doi:10.3969/j.issn.1000-436x.2012.12.014

可证明安全的智能移动终端私钥保护方案

马骏[1,2]，马建峰[1]，郭渊博[2]

（1. 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；
2. 解放军信息工程大学 电子技术学院，河南 郑州 450004）

摘 要：提出一种可证明安全的智能移动终端私钥保护方案。充分利用口令保护、密钥分割与服务器动态交互获取部分私钥等技术保证用户私钥安全。与其他方案相比，该方案的优势在于：减少了智能移动终端的计算量和存储量，简化了交互过程参数的设置；将时间同步贯穿整个方案的设计过程，防止重放攻击的同时，更提供了便捷高效的用户私钥失效方案。方案达到了安全私钥获取和高效私钥失效的效果，符合智能移动终端的安全应用需求，在随机预言机模型下是可证明安全的。

关键词：私钥保护；可证明安全；随机预言机模型

中图分类号：TP393 **文献标识码：**B **文章编号：**1000-436X(2012)12-0108-08

Provably secure private key protection scheme for smart mobile terminal

MA Jun[1, 2], MA Jian-feng[1], GUO Yuan-bo[2]

(1. Key Laboratory of Computer Networks and Informatio urity (Ministry of Education), Xidian University, Xi'an 710071, China;
2. Institute of Electronic Technique, PLA Information Engineering University, Zhengzhou 450004, China)

Abstract: A provable security scheme for private key protection of smart mobile terminal (SMT) was presented. In the scheme a improved security mechanism is incorporated, which includes password protection, key division and partial key retrieval from server of strong computing capability in order to protect private key security. Compared with previous proposals, the scheme has the following advantages. It reduces computation amount and storage of SMT, and simplifies parameter setting for interaction processes. It takes time synchronization between SMT and server into account. The latter characteristic not only provides better protection of scheme from replay attacks, but also offers a highly efficient mechanism of user private key disabling, and avoiding complex operation of user and extra storage of other device. The investigation has indicated that improved private key protection to SMT can be well achieved with this scheme. The scheme has also been proved to provide satisfactory security in the random oracle model.

Key words: private key protection; provable security; random oracle model

1 引言

随着 3G、WLAN、传感器等无线网络的普及，使用智能移动终端（SMT, smart mobile terminal，包括智能手机、PDA、MID、上网本等）处理个人业务（包括网络通信、电子支付、网上银行、网络监

收稿日期：2011-09-30；**修回日期：**2012-02-17
基金项目：长江学者和创新团队发展计划基金资助项目(IRT1078)；国家自然基金委员会——广东联合基金重点基金资助项目(U1135002)；国家科技部重大专项基金资助项目(2011ZX03005-002)；河南省科技创新杰出青年计划基金资助项目（104100510025）
Foundation Items: The Program for Changjiang Scholars and Innovative Research Team in University(IRT1078); The Key Program of NSFC-Guangdong Union Foundation (U1135002); The Major National S&T Program (2011ZX03005-002); The Scientific Innovation Talents Foundation of Henan Province (104100510025)

控等）逐渐成为用户访问网络的重要手段。然而，由于此类设备具有体积小、计算能力有限、持续工作能力低等特点，设备不仅容易丢失，而且不能够处理复杂的密码运算。一旦设备丢失或失窃，敌手以离线方式获取用户的私密信息，尤其是获取用户用于签名或加密的私钥后，便可冒充合法用户身份对网络展开僵尸网络、DDos 等攻击，危害网络业务的正常运行。此外，由于设备密码运算能力较弱，即使设备正常使用中，也存在被敌手展开在线攻击，从而获得用户有效私钥的风险。

针对用户的私钥保护，通常有以下三类解决方案。

方案 1　通过独立硬件模块实现私钥的存储。文献[1]通过一个 IR 传输器（IR transmitter）监控移动设备防止被窃，即使设备被窃取后，由于无法执行相应的私钥取回协议也无法查看敏感信息。文献[2]利用 TPM 硬件模块[3]来存储用户私钥，保证敌手无法直接从终端的存储设备中获取用户私钥。

方案 2　利用虚拟机技术的隔离特性实现私钥的存储。文献[4，5]利用虚拟机技术的隔离特性，将用户私钥存储虚拟的处理空间，通过定制的缓存接口完成私钥相应的签名、加密操作。这种方法通过在设备上开辟独立的虚拟空间存储私钥，不需要增加额外的硬件成本。

方案 3　基于口令的用户私钥保护机制。文献[6,7]利用用户口令对用户私钥进行加密并存储在用户设备，需要进行签名或加密时，通过用户输入正确的口令获得私钥进行相应操作。此外，文献[8]将用户私钥存放在远程服务器端，在进行签名或加密操作时，通过用户口令获取私钥到本地进行操作。

这 3 种方案中，方案 1 尽管能够提供高效的私钥保护，但由于增加了额外的硬件成本，目前尚未在 SMT 中大规模使用；方案 2 在不增加额外硬件的前提下能够提供用户私钥的强隔离保护，能够有效降低系统成本，但这种方法会带来额外的计算和存储负担，对 SMT 的性能影响较大；方案 3 是实际应用中常用的私钥保护手段，但也经常面临敌手通过字典攻击用户口令从而获取私钥的风险，然而通过安全可靠的私钥保护方案，高效的可证明安全私钥获取协议，将敌手攻陷方案归约到已证明安全的计算复杂度难题上，可以提供行之有效的用户私钥安全保护。

本文针对方案 3 存在的问题，设计在随机预言机模型下可证明安全的私钥保护方案。与现有相关同类方案相比，本文所做的工作和最终目标如下。

1) 考虑无线网络环境，SMT 使用私钥完成相应的签名或加密等业务操作之前，首先需要通过计算获取有效的用户私钥。作为终端设备，其具有较弱的计算能力和存储能力，因此，使用 < SMT, SERVER > 组合的设计思路，利用计算能力强的服务器端完成大量计算，而 SMT 端仅进行少量的指数运算和散列运算即可获得有效私钥。

2) 为避免敌手攻陷 SMT 或 SERVER 端获取用户私钥，采用密钥分割的设计思想，将部分私钥经用户口令 pwd 加密后存储在 SMT 端，另一部分经秘密处理保存在 SERVER 处，SMT 和 SERVER 并不直接存储用户私钥，从而增大敌手攻陷方案获取私钥的难度。

3) 针对无线网络环境的特点，考虑持有 SMT 的用户所处无线网络环境为非可信环境，因此，设计的方案中，与 SMT 进行密钥获取操作的 SERVER 也认为是非可信节点，SERVER 仅认为能够诚实地完成与 SMT 的交互，而 SERVER 与 SMT 一样，同样存在被敌手攻陷的风险，同时，SMT 端还要考虑用户隐私保护问题，采用匿名通信方式，与 SERVER 进行交互获取私钥。

4) 在交互过程中，方案采用时戳来保持用户获取私钥的新鲜性，防止敌手实施重放攻击。之所以不使用计数器，是考虑到 SMT 在联网获取私钥进行签名等操作过程中（例如，电子支付），必须满足时间同步需求。如果采用计数器方式，SMT 移动到不同无线网络进行私钥获取操作，会需要额外的存储空间来保存大量的计数状态信息，会增加 SMT 的存储管理负担。

整个方案的最终目标是通过 < pwd, SMT, SERVER > 的设计，在 SMT 获取私钥过程中，防止任何形式的敌手以任何手段得到私钥并篡改合法用户的签名信息，并且在私钥丢失的情况下，能够通过简单高效的方式使当前私钥失效。

2　预备知识

本节对文中要用到的符号和相关术语定义如下。

安全参数。设 l 和 k 分别为公钥系统中密钥长度和二进制字符串的长度，为安全起见，一般情况下 $l = 1\,024$，表示公钥加密算法的密钥长度为 1 024bit；$k = 160$，表示随机二进制字符串的长度为 160。

杂凑函数 H。一个杂凑函数 H 是安全的，如果该杂凑函数满足：1）给定 x，计算 $H(x)=y$ 是容易的，同时，给定 y，计算 $H^{-1}(y)=x$ 是困难的；2)给定 x，找到 $x'=x$ 满足 $H(x)=H(x')$ 在计算上是不可行的；3)找到一对 x 和 x' 满足 $x\neq x'$，而 $H(x)=H(x')$ 在计算上是不可行的，这里设 H 的取值范围在 $\{0,1)^k$。

可忽略函数 $negl(k)$。对于实函数 $negl(k)$，如果 $\forall c>0,\exists k_c>0$，使得 $negl(k)<k^{-c}$ 对于所有的 $k>k_c$ 都成立，就说 $ngel(k)$ 是可忽略的。

伪随机函数集合 $\{f_v\}$。指带密钥值 v 的散列函数集合，可表示为 $f(v,m)$。本文定义的 $\{f_v\}$ 符合文献[9]的标准，用于完成本文设计协议中加密和签名操作。

消息认证码 MAC。本文中的消息认证码是指利用伪随机函数集合生成的消息认证码[10]，该消息认证码满足如下性质：对于随机选择的密钥 a，生成对消息 m 的消息认证码 MAC，对于所有的多项式时间敌手 A，存在可忽略函数 $ngel(k)$，满足 $\Pr[MACa-forge(k)=1]\leq negl(k)$。

公钥加密方案。设 e 是一个概率多项式时间算法（Gen,E,D）的三元组，密钥生成算法 Gen 用安全参数 1^n 作为输入，输出一对密钥（pk,sk），加密算法 E 把公钥 pk 和来自某个明文空间的一个消息 m 作为输入，并输出密文 c；记为 $c\leftarrow E_{pk}(m)$；解密算法 D 把私钥 sk 和密文 c 作为输入，输出一个消息 m 或一个定义为失败的特殊符号 $\perp$；假设 e 能够抗选择明文攻击，在本文用于完成设备端与服务器端的加密需求。

数字签名方案。设 V 是一个概率多项式时间算法组成的三元组（Gen,S,V），密钥生成算法 Gen 用安全参数 1^n 作为输入，输出一对密钥（pk,sk），签名算法 S 以一个私钥 sk 和消息 $m\in\{0,1\}^*$ 作为输入，输出一个签名 s，表示为 $s\leftarrow S_{sk}(m)$；确定的验证算法 V 以 pk、m 和 s 作为输入，输出一位 b，当 $b=1$ 表示签名有效，$b=0$ 表示签名无效。

符号定义。v、a 表示 k 长度的二进制随机值，记作 $v\leftarrow_R\{0,1\}^k$，$a\leftarrow_R\{0,1\}^k$；$b\leftarrow h(m)$ 表示消息 m 经散列运算得到 b；d 表示用户的私钥，d_1,d_2 表示 d 的分割，其中 d_1 是经 $f(v,m)$ 产生的值，d_2 是 d 分割 d_1 后的其余部分，用 $d_2\leftarrow d-d_1 \bmod f(N)$ 表示，其中 $f(N)$ 是欧拉函数。

3 提出的私钥保护方案

3.1 方案初始化

SMT 端的初始化过程主要是得到 SERVER 端的公钥 pk_{server}，得到用户口令 pwd、公私钥对 $<pk_{\text{SMT}},sk_{\text{SMT}}>$，然后生成隐秘数据，并将显式的安全数据（例如，$pwd$、$sk_{\text{SMT}}$）从 SMT 设备中删除。此设计的目的是防止敌手仅攻陷 SMT 的情况下，就能得到 pwd 等明文信息，降低了方案的安全性。

设 $h:\{0,1\}^*\rightarrow\{0,1\}^k$，$f:\{0,1\}^*\rightarrow\{0,1\}^{l+k}$，输入数据 pk_{server}、pwd 和 $<pk_{\text{SMT}},sk_{\text{SMT}}>$，其中 $pk_{\text{SMT}}=<e,N>$，$sk_{\text{SMT}}=<d,N,f(N)>$，$ed=1 \bmod f(N)$，SMT 初始化过程可描述如下：

$$
\begin{aligned}
&v\leftarrow_R\{0,1\}^k\\
&a\leftarrow_R\{0,1\}^k\\
&b\leftarrow h(pwd)\\
&d_1\leftarrow f(v,pwd)\\
&d_2\leftarrow d-d_1 \bmod f(N)\\
&t\leftarrow E_{pk_{\text{server}}}(a,b,d_2,N)
\end{aligned}
$$

其中，v、a、t、pk_{server}、pk_{SMT} 作为与 SERVER 交互的必要参数保存在 SMT 设备中，其他值包括 b、d、d_1、d_2、$f(N)$ 全部删除。

3.2 基本私钥获取协议

在设计的方案中，由于用户私钥并不是直接存储在 SMT，因此用户使用私钥进行签名或加密操作过程之前，首先需要通过与 SERVER 之间的网络交互来获取用户的私钥。基本的私钥获取协议流程有如下步骤。

1) 用户 SMT 客户端软件输入 pwd，结合 SMT 保存的数据，生成 $b\leftarrow h(pwd)$，$r\leftarrow_R\{0,1\}^l$，$g\leftarrow E_{pk_{\text{server}}}(r,b)$，$d\leftarrow MACa(<g,t>)$，并将生成的 (g,t,d) 发送到 SERVER。

2) SERVER 端收到 (g,t,d)，先验证 t 是否已失效，通过验证，进行 $(a,b,d_2,N)\rightarrow D_{sk_{\text{server}}}(t)$ 操作；通过计算 $MAC_a(g,t)$ 验证是否与接收到的 d 一致，验证 d 是否来自 SMT；验证通过，则进行 $(b,r)\leftarrow D_{\text{sksever}}(g)$ 计算，比较 b 与 b 相等验证 SMT 发送的口令是否来自于合法用户的 pwd；以上步骤完成后进行 $h\leftarrow r\oplus d_2$ 操作，并将 h 返回给 SMT。

3) SMT 首先计算用户的私钥 $d_1\leftarrow f(v,pwd)$，然后通过 $d_2\leftarrow r\oplus h$ 运算得到服务器私钥 d_2，然后

通过 $d \leftarrow d_1 + d_2 \bmod f(N)$ 得到完整私钥 d，如果满足 $ed = 1 \bmod f(N)$，则表示 SMT 获取私钥成功，并能够进行接下来的签名或加密操作。

3.3　协议的防中间人攻击设计

上述协议中，由于 r 的取值对 SERVER 未知，因此可以防止非可信 SERVER 对 d_2 的获取，但是在发送给 SMT 过程中，仅发送 h，如果该过程被第三方敌手截获，并展开中间人攻击，一旦 h 值遭到篡改，SMT 端无法计算出有效的私钥，消息的完整性无法得到保障。因此，对上述协议进行扩展，在 SERVER 端利用 SMT 提供的秘密参数对 h 进行 MAC 计算，并将得到的值与 h 一起发送给 SMT，扩展的协议具体步骤如下。

1) 在 SMT 开始密钥获取时，分别随机取值：$r_1 \leftarrow_R \{0,1\}^l$ 和 $a_1 \leftarrow_R \{0,1\}^k$，并生成 $g \leftarrow E_{pk_{\text{server}}}(r, b, r_1, a_1)$。

2) 相应地，在 SERVER 收到 g 后，进行解密操作得到 r_1, a_1，并进行 $J \leftarrow MAC_{a_1}(<r_1, h>)$ 运算，最终将 (J, h) 返回给 SMT。

3)SMT 增加了 $j \leftarrow MAC_{a_1}(<r_1, h>)$ 运算，判断 j 和 J 是否相等，从而验证 h 未遭到篡改等非法操作。

3.4　协议的前向安全性设计

以上协议实现了用户一次操作中的安全密钥获取，然而，当 SMT 与同一 SERVER 进行多次密钥获取时，可能存在这样的情况：敌手在得到早期的初始计算结果，例如 (g, t, d)，通过与该 SERVER 进行交互仍能够得到有效的用户私钥，造成前期通过该私钥进行的签名全部失效，其原因是由于上述协议中未考虑协议的前向安全性设计。为杜绝此类情况，通过引入参数 t 对 SMT 每次进行交互的 g 值更新，这样即使早期的 g 值暴露给敌手，由于 SERVER 端验证其无效，敌手也无法获得合法私钥，从而达到协议的前向安全。因此，对 3.4 节协议继续扩展完善后的私钥获取协议如图 1 所示。

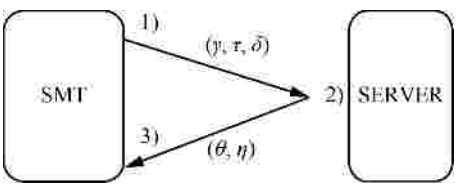

图 1　完整的用户私钥获取协议

1)$b \leftarrow h(pwd)$

$r \leftarrow_R (0,1)^l$

$r_1 \leftarrow_R (0,1)^l$

$a_1 \leftarrow_R (0,1)^k$

$g \leftarrow E_{pk_{\text{server}}}(r, b, r_1, a_1, t)$

$d \leftarrow MACa(<g, t>)$

2)如果 t 已失效，退出操作

$(a, b, d_2, N) \rightarrow D_{sk_{\text{server}}}(t)$

如果 $d \neq MACa(<g, t>)$，退出操作

如果 $D_{sk_{\text{server}}}(g) \neq (r, b, r_1, t)$，退出操作

如果 $b \neq b$，退出操作

如果 $t' \neq NULL$ 且 $t' > t$，退出操作

$t' = t$

$d_2 \leftarrow r \oplus h, J \leftarrow MAC_{a_1}(<r_1, h>)$

存储 (t', t)

3)$d_1 \leftarrow f(v, pwd)$

$j \leftarrow MACa1(<r_1, h>)$

如果 $j \neq J$，退出操作

$d_2 \leftarrow r \oplus h, d \leftarrow d_1 + d_2 \bmod f(N)$

如果 $ed \neq 1 \bmod f(N)$，退出操作

得到有效的用户私钥 sk

3.5　简单高效的私钥失效协议

当用户设备 SMT 遗失或遭到敌手窃取时，用户已无法通过 SMT 与 SERVER 进行交互，用户需要通过某种简单有效的方式使用户私钥失效，以免敌手在获得用户私钥后造成更大程度的破坏。文献[11]提出的私钥失效方法需要用户利用额外的存储空间存储一些状态参数值和 t，增加了用户的操作难度，效率不高。虽然文献[12]能够利用 username/password 访问 SERVER 完成用户的私钥失效，有较高的效率，然而，考虑到无线网络中用户身份的匿名性，暴露用户身份给非可信 SERVER，不利于用户的隐私保护。本文提出的私钥失效协议利用 SMT 与 SERVER 的时间同步特性，用户仅需要保存口令 pwd 和最后一次完成私钥获取过程的时间 t 提交给 SERVER 即可，SERVER 端通过 $(a, b, d_2, N) \rightarrow D_{sk_{\text{server}}}(t)$ 解密与该 SMT 端交互保存的 t，并验证 b 是否与 $b \leftarrow h(pwd)$ 相等，验证通过后比较保存的 t' 与用户提交的时间 t，如果 $t' > t$，说明在 SMT 失窃后，敌手已经进行过私钥获取操作，SERVER 则使与该 SMT 会话的凭据 t 失效，完成用户的私钥失效操作。

4 方案的安全性分析

随机预言机模型（random oracle model）是在标准模型的基础上增加公共可访问的随机预言机，将方案中所使用的散列函数理想化为随机预言机，敌手只能通过询问随机预言机来获得所需要的散列值，并且在仿真阶段通过一系列的步骤利用该敌手，将敌手的能力转化为攻破某已知困难问题的优势。随机预言机模型的提出，成为平衡密码方案可证安全和实用性的重要途径，使设计高效并且安全的协议成为可能。目前，许多著名的密码方案[13,14]在随机预言机模型下可证明安全的。本节也将在随机预言机模型下验证上述提出的协议可证明安全性。

4.1 敌手模型与系统目标

假设敌手能够控制整个网络，并且可以获得任何有用的资源，包括用户口令 pwd、用户设备 SMT 和服务器 SERVER。用 $ADV\{R\}$ 表示敌手能够获得的资源，其中 $R \subseteq \{pwd, \mathrm{SMT}, \mathrm{SERVER}\}$。相应地，在随机预言机模型下，敌手可进行询问包括 SMT 询问预言机 O_{SMT}（O_{SMT} 询问又可分为 O_{start} 和 O_{finish}），SERVER 询问预言机 O_{SERVER}，以及 h 和 f 的询问预言机 O_h 和 O_f。用 q_{SMT} 表示对 O_{SMT} 发起询问的次数，q_{SERVER} 表示对 O_{SERVER} 发起询问的次数，q_h, q_f 分别表示 O_h 和 O_f 发起询问的次数，另外，用 q_o 表示其他可能需要访问预言机的次数。令 $\bar{q} = (q_{\mathrm{SMT}}, q_{\mathrm{SERVER}}, q_h, q_f, q_o)$，$|\bar{q}| = q_{\mathrm{SMT}} + q_{\mathrm{SERVER}} + q_h + q_f + q_o$ 表示对方案预言机总的询问次数，如果敌手最多经过 $\bar{q}$ 次预言机询问后成功的概率至少是 e，就说敌手 $(\bar{q}, e)$ 攻破系统方案。如果 e 是一个可忽略的值，则认为方案是安全的，即敌手不能以不可忽略的概率攻陷系统设计的方案。

4.2 方案的安全性分析

为了便于描述，令 $R-RSA[\ell, D]$ 表示本文提出的私钥保护方案，其中 e 表示 SERVER 使用的加密方案，D 表示字典空间。敌手已得到用户公钥，以及根据敌手类型的不同，还可以得到一些其他的公开数据和私有数据。下面分别按 $ADV\{pwd, \mathrm{SERVER}\}$、$ADV\{\mathrm{SMT}, \mathrm{SERVER}\}$、$ADV\{\mathrm{SMT}\}$、$ADV\{\mathrm{SMT}, pwd\}$ 四类敌手模型给出命题并证明其安全性。

命题 1 设 $\{f_v\}$ 是一个伪随机函数集合。如果一个属于 $ADV\{pwd, \mathrm{SERVER}\}$ 的敌手 F 能够以 $(\bar{q}, e)$ 的概率攻陷 $R-RSA[e, D]$，则存在一个敌手 F' 能够以 (q_{SMT}, e') 的概念攻陷构成该方案的 RSA 签名方案，这里 $e' \approx e$。

证明 仿真阶段，F' 生成 SERVER 端的公私钥对 $(pk_{\mathrm{SERVER}}, sk_{\mathrm{SERVER}})$，生成用户口令 $pwd \leftarrow_R D$，并且使用 v 生成 $d_1 \leftarrow f(v, pwd)$，以及 $t \leftarrow E_{pk_{\mathrm{server}}}(a, b, d_2, N)$，只是这里的 d_2 取一个在 $\{0,1\}^l$ 内随机值，最后 F' 将 $pk_{\mathrm{SMT}}, pk_{\mathrm{SERVER}}, sk_{\mathrm{SERVER}}, pwd$ 传给 F。

F' 响应 O_{start} 询问，并执行相应的协议，最终输出 (g, t, d)；F' 响应 O_{SERVER} 询问，并按实际情况终止操作或最终返回 (J, h)；F' 响应 O_{finish} 询问，按实际运算情况，计算 d_1，验证 $J \leftarrow MAC_{a1}(< r_1, h >)$ 是否与 J 相等，计算 $d_2 \leftarrow r \oplus h$，得到 $d \leftarrow d_1 + d_2 \bmod f(N)$，验证 $ed = 1 \bmod f(N)$，其中，r、r_1、a_1 来自 O_{start}。

分析阶段，用 e' 表示 F 在仿真阶段成功攻陷方案的概率。考虑用 f_v 替换随机函数做实验，用 e'' 表示 F 在实验中成功攻陷方案的概率。根据实验操作和仿真操作的不可区分性，有 $e' \approx e''$。又由 f_v 的伪随机性可知，$e'' \approx e$，所以 $e \approx e'$ 成立，命题得证。

命题 2 设 h 和 f 是 2 个随机预言机。如果一个属于 $ADV\{\mathrm{SMT}, \mathrm{SERVER}\}$ 的敌手 F 能够以 $(\bar{q}, e)$ 的概率攻陷 $R-RSA[\ell, D]$，则存在一个敌手 F' 能够以 (q_{SMT}, e') 的概念攻陷构成该方案的 RSA 签名方案，这里 $e' \approx e - \dfrac{q_f + q_h}{|D|}$。

证明 仿真阶段，F' 生成 SERVER 端的公私钥对 $(pk_{\mathrm{SERVER}}, sk_{\mathrm{SERVER}})$，生成用户口令 $pwd \leftarrow_R D$，并且使用 v 生成 $d_1 \leftarrow f(v, pwd)$，以及 $t \leftarrow E_{pk_{\mathrm{server}}}(a, b, d_2, N)$，只是这里的 d_2 取一个在 $\{0,1\}^l$ 内在随机值，最后 F' 将 $pk_{\mathrm{SMT}}, pk_{\mathrm{SERVER}}, sk_{\mathrm{SERVER}}, pwd$ 传给 F。

F' 响应 O_{start} 询问，并执行相应的协议过程，最终输出 (g, t, d)；F' 响应 $h(pwd')$ 和 $f(v', pwd')$ 2 个随机预言机询问，如果在仿真阶段进行 O_h 询问，有 $pwd = pwd'$ 时，或者进行 O_f 询问，有 $v = v'$ 且 $pwd = pwd'$ 时，取消操作。F' 响应 O_{SERVER} 询问，并按实际情况终止操作或最终返回 (J, h)；F' 响应 O_{finish} 询问，按实际运算情况，计算 d_1，验证 $J \leftarrow MAC_{a1}(< r1, h >)$ 是否与 J 相等，计算

$d_2 \leftarrow r \oplus h$，得到 $d \leftarrow d_1 + d_2 \bmod f(N)$，验证 $ed = 1 \bmod f(N)$，其中，r、r_1、a_1 来自 O_{start}。

分析阶段，如果 F 命中 pwd，仿真过程才能够与实现操作满足不可区分性，而 F 命中的概率至多是 $\frac{q_f + q_h}{|D|}$，因此，F 如果攻陷 $R-RSA[e,D]$ 的概率是 e，那么 F' 在仿真阶段成功的概率 $e' \approx e - \frac{q_f + q_h}{|D|}$，命题得证。

命题 3　设 h 是一个在 D 域内可忽略的碰撞概率。如果一个属于 $ADV\{\text{SMT}\}$ 的敌手 F 能够以 $(\overline{q}, e)$ 的概率攻陷 $R-RSA[e,D]$，其中 $e = \frac{q_{\text{server}}}{|D|} + y$，那么既存在一个敌手 F' 能以 (q_{SMT}, e') 的概率攻陷 RSA 签名方案，其中 $e' \approx \frac{y}{2}$，又存在一个攻击者 A' 能以 $(2q_{\text{server}}, e'')$ 的概率攻陷 e 方案，其中 $e'' \approx \frac{y}{2(1+q_{\text{SMT}})}$。

证明　1) $t' = t$，g 不是 O_{start} 的输出，$d = MAC_a(<g,t'>)$，其中 a 是来自 SMT 初始化操作的加密密钥，$D_{sk_{\text{server}}}(g) = (b, r, r_1, a_1, t)$，$b = b$。

2) $t' \neq t$，而 g 来自于 O_{start} 的输出，$d = MAC_{a'}(<g,t'>)$，$D_{sk_{\text{server}}}(t') = (a', b', d_2', N')$，$b' = b$，其中 b 是 O_{start} 的输出。

仿真阶段，设 F' 已得到用户公钥 pk_{SMT}，F' 生成 SERVER 端的公私钥对 $(pk_{\text{SERVER}}, sk_{\text{SERVER}})$，生成用户口令 $pwd \leftarrow_R D$，并使用 v 生成 $d_1 \leftarrow f(v, pwd)$，以及 $t \leftarrow E_{pk_{\text{server}}}(a, b, d_2, N)$，只是这里的 d_2 取一个在 $\{0,1\}^l$ 内随机值。最后，F' 将 $a, v, t \leftarrow E_{pk_{\text{server}}}(0^{2k+2l})$ 交给 F。

F' 响应 O_{start} 询问，并执行相应的协议过程，最终输出 (g,t,d)，其中 $g = E_{pk_{\text{server}}}(0^{2l+2k})$。

F' 以 (g,d,t') 作为输入，按以下情况响应 O_{server} 询问。

① (g,d,t') 是来自 O_{start} 的输出。通过计算 $J \leftarrow MAC_{a_1}(<r_1, h>)$，$h \leftarrow r \oplus d_2$，其中 r_1, a_1, r 来自 O_{start} 询问，$d_2 \in \{0,1\}^l$，返回 (J,h)。

②只有 g 和 t' 是来自 O_{start} 的输出。而由于 d 不是来自 O_{start} 的输出，使 $MAC_a(g,t') \neq d$，退出操作。

③ $t' = t$，而 g 不是来自于 O_{start} 的输出，则通过仿真的 sk_{server} 解密 g 来验证 b 值，如果 $b = b$ 表示通过成功的在线字典攻击获得正确的 pwd，如果 $b \neq b$ 则退出操作。

④ g 来自于 O_{start} 的输出，而 $t' \neq t$。如果 $d \neq MAC_{a'}(<g,t'>)$，其中 a' 取自仿真过程中的随机值，则仿真过程退出操作。否则通过 $(r', b', r_1', a_1', t^*) \leftarrow D_{pk_{\text{server}}}(g)$ 得到 b'。如果 $b' \neq b$ 退出仿真操作，如果 $b' = b$，表示通过在线字典攻击获得正确的 pwd。

⑤ g 不是来自于 O_{start} 的输出，$t' \neq t$，则仿真过程与正常的协议交互过程相同。

F' 响应 O_{finish} 询问，按实际运算情况，计算 d_1，验证 $J \leftarrow MAC_{a1}(<r_1, h>)$ 是否与 J 相等，计算 $d_2 \leftarrow r \oplus h$，得到 $d \leftarrow d_1 + d_2 \bmod f(N)$，验证 $ed = 1 \bmod f(N)$，其中，r、r_1、a_1 来自 O_{start}。

分析阶段 1，在不考虑其他可忽略的概率前提下，F 能够命中 pwd 的概率至多是 $\frac{q_{\text{server}}}{|D|}$，因此，如果一个敌手 F 能以至少 $\frac{q_{\text{server}}}{|D|} + \frac{y}{2}$ 概率使仿真操作成功，则存在一个 F' 以 $e' \approx \frac{y}{2}$ 的概率攻陷 RSA 签名方案。第一部分证明完毕。

假设如果一个敌手 F 能以至多 $\frac{q_{\text{server}}}{|D|} + \frac{y}{2}$ 概率使仿真操作成功，则继续构造一个攻击者 A' 来证明该命题的第二部分。A' 按上一部分的方式构造仿真器，进行 SERVER 端的加密预言机询问。在 A' 的仿真阶段与 F' 的仿真阶段大致相同，唯一不同的地方是当 A' 能够命中 pwd 时，并不退出仿真过程。因此敌手 F 能攻陷此仿真过程是以至多 $\frac{q_{\text{server}}}{|D|} + \frac{y}{2}$ 的概率。

现在使用标准的混合理论（hybrid argument）来构造 A' 的一个实验 $EXPT_j$，设 $j \in_R \{0, \ldots, q_{\text{SMT}} + 1\}$，前 j 个密文是由 A' 产生的普通加密消息，其余的则以相应的全零串加密成密文，用 p_j 表示敌手 F 攻陷该实验的概率，对于 $i \in_R \{0, \ldots, q_{\text{SMT}} + 1\}$，$F$ 能成功区分普通加密消息还是由零串加密的消息的概率为 $\frac{1}{q_{\text{SMT}} + 1} \sum_{i=1}^{q_{\text{SMT}}+1} (p_{i+1} - p_i) \geq \frac{y}{2(1+q_{\text{SMT}})}$。因此，让 A' 任意选择一个 $i \in_R \{1, \ldots, q_{SMT} + 1\}$，并运行 $EXPT_i$，通过输入 2 个消息串 X_0, X_1 分别按仿真实验

操作，其中 X_1 经全零串进行加密输出。通过 $EXPT_j$ 的实验分析，A' 能够区分出哪个消息是经过加密操作的消息串的概率，即 A' 能够攻陷 e 的可忽略概率是 $\frac{y}{2(1+q_{\mathrm{SMT}})}$。整个命题得证。

命题 4 假定 $R-RSA[e,D]$ 中的 RSA 方案是确定的，如果一个属于 $ADV\{\mathrm{SMT},pwd\}$ 的敌手 F 能够以 $(\overline{q},e)$ 的概率攻陷 $R-RSA[e,\mathrm{D}]$，那么既存在一个敌手 F' 能以 (q_{server},e') 的概率攻陷 RSA 签名方案，其中 $e'\approx\frac{e}{2}$，又存在一个攻击者 A' 能以 $(2q_{\mathrm{server}},e'')$ 的概率攻陷 e 方案，其中 $e''\approx\frac{e}{2(1+q_{\mathrm{SMT}})}$。

证明 仿真阶段，设 F' 已得到用户公钥 pk_{SMT}，F' 生成 SERVER 端的公私钥对 $(pk_{\mathrm{SERVER}},sk_{\mathrm{SERVER}})$，生成用户口令 $pwd\leftarrow_R D$，并且使用 v 生成 $d_1\leftarrow f(v,pwd)$，以及 $t\leftarrow Epk_{\mathrm{server}}(a,b,d_2,N)$，只是这里的 d_2 取一个在 $\{0,1\}^l$ 内随机值。最后，F' 将 $a,v,t\leftarrow E_{pk_{\mathrm{server}}}(0^{2k+2l})$ 交给 F。

F' 响应 O_{start} 询问，除了输出 (g,t,d) 之外，其他按真实协议操作执行相应的过程，其中 $g=E_{pk_{\mathrm{server}}}(0^{2l+2k})$。

F' 以 (g,d,t') 作为输入，按以下情况响应 O_{server} 询问。

① (g,d,t') 是来自 O_{start} 的输出。通过计算 $J\leftarrow MAC_{a_1}(<r_1,h>)$，$h\leftarrow r\oplus d_2$，其中 r_1,a_1,r 来自 O_{start} 询问，$d_2\in\{0,1\}^l$，返回 (J,h)。

②只有 g 和 t' 是来自 O_{start} 的输出。而由于 d 不是来自 O_{start} 的输出，使 $MAC_a(g,t')\neq d$，退出操作。

③$t'=t$，而 g 不是来自 O_{start} 的输出，则通过仿真的 sk_{server} 解密 g 来验证 b 值，如果 $b\neq b$ 则退出操作，否则返回 (J,h)。

④g 来自 O_{start} 的输出，而 $t'\neq t$。除了用到的 b、r、r_1、a_1 来自 O_{start} 的输出外，其他按实际协议过程操作。

⑤g 不是来自 O_{start} 的输出，$t'\neq t$，则仿真过程同一正常的协议交互过程。

F' 响应 O_{finish} 询问，按实际运算情况，计算 d_1，验证 $J\leftarrow MAC_{a1}(<r_1,h>)$ 是否与 J 相等，计算 $d_2\leftarrow r\oplus h$，得到 $d\leftarrow d_1+d_2\bmod f(N)$，验证 $ed=1\bmod f(N)$，其中，r、r_1、a_1 来自 O_{start}。

分析阶段 1，如果一个敌手 F 能以至少 $\frac{e}{2}$ 概率使仿真操作成功，则存在一个 F' 以 (q_{server},e') 的概率攻陷 RSA 签名方案，其中 $e'\approx\frac{e}{2}$。第一部分证明完毕。

第二部分的证明与命题 3 的第二部分证明类似，此处略。

命题 4 得证。

5 结束语

本文针对无线网络环境下智能移动终端在进行安全业务操作过程中，面临私钥存储管理的安全问题，充分考虑用户匿名、网络同步操作等应用场景的前提下，通过服务器与智能移动终端之间交互动态获取用户私钥的方式，设计了安全高效的终端私钥保护方案。该方案对其他轻量级连网设备的隐私信息保护同样具有可参考性。与其他类似方案相比，从安全性和效率改进之处主要体现在两方面：第一，减少了智能移动终端的计算量（计算量仅为常数级）和存储量（仅存储个数级密钥参数），简化了交互过程参数的设置（仅通过两轮交互即可完成私钥获取），并证明了其安全性；第二，以终端与服务器端所在网络需时间同步的特性，贯穿整个方案的设计过程，能够防止重放攻击的同时，更提高了便捷高效的用户私钥失效方案，减少了用户的复杂操作和额外的数据存储。该方案的设计更符合无线网络智能移动终端计算能力和存储空间受限的应用需求。下一步研究重点主要集中在用户私钥失效后如何能够在避免初始化的一系列操作的同时，提供高效的私钥恢复操作。

参考文献：

[1] STUDER A, PERRIG A. Mobile user location-specific encryption (MULE): using your office as your password[A]. Proceedings of the 3rd ACM Conference on Wireless Network Security (WiSec '10)[C]. 2010.

[2] VILA E, BOROVSKA P. Data protection utilizing trusted platform module[J]. Opportunities in Opportunistic Computing, 2010, 43(1): 42-50.

[3] Trusted Computing Group.TPM main part 3 commands, spec fication version 1.2, level 2 revision 103[EB/OL]. http://www. trustedcomputinggroup.org, 2007.

[4] JOHN P, LEE R B. Protecting cryptographic keys and computations

via virtual secure coprocessing[A]. ACM SIGARCH Computer Architecture News[C]. 2005.

[5] LOCASTO M E, SIDIROGLOU S, KEROMYTIS A D. Speculative virtual verification: policy-constrained speculative execution[A]. Proceedings of the New Security Paradigms Workshop (NSPW)[C]. 2005. 170-175.

[6] BELLOVIN S, MERRITT M．Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and pass-word file compromise[A]. Proceedings of the 1st ACM Conference on Computer and Communication Security[C]. New York, 1993.244-250.

[7] FENG D G, XU J. A new client-to-client password-authenticated key agreement protocol[A]. Proceedings of IWCC 2009[C]. Berlin, Springer-Verlag, 2009.63-76.

[8] PERLMAN R, KAUFMAN C. Secure password-based protocol for downloading a private key[A]. Proc NDSS'99[C]. 1999.

[9] GOLDREICH O, GOLDWASSER S, MICALI S. How to construct random functions[J]. ACM, 1986, 33(4):210-217.

[10] BELLARE M. New proofs for NMAC and HMAC: security without collision-resistance[A]. CRYPTO 2006[C]. Springer Verlag, 2006. 602-619.

[11] MACKENZIE P, REITER M. Networked cryptographic devices resilient to capture[A]. Proc IEEE Symposium on Security and Privacy[C]. Springer Verlay, 2001.

[12] XU S, SANDHU R A. Scalable and security cryptographic service[A] Data and Applications Security XXI[C]. Berlin, Springer Verlag, 2007. 144-160.

[13] BELLARE M, ROGAWAY P. Random oracles are practical-a paradigm for designing efficient protocols[A]. Proceedings of the First ACM Conference on Computer and Communications Security[C]. 1993. 62-73.

[14] BELLARE M, ROGAWAY P. The exact security of digital signatures-how to sign with rsa and rabin[A]. Proceedings of EUROCRYPT'96[C]. 1996. 399-416.

作者简介：

马骏（1981-），男，河北安国人，西安电子科技大学博士生，主要研究方向为无线网络安全。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为信息安全、容忍入侵与无线网络安全等。

郭渊博（1975-），男，陕西周至人，博士，解放军信息工程大学副教授、硕士生导师，主要研究方向为容忍入侵、无线网络安全。