一种基于可信计算的多重签名方案的分析与改进

张 亚[1] 周 曜[2]
(安徽理工大学电气与信息工程学院 淮南 232001)[1] (中国电子科技集团第三十八研究所 合肥 230031)[2]

摘 要 对基于可信计算中DAA协议的一种匿名多重签名方案进行了安全分析,指出其不能抵抗签名伪造攻击,因此是不安全的。分析了这一安全缺陷产生的原因,并给出改进的多重签名方案。改进方案在每个签名者提交的部分签名中加入了DAA证书信息,使得最终生成的多重签名不可被伪造。它在保留了原方案的主要优点的前提下,克服了其安全缺陷。

关键词 密码学,可信计算,DAA协议,多重签名
中图法分类号 TP309.7 **文献标识码** A

Analysis and Improvement of a Multi-signature Scheme Based on Trusted Computing

ZHANG Ya[1] ZHOU Yao[2]
(School of Electrical and Information Engineering, Anhui University of Science and Technology, Huainan 232001, China)[1]
(No. 38 Research Institute, China Electronics Technology Group Corporation, Hefei 230031, China)[2]

Abstract Aimed at an anonymous multi-signature scheme based on DAA technology for trusted computing, this paper analyzed its security and demonstrates that it is vulnerable against signature forgery attack. The reasons why such security flaws exist in the scheme was investigated and an improved version was proposed. The improved scheme associates every signer's DAA certificate with its partial signature. The unforgeability of the final multi-signature is guaranteed because the attackers can not forge a DAA certificate. The new scheme not only retains the major advantages but also overcomes the security flaws of the original scheme.

Keywords Cryptography, Trusted computing, DAA protocol, Multi-signature

1 引言

多重签名是一种特殊的数字签名技术,用于多个用户对同一个消息进行签名,并且最终签名长度不随签名人数递增。一般来说,多重签名的参与方有消息发送者(Issuer)、消息签名者(Signer)、签名验证者(Verifier)和签名收集者(Collector)。就签名顺序而言,多重签名方案可分为顺序多重签名和广播多重签名。目前已有多种多重签名方案被提出,如代理多重签名[1]、多重盲签名[2]、基于二次剩余的多重签名[3]、基于身份的多重签名[4]、基于简化PKI的多重签名[5]等。

文献[6]中提出了一种基于可信计算(Trusted Computing,TC)技术的多重签名方案[6],该方案基于可信计算[7]所支持的直接匿名认证(Direct Anonymous Attestation,DAA)协议[8],主要思想是利用可信平台模块(Trusted Platform Module,TPM)中唯一不可迁移密钥以及与该密钥绑定的DAA证书来生成多重签名。方案的优点是可保证签名者的匿名性,并且在签名者身份发生变化时不需引入新的公钥验证开销。由于在方案中,签名者需基于其TPM密钥完成签名,而TPM密钥是受硬件保护的,很难发生泄漏或转储的情况,因此其安全性较传统多重签名方案得以加强。

签名不可伪造性是数字签名方案设计的基本安全需求[9],即对手在不知道签名者密钥的情况下,无法伪造出一个合法的签名。本文对文献[6]中的多重签名方案进行了安全性分析,表明对手可在不知道签名者TPM密钥以及DAA证书的情况下,伪造一个合法的多重签名,并针对这一安全缺陷产生的原因进行了分析,给出了一种改进的基于可信计算的多重签名方案。

2 DAA协议

DAA协议[8]由Brickell等人在2004年提出,目前已被可信计算组织(Trusted Computing Group,TCG)[10]采纳为可信计算中直接匿名认证的技术标准。DAA以CL签名方案[11]和基于离散对数的知识证明为基础,该协议简述如下:

1)初始设置:协议中包含一个可信的DAA证书颁发者。在初始阶段,证书颁发者确定并公布自己的公钥 $PK=(n,g,g',h,R_0,R_1,S,Z,\gamma,\Gamma,\rho)$,其中,$n$ 为安全RSA模数,$n=pq$,$p=2p'+1$,$q=2p'+1$,p,p',q,q' 均为大素数,g' 为模 n 的二次剩余群 QR_n 的随机生成元,$g:=(g')^{x_g}$,$h:=(g')^{x_h}$,$S:=h^{x_S}$,$Z:=h^{x_Z}$,$R_0:=S^{x_0}$,$R_1:=S^{x_1}$,$x_g,x_h,x_s,x_z,x_0,x_1\in_R[1,p'q']$;$\Gamma$ 和 ρ 分别是长度为1632位和208位的素数,$\gamma\in$

到稿日期:2010-07-19 返修日期:2010-10-18 本文受国家自然科学基金资助项目(90718021)资助。
张 亚(1978—),男,硕士,讲师,主要研究方向为信息处理技术,E-mail:zhangya@aust.edu.cn;周 曜(1975—),男,博士,高级工程师,主要研究方向为信息安全与可信计算。

Z_Γ^* 是阶为 ρ 的元素。证书颁发者的私钥为(p',q')。上述参数设置是为了满足 CL 签名和零知识证明的要求，更具体的说明可参见文献[8]。

2)可信平台模块(TPM)的加入：配有 TPM 的平台首先与 DAA 证书颁发者进行交互，使用保留在 TPM 中的唯一不可迁移密钥 f(248 位)向证书颁发者注册并获得一张 DAA 证书：(A,e,v)，该证书满足：

$$R_0^{f_0} R_1^{f_1} S^v A^e = Z (\mathrm{mod}\ n) \tag{1}$$

式中，f_0 和 f_1 分别为 f 的前 104 位和后 104 位。注意根据强 RSA 假设[9]，只有知道 n 分解因子的证书颁布者才可计算出正确的(A,e,v)。

3)DAA 签名与验证：申请了 DAA 证书的签名者从验证者那里获取一个随机数 bsn 作为名字基，生成假名 $N_v=\zeta^f (\mathrm{mod}\ \Gamma)$，其中 $\zeta=H(1||\mathrm{bsn})^{(\Gamma-1)/\rho} (\mathrm{mod}\ \Gamma)$，$H(.)$为散列函数；之后，签名者基于其 TPM 密钥，DAA 证书和待签名消息共同生成一个“知识签名”，向验证者证明自己知道 N_v 以 ζ 为底的离散对数 f，并且拥有一个与 f 相关联的 DAA 证书。

3 基于 DAA 技术的多重签名方案及安全分析

3.1 方案概述

文献[6]提出了一种基于 DAA 技术的多重签名方案，具体如下：

1)设 k 个签名者需对同一消息 m 进行签名，并且每个签名者 $U_i(1\leqslant i\leqslant k)$均已申请了一个与其 TPM 密钥 f_i 绑定的 DAA 证书：(A_i,e_i,v_i)。

2)每个签名者 U_i 随机选择整数 w_i，计算

$$T_{1_i} := (A_i h^{w_i})^{e_i} (\mathrm{mod}\ n)$$

$$T'_{1_i} := R_0^{f_{0_i}} R_1^{f_{1_i}} S^{v_i} h^{-e_i w_i} (\mathrm{mod}\ n)$$

$$T_{2_i} := g^{e_i w_i} h^{e_i e_i} (g')^{e_i H(m)} (\mathrm{mod}\ n)$$

$$N_i := \zeta^{f_{0_i}+f_{1_i} 2^{104}} (\mathrm{mod}\ \Gamma)$$

将$(T_{1_i}, T'_{1_i}, T_{2_i}, N_i)$发给签名收集者 C。

3)C 计算

$$T_1 \equiv \prod_{i=1}^{k} (A_i h^{w_i})^{e_i} (\mathrm{mod}\ n)$$

$$Z^k \equiv \pm T_1 \prod_{i=1}^{k} T'_{1_i} (\mathrm{mod}\ n)$$

$$T_2 \equiv \pm \prod_{i=1}^{k} g^{e_i w_i} h^{e_i e_i} (g')^{e_i H(m)} (\mathrm{mod}\ n)$$

$$N_s \equiv \prod_{i=1}^{k} \zeta^{f_{0_i}+f_{1_i} 2^{104}} (\mathrm{mod}\ \Gamma)$$

并按零知识证明要求，随机选取 $r_0, r_1, r_v, r_{ew}, r_{e'}, r_e, c$，计算

$$Z' = T_1^c R_0^{r_0} R_1^{r_1} S^{r_v} h^{-r_{ew}} (\mathrm{mod}\ n)$$

$$T_2' = g^{r_{ew}} h^{r_{e'}} (g')^{r_e H(m)} (\mathrm{mod}\ n)$$

$$N_s' = \zeta^{r_0+r_1 2^{104}} (\mathrm{mod}\ \Gamma)$$

以及

$$s_v := r_v + cv, s_0 := r_0 + cf_0, s_1 := r_1 + cf_1$$

$$s_{e'} := r_{e'} + ce', s_{ew} := r_{ew} + c\omega'$$

$$s_e := r_e + ce''$$

其中，$v=\sum_{i=1}^{k} v_i, f_0=\sum_{i=1}^{k} f_{0i}, f_1=\sum_{i=1}^{k} f_{1i}, e'=\sum_{i=1}^{k} e_i^2, w'=\sum_{i=1}^{k} e_i w_i, e''=\sum_{i=1}^{k} e_i$；

最后输出多重签名

$$\sigma := \{(T_1||T_2)||(Z'||T_2'||N_s')||c||s_v||s_0||s_1||s_{e'} ||s_{ew}||s_e||\langle N_i||T_{1_i}||T_{2_i}\rangle_k||k||\mathrm{exp\text{-}date}(N_s,\zeta)\}$$

其中 exp-date 为签名有效时间。

4)验证过程：验证者 V 检查以下方程组：

$$\begin{cases} Z' := (Z^k)^{-c} T_1^{c+1} R_0^{s_0} R_1^{s_1} S^{s_v} h^{-s_{ew}} (\mathrm{mod}\ n) & (2.1) \\ T_2' := T_2^{-c} g^{s_{ew}} h^{s_{e'}} (g')^{s_e H(m)} (\mathrm{mod}\ n) & (2.2) \\ N_s' := N_s^{-c} \zeta^{s_0+s_1 2^{104}} (\mathrm{mod}\ \Gamma) & (2.3) \\ N_i \neq N_j, (i\neq j, \text{and } i,j\in[1,k]) & (2.4) \\ T_1 \equiv \prod_{i=1}^{k} T_{1_i} (\mathrm{mod}\ n) & (2.5) \\ T_2 \equiv \prod_{i=1}^{k} T_{2_i} (\mathrm{mod}\ n), N_s \equiv \prod_{i=1}^{k} N_i (\mathrm{mod}\ \Gamma) & (2.6) \end{cases} \tag{2}$$

当且仅当以上条件全部满足时，V 接受签名，否则拒绝签名。

3.2 方案的安全性

文献[6]认为，签名者需依赖其 TPM 密钥和 DAA 证书来生成签名，而 DAA 证书不可伪造，并且 TCP 密钥受到硬件(即 TPM)保护，很难发生泄漏或转储的情况，因此多重签名不可伪造。但从下面对该方案的安全分析可以看出，即使所有签名者密钥与证书都没有泄漏，该多重签名仍可能被伪造。

从验证方程本身出发分析方案的安全性。不难看出，对于一个 DAA 证书(A,e,v)，最关键部分是数 A。这是因为只有知道 n 分解因子的证书颁发者才可根据式(1)计算出正确的 A，而其他任何一方(包括签名者自己)均无法得到 A。在验证方程组(2)中，与数 A 相关的方程只有式(2.1)和式(2.5)。将 $Z', s_0, s_1, s_v, s_{ew}$ 的表达式以及式(2.5)代入，式(2.1)可重写为：

$$(R_0^{f_0} R_1^{f_1} S^v h^{-w'} \prod_{i=1}^{k} T_{1_i})^c = (Z^k)^c (\mathrm{mod}\ n)$$

即如果可以找到 k 个 T_{1_i}，使得

$$\prod_{i=1}^{k} T_{1_i} = Z^k (R_0^{f_0} R_1^{f_1} S^v h^{-w'})^{-1} (\mathrm{mod}\ n) \tag{3}$$

则可通过签名验证。

对于拥有 DAA 证书(A_i,e_i,v_i)的合法签名者 U_i 而言，它可令 $T_{1_i}=(A_i h^{w_i})^{e_i}$，则根据式(1)，$T_{1_i}$ 显然满足式(3)。但对于一个攻击者 B 来说，即使它不拥有任何签名者密钥以及 DAA 证书，它构造满足式(3)的 k 个 T_{1_i} 也并不是困难的。事实上，B 可以任选 k 组$(f_{0_i}, f_{0_i}, v_i, e_i, w_i)$，并计算 $T_{1_i}=Z(R_0^{f_{0_i}} R_1^{f_{1_i}} S^{v_i} h^{-e_i w_i})^{-1} (\mathrm{mod}\ n), 1\leqslant i\leqslant k$，则有 $\prod_{i=1}^{k} T_{1_i} = Z^k (R_0^{f_0} R_1^{f_1} S^v h^{-w'})^{-1} (\mathrm{mod}\ n)$。

基于以上分析，可构造一个签名伪造攻击如下：

1)设攻击者 B 试图伪造 k 个签名者对于同一消息 m 的多重签名，则 B 任选 k 组$(f_{0_i}, f_{0_i}, v_i, e_i, w_i)$，计算

$$T_{1_i}' := R_0^{f_{0_i}} R_1^{f_{1_i}} S^{v_i} h^{-e_i w_i} (\mathrm{mod}\ n)$$

$$T_{1_i} := Z(T'_{1_i})^{-1} (\mathrm{mod}\ n)$$

$$T_{2_i} := g^{e_i w_i} h^{e_i e_i} (g')^{e_i H(m)} (\mathrm{mod}\ n)$$

$$N_i := \zeta^{f_{0_i}+f_{1_i} 2^{104}} (\mathrm{mod}\ \Gamma)$$

以及

$$T_1 = \prod_{i=1}^{k} T_{1_i}, T_2 = \prod_{i=1}^{k} T_{2_i}, N_s = \prod_{i=1}^{k} N_i。$$

2)B 按零知识证明要求，随机选取 $r_0, r_1, r_v, r_{ew}, r_{e'}, r_e, c$，计算

$$Z' = T_1^c R_0^{r_0} R_1^{r_1} S^{r_v} h^{-r_{ew}} (\mathrm{mod}\ n)$$

$$T_2' = g^{r_{ew}} h^{r_{e'}} (g')^{r_e H(m)} (\mathrm{mod}\ n)$$

$$N_s' = \zeta^{r_0+r_1 2^{104}} (\mathrm{mod}\ \Gamma)$$

以及

$s_0:=r_0+c\sum_{i=1}^{k}f_{0_i}$，$s_1:=r_1+c\sum_{i=1}^{k}f_{1_i}$，$s_v:=r_v+c\sum_{i=1}^{k}v_i$

$s_{ee}:=r_{ee}+c\sum_{i=1}^{k}{e_i}^2$，$s_{ew}:=r_{ew}+c\sum_{i=1}^{k}e_iw_i$，$s_e:=r_e+c\sum_{i=1}^{k}e_i$

3)最后生成多重签名

$\sigma:=\{(T_1||T_2)||(Z'||T'_2||N'_s)||c||s_v||s_0||s_1||s_{ee}||s_{ew}||s_e||\langle N_i||T_{1_i}||T_{2_i}\rangle_k||k||\exp\text{-date}(N_s,\zeta)\}$

不难看出，σ 可以通过方程组(2)中的所有验证，以式(2.1)为例

$$(Z^k)^{-c}T_1{}^{c+1}R_0{}^{s_0}R_1{}^{s_1}S^{s_v}h^{-s_{ew}}$$
$$=(Z^k)^{-c}T_1(\prod_{i=1}^{k}ZT_{1_i}{}'^{-1})^cR_0^{s_0}R_1^{s_1}S^{s_v}h^{-s_{ew}}$$
$$=(Z^k)^{-c}(Z^k)^cT_1R_0^{r_0}R_1^{r_1}S^{r_v}h^{-r_{ew}}=Z'$$

从以上攻击可以看出，攻击者 B 并不需知道任何 TPM 密钥及 DAA 证书即可构造一个合法的多重签名，因此原方案是不安全的。

4 改进方案及分析

4.1 改进方案

之所以存在以上攻击，关键在于：原方案中签名不可伪造性依赖于 DAA 证书的不可伪造性，而 DAA 证书的不可伪造性基于强 RSA 假设[9]，即：对于给定的 f_0，f_1 和 v，找到这样的两个数 A,e，使得 $A^e=Z(R_0^{f_0}R_1^{f_1}S^v)^{-1}\pmod n$ 是困难的。在原方案中，虽然每个签名者提交的 T_{1_i} 具有 $A_i^{e_i}$（去除盲化因子 h^{w_i} 后）的形式，但在签名验证过程中并没有体现这一点，即并没有要求签名者向验证者证明自己知道 A_i 或 e_i 的具体值，因此签名伪造者可以任意构造 T_{1i} 并通过验证。

根据以上分析，我们提出一个改进方案，即基于 Schnorr 机制，通过对每个签名者的 DAA 证书中的 A_i 和 e_i 分别生成签名，使得方案可抵抗签名伪造攻击。方案如下：

1)假设 k 个签名者需对同一消息 m 进行签名，其中每个签名者 U_i 拥有 TPM 密钥 f_i 和与 f_i 相关的 DAA 证书(A_i,e_i,v_i)。

2)每个 U_i 任选 w_i，计算

$T_{1_i}:=A_ih^{w_i}\pmod n$

$T_{2_i}:=g^{e_iw_i}h^{w_i}(g')^{v_i}\pmod n$

$N_i:=\zeta^{f_{0_i}+f_{1_i}2^{104}}\pmod\Gamma$

并按照零知识证明要求，随机选取 $r_{e_i},r_{0_i},r_{1_i},r_{v_i},r_{ew_i},r_{w_i}$，计算

$T_{1_i}{}'=T_{1_i}^{r_{e_i}}R_0^{r_{0_i}}R_1^{r_{1_i}}S^{r_{v_i}}h^{-r_{ew_i}}\pmod n$

$T_{2_i}{}'=g^{r_{ew_i}}h^{r_{w_i}}(g')^{r_{v_i}}\pmod n$

$N_i':=\zeta^{r_{0_i}+r_{1_i}2^{104}}\pmod\Gamma$

将$(T_{1_i}{}',T_{2_i}{}',N_i')$发送给其他签名者。

3)在收到来自其他签名者的上述参数后，每个 U_i 计算

$T_1':=\prod_{i=1}^{k}T'_{1_i}\pmod n$，$T'_2:=\prod_{i=1}^{k}T'_{2_i}\pmod n$

$N':=\prod_{i=1}^{k}N'_i\pmod\Gamma$

$c:=H(PK||T_1'||T_2'||N'||m)$

以及

$t_i=r_{e_i}+ce_i$，$s_{0_i}=r_{0_i}+cf_{0_i}$，$s_{1_i}=r_{1_i}+cf_{1_i}$

$s_{v_i}=r_{v_i}+cv_i$，$s_{w_i}=r_{w_i}+cw_i$，$s_{ew_i}=r_{ew_i}+ce_iw_i$；

将部分签名$(c,t_i,s_{0_i},s_{1_i},s_{v_i},s_{w_i},s_{ew_i},T_{1_i},T_{2_i},N_i)$提交给签名收集者 C。

4)C 计算

$s_0=\sum_{i=1}^{k}s_{0_i}$，$s_1=\sum_{i=1}^{k}s_{1_i}$，$s_v=\sum_{i=1}^{k}s_{v_i}$，$s_w=\sum_{i=1}^{k}s_{w_i}$

$s_{ew}=\sum_{i=1}^{k}s_{ew_i}$，$T_2=\prod_{i=1}^{k}T_{2_i}\pmod n$

最后输出多重签名

$\sigma:=\{PK||\zeta||k||c||s_0||s_1||s_v||s_w||s_{ew}||T_2||\langle N_i||T_{1_i}||t_i\rangle_k\}$

5)验证过程

签名验证者 V 计算

$$\begin{cases}T_1=\prod_{i=1}^{k}T_{1_i}^{t_i}\pmod n,N=\prod_{i=1}^{k}N_i\pmod\Gamma & (4.1)\\ T_1'=(Z^k)^{-c}T_1R_0^{s_0}R_1^{s_1}S^{s_v}h^{-s_{ew}}\pmod n & (4.2)\\ T_2'=T_2{}^{-c}g^{s_{ew}}h^{s_w}(g')^{s_v}\pmod n & (4.3)\\ N'=N^{-c}\zeta^{s_0+s_12^{104}}\pmod\Gamma & (4.4)\end{cases}\quad(4)$$

当且仅当 $c=H(PK||T_1'||T_2'||N'||m)$ 时，V 接受签名。

容易看出，来自合法签名者的多重签名可以通过验证。以式(4.2)为例，根据签名设置和 DAA 证书定义，易知

$Z=T_{1i}^{r_i}R_0^{f_{0_i}}R_1^{f_{1_i}}S^{v_i}h^{-e_iw_i}\pmod n$，则

$$(Z^k)^{-c}T_1R_0{}^{s_0}R_1{}^{s_1}S^{s_v}h^{-s_{ew}}$$
$$=(Z^k)^{-c}\prod_{i=1}^{k}(T_{1i}^{r_i}R_0^{s_{0_i}}R_1^{s_{1_i}}S^{s_{v_i}}h^{-s_{ew_i}})$$
$$=(Z^k)^{-c}\prod_{i=1}^{k}(T_{1i}^{r_{e_i}+\alpha_i}R_0^{r_{0_i}+cf_{0_i}}R_1^{r_{1_i}+cf_{1_i}}S^{r_{v_i}+cv_i}h^{-r_{ew_i}-\alpha_iw_i})$$
$$=(Z^k)^{-c}(Z^k)^c\prod_{i=1}^{k}(T_{1i}^{r_{e_i}}R_0^{r_{0_i}}R_1^{r_{1_i}}S^{r_{v_i}}h^{-r_{ew_i}})=T_1'\pmod n$$

4.2 安全及性能分析

改进方案的安全性基于以下假设[9]：

定义 1(强 RSA 假设) Flexible RSA 问题如下：给定一个 RSA 模数 n 及随机数 $z\in Z_n^*$，找出 r 和 y，使得 $y^r=z\pmod n$ 成立$(r>1,y\in Z_n^*)$。强 RSA 假设即是假定 Flexible RSA 问题是难于求解的。

引理 1 给定一个 RSA 模数 n 及随机数 $z\in Z_n^*$，$k<<n$，找出 k 组(y_i,r_i)，满足$\prod_{i=1}^{k}y_i^{r_i}=(\bmod n)$，$r_i>1,y_i\in Z_n^*$ 是困难的。

证明：假设可以找到这样的 k 组(y_i,r_i)，那么有

$y_1^{r_1}=z(\prod_{i=1}^{k-1}y_i^{r_i})^{-1}(\bmod n)$

由于 $z,(y_i,r_i)(1\leqslant i\leqslant k)$ 均为已知值，故对于 $z'=z(\prod_{i=1}^{k-1}y_i^{r_i})^{-1}(\bmod n)\in Z_n{}^*$，可找到$(y_1,r_1)$，使得 $y_1^{r_1}=z'(\bmod n)$，这解决了一个 Flexible RSA 问题，与强 RSA 假设产生矛盾。证毕。

定理 1 改进方案中多重签名不可伪造。

证明：首先，若攻击者 B 不知道签名者的 TPM 密钥 f_{0_i} 和 f_{1_i}，则无法伪造多重签名中的 s_0 和 s_1，因为 s_0 和 s_1 是关于 f_{0_i} 和 f_{1_i} 的 Schnorr 多重签名，而 Schnorr 多重签名是可证安全的。

其次，若 B 不知道与 f_{0_i} 和 f_{1_i} 对应的 DAA 证书(A_i,e_i,v_i)，则它无法伪造多重签名中的$\langle T_{1_i},t_i\rangle_k$。从上面的签名过程可知，假设 B 知道 f_{0_i} 和 f_{1_i}，它虽然可以类似 3.2 节中的攻击构造签名中除$\langle T_{1_i},t_i\rangle_k$ 以外的其他部分，并通过验证方程

组(4)中式(4.3)和式(4.4)的验证,但 B 要找到$\langle T_{1_i}, t_i\rangle_k$,并通过式(4.2)的验证则是困难的,因为根据式(4.2),有

$$\prod_{i=1}^{k} T_{1_i}^{t_i} = T_1'(Z^k)^c (R_0^{s_0} R_1^{s_1} S^{s_v} h^{-s_{ew}})^{-1} \pmod n$$

根据哈希函数的抗碰撞性,c 对应唯一的 T_1',而 c, s_0, s_1, s_v, s_{ew} 均已给定,故 $d = T_1'(Z^k)^c (R_0^{s_0} R_1^{s_1} S^{s_v} h^{-s_{ew}})^{-1} \pmod n$ 为给定值。因此如果 B 可找到$\langle T_{1_i}, t_i\rangle_k$,使得 $\prod_{i=1}^{k} T_{1_i}^{t_i} = d \pmod n$,则与引理 1 相矛盾。

综上,除非签名者的密钥和 DAA 证书同时泄漏,否则改进方案中多重签名不可伪造。证毕。

计算开销方面,基于离散对数的多重签名主要开销在于签名过程中的指数运算次数。假设共有 k 个签名者,则在原方案中共需进行 $16k+11$ 次指数运算,而在改进方案中需 $15k+10$次,因此性能也得以提高。特别是改进方案显著削减了签名收集者的运算开销(由原 $6k$ 次缩减为 0 次)。收集者通常会成为多重签名方案中的性能瓶颈,这一点对提高方案的效率有着实际意义。通信开销方面,改进方案较原方案增加了一轮签名者之间的交互,因此开销有所增加,之后的工作将就此方面做进一步优化。

结束语 本文对一种基于可信计算技术的多重签名方案进行了安全分析,表明其不能抵抗签名伪造攻击。分析了该安全缺陷产生的原因,并给出一种可证安全的改进方案。研究结果表明,对多重签名方案,对手的攻击手段往往更为多样,因此仅仅考虑部分签名的安全性是不够的,对于部分签名合成过程中可能存在的安全隐患也必须加以重视。

参 考 文 献

[1] Lu R B, He Dake, Wang C J. Security analysis and improvement of a new threshold multi-proxy multi-signature scheme [J]. Journal of Electronics, 2008, 25(3): 372-377

[2] Meng Tao, Zhang Xiao-ping, Yu Long-jiang, et al. An ID-Based Blind Multisignature Scheme [A]// Proc of the 3rd International Conference on Innovative Computing Information and Control [C]. Washington, USA: IEEE Computer Society, 2008: 556-568

[3] 王晓峰,张璟,王尚平. 多重数字签名及其安全性证明[J]. 计算机学报,2008,31(1):176-183

[4] Alexandra B, Craig D, O'Neil A. Ordered multisignatures and identity-based sequential aggregate signatures with applications to secure routing [A]// Proc of the 14th ACM Conference on Computer and Communications Security [C]. Alexandria, USA: ACM Press, 2007: 276-285

[5] Bellare M, Neven G. Multi-Signatures in the plain public key model and a general forking lemma [A]// Proc of the 13th ACM Conference on Computer and Communication Security [C]. Alexandria, USA: ACM Press, 2006: 390-399

[6] Hao Li-ming, Yang Shu-tang, Lu Song-nian, et al. Efficient and secure multiSignature scheme based on trusted computing [J]. Wuhan University Journal of Natural Sciences, 2008, 13(2): 180-184

[7] 张焕国,罗捷,金刚,等. 可信计算研究进展[J]. 武汉大学学报:理学版,2006,52(5):513-518

[8] Brickell E, Camenisch J, Chen Liqun. Direct anonymous attestation [A]// Proc of the 11th ACM Conference on Computer and Communication Security [C]. Washington, USA: ACM Press, 2004: 132-145

[9] Cramer R, Shoup V. Signature schemes based on the strong RSA assumption [J]. ACM Transactions on Information and System Security (ACM TISSEC), 2000, 3(3): 161-185

[10] Trusted Computing Group. TCG Specification Architecture Overview[EB/OL]. http://www.trustedcomputinggroup.org, 2009

[11] Camenisch J, Lysyanskaya A. A signature scheme with efficient protocols[J]. LNCS, 2003, 2576: 268-289

(上接第 57 页)

[6] Boneh D, Gentry C, Lynn B, et al. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps[C]// Proc. of the 22th Annual International Conference on the Theory and Applications of Cryptographic Techniques 2003. Berlin: Springer-Verlag, 2003: 416-432

[7] Xu Jing, Zhang Zhen-feng, Feng Deng-guo. ID-Based Aggregate Signatures from Bilinear Pairings[C]// Proc. of the Chinese-American Networking Symposium 2005. Berlin: Springer-Verlag, 2005: 110-119

[8] 程相国,刘景美,王新梅. m_挠群上一种基于身份的聚合签名方案[J]. 西安电子科技大学学报,2005,32(3):427-431

[9] Gentry C, Ramzan Z. Identity-based Aggregate Signatures[C]// Proc. of the 9th International Conference on Practice and Theory in Public Key Cryptography 2006. Berlin: Springer-Verlag, 2006: 257-273

[10] Sakai R, Ohgish K, Kasahara M. Cryptosystems Based on Pairing[C] //Proc. of 2000 Symposium on Cryptography and Information Security. Okinawa, Japan, 2000: 26-28

[11] Cheng Xiang-guo, Liu Jing-mei, Wang Xin-mei. Identity-Based Aggregate and Verifiably Encrypted Signatures from Bilinear Pairing[C] // Proc. of The 2005 International Conference on Computational Science and Applications. Berlin: Springer-Verlag, 2005: 1046-1054

[12] Mihara A, Tanaka K. Universal Designated-verifier Signature with Aggregation[C] // Proc. of the 2th International Conference In IT & Application 2005. Sydney, Australia, 2005, II: 514-519

[13] Gong Zheng, Long Yu, Hong Xuan, et al. Two Certificateless Aggregate Signatures From Bilinear Maps[C]// Proc. of the International Association for Computer and Information Science 2007. Toowoomba, Australia, 2007: 188-193

[14] Li Jin, Kim K, Zhang Fang-guo, et al. Aggregate Proxy Signature and Verifiably Encrypted Proxy Signature[C]// Proc. of International Conference on Provable Security 2007. Berlin: Springer-Veralg, 2007: 208-217

[15] Mu Yi, Susilo W, Zhu Hua-fei. Compact Sequential Aggregate Signatures[C]// Proc. of the 22th Annual ACM Symposium on Applied Computing. Seoul, Korea, 2007: 249-253

[16] Wen Yiling, Ma Jian-feng. An Aggregate Signature Scheme with Constant Pairing Operations[C]// Proc. of the 2008 International Conference on Computer Science and Software Engineering. 2008, 3: 830-833

[17] Zhang Fang-guo, Safavi-Naini R, Susilo W. An Efficient Signature Scheme from Bbilinear Pairings and Its Applications[C]// Proc. of the 7th International Conference on Practice and Theory in Public Key Cryptography 2004. Berlin: Springer-Veralg, 2004: 277-290