_Y, T_Y|\})) \supset (\text{New}(Y, n_{X1}) \vee \text{Receive}(Y, msg_1) < \text{Send}(Y, msg_2))$

9) 7),8) $\top [\text{Init}_{\text{AKEBSP}}]_X \text{Honest}(\hat{Y}) \supset (\exists Y.\text{New}(Y, n_{X1}) \vee (\text{Receive}(Y, msg_1) < \text{Send}(Y, msg_2)))$

10) AA1 $\top [\text{new } n_{X1}]_X \text{New}(X, n_{X1})$

11) 10),P1,SEQ $\top [\text{Init}_{\text{AKEBSP}}]_X \text{New}(X, n_{X1})$

12) 9),11),AN1 $\top [\text{Init}_{\text{AKEBSP}}]_X \text{Honest}(\hat{Y}) \wedge \hat{Y} \neq \hat{X} \supset (\exists Y.\text{Receive}(Y, msg_1) < \text{Send}(Y, msg_2))$

13) $\text{HON}_{Q_{\text{AKEBSP}}}$ $(\text{Honest}(\hat{Y}) \wedge \text{Receive}(Y, msg_1) \wedge \text{Send}(Y, msg_2)) \supset \text{FirstSend}(Y, n_{Y2}, msg_2)$

14) AA1,AR3,SEQ $\top [\text{Init}_{\text{AKEBSP}}]_X \text{Receive}(X, msg_2)$

15) 13),14),FS2 $\top [\text{Init}_{\text{AKEBSP}}]_X \text{Honest}(\hat{Y}) \wedge \hat{Y} \neq \hat{X} \wedge (\text{Receive}(Y, msg_1) < \text{Send}(Y, msg_2)) \supset (\text{Send}(Y, msg_2) < \text{Receive}(X, msg_2))$

16) AA4,P1 $\top [\text{Init}_{\text{AKEBSP}}]_X \text{Receive}(X, msg_2) < \text{Send}(X, msg_3)$

17) AN3,FS1 $\top [\text{new } n_{X2}; \text{send } \hat{X}, \hat{Y}, r_2]_X \text{FirstSend}(X, n_{X2}, msg_3)$

18) 17),SEQ,P1 $\top [\text{Init}_{\text{AKEBSP}}]_X \text{FirstSend}(X, n_{X2}, msg_3)$

19) 18),FS2 $\top [\text{Init}_{\text{AKEBSP}}]_X \text{Receive}(Y, msg_3) \wedge \hat{Y} \neq \hat{X} \supset (\text{Send(X}, msg_3) < \text{Receive}(Y, msg_3))$

20) AA1 $\top [s_2 := \text{dec } r_3, \text{K}; \text{match } s_2/(R_X, TID_X)]_X \text{Decrypt}(X, r_3)$

21) 20),P1,SEQ $\top [\text{Init}_{\text{AKEBSP}}]_X \text{Decrypt}(X, r_3)$

22) 21),ENC4 $\top [\text{Init}_{\text{AKEBSP}}]_X \exists Y.\text{Enc}(Y, r_3) \wedge \text{S}end(Y, r_3)$

23) $\text{HON}_{Q_{\text{AKEBSP}}}$ $(\text{Honest}(\hat{Y}) \wedge \text{Send}(Y, r_3) \supset (\text{New}(Y, R_X) \vee (\text{Receive}(Y, msg_3) < \text{Send}(Y, msg_4)))$

24) 22),23) $\top [\text{Init}_{\text{AKEBSP}}]_X \text{Honest}(\hat{Y}) \supset (\exists Y.\text{New}(Y, R_X) \vee (\text{Receive}(Y, msg_3) < \text{Send}(Y, msg_4)))$

25) AA1 $\top [\text{new } n_{X2}; \text{match g}(n_{X2})/R_X]_X \text{New}(X, R_X)$

26) 25),P1,SEQ $\top [\text{Init}_{\text{AKEBSP}}]_X \text{New}(X, R_X)$

27) 24),26),AN1 $\top[\text{Init}_{\text{AKEBSP}}]_X$
$\text{Honest}(\hat{Y}) \wedge \hat{Y} \neq \hat{X} \supset$
$(\exists Y.\text{Receive}(Y, msg_3) < \text{Send}(Y, msg_4))$

28) $\text{HON}_{Q_{\text{AKEBSP}}}$ $(\text{Honest}(\hat{Y}) \wedge \text{Receive}(Y, msg_3)$
$\wedge \text{Send}(Y, msg_4)) \supset$
$\text{FirstSend}(Y, TID_X, msg_4)$

29) AA1,AR3,SEQ $\top[\text{Init}_{\text{AKEBSP}}]_X$
$\text{Receive}(X, msg_4)$

30) 28),29),FS2 $\top[\text{Init}_{\text{AKEBSP}}]_X$
$\text{Honest}(\hat{Y}) \wedge \hat{Y} \neq \hat{X} \wedge$
$(\text{Receive}(Y, msg_3) < \text{Send}(Y, msg_4)) \supset$
$(\text{Send}(Y, msg_4) < \text{Receive}(X, msg_4))$

31) 4),12),15),16),19),27),30)
$\top[\text{Init}_{\text{AKEBSP}}]_X \text{Honest}(\hat{Y}) \wedge \hat{Y} \neq \hat{X} \supset \phi_{\text{auth}}$

定理 2 AKEBSP 安全认证协议具有密钥机密性。

根据协议组合逻辑 PCL，需要证明的发起者角色密钥机密性的形式化表示为

$$\vdash Q_{\text{AKEBSP}} \top [\text{Init}_{\text{AKEBSP}}]_X \text{Honest}(\hat{Y}) \wedge \hat{Y} \neq \hat{X} \supset \phi_{\text{sec}}$$

其中，

$$\phi_{\text{sec}} \equiv \text{Has}(Z, g(n_{X2} n_{Y1})) \supset (Z = X \vee Z = Y)$$

当上式成立时，AKEBSP 协议的发起者角色能够保证密钥机密性。这里仅给出 ME 端的证明情况，AN 端的证明情况类似。

证明

1) AN2,AN3 $\top[\text{new } n_{X2};\ \text{match } g(n_{X2})/R_X]_X$
$(\text{Has}(Y, n_{X2}) \supset (Y = X)) \wedge$
$\text{Fresh}(X, g(n_{X2}))$

2) HasAlone,1),P1,P3 $\text{HasAlone}(X, n_{X2}) \wedge$
$\text{Fresh}(X, g(n_{X2}))\ [\text{Init}_{\text{AKEBSP}}]_X$
$\text{HasAlone}(X, n_{X2})$

3) AKEBSP $\text{HasAlone}(X, n_{X2}) \wedge$
$\text{Fresh}(X, g(n_{X2}))\ [\text{Init}_{\text{AKEBSP}}]_X$
$\text{Honest}(\hat{Y}) \supset \phi_{\text{auth}}$

4) $\text{HON}_{Q_{\text{AKEBSP}}}$ $\text{Honest}(\hat{Y}) \wedge \text{Send}(Y, msg_2) \supset$
$\exists n_{Y1}'.(R_Y = g(n_{Y1}') \wedge$
$\text{HasAlone}(Y, n_{Y1}'))$

5) 3),4) $\text{HasAlone}(X, n_{X2}) \wedge$
$\text{Fresh}(X, g(n_{X2}))[\text{Init}_{\text{AKEBSP}}]_X$
$\text{Honest}(\hat{Y}) \supset \exists Y, n_{Y1}.(R_Y = g(n_{Y1}) \wedge$
$\text{HasAlone}(Y, n_{Y1}))$

6) AA1,REC,PROJ,P1 $\text{HasAlone}(X, n_{X2}) \wedge$
$\text{Fresh}(X, g(n_{X2}))[\text{Init}_{\text{AKEBSP}}]_X$
$\text{Has}(X, g(n_{X2}))$

7) 2),5),Computes $\text{HasAlone}(X, n_{X2}) \wedge$
$\text{Fresh}(X, g(n_{X2}))[\text{Init}_{\text{AKEBSP}}]_X$
$\text{Honest}(\hat{Y}) \supset \exists Y, n_{Y1}.(R_Y = g(n_{Y1}) \wedge$
$(\text{Computes}(Z, g(n_{X2} n_{Y1})) \supset$
$(Z = X \vee Z = Y)))$

8) 2),5),6),Computes $\text{HasAlone}(X, n_{X2}) \wedge$
$\text{Fresh}(X, g(n_{X2}))[\text{Init}_{\text{AKEBSP}}]_X$
$\text{Honest}(\hat{Y}) \supset \exists Y, n_{Y1}.$
$(R_Y = g(n_{Y1}) \wedge$
$(\text{Computes}(X, g(n_{X2} n_{Y1})))$

9) 7),8) $\text{HasAlone}(X, n_{X2}) \wedge$
$\text{Fresh}(X, g(n_{X2}))[\text{Init}_{\text{AKEBSP}}]_X$
$\text{Honest}(\hat{Y}) \supset \exists Y, n_{Y1}.(_Y = g(n_{Y1}) \wedge$
$\text{Computes}(X, g(n_{X2} n_{Y1})) \wedge$
$(\text{Computes}(Z, g(n_{X2} n_{Y1})) \supset$
$(Z = X \vee Z = Y)))$

10) DH2,DH3 $\text{Has}(X, g(n_{X2} n_{Y1})) \supset$
$(\text{Computes}(X, g(n_{X2} n_{Y1}))\ \vee$
$\exists Y, m.(\text{Computes}(Y, g(n_{X2} n_{Y1})) \wedge$
$\text{Send}(Y, m) \wedge \text{Contains}(m, g(n_{X2} n_{Y1}))))$

11) $\text{HON}_{Q_{\text{AKEBSP}}}$ $\text{Honest}(\hat{Y}) \supset$
$(\text{Computes}(Y, g(n_{X2} n_{Y1})) \supset$
$\top\ \exists m.(\text{Send}(Y, m) \wedge$
$\text{Contains}(m, g(n_{X2} n_{Y1})))$

12) 9),10),11),DH1 $\text{HasAlone}(X, n_{X2}) \wedge$
$\text{Fresh}(X, g(n_{X2} n_{Y1}))[\text{Init}_{\text{AKEBSP}}]_X \supset \phi_{\text{sec}}$

5.3 新方案的综合分析

从认证协议的可证明安全性、通信效率和计算效率等方面对新方案中的 AKEBSP 协议和文献[6]提出的 SPAKA 协议进行比较，结果如表 1 所示，其中有关符号说明如下：|SV|表示一次签名验证操作，|SED|表示一次对称密钥加解密操作，|PED|表示一次非对称密钥加解密操作。

新方案是基于自证实公钥系统提出的，节省了存储空间，减少了 ME 的计算量和认证时延。根据协议的演绎过程可知，ME 和 AN 之间传递的所有

消息均具有新鲜性和不可预测性，所以新方案能抵御重放攻击。

表 1 本方案与相关方案的比较

性质	方案	
	SPAKA[6]	AKEBSP（本文）
伪基站攻击	无防御	有效防御
协议交互次数	5 次	4 次
计算复杂性	|SV|+2|PED|	|SV|+|PED|+|SED|
可证明安全	无分析	PCL 安全

新方案能提供不可否认服务，整个系统中只有拥有正确私钥的终端用户才可以根据 c_{AN} 构造出合法的 T_{ME}，一旦终端用户通过了认证，则不能否认自己的接入。当出现纠纷的时候，AN 可以提供 R_{AN}、T_{ME} 和 c_{AN} 进行验证，以作为不可否认凭证。

新方案中，ME 的身份（ID_{ME}/*IMSI*）是在用户验证接入网络的身份之后发送出去的，没有以明文形式在空中接口和有线链路传输，且只有 TA 知道用户公钥和用户身份的对应关系，攻击者无法对用户进行非法跟踪，提供了身份保护。每次认证后，AN 都会动态更换用户的临时身份，使得用户身份的安全性大大增强。

6 结束语

本文分析了 4G 无线网络中移动终端的安全接入认证问题，基于自证实公钥设计了一个新的终端接入认证方案。新方案包括首次/切换接入场景下的认证及密钥交换 AKEBSP 协议和再次接入场景下的认证协议，适应了 4G 无线网络的移动和漫游特性。本文应用 DDMP 理论中的协议演绎系统 PDS 对新协议进行了演绎推导，用协议组合逻辑 PCL 对协议进行了形式化证明，并综合分析了协议的安全性能。结果表明，新方案具有会话认证性和密钥机密性，不仅能抵御伪基站攻击和重放攻击，还能提供不可否认服务和身份隐私性，同时提高了移动终端的接入效率。

参考文献：

[1] PIYUSH G,PRIYADARSHAN P.4G-A new era in wireless telecommunication[EB/OL]. http://www.idt.mdh.se/kurser/ct3340/ht09/ADMINISTRATION/IRCSE09-submissions/ircse09_submission_13.pdf, 2009.

[2] AQSACOM S,AQSACOM I. Lawful interception for 3G and 4G networks[EB/OL].http://www.aqsacomna.com/us/articles/Aqsacom_White_paper_4G_LI_v1.pdf,2010.

[3] 3GPP. Technical Specification Group Services and System Aspects; Rationale and Track of Security Decisions in Long Term Evolved(LTE) RAN/3GPP System Architecture Evolution(SAE)(Release 9)[S]. Tech Spec 3GPP TS 33.102 V9.0.0. 2009.

[4] IEEE P802.16m. Part 16:air interface for fixed and mobile broadband wireless access systems[EB/OL].http://lichun.cm.nctu.edu.tw/pa pers/P80216m_D4.pdf,2010.

[5] GIRAULT M. Self-certified public keys[A]. Eurocrypt'91 [C]. Brighton UK,1991.490-497.

[6] HE D K, WANG J,ZHENG Y. User authentication scheme based on self-certified public key for next generation wireless network[A]. IEEE International Symposium on Biometrics and Security Technologies [C]. Islamabad, Pakistan, 2008.

[7] DATTA A. Security Analysis of Network Protocol: Compositional Reasoning and Complexity Theoretic Foundations[D]. Computer Science Department, Stanford University, 2005.8-72.

[8] POUPARD C,STERN J. Security analysis of a practical on the fly authentication and signature generation[A]. Eurocrypt'1998[C]. Espoo Finland, 1998. 422-436.

[9] HE C,SUNDARARAJAN M,DATTA A. A modular correctness proof of IEEE 802.11i and TLS[A]. CCS2005-12th ACM Conference on Computer and Communications Security[C].Alexandria,VA, United States,2005.2-15.

[10] ROY A,DATTA A, DEREK A. Secrecy analysis in protocol composition logic[A]. The 11th Asian Computing Science Conference [C]. Tokyo,Japan,2006.197-213.

[11] DATTA A, ROY A, MITCHELL J. Protocol composition logic (PCL)[J]. Electronic Notes in Theoretical Computer Science, 2007, 172(1): 311-358.

[12] CAS C. On the protocol composition logic PCL[A]. Preceedings of 2008 ACM Symposium on Information, Computer and Communications Security[C].Tokyo, Japan, 2008.18-20.

作者简介：

王丽丽（1986-），女，江西永修人，兰州理工大学硕士生，主要研究方向为网络安全和安全协议。

冯涛（1970-），男，甘肃临洮人，博士，兰州理工大学研究员、博士生导师，主要研究方向为可证明安全协议理论、无线和移动网络安全。

马建峰（1963-），男，陕西西安人，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、移动与无线网络安全。