DOI:10.16707/j.cnki.fjpc.2017.06.001

隐私保护数字签名技术研究

康昌春
(山东省肿瘤防治研究院信息中心 山东 济南 250117)

【摘 要】在当前的电子商务环境下,用户隐私保护是任何应用系统都需要考虑的问题。这一问题的解决,要求使用现代密码学中的隐私保护数字签名技术。本文对三类典型的隐私保护的数字签名方案(群签名、盲签名、直接匿名证明)进行了研究,分析了这些方案的算法结构和设计过程。最后,指出了隐私保护数字签名领域的热点研究方向。

【关键词】隐私保护 数字签名 群签名 盲签名 直接匿名证明

1 引言

数字签名(Digital Signature)[1]是现代密码学研究的一个重要分支。数字签名可以理解为手写签名的电子版本:用户为消息 m 产生的数字签名是一个字符串,其值依赖于消息 m 和公共数据(具体涉及用户的私有数据以及随机选取的数据),使得任何人都能仅利用公开数据验证签名的有效性。具体地,在数字签名方案中,每个用户都公开一个公钥 pk,同时将对应的私钥 sk 保密。用户对消息 m 的签名 σ 是一个由消息 m,用户的公钥 pk 及私钥 sk 共同决定的值。同时,任何人都能够利用签名者的公钥 pk 对签名 σ 的有效性进行验证。然而,在不掌握签名者私钥 sk 的情况下,企图伪造签名的做法都是徒劳的。

然而,在 PKI(Public Key Infrastructure)环境下,用户的身份与公钥 pk 是直接绑定的。因此,标准数字签名方案的最大缺点是签名者无法对自己的身份进行隐藏。在电子商务环境下,为了保护签名者(或用户)隐私,需要为他们提供隐私性保护。为此,需要对标准的数字签名进行增强,从而得到许多满足特殊性质的数字签名方案。在当前的密码学研究中,能为用户提供隐私保护的特殊数字签名方案主要包括群签名、盲签名以及可信计算领域中的直接匿名证明方案。本文的研究目标是,对这些方案的特点、语法结构以及典型方案的具体设计进行研究,从而为今后构造安全性更强和效率更高的方案打下基础。

2 群签名技术

群签名(Group Signature)是一类特殊的数字签名技术。在群签名方案中,假设存在 3 类参与方,即群管理员(GM, Group Manager)、群用户(User)和打开权威(OA,Open Authority)。此类技术的设计动机在于,使得 User 能在不泄露身份的条件下代表整个群体进行签名。同时当发生争议时,可以由 GM 或者 OA 揭开签名者的身份。群签名的应用非常广泛,如可以构造电子现金系统[2]、匿名订购系统[3]和车联网系统[4]等。

群签名方案应当至少包含 5 个算法或协议,即 *Setup*,*Join*,*GSig*,*GVer*,*Open*。其中,*Setup* 算法由执行,用于产生必要的系统参数。*Join* 是一个在与间执行的交互式协议,该协议相当于用户的注册过程。*GSig* 是一个由任何 User 执行的算法。借助该算法,User 可以产生一个有效的群签名 σ。任何人都能通过执行 *GVer* 算法来检查给定群签名 σ 的有效性。*Open* 算法由 GM 或 OA 执行,该算法用于确定给定群签名的签名者身份。需要指出的是,有些群签名方案要求增加 *Judge* 算法,即要求 OA 通过 *Judge* 算法产生一个打开正确性证明 π。同时,仲裁机构负责利用 *Judge* 算法验证该证明是否有效。

在文献[5]中,Makita 等人提出一个支持用户灵活注册的群签名方案。与著名的 BBS(Boneh-Boyen-Shacham)群签名方案[6]相比,Makita 等人的方案不但在签名长度方面与前者相当,而且弥补了前者不允许动态申请注册的缺点。Makita 等人方案的主要过程如下:

1)在 *Setup* 算法中,GM 产生群公钥 (g_1,g_2,u,v,w,U,V) 和群私钥 (x,ξ_1,ξ_2)。同时,用户 User 借助 PKI 获得一个标准数字签名方案下的公钥 pk_i 和私钥 sk_i。

2)在 *Join* 协议中,User 选取随机数 $q_i\in Z^*_p$,计算 $B_i=g_2^{q_i}$。同时,利用 sk_i 产生对 B_i 的签名 Sig_i,并且向 GM 提供 (B_i,Sig)。若签名 Sig_i 有效,则 GM 选取随机数 $r_i,s_i\in Z^*_p$,计算 $A_i=\psi(Biuv^{s_i})^{\frac{1}{x+r_i}}$,并且向 User 返回群成员证书 (A_i,r_i,s_i)。此外,GM 需要将 User 的注册信息 (A_i,B_i,r_i,s_i,Sig) 保存在数据库 *Reg* 中。

3)在 *GSig* 算法中,User 选取随机数 $\alpha_1,\alpha_2,\beta\in Z_p$,并且计算 $\alpha=A_ig_1^{\alpha_1+\alpha_2}$,$b=(wg_2^{r})^{\beta}$,$c=(B_iuv^{s})^{\beta}b^{\alpha_1+\alpha_2}$,$d_1=\psi(U)^{\alpha_1}$,$d_2=\psi(V)^{\alpha_2}$。然后,产生知识签名 $\pi_1=SPK\{(\alpha_1,\alpha_2,\beta,\beta r_i,\beta q_i,\beta s):b=(wg_2^{r})^{\beta}\wedge c=(B_iuv^{s})^{\beta}b^{\alpha_1+\alpha_2}\wedge d_1=\psi(U)^{\alpha_1}\wedge d_2=\psi(V)^{\alpha_2}\}(m)$。最后,输出群签名 $\sigma=(a,b,c,d_1,d_2,\pi)$。

4)在 *GVer* 算法中,对于给定的消息 m 和群签名 $\sigma=(a,b,c,d_1,d_2,\pi)$,验证者验证是否满足 $e(a,b)=e(g_1,c)$。此外,还需验证知识签名 π_1 的有效性。若验证通过,则判定 σ 是有效的。

5)在 *Open* 算法中,对于给定的消息 m 和群签名 $\sigma=(a,b,c,d_1,d_2,\pi)$,*OA* 计算 $A_i=\psi(Biuv^{s})^{\frac{1}{x+r_i}}$,并且根据 A_i 在数据库 *Reg* 中找到用户注册时产生的数字签名 sig_i,进而确定用户的真实身份。此外,*OA* 产生证明 $\pi_2=SPK\{(\xi_1,\xi_2):A_i=\alpha/(d_1^{1/\xi_1}d_2^{1/\xi_2}),U=g_2^{\xi_1},V=g_2^{\xi_2}\}(\prime)$,并将 $\tau=(sig_i,B_i,A_i,r_i,s_i,\pi_2)$ 作为关于"打开操作满足正确性"的证明。

6)在 *Judge* 算法中,给定 *OA* 提供的证明 $\tau=(sig_i,B_i,A_i,r_i,s_i,\pi_2)$,仲裁机构验证是否满足 $e(A_i,wg_2^{r})=e(g_1,B_iuv^{s})$,$A_i=\alpha/(X_1X_2)$。此外,验证 π_2 是否有效。若上述验证通过,则判定 *OA* 执行的打开操作是正确的。

基金项目:国家高技术研究发展计划(863 计划)项目(编号:2015AA020106),山东省自然科学基金项目(编号:ZR2012HL09),山东省医药卫生科技发展计划项目(编号:2015WSA18068)。

3 盲签名技术

盲签名(Blind Signature)是一类特殊的数字签名方案。盲签名方案解决了这样一个现实问题，即允许 Bob 从签名者 Alice 那里得到一个对消息 m 的有效签名 $\sigma(m)$，同时不让她见到被签名的消息或自己产生的签名。今后，若 Alice 见到消息 m 及对其的签名 $\sigma(m)$，她能验证该签名的有效性，但无法将这个消息-签名对与导致该数对产生的签名协议的特定实例联系起来。目前，盲签名已经成为设计更为复杂的密码方案的基础，如构造电子选举系统[7]与车载网隐私保护方案[8]等。

盲签名方案是由以下的算法或协议构成的，即 *Gen*，*Issue*，*Verify*。其中，*Gen* 算法的作用是产生签名者的公钥 pk 和私钥 sk。*Issue* 是一个由用户和签名者执行的交互协议。在该协议中，用户首先向签名者提供经过盲化的消息 $\widetilde{m}$，后者返回对 $\widetilde{m}$ 的签名 $\sigma(\widetilde{m})$。最后，用户将 $\sigma(\widetilde{m})$ 还原为真正的签名 $\sigma(m)$。*Verify* 是标准的数字签名验证算法，用于验证用户所获的签名 $\sigma(m)$ 是否有效。

在文献[9]中，Abe 提出一个高效的盲签名方案，其显著特点是签名者可以以安全方式发布多项式数量的签名，且仅要求签名者和用户执行 3 次数据交换。假设用户的待签名消息为 m，该方案的 *Issue* 协议执行过程如下：

1) 签名者选取随机数 $rnd \in_R \{0,1\}^*$，计算 $z_1=H_2(rnd)$，$z_2=z/z_1$，其中 $H_1(\cdot)$ 表示散列函数。此外，签名者选取随机数 $u,s_1,s_2,d \in_R Z_q$，计算 $\alpha=g^u$，$b_1=g^{s_1}z_1^d$。随后，签名者向用户发送 rnd,a,b_1,b_2。

2) 用户验证 b_1,b_2 是否位于由 g 生成的群上。若是，则选取随机数 $\gamma,t_1,t_2,t_3,t_4,t_5,\tau \in_R Z_q$，并且计算 $z_1=H_1(rnd)$，$\zeta=z^\gamma$，$\zeta_1=z_1^\gamma$，$\zeta_2=\zeta/\zeta_1$，$\alpha=\alpha g^{t_1}y^{t_2}$，$\beta_1=b_1^\gamma g^{t_3}\zeta_1^{t_4}$，$\beta_2=b_2^\gamma h^{t_5}\zeta_2^{t_4}$，$\eta=z^\tau$，$\varepsilon=H_2(\zeta \| \zeta_1 \| \alpha \| \beta_1 \| \beta_2 \| \eta \| m)$，$e=\varepsilon-t_2-t_4 \bmod q$。接下来，用户向签名者发送 e。

3) 签名者计算 $c=e-d \bmod q$，$r=u-cx \bmod q$ 并且向用户返回 (r,c,s_1,s_2,d)。

4) 用户计算 $\rho=r+t_1 \bmod q$，$\omega=c+t_2 \bmod q$，$\sigma_1=\gamma s_1+t_3 \bmod q$，$\sigma_2=\gamma s_2+t_5 \bmod q$，$\delta=d+t_4 \bmod q$，$\mu=\tau-\delta\gamma \bmod q$，并且验证是否同时满足 $\omega+\delta=H_2(\zeta \| \zeta_1 \| g^\rho y^\omega \| g^{\sigma_1}\zeta_1^\delta \| h^{\sigma_2}\zeta_2^\delta \| z^\mu\zeta^\delta \| m) \bmod q$。若满足，则将 $(\zeta,\zeta_1,\rho,\omega,\sigma_1,\sigma_2,\delta,\mu)$ 作为所得到的签名。

4 直接匿名证明技术

直接匿名证明(DAA，Direct Anonymous Attestation)是一类特殊的数字签名方案，用于以合理方式实现用户隐私保护与签名者认证间的平衡。DAA 方案的参与方包括发布者、签名者以及验证者。负责验证签名者的合法性，并且为每个合法颁发惟一的 DAA 证书。通过提供 DAA 签名，可以向证明自己掌握合法的证书，且该签名不会泄露自己的真实身份。DAA 方案与群签名方案有着天然的“继承”关系，可以将 DAA 方案视为群签名方案的修改版本。与群签名方案不同，DAA 方案不支持“打开”操作，即使是在验证者与发布者合谋的情况下，由 DAA 签名者产生的签名仍然可以保持匿名。相反，DAA 方案满足用户受控制的可追踪性，即 DAA 签名者与验证者可以联合决定是否允许验证者在此后对由签名者产生的两个签名进行关联。

与其他类型的数字签名方案相比，DAA 方案的最大特点是将签名者的角色分为两个参与方，即资源受限的主要签名者(Trusted Platform Module)芯片以及拥有足够计算能力但是具有更低安全性容忍度的辅助签名者(Host)。仅仅是的协助者。不允许获得 DAA 私钥，也不允许它在不参与的条件下产生签名。此外，DAA 方案允许用户利用基本名(basename)控制所产生的签名是否能被关联。具体地，若签名者在签名过程中使用了非空的基本名，则所产生的签名满足可关联性。相反，若签名者希望保护隐私，他可以在签名过程中使用空的基本名。此时，所产生的签名是不可关联的。

DAA 方案是由 5 个算法或协议构成的，具体包括 *Setup*，*Join*，*Sign*，*Verify*，*Link*。其中，*Setup* 算法用于产生系统参数 par 和 Issur 的密钥对 (ipk,isk)。*Join* 是由 TPM，Host 与 Issur 执行的协议，目的是为用户的 TPM 私钥 tsk 产生成员证书 cre。在 *Sign* 算法中，TPM 与 Host 合作产生对消息 m 和基本名 $basename$ 的 DAA 签名 $\sigma(m \| basename)$。*Verify* 算法用于验证签名的有效性。*Link* 算法用于判定两个签名 $\sigma_1(m_1 \| basename)$，$\sigma_2(m_2 \| basename)$ 是否由同一个用户产生，条件是两个签名均能通过算法的验证，且 Signer 使用的 bsn 非空。

最近，Brickell 等人[10]提出一个高效的 DAA 方案，其特点是签名验证过程支持批验证，从而显著提高了验证过程的效率。假设待签名消息为，该方案的算法执行过程如下：

1) Verifier 向 Host 发送挑战 $n_V \in_R \{0,1\}^t$。

2) Host 将成员证书 $cre=(A,B,C,D)$ 随机化为 $cre'=(R,S,T,W)$ 的形式，即选取 $l \in Z_q$，设置 $cre'=(R,S,T,W)=(A_l,B_l,C_l,D)$。

3) 接下来的执行过程分为以下两个模式：

3.1) 模式 1 $basename \neq \perp$

在该模式下，Host 设置 $J=H_3(bsn)$。然后，Host 与 TPM 联合产生知识签名 $\pi=\mathrm{SPK}\{(f):W=S^f \wedge K=J^f\}(n_v)$，其中 f 表示 TPM 私钥。最后，Host 向 Verifier 发送 DAA 签名 $\sigma=(R,S,T,W,K,\pi)$。

3.2) 模式 1 $basename=\perp$

在该模式下，Host 与 TPM 联合产生知识签名 $\pi=\mathrm{SPK}\{(f):W=S^f\}(n_v)$。最后，Host 向 Verifier 发送 DAA 签名 $\sigma=(R,S,T,W,\pi)$。

5 结论

在隐私保护数字签名技术领域，尽管已经提出许多具有较好性质的方案，但是这些方案在不同程度上还存在缺陷。在群签名的研究方面，尚未解决的主要问题包括群签名的效率、安全、应用以及群成员废除问题等。在盲签名的研究方面，大多数方案的签名发布协议都要求执行 3 轮或更多的轮次，且通常要证明方案能在签名产生协议并发执行的条件下满足安全性质是困难的。值得注意的是，这个问题在仅需执行 2 轮(交互)的方案下可以得到避免。在 DAA 方案的研究方面，DAA 的安全模型还有待完善，针对 DAA 的安全部署以及应用拓展研究尚不充分，关于 DAA 的安全性扩展和增强还有待深入研究等。上述分析表明，隐私保护数字签名技术仍然是一个热门的研究方向，还具有很大的理论研究和应用开发价值。

参考文献：

[1] (美) J. Katz (著)，任伟 (译). 数字签名 [M]. 国防工业出版社, 2012

[2] 梁艳, 张筱, 郑志明. 基于无证书群签名方案的电子现金系统 [J]. 通信学报, 2016, 37(5): 184- 190.

[3] 柳欣, 徐秋亮, 张波. 满足可控关联性的合作群签名方案 [J]. 山东大学学报 (理学版), 2016, 51(9): 18- 35.

(下转第 19 页)

表 1　RRPP 环网设计

环网	名称	主控设备	主端口	副端口	控制 VLAN
主环	Ring 1	SA	Agg 2	Agg 1	4092
子环 1	Ring 2	SD	Agg 4	Agg 5	4093
子环 2	Ring 3	SD	Agg 6	Agg 5	4094

当环网链路出现故障后，如交换机 SA 和 SB 之间的链路中断了，两台设备立即发送“Link- Down”报文，Master 设备收到“Link- Down”报文后，立即恢复副端口的数据 VLAN 转发，并同时所有节点，整个故障收敛时间会控制在毫秒级。

2.2 RPP 环网优化实现

RRPP 协议的配置方法如下：

(1)定义数据 VLAN 100、101 的方法

[H3C] vlan 100 to 101　//创建 vlan 100、101

[H3C] stp region-configuration　//定义 MST 域

[H3C-mst-region] instance 1 vlan 100 to 101//定义 instance 1

[H3C-mst-region] active region-configuration//激活 MST 域

[H3C-mst-region] quit

(2)定义 RRPP 域的方法

[H3C] rrpp domain 1//定义 RRPP 域 1

[H3C-rrpp-domain1] control-vlan 4092　//定义控制 VLAN 4092

[H3C-rrpp-domain1] protected-vlan reference-instance 1　//将 MST 1 所包含的 VLAN 定义为保护 VLAN

(3) 定义主环 Ring 1 主设备的方法

[H3C-rrpp-domain1] ring 1 node-mode master primary-port agg 2 secondary-port agg 1 level 0　//将 Agg2、Agg1 分别定义为主、副端口

[H3C-rrpp-domain1] ring 1 enable//激活该环

(4) 关闭 STP 协议

[H3C] int GigabitEthernet 1/0/1

[H3C-GigabitEthernet1/0/1] undo stp enable　//关闭 STP 协议

[H3C-GigabitEthernet1/0/1] qos trust dot1p//信任报文 802.1p

[H3C-GigabitEthernet1/0/1] undo link-delay　//关闭端口抑制时间

2.3 测试数据

在实验环境中，先后模拟 1000 用户同时在线，设备宕机、物理端口出现故障或者通信链路断开后，最快收敛时间是 36ms，最慢收敛时间是 202ms，收敛时间控制在毫秒级，完全达到了用户对于网络的高性能要求。表 2 为部分测试数据。

表 2　测试数据

步骤	描述	故障点	收敛时间 (ms)
1	设备宕机	设备 SA	202
2		设备 SB	112
3		设备 SC	146
4		设备 SD	40
5	物理端口故障	设备 SA.Agg2	67
6		设备 SB.Agg5	126
7		设备 SD.Agg5	52
8	通信链路断开	设备 SA 与 SB 直连链路	66
9		设备 SB 与 SC 直连链路	75
10		设备 SB 与 SD 直连链路	130

结语

技术的发展瞬息万变，现实中已有大量“云计算”的应用，用户对网络的可靠性、稳定性提出了更高的要求，MSTP 固然可以解决交换环路问题，但收敛时间过长，用户体验不好，使用 RRPP 优化后，收敛速度大幅提高，由数秒级的收敛速度提升到毫秒级，大大提升了网络的质量。

参考文献：

[1] 金海峰. 核心虚拟化技术在私有云平台架构中的应用研究 [J]. 湖南工业职业技术学院学报, 2016, 16(3): 10- 10

[2] 杭州华三通信技术有限公司. H3C S5820X&S5800 系列以太网交换机配置指导 [EB/OL]. www.h3c.com.cn.

作者简介：

金海峰 (197902)，男 (汉族)，江苏如皋人，讲师，大学本科，主要研究方向为云计算及教育教学改革。

(上接第 2 页)

[4] 赵臻, 陈杰, 张跃宇, 等. VANET 中高效撤销的批量验证群签名方案 [J]. 密码学报, 2016, 3(3): 292- 306.

[5] Makita T, Manabe Y, Okamoto T. Short group signatures with efficient flexible join [C] //Proc of SCIS 2006. 2006: 1- 6.

[6] Boneh D, Boyen X,Shacham H. Short group signatures [C] //Proc of CRYPTO 2004, LNCS 3152, Berlin: Springer- Verlag, 2004: 41- 55.

[7] 张碧军, 何明星. 一个基于代理盲签名的电子选举方案 [J]. 西华大学学报 (自然科学版), 2013, 32(4): 10- 13.

[8] 王晓亮, 黎水凡. FBSS: 一种基于公平盲签名和秘密共享的车载网隐私保护方案 [J]. 计算机应用研究, 2016, 33(12): 3780- 3784.

[9] Abe M. A secure three- move blind signature scheme for polynomially many signatures [C] //Proc of EUROCRYPT 2001. LNCS 2045, Berlin: Springer- Verlag, 2001: 136- 151.

[10] Brickell E, Chen L, Li J. A (corrected) DAA scheme using batch proof and verification [C] //Proc of INTRUST 2011. LNCS 7222, Berlin: Springer- Verlag, 2012: 304- 337.

作者简介：

康昌春 (1976-)，男，汉族，山东济南人，工程师，工学学士，主要研究方向为网络与信息安全。