

引用格式:胡如会,张起荣,贺道德.基于双线性映射直接匿名认证方案的改进[J].科学技术与工程,2018;18(3):264—267

Hu Ruhui, Zhang Qirong, He Daode. Improvement of direct anonymous attestation protocol based on bilinear maps[J]. Science Technology and Engineering, 2018; 18(3): 264—267

基于双线性映射直接匿名认证方案的改进

胡如会 张起荣 贺道德

(贵州工程应用技术学院信息工程学院,毕节 551700)

摘要 针对目前可信计算中直接匿名认证(DAA)方案存在协议交互流程繁琐、计算量大的问题,提出了一种直接匿名认证方案IMP-DAA。以椭圆曲线上的双线性映射为理论依据,以 q -SDH困难假设为安全基础,简化了协议交互流程;在保证可信计算平台安全的前提下,降低了各参与方的计算量;并从安全性和有效性两个方面进行了分析。

关键词 可信计算 双线性映射 q -SDH 假设 直接匿名认证

中图法分类号 TP309.2; **文献标志码** A

在互联网大数据时代,网络安全和个人隐私泄露的问题越来越严重。可信计算是实现网络安全和隐私保护最有效的手段之一,其核心技术是对TPM(trusted platform module)身份的直接匿名认证。最初由可信计算联盟(trusted computing group, TCG)提出的直接匿名认证是基于RSA的DAA^[1]方案;但其认证过程复杂,并且计算量和通信开销较高,限制了其更广泛的应用。后人在RSA-DAA基础上提出了基于椭圆曲线双线性映射的直接匿名认证ECC-DAA^[2]方案;该方案较RSA-DAA方案更加简化,计算效率更高^[3]。在ECC-DAA被首次提出后,出现了一系列的改进方案^[4—6],这些方案都保留了原DAA方案的基本流程,都是用双线性映射代替RSA指数运算来降低计算量,性能上虽有所提高;但在匿名认证过程中仍存在以下不足:加入协议和签名协议阶段的消息交互流程描述复杂;各参与方的计算量较大,有待进一步改进。针对上述不足,提出了以 q -SDH假设为安全基础的基于双线性映射的IMP-DAA认证方案。该方案仍属于ECC-DAA类认证方案,但与文献[4—6]中的方案相比,该方案在加入协议和签名协议阶段的消息交互流程更简化、更清晰,涉及到的主要运算是椭圆曲线上点的指数运算和双线性映射运算,在保证可信计算平台安全的前提下,进一步降低了计算复杂度,减少了各参与方

的计算量,使得总性能有所提高。

1 相关知识

1.1 双线性映射^[7,8]

G_1 、 G_2 和 G_T 是素数 p 阶的循环群, G_1 和 G_2 是加法群, g_1 和 g_2 分别是 G_1 和 G_2 的生成元, G_T 是乘法群,假设 G_1 、 G_2 、 G_T 中的离散对数都是困难的。如果一个二元函数 $e: G_1 \times G_2 \rightarrow G_T$ 满足以下条件:

- (1) 双线性:对于 $\forall u \in G_1$, $\forall v \in G_2$, $\forall a$, $b \in \mathbf{Z}_p$, 都有 $e(au, bv) = e(u, v)^{ab}$ 。
- (2) 非退化性: $e(g_1, g_2) \neq 1$ 。
- (3) 可计算性:对于 $\forall u \in G_1$, $\forall v \in G_2$, 存在 $e(u, v)$ 的有效算法。

则称 $e: G_1 \times G_2 \rightarrow G_T$ 是一个双线性映射。

1.2 q -SDH 假设^[9,10]

G_1 和 G_2 是素数 p 阶的循环群, g_1 和 g_2 分别是 G_1 和 G_2 的生成元, A 是任意 q -SDH 假设在 (G_1, G_2) 中成立的概率多项式时间算法。以 $(g_1, g_2, g_2^\gamma, g_2^{\gamma^2}, \dots, g_2^{\gamma^q})$ 作为算法 A 的输入,以 $(g_1^{1/(\gamma+x)}, x)$ 作为输出,其中 x 和 $\gamma \in \mathbf{Z}_p$, 若概率 $P_r[A(g_1, g_2, g_2^\gamma, g_2^{\gamma^2}, \dots, g_2^{\gamma^q}) = (g_1^{1/(\gamma+x)}, x)] \geq \varepsilon$, 则称算法 A 以不小于 ε 的概率优势解决了 q -SDH 问题。若 ε 可忽略,则称 q -SDH 问题是难解的。

2 IMP-DAA 方案

IMP-DAA 方案包括 TPM、Host(TPM 所在的主机)、Issuer(发布者)和 Verifier(验证者)四个参与方,分为初始化设置、加入(Join)协议、签名(Sign)协议和签名验证(Verify)四个阶段。

2017 年 6 月 30 日收到

贵州省科技厅联合基金
(黔科合 J 字 LKB[2013]14 号)和毕节市科技局

基金(毕科合字[2014]30 号)资助
第一作者简介:胡如会(1978—),女,硕士,副教授。研究方向:信息安全。E-mail:243845783@qq.com。

2.1 初始化设置

初始化设置阶段 Issuer 建立参数并产生公、私钥对。设置阶为素数 p 的双线性映射关系 $e: G_1 \times G_2 \rightarrow G_T$, g_1, g_2 分别是 G_1, G_2 的生成元;随机选择 $x \in \mathbf{Z}_p$ 作为私钥 k_s , 计算 $X = g_2^x$; 设置 Hash 函数的输出长度为 $l_H = 256$, 设置 5 个抗碰撞安全的 Hash 函数:

$$H_1, H_2, H_4, H_5 : \{0,1\}^* \rightarrow \mathbf{Z}_p;$$

$$H_3 : \{0,1\}^* \rightarrow G_1.$$

最后由 Issuer 发布公钥 k_p 和私钥 k_s :

$$\begin{aligned} k_p &: \{G_1, G_2, G_T, p, e, g_1, g_2, X, H_1, H_2, H_3, H_4, \\ &H_5\}; \\ k_s &: x. \end{aligned}$$

2.2 加入协议

加入协议阶段是 TPM 申请 DAA 证书的过程, 主要涉及 TPM、Host 和 Issuer 三个参与方。假定 Issuer 与签名者(即 TPM 和 Host)通过背书密钥(EK)已经建立了认证通道, 假定 Issuer 在初始化设置阶段产生的公钥 k_p 公开并被终端平台 Host 获取, 令 K 为 Issuer 的长期公钥并作为公钥 k_p 的认证, 令 DAAseed 为 TPM 内部密钥种子, cnt 作为跟踪 TPM 执行加入协议次数的计数器。加入协议的消息交互流程如图 1 所示。

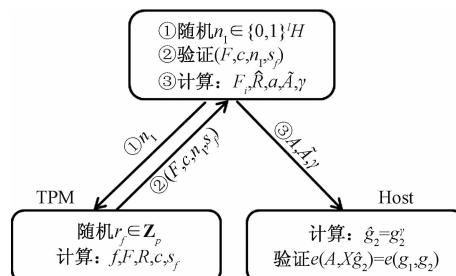


图 1 加入协议消息交互流程图

Fig. 1 Flow chart of join protocol message interaction

由图 1 可知, 加入协议阶段的消息交互流程较目前 DAA 方案的流程更简化。Issuer 选择随机数 n_1 发给 TPM; TPM 计算 $f: = H_1(\text{DAAseed} \parallel \text{cnt} \parallel K)$, 将 f 作为 TPM 的隐私密钥, TPM 选择随机数 r_f , 计算 $F: = g_1^{r_f}$, $R: = g_1^{r_f}$, $c: = H_2(k_p \parallel n_1 \parallel F \parallel R)$, $s_f: = r_f + cf \pmod{p}$, 并将 (F, c, n_1, s_f) 发送给 Issuer。Issuer 收到 (F, c, n_1, s_f) 后, 首先验证 n_1 是否与①发送的 n_1 相同, 通过检测 F 判断该 TPM 是否为恶意平台, 然后计算 $R: = g_1^{r_f} \cdot F^{-c}$, 验证 $c: = H_2(k_p \parallel n_1 \parallel F \parallel R)$ 是否成立, 选择随机数 $\gamma \in \mathbf{Z}_p$, 计算 $A: = g_1^{1/(γ+x)}$, $\tilde{X}: = F^{1/(γ+x)}$, 最后将 (A, \tilde{X}, γ) 作为 TPM 申请到的 DAA 证书发给 Host。在 Issuer 对 (F, c, n_1, s_f) 的验证中, 如果 n_1 不

相同或 TPM 是恶意平台或 $c: = H_2(k_p \parallel n_1 \parallel F \parallel R)$ 不成立, 系统将终止协议, 否则执行③。Host 收到 (A, \tilde{X}, γ) 后, 计算 $\hat{g}_2: = g_2^\gamma$, 并验证 $e(A, X \hat{g}_2) = e(g_1, g_2)$ 是否成立, 如果验证失败, 终止协议; 否则, 进入下一个流程, 即签名协议。

2.3 签名协议

签名协议阶段是 TPM 用 DAA 证书对传送信息进行签名的过程, 只有通过签名操作, 平台才能向验证者匿名的证明自己可信, 该过程主要涉及 TPM 和 Host 两个参与方。令 m 为需要签名的信息, bsn 为签名者(主机 Host)基名, n_v 是 Host 获取的一个随机数, TPM 拥有隐私密钥 f , Host 拥有 DAA 证书 (A, \tilde{X}, γ) 和 \hat{g}_2 , 签名协议消息交互流程如图 2 所示。

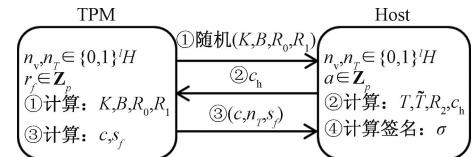


图 2 签名协议消息交互流程图

Fig. 2 Flow chart of signature protocol message interaction

由图 2 可知, TPM 计算 $B: = H_3(bsn)$, 选择随机数 r_f , 计算 $K: = B^r$, $R_0: = g_1^{r_f}$, $R_1: = B^{r_f}$, 然后将 (K, B, R_0, R_1) 发送给 Host; Host 选择随机数 a , 计算 $T: = A^a$, $\tilde{T}: = X^a$, $R_2: = e(R_0, g_2)^a$, c_h 为盲化后的 DAA 证书, 计算 $c_h: = H_4(k_p \parallel B \parallel K \parallel T \parallel \tilde{T} \parallel \hat{g}_2 \parallel R_1 \parallel R_2 \parallel n_v)$, Host 将 c_h 发送给 TPM; TPM 选择随机数 n_r , 计算 $c: = H_5(c_h \parallel n_r \parallel m)$, $s_f: = r_f + f$, 将 (c, n_r, s_f) 发送给 Host; Host 计算 $\sigma: = (B, K, T, \tilde{T}, \hat{g}_2, c, n_r, s_f)$, σ 即为信息 m 的签名。

本方案在签名协议阶段的计算中引入公开参数 H_3, H_4 和 H_5 , 不仅减少了计算量, 还增强了签名协议阶段平台的匿名性和安全性。

2.4 签名验证

签名验证阶段是由 Verifier 利用已知参数验证签名 σ 的合法性。Verifier 首先检测所有的 $f' \in RL$, 是否存在 $K = B^{r_f}$, 若存在, 则该平台为恶意 TPM, 终止验证; 否则验证 $B, K, T \in G_1$ 和 $s_f \in \mathbf{Z}_p$ 是否成立, 若成立则计算 $R_1: = B^{s_f} \cdot K^{-c}$, $R_2: = e(T^{r_f} \cdot \tilde{T}^{-c}, X \hat{g}_2)$, $c': = H_5(H_4(k_p \parallel B \parallel K \parallel T \parallel \tilde{T} \parallel \hat{g}_2 \parallel R_1 \parallel R_2 \parallel n_v) \parallel n_r \parallel m)$, 并验证 $c = c'$ 是否成立, 如果均成立, 则验证通过。只有上述验证均通过才能证明 Host 发来的签名 σ 合法, 验证者才可确认该平台确有 Issuer 为其颁发的 DAA 证书, 从而确定该平台可信。

IMP-DAA 方案在保证安全的前提下, 不但使加

入协议和签名协议的交互流程更简化、更清晰,而且降低了加入协议、签名协议和签名验证各阶段中各参与方的计算量。

3 IMP-DAA 方案的性能分析

在直接匿名认证方案中,安全性和有效性是衡量其性能的重要指标。

3.1 安全性分析

IMP-DAA 方案是以双线性映射为工具,以 q-SDH 困难假设为安全基础,以椭圆曲线密码算法的不可攻击性作为安全保障。该方案的安全性分析主要包括^[11]防恶意 TPM 欺骗性、平台匿名性和签名不可伪造性三个方面。

3.1.1 防恶意 TPM 欺骗性

在加入协议阶段,TPM 将 $F := g_1^f$ 发送给 Issuer 后,Issuer 利用恶意 TPM 列表 RL 中所有的 f_i 检测是否存在 $F := F_i$,判断该 TPM 是否是一个恶意的 TPM。在签名验证阶段,Verifier 收到签名 σ 后,首先检测所有的 $f' \in RL$,是否存在 $K = B'$,从而判断该 TPM 是否是一个恶意的 TPM。通过上述方法,IMP-DAA 方案在加入协议和签名验证两个阶段都能有效地阻止恶意 TPM 的攻击。

3.1.2 平台匿名性

在签名协议阶段,Host 先将 Issuer 发送的信任证书 (A, \bar{X}, γ) 盲化,然后将其与需要签名的信息 m 计算成签名 σ 后发送给 Verifier,使得 Verifier 和 Issuer 之间不存在相同的信息,即使 Verifier 和 Issuer 合谋也无法识别出具体的 TPM,防止了 Issuer 和 Verifier 的合谋攻击,实现了平台的匿名性,保证了平台的隐私性。

3.1.3 签名不可伪造性

在加入协议阶段,Issuer 在生成 DAA 证书时需要计算 A 和 \bar{X} ,计算过程中使用了 Issuer 的私钥 x ,Host 接收到 DAA 证书 (A, \bar{X}, γ) 后,计算 $\hat{g}_2 := g_2^\gamma$,并用公共参数 X 验证 $e(A, X\hat{g}_2) = e(g_1, g_2)$ 是否成立,进而确定 Issuer 是否伪造了 DAA 证书。在签名协议阶段,可信计算平台(TPM 和 Host)对 Issuer 发来的 DAA 证书进行盲化,并生成自己的签名。在签名验证阶段通过相关验证来证明该可信计算平台确有 Issuer 为其颁发的 DAA 证书,使得签名具有不可伪造性。

3.2 有效性分析

由于在整个认证过程中指数运算和双线性映射运算是最耗时的运算,所以将根据方案中各参与方用到的指数运算和双线性映射运算来衡量 DAA 方案的计算效率,即有效性分析。

通过与文献[4]中的 SC-DAA 方案、文献[5]中的 I-DAA 方案和文献[6]中的 TMZ-DAA 方案进行比较来分析 IMP-DAA 方案的效率,如表 1 所示。

表 1 IMP-DAA 方案与部分已有方案的比较

Table 1 Comparison of IMP-DAA with other existed schemes

方案	阶段	参与方	运算量
SC-DAA	Join	TPM	$3 G_1$
		Host	$G_1 + 2P$
		Issuer	$2 G_1 + n G_1 + G_1^2$
	Sign	TPM	$3 G_1$
		Host	$3 G_1 + G_T + P$
	Verify	Verifier	$2 G_1 + G_1^2 + 2P + n G_1$
I-DAA	Join	TPM	G_1
		Host	$2P$
		Issuer	$n G_1 + G_1^2$
	Sign	TPM	$G_1 + G_T$
		Host	$4 G_1$
	Verify	Verifier	$G_1^2 + G_2^2 + 4P + n G_1$
TMZ-DAA	Join	TPM	$4 G_1$
		Host	0
		Issuer	$2 G_1^2$
	Sign	TPM	$3 G_1$
		Host	$2 G_1$
	Verify	Verifier	$2 G_1^2 + n G_1$
IMP-DAA	Join	TPM	$3 G_1$
		Host	$G_1 + 2P$
		Issuer	$n G_1 + G_1^2$
	Sign	TPM	G_1
		Host	$4 G_1$
	Verify	Verifier	$G_1^2 + 2P + n G_1$

在表 1 中,主要对 DAA 方案在加入协议、签名协议和签名验证三个阶段中各参与方的计算量进行比较,不包括初始化设置阶段的计算量,因为各参数的初始化在整个执行过程中只运行一次,初始化算法所需的计算费用不高^[4]。为了便于比较,将运算符号化,约定:群 G_1 、 G_2 、 G_T 表示 1 指数运算, G_i^m ($i = 1, 2, T; m \in \mathbb{N}^*$) 表示群 G_i 的 m 指数运算, P 表示双线性映射运算, n 表示恶意 TPM 列表中的密钥个数。

由表 1 可以看出,IMP-DAA 方案在三个阶段各参与方的计算量都明显优于 SC-DAA 方案;与 I-DAA 方案比较,在 Join 协议中,该方案运算量没有减少,但在 Sign 协议中,I-DAA 方案中的 TPM 多了一次 G_T 运算,通常情况下, G_T 运算量是 G_1 的 4 倍^[4];与 TMZ-DAA 方案比较,在 Join 阶段和 Verify 阶段的运算量也有明显降低。综合考虑,该方案降低了各参与方的计算量,在效率上较文献[4—6]中的各方案有所改进。

4 结束语

直接匿名认证是可信计算平台必备的重要功能之一,面对目前复杂的网络环境中不断涌现的各种攻击手段,提高直接匿名认证方案的效率具有重要意义^[12]。针对现有 DAA 方案存在的不足,提出了以 q -SDH 假设为安全基础的基于双线性映射的 DAA 认证方案。TPM 获得 DAA 证书后通过平台验证其合法性来防止恶意 TPM 欺骗,针对可能发生的攻击则采取在计算时加入随机数来进行保障。该方案中涉及到的主要运算是椭圆曲线上点的指数运算和双线性映射运算,有效降低了认证各阶段中各参与方的计算量,在保证安全的前提下,不仅使加入协议和签名协议的交互流程更简化,也为大数据时代下的网络安全和个人隐私提供了可行的保护措施。

参 考 文 献

- 1 Brickell E, Camenisch J, Chen Liqun. Direct anonymous attestation. Proc of the 11th ACM Conf on Computer and Communications Security. New York: ACM, 2004: 132—145
- 2 Ernie B, chen Liqun, Li Jiangtao. A new direct anonymous attestation scheme from bilinear maps. 1 st International Conference on Trusted Computing and Trust in Information Technologies (TRUST 2008). VillachAustria, Germany: Springer, 2008: 166—178
- 3 Chen Liqun, Morrissey P, Smart N P. Pairings in trusted computing. 2nd International Conference on Pairing-Based Cryptography. London, Germany: Springer, 2008; 1—17
- 4 宋成,孙宇琼,彭维平,等.改进的直接匿名认证方案.北京邮电大学学报,2011;34(3): 62—65
Song Cheng, Sun Yuqiong, Peng Weiping, et al. Improved direct anonymous attestation scheme. Journal of Beijing University of Posts and Telecommunications, 2011;34(3): 62—65
- 5 陈立全,何营营,王玲玲. M2M 网络上的改进直接匿名认证方案.东南大学学报(自然科学版),2012;42(4): 604—608
Chen Liqun, He Yingying, Wang Lingling. Improved direct anonymous attestation scheme in M2M network system. Journal of Southeast University (Natural Science Edition),2012; 42 (4): 604—608
- 6 谭良,孟伟明,周明天.一种优化的直接匿名证言协议方案.计算机研究与发展,2014; 51(2): 334—343
Tan Liang, Meng Weiming, Zhou Mingtian. An improved direct anonymous attestation scheme. Computer Research & Development, 2014; 51 (2): 334—343
- 7 Chen Liqun. A DAA scheme using batch proof and verification. 3rd International Conference on Trust and Trustworthy Computing. Berlin, Germany: 2010: 166—180
- 8 Okamoto T. Cryptography based on bilinear maps. 16th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Las Vegas, Germany: Springer, 2006: 35—50
- 9 Chen Liqun, Page D, Smart N P. On the design and implementation of an efficient DAA scheme. 9th IFIP International Conference on Smart Card Research and Advanced Application. Passau, Germany: Springer, 2010: 223—237
- 10 陈小峰,冯登国.一种基于双线性映射的直接匿名证明方案.软件学报,2010;21(8):2070—2078
Chen X F, Feng D G. Direct anonymous attestation based on bilinear maps. Journal of Software, 2010;21(8):2070—2078
- 11 Ernie B, LiJiangtao. A pairing-based DAA scheme further reducing TPM resources. 3rd International Conference on Trust and Trustworthy Computing. Berlin, Germany: Springer, 2010: 181—195
- 12 林国勇,黄帆.一种用于云计算的数据容灾分配算法的改进.科学技术与工程,2017; 17(1): 260—264
Lin Guoyong, Huang Fan. An improved data disaster allocation algorithm for cloud computing. Science Technologyand Engineering, 2017; 17 (1): 260—264

Improvement of Direct Anonymous Attestation Protocol Based on Bilinear Maps

HU Ru-hui, ZHANG Qi-rong, HE Dao-de

(School of Information Engineering, Guizhou University of Engineering Science, Bijie 551700, China)

[Abstract] A direct anonymous attestation scheme IMP-DAA is proposed to solve the problems, which are cumbersome protocol interaction process and large amount of calculation. The scheme is based on the theory of elliptic curve bilinear maps and the safety of q -SDH difficult assumption, and the protocol interaction process is simplified. The scheme is analyzed from the security and effectiveness, and not only remains security but also reduces the computation cost of the parties.

[Key words] trusted computing bilinear map q -SDH assumption direct anonymous attestation (DAA)