基于可信计算的移动终端用户认证方案

郑 宇[1] 何大可[1] 何明星[2]

[1](西南交通大学信息安全与国家计算网格实验室 成都 610031)

[2](西华大学数学与计算机学院 成都 610039)

摘 要 针对移动终端(ME)的特性,提出了结合 USIM(Universal Subscriber Identity Module)和 TPM(可信平台模块)的可信移动平台(TMP),并以智能手机主流处理器为基础,讨论了 TMP 的设计案例以及 TPM 在 ME 中的三种构建方法.在提出的 TMP 框架内,利用 RSA-KEM(密钥封装)机制和 Hash 函数,设计了口令、指纹和 USIM 相结合的用户域认证方案,实现了用户和 ME、用户和 USIM 间的相互认证,强化了用户域的安全,并可满足 TMP 标准草案中安全等级 3 对用户认证的要求.该方案在不要求使用者与 ME 预先协商信任关系的前提下,既可区分攻击者和合法用户,又可辨别 ME 的主人和普通使用者,并能在认证过程中及早发现攻击行为,避免不必要的计算花销.定量及定性分析表明,该方案的离线和在线两种工作模式在三种不同的 TPM 架构下的安全性、通用性和执行效率均优于 TMP 标准中引用的方案,且获得了比 Lee 等众方法更高的安全性和通用性.

关键词 可信计算;可信移动平台;移动终端;身份认证;指纹

中图法分类号 TP309

Trusted Computing Based User Authentication for Mobile Equipment

ZHENG Yu[1] HE Da-Ke[1] HE Ming-Xing[2]

[1](*Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu* 610031)

[2](*School of Mathematics and Computer Science, Xihua University, Chengdu* 610039)

Abstract In this paper, according to the features of mobile equipment (ME) an example of constructing trusted mobile platform (TMP) is presented based on the smart phone's processor, along with which three alternative methods to build trusted platform module (TPM) are discussed as well. In the framework of TMP, through combining password and fingerprint with the USIM card via RSA-KEM (Key Encapsulate Mechanism) and Hash function, a user authentication scheme is proposed to improve the security of the user domain, which achieves the mutual identification among user, ME and USIM even if their public-key certificates are issued by different certificate authorities (CAs). Moreover, the user authentication can not only easily distinguish the valid users from the pretenders but also identify the owner of ME from the genuine operators without any pre-negotiation. The performance analysis and experimental test result show that no matter what kinds of TPM is employed authors' authentication scheme is more secure, efficient and flexible than the corresponding scheme presented in TMP draft standard and achieves advanced security and better flexibility as compared to the schemes proposed by Lee, Lin *et al*..

Keywords trusted computing; trusted mobile platform; mobile equipment; identity authentication; fingerprint

---

收稿日期:2006-03-27;**修改稿收到日期**:2006-06-07.**本课题得到国家自然科学基金**(60473030)**和现代通信科技重点实验室基金**(51436050404QT2202)**资助.郑 宇,男,**1979 **年生,博士,主要研究方向为信息安全、密码学与无线网络.**E-mail:zhyu_swjtu@163.com.**何大可,男,**1944 **年生,教授,博士生导师,主要研究领域为密码学、信息安全与并行计算.何明星,男,**1964 **年生,博士,教授,主要研究领域为信息安全与密码学.**

1 引 言

随着无线通信技术与计算机技术的不断融合，移动终端(ME)正逐步取代 PC 成为人机接口的主要设备.但伴随着计算和存储资源的不断丰富，移动操作系统和各种无线应用的问世，ME 也面临着越来越多的安全威胁[1~3].现有的用户域安全保护方案，尤其是用户与 ME 间的身份认证方案已暴露出诸多的安全隐患.传统的基于 PIN 的用户身份认证方案，由于密钥长度短且通常包含用户的个人信息，容易遭到字典攻击和穷搜索攻击.而将单纯基于生物特征(如指纹)的身份认证方法[4]用于智能手机和 PDA 等移动平台也易遭到重放攻击.文献[5,6]等给出的方案是借助智能卡的帮助，基于口令和指纹的双因素进行用户身份认证.但此类方案也仅仅是先比较指纹，然后再利用动态口令的思想接入远端服务器.口令和指纹唯一的联系仅限于利用活体指纹数据来产生一个无关紧要的随机数，并没有将两者紧密结合.而且，以上方案均未考虑以下几个问题：

(1)未检验终端平台本身是否安全可信.若 ME 本身已经被病毒感染，或攻击者已经恶意修改移动平台的操作系统、应用软件或固件，用户输入的口令和指纹很容易被非法窃取，然后存储在 ME 中或利用短信、蓝牙等通道转发给他人.

(2)由于现有平台不支持域隔离机制，用户在认证过程中使用的敏感信息很可能被其它程序读取.

(3)现有的移动终端中的接口未受到保护，例如在 USIM(Universal Subscriber Identity Module)和 ME 间接口上传送的 PIN 码或指纹数据很容易被截获或重放.

(4)以上方案可在不同程度上实现终端或 USIM 对用户身份的鉴别，但用户却无法认证终端和 USIM.用户很可能在不知情的状态下向非法的 USIM 或终端提供自己的口令、PIN 和指纹数据.

(5)由于很多方案都需要在 USIM 和 ME 间传送数据，缺乏 USIM 和 ME 间的相互认证机制将导致合法的 USIM 被恶意的 ME 欺骗，或合法的 ME 被恶意的 USIM 欺骗.

(6)现有的方案均未考虑用户的私隐问题.当利用自己的 USIM 使用他人或公共 ME 时，用户通常不希望由于 ME 记录自己的真实身份而被追踪或造成的隐私外泄.

1999 年 TCPA[7](Trusted Computing Platform Alliance，后改名为 TCG[8])提出了可信计算的思想用以保护计算终端的安全.其主要思路是基于安全硬件和安全操作系统来实现一个可信的平台，并将信任延伸到客户端、服务器、网络和通信平台.TCG 在公布的标准[9]中提出了 OIAP(Object-Independent Authorization Protocol)、OSAP(Object-Specified Authorization Protocol)和 DSAP(Delegate Specific Authorization Protocol)3 个对用户的认证及授权协议，并利用 ADIP(Authentication Data Insert Protocol)、ADCP(Authentication Data Change Protocol)和 AACP(Asymmetric Authentication Change Protocol)协议来新建或修改 TPM 中的认证信息.在这些协议中，移动终端主人(Owner)与可信平台模块(TPM)[9,10]共享一个 20 字节的机密信息 *AuthData*，通过挑战应答的方式来实现相互认证.由于 20 字节的数据难于记忆，*AuthData* 实际上都是通过对用户口令作 Hash 运算后得到的.因此，此类方案虽然实现了用户和 TPM 间的双向认证，但仍未能摆脱基于口令的认证方式的脆弱性.

文献[11]以 OSAP 为例，对 TCG 定义的用户认证协议进行了改进，在可信计算的框架里提出了结合口令和智能卡的双因素用户认证方案，安全性较 TCG 的初始方案有所提高.其核心思想在于，用户向智能卡提供 PIN 码，在卡内计算共享的认证信息 *AuthData*，再利用智能卡与 TPM 进行相互认证.但此方案的薄弱环节仍在于用户与智能卡间的 PIN 码.同时，由于文献[11]和 TCG 定义的认证方式均要求用户和 ME 在认证前先共享认证数据，因此，只适用于主人和自己的 ME 之间的认证，而无法方便地实现 ME 和其它合法用户间的认证.这就意味着持有合法 USIM 的合法用户无法方便地使用其它合法 ME(包括公共的 ME)接入网络.出现此类现象的原因在于最初的 TCG 在设计可信计算的标准时，并未将认证和授权过程严格分开，也没有严格区分不同用户的权限[7,9].

2004 年 10 月，TCG 将可信计算的思想引入硬件资源紧张和电池容量有限的移动终端，提出了可信移动平台(TMP)的软、硬件体系和协议三个技术标准草案[12~14]，用以提供端到端的安全移动计算环境.在 TMP 的标准中已开始将认证和授权分开，并开始考虑用户的具体权限问题.因此，ME 的认证方案也应该可区分终端主人和普通使用者.文献[15]在可信计算框架内提出了基于生物特征的认证方案，并被 TMP 标准[13]引用为认证案例(以下简称 TMP 方案).该方案可解决以上前 5 条缺陷，但仍存在以下不足：

(1) 此方案是在假设 TPM 和 SIM 卡归属于同一 CA 的前提下构建的离线认证方案. 由于 SIM 和 TPM 的数字证书通常由移动网络运营商和移动设备制造商的 CA 分别颁发. 因此，SIM 很难在无可信第三方帮助的前提下直接验证 TPM 的数字签名.

(2) 该方案要求移动平台的各个部件(如 SIM 和 TPM)作大量负载繁重的数字签名和验证运算，严重影响了认证方案的效率，不适合于计算能力和电池容量有限的移动终端.

(3) 该方案的核心思想仍只是对指纹和模板进行了简单的匹配运算，并没有将指纹和口令相结合，仍不能满足可信移动平台安全等级 3 的要求.

同时，现有文献(包括 TMP 的标准)仍停留在设想和理论探讨阶段，并未给出具体构建可信移动平台的方法和实例，更未讨论在 TMP 基础上结合口令和指纹的用户认证方案及其具体工作流程. 鉴于以上原因，本文针对 ME 的特性，以处理器 OMAP730[16] 为硬件平台，给出了 TPM 的三种构建案例，并提出了 USIM 和 TPM 相结合的 TMP 框架. 利用 RSA-KEM[17](RSA 密钥封装)机制和 Hash 函数将口令和指纹紧密融合，并借助无线接入网络(AN)提供在线证书验证功能，本方案在不要求 TPM 和 USIM 的数字证书为同一 CA 颁发的前提下，实现了用户、ME 和 USIM 间的相互认证，获得了高于文献[13,15]的效率以及比文献[5,6,9,11,13,15]更好的安全性和通用性.

2　基于 OMAP730 的可信移动平台

OMAP730[16] 是 TI 公司目前采用的主流智能手机处理器，它集成了 GSM/GPRS 数字基带单芯片处理器，带有 384KB 的 SRAM、128MB 的 SDRAM 和 256MB 的 FLASH. 另外，OMAP 还集成了 48KB 的安全 ROM 和 16KB 的安全 RAM，并配置了硬件的安全算法加速器和随机数产生器. 虽然单纯的 OMAP730 并不满足可信计算的要求，但这些硬件资源为 TMP 的构建提供了良好的基础. 因此，在 OMAP730 之上作以下硬件配置便可满足 TMP 的要求：

(1) 添加 TPM. 按照 TMP 标准[12~14] 和 TPM 标准[9,10]，可用以下三种不同的方式来构建 TPM：① 将 OMAP730 内部已配置的硬件安全算法模块、随机数产生器和安全 RAM 等资源进行封装整合，以构建内置 TPM；② 选择独立的外置 TPM 芯片(如本文在后面选择的 AT97SC3203S[18,19])，并通过总线 SMBus[20] 与 OMAP730 相连；③ 为节约硬件成本，借助 OMAP730 内部 ARM9 和存储器，以纯软件方式(但仍需要配置内置安全 RAM 和 ROM)来实现 TPM 应具备的功能.

(2) 将 CRTM(Core Root for Trusted Measurement)[12] 固化于安全 ROM 中，以配合 TPM 完成可信启动. TPM 可通过 DMA 方式读取 ROM 中的 CRTM 代码.

(3) 利用高速 UART 接口外接生物特征读取设备 BR(Biometric Reader). 此处选用较为通用的指纹采集仪，以弥补单纯口令认证方式的脆弱性，从而满足 TMP 安全等级 3 对认证方式的要求.

(4) 在外围添加 TMI(可信模式指示器)用以指示平台当前状态是否可信. TMI 可为简单的 LED.

图 1 描述了以 OMAP730 为基础构建的 TMP

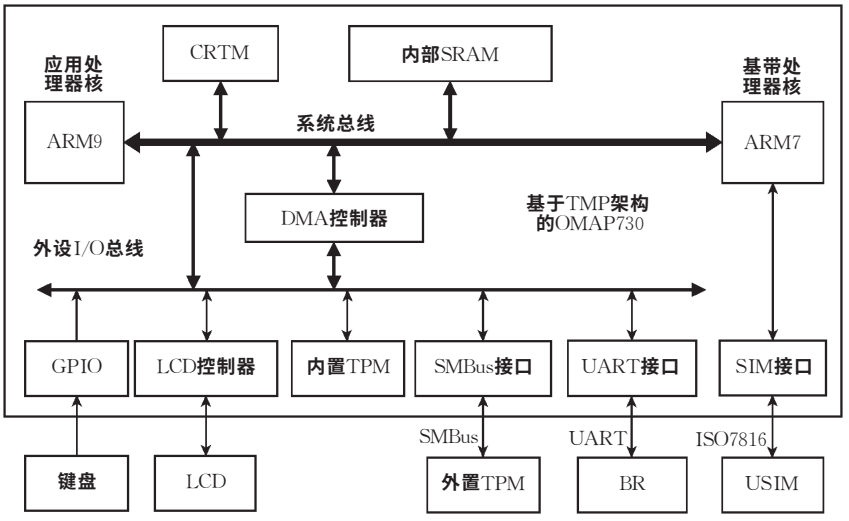

图 1　基于 OMAP730 的 TMP 抽象模型

抽象框架,图中的部件组成了本案例中 TMP 的安全边界,所有认证过程均在该边界内完成,以确保认证方案的安全性. LCD 控制器、TPM 和 UART 接口共享同一个 DMA 控制器,但使用不同的 DMA 通道分时占用系统总线. TPM 即可利用 DMA 接口直接访问 SRAM,也可通过局部 I/O 总线与 BR 传送数据. BR 通过 UART 接口与加固后的 OMAP730 相连. 而 USIM 则通过 SIM 口连接到 OMAP730 内部的基带处理器内核 ARM7 上,并利用 ISO7816 标准协议与 SIM 口通信.

3 基于口令、指纹和 USIM 的用户域认证方案

如图 2 所示,与现有的单纯口令或指纹的用户域认证方案相比,本方案的总体工作流程具有以下特点:

(1) 当需要使用移动终端时,用户首先插入 USIM 卡验证平台的合法性. 只有在确认平台当前状态可信之后,用户才通过键盘输入口令,并利用 BR 提供自己的指纹,以防止用户的敏感信息被恶意终端窃取.

(2) 不是分别将口令或指纹与模板进行简单地比较,而是利用 RSA-KEM 体制和 Hash 算法将指纹和口令相融合,并在 TMP 的可信边界内完成计算过程,可满足 TMP 中安全等级 3 的要求.

(3) 可分别实现用户、ME 和 USIM 之间的认证.

(4) 利用 TID_{User}(用户的临时身份)和 K_{AU}(与网络的共享密钥),USIM 可借助无线网络来在线校验 TPM 证书和签名的合法性,以实现不同 CA 域中 TPM 和 USIM 的认证.

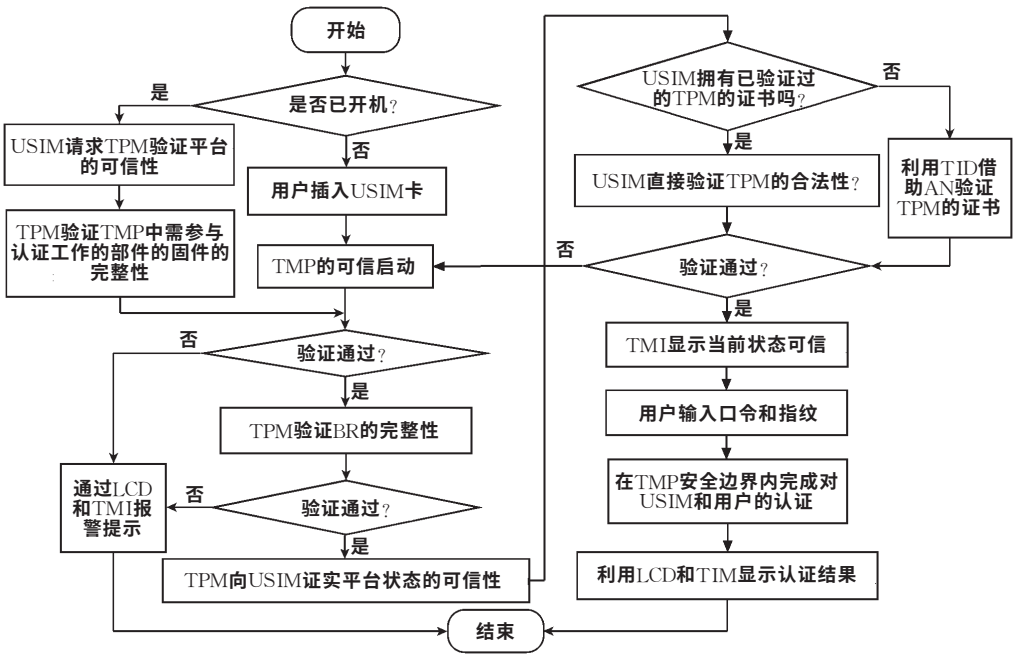

图 2 基于可信移动平台的口令、指纹和 USIM 相结合的认证流程

在本方案中,用户记住自己的口令,并持有无线网络运营商颁发的 USIM 卡. 该 USIM 卡除完成基本的密码运算以外,还负责存储用户的数字证书和敏感信息,如认证参数、指纹模板 F_{U} 和匹配软件 CS 等. 其中认证参数包括用户接入无线网络时需要的参数以及用户与终端进行认证的参数 (x,y,z). (x,y,z) 的具体计算方法如式(1)~(4). 其中,PW 为用户口令,SK_{HE} 和 n 分别表示用户归属环境(HE)的签字私钥和模数,$H(x)$ 表示计算 x 的 Hash 值. TPM 中存储着自己的私钥 SK_{TPM}、证书 $Cert_{\mathrm{TPM}}$、与 BR 共享的密钥 K_{BT}、其它模块的完整性向量值以及移动终端主人的 x(在以下的描述中分别用 x_{O} 和 x_{U} 来区分主人和使用者的 x). ME 的 HE 在自己的数据库中存储 S. 用户域认证完成后,USIM 在接入无线网络的认证协议中包含 S,以作为自己在场并参与了无线应用的凭证.

$$x=H(F_{\mathrm{U}}\parallel PW) \tag{1}$$

$$y=x\oplus H(PW) \tag{2}$$

$$z=S\oplus H(F_{\mathrm{U}}\oplus PW) \tag{3}$$

$$S=H(ID_{\mathrm{User}}\parallel PW\parallel F_{\mathrm{U}})^{SK_{\mathrm{HE}}} \bmod n \tag{4}$$

结合图 1 的硬件框架,图 3 将 ME 和 TPM 视为一个整体,从较高的层次描述了认证协议的流程.

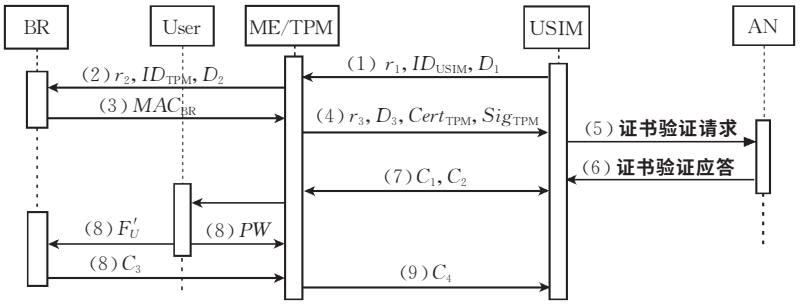

图 3　用户域认证协议的流程

1. USIM→ME/TPM: r_1, ID_{USIM}, D_1.

USIM 利用 UART 接口向 ME/TPM 发送随机数 r_1、身份标识 ID_{USIM} 和平台验证请求 D_1.

2. ME/TPM→BR: r_2, ID_{TPM}, D_2.

ME/TPM 通过外设 I/O 总线向 BR 发送随机数 r_2、TPM 的身份标识 ID_{TPM} 和 BR 验证请求 D_2.

3. BR→ME/TPM: MAC_{BR}.

$$K_C = E(K_{BT}, r_2) \tag{5}$$

$$MAC_{BR} = MAC(K_C, ID_{TPM} \| H_{BR}) \tag{6}$$

BR 收到完整性校验请求 D_2 后，计算自身关键代码的 Hash 值 H_{BR}，然后利用式(5)计算 K_C，并按照式(6)计算认证码. 随后 BR 通过 I/O 总线将 MAC_{BR} 传送给 TPM. 其中 $E(k,x)$ 和 $MAC(k,x)$ 分别表示以 k 为密钥对 x 加密和计算认证码. 而 ‖ 为级连符号.

4. ME/TPM→USIM: r_3, D_3, $Cert_{TPM}$, Sig_{TPM}.

$$Sig_{TPM} = Sig(SK_{TPM}, r_1 \| r_3 \| ID_{USIM} \| PCR) \tag{7}$$

利用自己发送的 r_2、预先存储在其内部的 BR 的代码 Hash 值和共享密钥 K_{BT}，TPM 同样按照式(5)和式(6)计算 MAC'_{BR}，并与收到的 MAC_{BR} 进行比较. 如不相同，ME/TPM 终止认证过程，并通过 LCD 和 TMI 提示用户. 否则，表明 BR 的固件完整，用户可以使用. 随后，TPM 用自己的私钥 SK_{TPM} 对产生的随机数 r_3、操作事务记录 D_3 和 PCR 值按照式(7)进行签名，并通过 SIM 接口传送给 USIM，必要时消息中应包含 TPM 的证书 $Cert_{TPM}$.

5. 如拥有已验证过的 $Cert_{TPM}$，则 USIM 直接校验 Sig_{TPM} 的合法性(以下将其称为离线工作模式). 若验证通过，则跳至步 7；否则，表明当前状态不可信，USIM 触发可信启动过程重新启动 ME.

如 USIM 没有已验证过的 $Cert_{TPM}$，则利用 TID_{User} 和 K_{AU} 来借助 AN 验证 $Cert_{TPM}$ 及平台状态的合法性(以下将其称为在线认证模式). 其中，IDC_{TPM} 和 NAI 分别表示 TPM 的证书标识以及为用户分配临时身份的网络域标识.

USIM→AN: r_1, r_3, TS, IDC_{TPM}, NAI, TID_{User}, D_3, Sig_{TPM}, MAC_{User}.

$$MAC_{User} = MAC(K_{AU}, IDC_{TPM} \| r_1 \| r_3 \| D_3 \| TS) \tag{8}$$

6. AN→USIM: D_5, MAC_{AN}.

$$MAC_{AN} = MAC(K_{AU}, r_3 \| ID_{User} \| ID_{TPM} \| D_5) \tag{9}$$

AN 根据 TID_{User} 和 NAI 恢复出 ID_{User} 和 K_{AU}，然后按照式(8)检验 MAC_{User} 的合法性. 如验证通过，AN 利用 IDC_{TPM} 从 PKI 获取合法的 $Cert_{TPM}$，并检验 Sig_{TPM}. 随后，AN 利用 K_{AU} 按照式(9)计算认证码. 其中，D_5 包含 $Cert_{TPM}$ 和 Sig_{TPM} 的合法性验证结果.

7. USIM→ME/TPM: C_1, C_2.

$$C_1 = E(PK_{TPM}, r_4 \| y \| ID_{USIM}) \tag{10}$$

$$K_{ST} = KDF(r_4 \oplus r_3, x, ID_{TPM}) \tag{11}$$

$$C_2 = E(K_{ST}, r_4 \| F_U \| ID_{TPM} \| CS) \tag{12}$$

如 USIM 验证消息 6 中收到的 MAC_{AN} 不合法，或 D_5 表明 ME 当前状态不可信，则触发可信启动过程，并通过 LCD 和 TMI 向用户报警；否则，如图 4 所示，USIM 产生随机数 r_4，并利用 TPM 的公钥 PK_{TPM} 以及隐含口令信息的 x 和 y，结合 RSA-KEM 机制，按式(10)～(12)分别计算 C_1 和 C_2，并通过 SIM 口将 (C_1, C_2) 传送给 TPM/ME. 其中，KDF 为密钥生成函数，产生的对称密钥 K_{ST} 用于保护指纹数据，必要时可将指纹匹配算法 CS 一并包含在 C_2 中，以进一步增加方案的通用性.

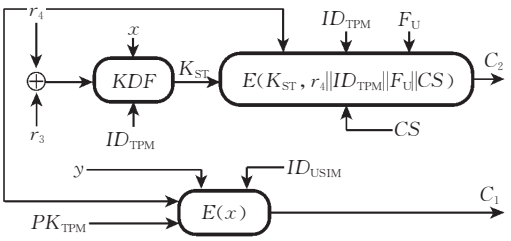

图 4　USIM 中完成的数据封装过程

8. BR→ME/TPM: C_3.

$$C_3 = E(K_C, ID_{BR} \| ID_{TPM} \| r_2 \| F'_U) \tag{13}$$

在 TMI 提示移动平台当前状态可信后，用户通过键盘和 BR 分别输入口令 PW 和指纹 F'_U. BR 按照式(13)对采集的 F'_U 加密并将计算的 C_3 发送至 ME/TPM. ME/TPM 根据图 5 中描述的算法来验证用户和 USIM 的合法性. 图 5 中包含的 6 个比较过程(Comp-x)应按标识顺序执行，以便及早发现错误，从而避免不必要的计算量. TPM 首先利用自己的私钥 SK_{TPM} 解密 C_1，计算用户输入口令的 Hash 值，并以此从 y 中恢复出 x_U. 若在 Comp-2 过程中，x_U 与 TPM 内部存储的 x_O 一致，则初步表明示证者为 ME 的主人(对主人的强认证还需等待指纹认证结果). 如不一致，但接下来的 4 个匹配运算(包含指纹匹配算法)均顺利完成，则证明示证者为普通使用者. 若 6 个匹配过程均通过，用户也可根据此结果来

证实自己持有的 USIM 是合法的，从而实现了对 USIM 卡的隐性认证. 由此可见，本算法即可实现终端主人和 ME 间的认证，也可方便地满足合法用户使用合法终端时的认证需求.

9. TPM→USIM: C_4.

$$w=H(F_U\oplus PW) \tag{14}$$

$$C_4=E(K_{ST}, ID_{USIM}\parallel r_4\parallel w\parallel D_6) \tag{15}$$

随后，ME/TPM 按照式(14)和式(15)计算 C_4 并返还给 USIM. 其中 D_6 为 ME/TPM 对用户的认证结果. 若 r_4 与消息 7 中发送的随机数一致且 D_6 表明用户身份合法，USIM 从 C_4 中还原出 w，并计算 $S=z\oplus w$. 由于恢复 S 必须拥有 w 和 z，而 w 的计算参数分别是用户的口令和指纹模板，因此，一旦 USIM 还原出 S，则表明持有 USIM 的合法用户必定在场且顺利完成了用户域认证. USIM 在以后与无线网络交互的认证协议中包含 S，便可作为用户在场并参与无线业务的凭证.

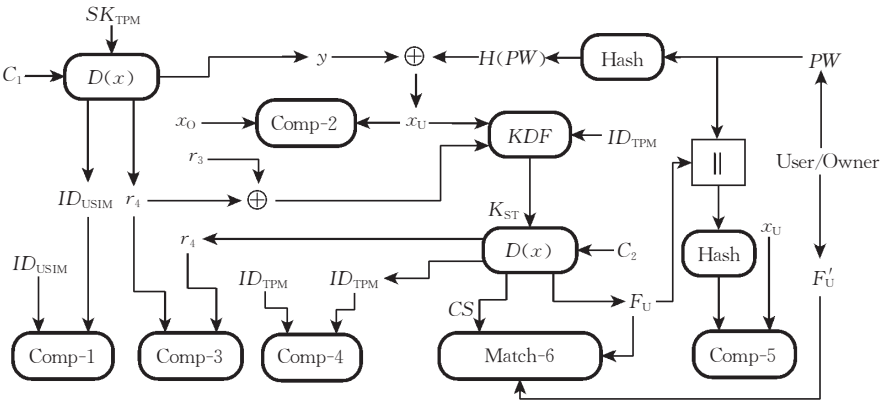

图 5 ME/TPM 中的数据验证算法

4 性能分析

4.1 安全性分析

表 1 给出了本文提出的认证方案与文献[5,6]、TCG 标准授权方案[9]、TCG 改进方案[11]和 TMP 标准草案[13]中引用的方案在安全特性方面的详细比较. 表中√、×和－分别表示方案具备、不具备和不涉及某个安全特性. 从比较结果中可发现，本方案在可信移动平台的框架下，实现了用户、USIM 和 ME 间的双向认证，确保了用户口令和指纹数据在认证过程中的安全性，强化了用户对 ME 或 USIM 中数据的访问控制，并减少了 ME 或 USIM 丢失后造成的危害. 同时，利用在线认证方式，本方案既可实现 ME 和其所有者之间的认证，也可让合法用户利用自己的 USIM，按照规定权限使用其它合法 ME(如此时只允许用户访问其 USIM 卡中的内容及使用基本通话功能)，并可方便地实现不同 CA 下的用户和 ME 之间的认证. 因此，本方案在效率高于文献[13,15]的前提下，获得了比文献[5,6,9,11,13,15]更高的安全性和通用性.

表 1 本文提出的方案和其它方案的性能比较

安全特性	文献[5,6]方案	TCG 标准	TCG 改进方案	TMP 方案	本文的方案
采用的密码机制	指纹,口令	基于口令的单钥	口令和单钥	公钥,指纹	口令,指纹,RSA-KEM
需(U)SIM 或智能卡	√	×	√	√	√
多因素认证	三因素	单因素	双因素	双因素	三因素
USIM 鉴别用户	√	×	√	√	√
用户鉴别 USIM	×	－	×	×	√
用户鉴别 ME	×	×	×	√	√
ME 鉴别用户	×	√	√	√	√
ME 鉴别 USIM	×	－	√	√	√
USIM 鉴别 ME	×	－	√	√	√
口令/指纹紧密结合	×	×	×	×	√
口令/指纹的机密性	×	×	×	√	√
口令/指纹的完整性	×	×	×	√	√
对 ME 状态的验证	×	×	×	√	√
UISM-ME 接口保护	×	√	√	√	√
ME-BR 接口保护	×	－	－	√	√
抵抗重放攻击	×	√	√	√	√
减少 USIM 丢失危害	√	－	√	√	√

（续　表）

安全特性	文献[5,6]方案	TCG 标准	TCG 改进方案	TMP 方案	本文的方案
减少 ME 丢失的危害	−	√	√	×	√
户身份的私隐性	×	×	×	×	√
通用性	中	差	较差	中	好
安全级别	较高	低	中	较高	高
执行效率	中	高	较高	低	中

在本文提出的用户域认证方案中，用户需要插入相应的 USIM 卡，提供正确的口令以及合法的指纹才可以使用 ME，属于三因素认证. 从式(1)～(4)以及式(10)～(12)可以看出，基于 RSA-KEM(在 OW-CPA 模型中，其安全性可归结为 RSA 问题的困难性[17])和 Hash 函数的安全性，只有合法的 TPM 才可用自己的私钥从 C_1 中恢复出 y 和 r_4，且只有在用户输入了正确的 PW 后，TPM 才可从 y 中还原出 x，进而以(x，r_4，r_3)为种子来计算 C_2 的解密密钥 K_{ST}，从而还原指纹模板 F_U. 因此，本方案借助 USIM、TPM、RSA-KEM 和 Hash 函数的安全特性，弥补了单纯口令或指纹认证方案的脆弱性. 由于 TPM 和 USIM 不直接存储用户原始口令，且指纹和口令信息在各个接口与相应实体生成的随机数一起加密传送，指纹和口令自身的机密性、新鲜性和完整性得到了保证，自身安全性在存储、通信和计算过程中都大大提高.

另一方面，本方案可实现用户、USIM 和 ME/TPM 彼此间的相互认证，不但可识别合法使用者和攻击者，还可区分 ME 的主人和普通使用者的不同权限. 其中，USIM 利用消息 4 中包含的 Sig_{TPM} 可检验 TPM 的身份及 ME 当前状态的合法性(当用户与 ME/TPM 的证书为不同 CA 颁发时，USIM 可借助 AN 来验证 Sig_{TPM} 的合法性). 在图 5 中描述的 Comp-2 过程中，如 $x_U=x_O$ 且其它匹配算法均顺利通过，则 TPM/ME 相信示证者就是 ME 的主人. 若 Comp-2 不成立，但其它匹配算法均成立，则示证者为普通合法使用者. 基于 RSA-KEM 的安全性，只有同时具备正确的 PW 和指纹模板，TPM 才可以根据式(11)和式(14)计算出 K_{ST} 和 w. 若在消息 8 中包含的 r_4 和 ID_{USIM} 均正确，USIM 可确认 TPM/ME 为合法，且确信此次认证过程必定有合法用户的参与，从而也实现了对用户身份的认证. 由于只有合法的 USIM 才可以提供用户的 y 和指纹模板，在通过了图 5 中描述的 2，5，6 项匹配算法后，借助用户输入的口令和指纹，TPM/ME 可鉴别该 USIM 为合法用户所有. 当 USIM 和 ME/TPM 均成功完成图 5 的验证算法后，用户可根据 LCD 和 TMI 的提示来隐性地确认 ME/TPM 及 USIM 的合法性.

4.2　效率分析

根据表 1 的分析结果，本文将安全特性较为相近的 TMP 方案[13]与本方案的两种工作模式进行了详细的效率比较. 表 2 分析了认证协议在 TPM、USIM、ARM 和 BR 中完成的密码运算量. 从比较结果可看出，由于利用运算速度快的 Hash 函数和认证码算法替代了 TMP 标准方案中的数字签名和验证算法以及以单钥和公钥相结合的体制替代了纯公钥加、解密过程，本方案大大提高了 ME 的认证效率.

表 2　用户域认证方案的密码计算量比较

协议	公钥加密	公钥解密	对称加、解密	签名	验签	KDF	认证码	Hash 函数
本方案在线认证模式	1	1	8	1	0	2	4	4
本方案离线认证模式	1	1	8	1	1	2	2	5
TMP 标准中的方案	2	2	4	5	5	0	0	0

为定量分析本文提出协议的性能，现以 OMAP730 为基础，构建图 6 所示的两种系统硬件仿真平台. 其中，TPM 的构建方式可分为内置 TPM(如图 6(a))和外置 TPM(图 6(b))两种，而内置 TPM 又包括软件 TPM(由应用处理器 ARM9 来分担密码运算任务)和硬件 TPM(利用 OMAP 内部硬件密码模块来完成密码算法). AT97SC3203S[18,19]是工作时钟为 33MHz 的 TPM 独立芯片，满足 TCG1.2 标准，可通过最高速率为 100Kbps 的 SMBus[20]与 OMAP730 相连. SLE66CX 是工作时钟频率为 3.57MHz 的 16 位智能卡模块[21](符合 SIM 标准)，采用速率为 78600bps 的 ISO7816 协议与 OMPA730 通信. 指纹采集传感器 OPP02MM1[22]与 89C52 单片机(时钟频率为 25MHz)一起完成对指纹数据的采集和预处理过程，并通过速率为 115200bps 的 UART 口与 OMAP730 相连. 由于尚不具备改造 AN 体系和协议的能力，本实验平台选用 PC 机(配置 2.4GHz 赛扬-D CPU、512MB 内存、Window XP 操作系统和 Cryptlib 3.2 密码算法包)来模拟 AN 的功能，并利用串口以 9600bps 的速率与 OMAP 交互数据，从而模拟 USIM 与 AN 在随机接入信道(RACH)上的通信环境.

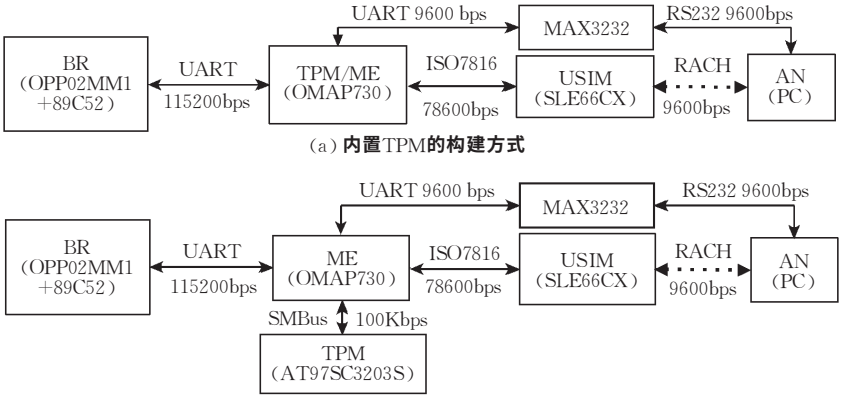

图 6 采用内置和外置 TPM 模型的 TMP 硬件仿真环境

为保障执行效率的可比性,选用文献[23～28]设计的算法实现方式以及文献[18,19,21,22]提供的参数,并采用以下具体算法:公钥加密、解密、签名和验证算法均选取模指数长度为 1024bits 的 RSA 算法;BR 与 TPM/ME 间信道上的对称加密及认证码算法分别采用 128bits AES 及 AES-CBC-MAC;而 TPM/ME 与 USIM 以及 USIM 与 AN 间信道上的数据对称加密及认证码算法分别采用 128bits 密钥的 3DES 及 3DES-CBC-MAC. 同时,协议以 SHA-1(160bits 输出)作为 Hash 算法和 KDF 算法,且所有随机数长度均为 128bits. 协议中使用的永久标识(如 ID_{TPM}、ID_{USIM}、和 ID_{User})和时间戳 TS 长度均为 64bits,NAI 和 TID_{User} 为 32bits,如无特殊申明证书长度按 300B 计算. 选用文献[23,24]设计的指纹提取和匹配算法,经 BR 预处理后的加密指纹数据大小为 400B,指纹模板 F_{U} 大小为 256B.

图 7～图 10 在三种不同的 TPM 架构下,分别在通信数据量、通信时间、在线计算时间和协议执行总时间四个方面,将本方案的两种工作方式和 TMP 标准中引用的方案进行了详尽的对比(协议执行时间不包括可信启动过程). 对比结果说明,无论在哪种 TPM 架构下,本文提出的离线认证方案在以上四个方面均优于 TMP 标准中采用的方案. 虽然本方案的在线认证模式在传输数据量和通信时间上略多于 TMP 方案,但其在线计算时间均小于 TMP 方案,因此,协议执行总时间仍优于 TMP 方案.

此外根据图 7～图 10 的结果,表 3 比较了三种不同方式 TPM 架构的特性. 其中,内置硬件 TPM 的算法执行速度最快,通信时间最少,且与应用处理器的接口隐蔽在芯片内部,因此,效率和安全性均最高. 利用 ARM9 以软件方式来实现 TPM 的功能(但仍需要在内部配置安全 RAM 和 ROM),同样可以节约大量的通信时间和硬件开销,但必须以加大时钟频率为代价才可达到硬件 TPM 的运算速度,所以,功耗较大. 鉴于外置 TPM 必须考虑对其与 ARM 的通信接口予以保护,其安全威胁要大于前两种架构. 但由于 TPM 和应用处理器相互独立,不同的平台可与不同的独立 TPM 相连,因此,该架构的灵活性较好.

表 3 三种 TPM 架构的性能比较

	算法速度	安全性	功耗	成本	灵活性
内置硬件 TPM	快	高	小	中	低
内置软件 TPM	慢	中	大	低	中
分离式 TPM	中	低	中	高	高

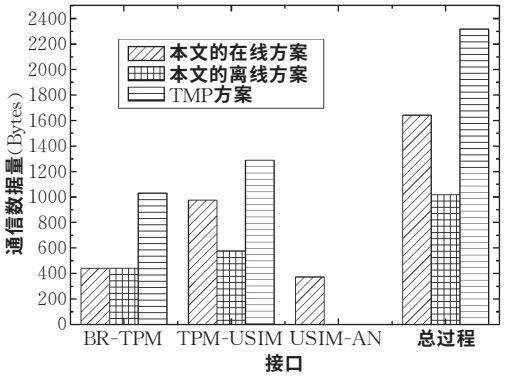

图 7 协议的数据传输量

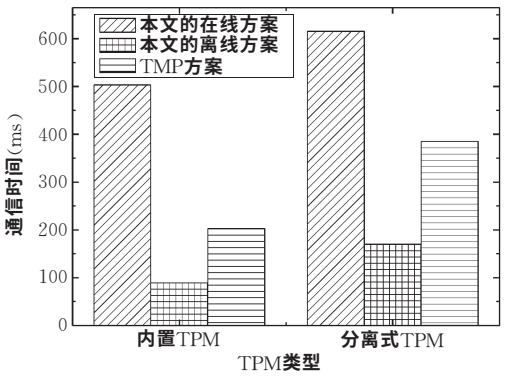

图 8 不同 TPM 模式下协议的通信时间

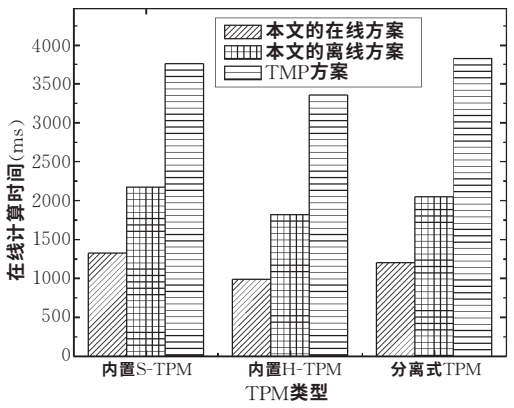

图 9　协议在不同 TPM 模式下的在线计算时间

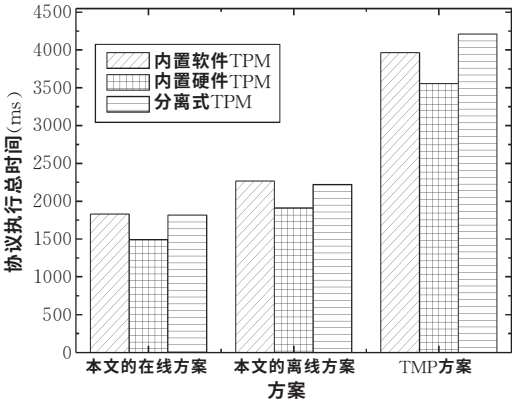

图 10　协议执行的总时间

5　结　论

本文在 OMAP730 基础上分别给出了基于内置(包括硬件和软件方式)TPM 和外置独立 TPM 架构的三种可信移动平台的构建案例. 本方案结合 USIM 和 TPM 的安全特性,并利用 RSA-KEM 机制将口令和指纹紧密融合,实现了用户、USIM 和 ME/TPM 间的相互认证,确保了用户口令和指纹数据在认证过程中的安全性,减少了 ME 或 USIM 丢失后造成的危害,强化了用户域安全,并可满足 TMP 中安全等级 3 对用户认证的要求. 同时,利用在线认证方式,本方案既可实现 ME 和其所有者之间的认证,也可让合法用户利用自己的 USIM,按照规定权限使用其它合法 ME,并可方便地实现不同 CA 下的用户和 ME 之间认证. 根据详细的性能分析,与现有方案相比,本方案的两种工作模式在三种不同的 TPM 架构下,其安全性、效率和通用性均优于 TMP 标准[9](和文献[15])方案,并获得了比文献[5,6,9,11,13,15]更高的安全性和通用性. 而在 3 种 TPM 实现方式中,基于内置硬件 TPM 的方案以牺牲通用性为代价,获得了最高的运算速度、最少的通信时间和最高的安全性.

参　考　文　献

1　Ghosh A. K., Swaminatha T. M.. Software security and privacy risks in mobile e-commerce. Communications of the ACM, 2001, 44(2): 51～57

2　Olivier B., Nora D., Laurent G.. Mobile Terminal Security [EB/OL], 2005. 2. http://eprint. iacr. org/2004/158. pdf

3　Guo Chuan-Xiong, Wan H. J., Zhu Wen-Wu. Smart phone attacks and defenses. In: Proceedings of the 3rd Workshop on Hot Topic in Networks, San Diego, CA, USA, 2005, 94～100

4　Jain A. K., Lin Hong, Pankanti S. B.. An identity-authentication system using fingerprints. Proceedings of the IEEE, 1997, 85(9): 1365～1388

5　Lee J. K., Ryu S. R., Yoo K. Y.. Fingerprint-based remote user authentication scheme using smart cards. Electronics Letters, 2002, 38(12): 554～555

6　Lin C. H., Lai Y. Y.. A flexible biometrics remote user authentication scheme. Computer Standards & Interfaces, 2004, 27(1): 19～23

7　Trusted Computing Platform Alliance(TCPA). Main Specification Version 1. 1b

8　TCG. Trusted Computing Group[EB/OL], 2004-12. http://www. trustedcomputinggroup. org

9　Trusted Computing Group. TPM Main Specifications—Part 1 Design Principles, Version 1. 2, October 2003

10　TPM Main Part 2: TPM Structures. http://www. trustedcomputinggroup. org/downloads/tpmwgmainrev62_Part2_TPM_Structures

11　George P.. User authentication with smart cards in trusted computing architecture. In: Proceedings of the International Conference on Security and Management, Las Vegas, Nevada, USA, 2004, 25～31

12　Trusted Mobile Platform Hardware Architecture Description. http://www. trusted-mobile. org/TMP_HWAD_rev1_00. pdf

13　Trusted Mobile Platform Software Architecture Description. http://www. trusted-mobile. org/TMP_SWAD_rev1_00. pdf

14　Trusted Mobile Platform Protocol Specification Document. http://www. trusted-mobile. org/TMP_Protocol_rev1_00. pdf

15　Balacheff B., Chan D., Chen L.. Securing smart card intelligent adjuncts using trusted computing platform technology. In: Proceedings of the International Conference on IEIF Fourth Smart Card Research and Advanced Application, Bristol, UK, 2000, 177～195

16　OMAP730. http://focus. ti. com/general/docs/wtbu/wtbuproductcontent. tsp ?templateId = 6123&navigationId = 12003&contentId=4676

17　Feng Den-Guo, Lin Dong-Dai, Wu Wen-Lin. New European Engineering for Information Security Scheme. Beijing: Science Press, 2003, 168～190(in Chinese)
(冯登国,林东岱,吴文玲. 欧洲信息安全算法工程. 北京:科学出版社, 2003, 168～190)

18　Trusted Platform Module AT97SC3203 Advance Information [EB/OL], 2005. 12. http://www. atmel. com/dyn/resources/

prod_documents/5116s. pdf
19 Trusted Platform Module AT97SC3203S for SMBus Protocol Summary[EB/OL]. http://www. atmel. com/dyn/resources/prod_documents/5132s. pdf
20 System Management Bus Specification [EB/OL]. http://www. smbus. org/specs/smb10. pdf
21 [EB/OL]. http://www. infineon. com/
22 NITGEN FIM10 Datasheet [EB/OL]. http://classes. engr. oregonstate. edu/eecs/fall2004/ece441/groups/g13/fim10 _DataSheetv1. 0. pdf
23 Chen Ching-Han, Dai Jia-Hong. An embedded fingerprint authentication system with reduced hardware resources requirement. In: Proceedings of the International Symposium on Consumer Electronics. Hong Kong, China, 2005, 145～150
24 Gupta P., Ravi S., Raghunathan A., Jha N. K.. Efficient fingerprint-based user authentication for embedded systems. In: Proceedings of International Conference on Design Automation, San Diego, USA, 2005, 244～247
25 Bertoni G. J., Guajardo, Paar C.. Architecture for advanced cryptographic system. In: Proceedings of the International Conference on Policies and Actions in Modern Integrated Systems, in Information Security, Hershey(PA), USA, 2004
26 McIvor C., McLoone M., McCanny J., Daly A.. Fast Montgomery modular multiplication and RSA cryptographic processor architectures. In: Proceedings of the Asilomar Conference on Signals, Systems, and Computers, Monterey, USA, 2003, 379～384
27 Gupta V., Gupta S., Chang S.. Performance analysis of elliptic curve cryptography for SSL. In: Proceedings of the ACM Workshop on Wireless Security, Atlanta, USA, 2002, 87～94
28 Thull D., Sannino R.. Performance considerations for an embedded implementation of OMA DRM 2. In: Proceedings of the Europe Conference on Design, Automation and Test in and Exhibition, Agrate Brianza, Italy, 2005, 46～51

ZHENG Yu, born in 1979, Ph. D.. His research interests include information security, cryptography and wireless network.

HE Da-Ke, born in 1944, professor, Ph. D. supervisor. His current research interests include information security, cryptography and parallel computing.

HE Ming-Xing, born in 1964, professor. His current research interests include information security and cryptography.

Background

This work is partially supported by the National Natural Science Foundation of China under grant No. 60473030 and the Foundation of National Laboratory for Modern Communications of China under grant No. 51436050404QT2202.

With the advanced functionalities and interoperation with the Internet, mobile equipments(ME) are becoming ever more powerful to create numerous service and application for the users but have to face more and more security threats simultaneously. It is essential to enhance the security of user domain especially the authentication scheme for ME. The traditional password based or simple fingerprint based user authentication for the mobile equipment are suffering from many attacks thus unable to satisfy the developing security requirements. TCG proposed the concept of trusted computing to provide end-to-end security from the viewpoint of terminal and presented authorization scheme to authorize the owner of TPM object. Meanwhile TCG developed the draft specifications of Trusted Mobile Platform(TMP) to prove trusted computing for mobile user. However, the introduced user authentication scheme in the TMP draft specification brings heavy computation to the ME and can not be performed between the TPM and the user when they belong to different certificate authority(CA).

In this paper, on one hand, how to build a TMP according to the features of ME is discussed and three alternative methods of constructing a TPM for ME are presented to satisfy the requirements of different applications. On the other hand, a TMP-based user authentication scheme, which associates password and fingerprint with USIM card closely via RSA-KEM and Hash algorithm, is proposed to perform the mutual authentication among USIM, ME and user even if their public-key certificates are issued by different CAs. Authors' user authentication can not only conveniently distinguish valid users form the pretenders but also identify owner from genuine operators without any pre-negotiation. Thus it enhances the security, flexibility and universality of the current schemes including TCG's authorization and TMP's authentication sample etc. Furthermore, it offers better security and better efficiency simultaneously over TPM's authentication scheme.

The authors also proposed the TMP base security architecture, TMP based Authentication and Key Agreement (AKA) protocol and the TMP based Digital Right Management(DRM) scheme for the future mobile network. They have published more than ten papers in the international and internal conference and journals.