一种基于标准模型的盲签名方案

左黎明，张婷婷*，陈祚松，周 庆，王 露

（华东交通大学 理学院，江西 南昌 330013）

摘 要： 信号检测系统中，各检测终端和传感器收集信号的传输安全性和可靠性至关重要，将标准模型盲签名方案用于树莓派的数据传输及认证服务，能很好的保护消息的安全性。针对现有方案签名请求者信息被篡改的问题，提出了一种盲签名方案，并在标准模型下，证明了方案对自适应选择消息和假定敌手攻击是存在性不可伪造的。由于方案设计过程中采用了标准模型的框架，实用性强。

关键词： 盲签名；标准模型；双线性映射

中图分类号： TP309 **文献标识码：** A **文章编号：** 1671 - 380X（2017）09 - 0001 - 04

A Blind Scheme Based on *Stan*dard Model

ZUO Li - ming，ZHANG Ting - ting*，CHEN Zuo - song，ZHOU Qing，WANG Lu

（*School of Basic Science*，*East China Jiaotong University*，*Nanchang* 330013，*China*）

Abstract: It is crucial to enhance reliability and *sec*urity of the detection terminal or transmission of signals collected by the sensors in signal detection system. The Blind Scheme Based on S*tan*dard Model is used for the data transmission and authentication service of raspberry faction. A blind scheme based on s*tan*dard model and a new adversary model are proposed. The proposed scheme is provably unforgeable in the s*tan*dard model under adaptive chosen - message attack or adversary assumption attack. The scheme is practicality as it is designed u*sin*g the framework of s*tan*dard model.

Key words: blind signature; s*tan*dard model; bi - linear map

盲签名方案于 1982 年被 Chaum[1] 提出，它是一种具有附加性质的数字签名，主要应用背景于电子现金交易，现已提出多种盲签名方案[2-4]。目前，大多数的盲签名方案都是基于随机预言机模型的，但是随机预言机模型的假想环境在现实生活中很难实现。随后，Waters 签名方案被提出并进行研究，基于 Waters 方案的 Okamoto 方案在方案的传输、消息盲化和去盲等方面都比较成功，不足的是此方案存在计算复杂和传输消息较长的缺陷[5]。基于对盲签名方案安全性、算法效率及计算复杂性的考虑，它的构造变得越来越复杂，如文献[6-7]。如何节省传输带宽、提高运算效率需要进一步研究。

近几年，大部分学者主要研究的仍是基于随机预言机模型的签名方案，Waters 签名方案被提出后，部分学者开始研究基于标准模型的签名方案[8-10]。考虑到随机预言机模型在实际应用中的不安全因素以及现有方案效率低的问题，本文提出的方案基于标准模型，进行完整的安全性分析与证明。树莓派又称卡片式电脑，外形只有信用卡大小，却具有电脑的所有基本功能，方案处理过程

收稿日期： 2017 - 05 - 27

基金项目： 国家自然科学基金项目（11361024，11261019），江西省自然科学基金项目（2015BAB201002，2017BAB201009），江西省研究生创新专项资金项目（YC2016 - S264）。

作者简介： 左黎明（1981 - ），男，江西鹰潭人，副教授，硕士，CCF 会员（会员号：E20 - 0013632M），研究方向：信息安全、非线性系统。

* 通讯作者：张婷婷（1991 - ），女，河南濮阳人，硕士研究生，研究方向：信息安全。

中，树莓派扮演服务器的作用，将传感器或其他服务器端收集到的数据应用盲签名方案协议传输给树莓派，树莓派与传感器对数据进行解析与相互认证，可抵抗网络攻击，较好地保护消息的完整性及安全性。

1　基础知识

1.1　*Diffie – Hellman* 问题[11]：

给定一个素数 p，Z_P^* 的一个生成元 α 及元素 $\alpha^a \bmod p$ 和 $\alpha^b \bmod p$，求 $\alpha^{ab} \bmod p$ 是困难的。

1.2　双线性映射

假设 g 是加法循环群 G 的一个生成元，且 $ord(G) = p$，G_1 为阶为 p 的乘法循环群。若满足 $\forall u,v \in G$ 和 $a,b \in \{0,\cdots,p-1\}$，均有 $e(u^a,v^b) = e(u,v)^{ab}$ 且 $e(g,g) \neq 1$，则 $e: G \times G \to G_1$ 即为双线性的。

1.3　盲签名的定义

盲签名。盲签名方案一般包括：签名者 S、用户 U 以及一组多项式时间算法（KeyGen，Sign，Verify）。

1）KeyGen 为密钥生成算法，输入安全参数 1^k，输出系统参数 Params 和 KeyGen 生成的公私钥对 (pk,sk)。

2）Sign 此为概率多项式时间交互式协议，输入系统参数和公钥 pk，用户 U 先对消息 m 进行盲化，再将盲化后的消息 m' 传给 S。S 秘密输入签名者私钥 sk，若协议在多项式时间内停止，算法 Sign 输出签名 $\sigma(m)$ 或 fail。

3）Verify 这也是多项式时间算法，其以 Params、pk、m 和 $\sigma(m)$ 为输入，若 $\sigma(m)$ 是消息 m 的签名，它输出 true，否则输出 false。

2　标准模型下的盲签名方案

本文提出的盲签名方案基于标准模型。该方案建立在 Waters 标准方案[12]的基础上，假设被签名消息可由 n_m 长的比特字符串表示，$H: \{0,1\}^* \to \{0,1\}^{n_m}$ 是一个抗碰撞的哈希函数。该签名方案主要由三个算法组成[13]。

系统参数产生：设 G_1 为阶数为 q 的加法循环群，G_2 为阶数同为 q 的乘法循环群，g 是 G_1 的生成元，选择一个双线性映射：$e: G_1 \times G_1 \to G_2$。对 $\forall a \in \mathbf{Z}_q^*$，从 G_1 中选择 $n_m + 2$ 个数 $(g_2,u',u_1,\cdots,u_{n_m})$。假设公钥为 $pk = g_1 = g^a$，私钥 $sk = a$，公开系统参数 $Params = (G_1,G_2,e,pk,g_2,u',u_1,\cdots,u_{n_m})$，秘密保存 a。

签名：输入公共安全参数 1^k，公共参数 $Params$。S 秘密输入其私钥 a，U 以秘密的方式输入待签名消息 m。该协议分为三个子协议：

i）盲化：用户输入待签名消息 m 对应的值 ω，$\omega = u' \prod_{i \in U} u_i$，$U \subset \{1,\cdots,n_m\}$ 为 $m[i] = 1$ 的索引 i 的集合，$m[i]$ 是消息 m 的第 i 比特的值。U 选取 $k \in_R Z_q^*$，计算 $\omega' = \omega \times g^k$ 发送给签名者 S。

ii）盲签名：S 接收到 ω' 后，输出对消息 m' 签名 $\sigma' = (\sigma'_1,\sigma'_2) = (g_2^a \omega'^r, g^r)$ 并发送给用户 U。

iii）去盲：用户 U 获取 σ' 后，对其进行脱盲可得

$$\sigma = (\sigma'_1 \cdot (\sigma'_2)^{-k}, \sigma'_2) = (g_2^a \omega'^r \cdot g^{-kr}, g^r) = (g_2^a \omega^r, g^r)。$$

签名验证：输入待签名消息 m（长度为 n_m 比特）、验证公钥 pk 以及 m 的签名 $\sigma = (g_2^a \omega^r, g^r)$，验证是否有

$$e(\sigma_1,g) = g(g_1,g_2)\, e(\omega,\sigma_2) \tag{1}$$

若等式（1）成立，输出 1，否则为 0。

3　安全性分析

3.1　消息盲性的证明

本文所写方案具有一定的消息盲性。因为本文方案 U 对 ω 经过 $\omega' = \omega \times g^k$ 处理（U 秘密选取 k），签名者 S 想通过 ω' 求出 ω 是不可能的，而 ω 与 m 密切相关。所以，所提方案具有消息盲性。

3.2　正确性分析

经过盲化后的签名 $\sigma' = (\sigma'_1,\sigma'_2)$ 是正确的，这是因为：

$$\begin{aligned} e(\sigma'_1,g) &= e(g_2^a \omega'^r, g) \\ &= e(g_2^a,g)\, e(\omega'^r,g) \\ &= e(g_2,g^a)\, e(\omega',g^r) \\ &= e(g_1,g_2)\, e(\sigma'_2,\omega') \end{aligned} \tag{2}$$

3.3　安全性证明

假设 CDH 假设成立，那么建立在 CDH 假设成立基础上的本文方案是可证明安全的。

方案的安全性证明可参考文献[14]，主要根据以下定理证明。

定理 CDH 假设为对于任何 $\forall g \in G_1$，$x,y \in \mathbf{Z}_q^*$，给定 (g,g^x,g^y)，计算 g^{xy} 是难解的，本文方案是在标准模型下实现的，它在 CDH 假设下具有不可伪造的性质。

证明　假定在某次模拟攻击的环节，系统最多

提供 q_k 个用户公钥，最多询问 q_s 次签名，若存在攻击者 A 以不可忽略的 ε 破解本文方案，就存在攻击者 B 可以以概率 $\frac{\varepsilon}{4q_kq_s(n_m+1)}$ 解决在群 G_1 上的 CDH 假设[15]。

输入 (g,g^a,g^b)，CDH 假设下的攻击者 B 模拟以下盲签名的过程。为了实现整个模拟过程，攻击者 B 假设 $I_m=2q_s$，选择随机数 k_m 使得它满足 $0\leqslant k_m\leqslant n_m$ 且 $I_m(n_m+1)<q$。随后，B 随机选择任意 n_m+1 个的正整数 $x',x_i(i=1,\cdots,n_m)$ $(x',x_i<I_m)$ 和 $y',y_i(i=1,\cdots,n_m)$ $(y',y_i\in\mathbf{Z}_q^*)$。定义 $F(m)=x'+\sum_{i\in U}x_i-I_mk_m$ 和 $J(m)=y'+\sum_{i\in U}y_i$，B 设置公开参数 $g_2=g^b$，$u'=g_2^{x'-I_mk_m}g^{y'}$，$u_i=g_2^{x_i}g^{y_i}$，因此，对 $\forall m$ 有 $\omega=u'\prod u_i=g_2^{F(m)}g^{J(m)}$。当 A 向 B 请求用户公钥时，B 猜测 A 伪造公钥为 pk_t 的用户签名。B 假设 $pk_t=g^a$，对剩余的公钥询问，B 任选 $x_i\in\mathbf{Z}_q$，计算 $pk_i=g^{x_i}$ 并返回。

签名询问：输入 (pk_i,m)，若 A 请求的签名公钥满足 $pk_i\neq pk_t$，攻击者 B 返回签名 $\sigma=(g_2^{x_i}\omega^r,g^r)$，$\omega=u'\prod u_i$，否则，$B$ 可执行如下操作：

1）如果 $F(m)\neq 0\bmod q$，B 任意选取 $r\in\mathbf{Z}_q$，并计算 $\sigma=(g_1^{-J(m)/F(m)}(u'\prod_{i\in U}u_i)^r,g_1^{-1/F(m)}g^r)$，令 $\tilde{r}=r-a/F(m)$，则

$$\begin{aligned}&g_1^{-J(m)/F(m)}(u'\prod_{i\in U}u_i)^r=g_1^{-J(m)/F(m)}(g^{J(m)}g_2^{F(m)})^r\\&=g_2^a(g_2^{F(m)}g^{J(m)})^{-a/F(m)}(g_2^{F(m)}g^{J(m)})^r\\&=g_2^a(g_2^{F(m)}g^{J(m)})^{r-a/F(m)}\\&=g^{ab}(u'\prod_{i\in U}u_i)^{\tilde{r}}\end{aligned}$$

和 $g_1^{-1/F(m)}g^r=g^{r-a/F(m)}=g^{\tilde{r}}$

上述推导过程说明生成的 σ 与方案运行生成的签名一致。

2）若 $F(m)\equiv 0(\bmod q)$，B 无法计算出签名 σ，模拟过程宣布失败。

首先检查输入的盲化签名 $\sigma'_i(m)$ 是否满足等式（1），若不满足，立即终止该过程；若满足即返回 $\sigma=(g_2^{x_i}\omega^{r'},g^r)$。

以上是 B 模拟整个签名的环节，由假设，A 可在某个时刻返回一个关于 m^* 伪造签名 $\sigma^*=(\sigma_1^*,\sigma_2^*)$，验证公钥为 pk_t。如果 $F(m^*)\neq 0(\bmod q)$，那么 B 退出，模拟过程失败。否则，该伪造必然满足：

$$\begin{aligned}\sigma^*&=(g^{ab}(u'\prod_{i\in U}u_i)^{r^*},g^{r^*})\\&=(g^{ab}(g_2^{F(m^*)}g^{J(m^*)})^{r^*},g^{r^*})\\&=(g^{ab+J(m^*)r^*},g^{r^*})\\&=(\sigma_1^*,\sigma_2^*)\end{aligned}$$

因此，攻击者 B 由 $\sigma^*=(\sigma_1^*,\sigma_2^*)$ 可得 $(\sigma_1^*)\cdot(\sigma_2^*)^{-J(m^*)}=g^{ab}$。

以下计算 B 完成整个模拟过程的概率。若完成整个模拟环节，待输入消息 m 必须满足 $F(m)\neq 0(\bmod q)$ 与 $F(m^*)\equiv 0(\bmod q)$，且 A 可伪造出公钥为 pk_t 的用户的签名。

将 B 成功猜出 A 试图伪造的用户公钥定义为事件 E_k，容易得出 $\Pr[E_k]=1/q_k$。以下计算 $F(m)\neq 0(\bmod q)$ 与 $F(m^*)\equiv 0(\bmod q)$ 满足的概率。

假设 $m_1,m_2,\cdots,m_{q_Q}$ 是查询中出现的消息且 $m_i\neq m^*$ $(i=1,2,\cdots,m_{q_Q})$，显然有 $q_Q\leqslant q_S$，定义事件 E_i,E'_i,E^* 如下：

E_i: $F(m_i)\neq 0(\bmod q)$，

E'_i: $F(m_i)\neq 0(\bmod I_m)$，

E^*: $F(m^*)\equiv 0(\bmod q)$

容易看出，事件 $\wedge_{i=1}^{q_Q}E_i\wedge E^*$ 与事件 E_k 相互独立，则攻击者 B 模拟不退出的概率为

$$\Pr[\neg\, abort]\geqslant\Pr[\wedge_{i=1}^{q_Q}E_i\wedge E^*]\Pr[E_K]。$$

事件 $(\wedge_{i=1}^{q_Q}E_i)$ 与 E^* 彼此不相关。由于 $I_m(n_m+1)<q$、$x',x_i<I_m(i=1,\cdots,n_m)$，因此 $0\leqslant I_m$，$k_m<q$ 和 $0\leqslant\sum_{i\in U}x_i<q$。

其次，可从 $F(m)\equiv 0(\bmod q)$ 推出 $F(m)\equiv 0(\bmod I_m)$，从 $F(m)\neq 0(\bmod I_m)$ 得到 $F(m)\neq 0(\bmod q)$。则 $\Pr[E_i]\geqslant\Pr[E'_i]$ 且

$$\begin{aligned}&\Pr[E^*]=\Pr[F(m^*)\equiv 0\bmod q\wedge F(m^*)\equiv 0\bmod I_m]\\&=\Pr[F(m^*)\equiv 0\bmod I_m]\Pr[F(m^*)\equiv 0\bmod q\mid F(m^*)\equiv 0\bmod I_m]\\&=\frac{1}{I_m}\frac{1}{n_m+1}\\&\Pr[\wedge_{i=1}^{q_Q}E_i]\geqslant\Pr[\wedge_{i=1}^{q_Q}E'_i]\\&=1-\Pr[\vee_{i=1}^{q_Q}E'_i]\\&\geqslant 1-\sum_{i=1}^{q_Q}\Pr[\neg\, E'_i]\\&=1-\frac{q_Q}{I_m}\\&\geqslant 1-\frac{q_s}{I_m}(I_m=2q_S)\end{aligned}$$

因此

$$\Pr[\neg abort] \geqslant \Pr[\wedge_{i=1}^{q_Q} E_i]\Pr[E^*]\Pr[E_K]$$

$$\geqslant \frac{1}{I_m(n_m+1)} \cdot \left(1-\frac{q_S}{I_m}\right)\frac{1}{q_K}$$

$$\geqslant \frac{1}{2q_s(n_m+1)} \cdot \frac{1}{2} \cdot \frac{1}{q_K}$$

$$= \frac{1}{4q_Kq_s(n_m+1)}$$

因为 $\Pr[\neg abort]$ 的概率是不可忽略的，因此 B 能够成功解决 CDH 困难问题。

4　结语

依据盲签名的原理，在双线性映射的基础上提出一个盲签名方案，将消息的盲因子嵌入到方案中，签名者则无法获知消息的具体信息。该方案假定敌手攻击是存在性不可伪造的。本方案的提出主要基于标准模型的思想，脱离随机预言机模型，并做了安全性分析，且具有较高的效率，更适用于实际环境的认证。近年来，树莓派的使用越来越普遍，外部用户（以传感器为例）需访问树莓派内部节点获取相应服务，因此认证用户身份及允许合法用户获取数据是亟需解决的问题。将本文方案运用到树莓派与传感器的数据传输及认证服务，通过盲签名的认证协议，能够确认消息是否被篡改[16]，能够极大地保护消息的完整性。

参考文献:

[1] Chaum D. Blind signature for untraceable payments. Advances in Cryptology – Crypto 82, Burg Feuerstein, Germany, 1982: 199 – 203.

[2] Abe M and Fujisaki E. How to date blind signatures. Advances in Cryptology Asiacrypto'96, Kyongju, Korea, 1996, 163: 244 – 251.

[3] Abe M and Okamoto T. Provably secure partially blind signatures. Proceedings of the 20th Annual International Cryptology Conference On Advances in Cryptology, California, USA, 2000: 271 – 286.

[4] Maitland G and Boyd C. A provably secure restrictive partially blind signature scheme. Public Key Cryptography PKC 2002, Paris, France, 2002: 99 – 114.

[5] 王静然,钱海峰. 无随机预言模型的盲签名[J]. 计算机应用研究,2010,(05):1837 – 1839,1844.

[6] LIU Y T, NGU A H H, ZENG L Z. QoS computation and policing in dynamic Web service selection [C] // Proc of the 13th International World Wide Web Conference(WWW 2004). New York: ACM Press, 2004: 66 – 73.

[7] UMUHOZA D, AGBINYA J I, MOODLEY D, et al. A reputation based trust model for geospatial Web services [C] // Proc of 1st WSEAS International Conference on Environment and Gspatial Science and Engineering (EC'08). 2008: 220 – 225.

[8] 张延红,陈明. 标准模型下增强的基于身份部分盲签名[J]. 四川大学学报(工程科学版),2014,(01):95 – 101.

[9] 周才学. 标准模型下基于身份的广义代理签密[J]. 密码学报,2016,(03):307 – 320.

[10] 王学庆,薛锐. 标准模型下适应性安全的 BF – IBE 方案[J]. 密码学报,2017,(01):38 – 48.

[11] 周玉洁,冯登国. 公开密钥密码算法及其快速实现[M]. 北京:国防工业出版社,2002.

[12] Waters B. Efficient Identity – based Encryption Without Random Oracles [C]. EUROCRYPT 2005, Aarhus, Denmark, 2005: 114 – 127.

[13] 邓宇乔,杜明辉,尤再来,等. 一种基于标准模型的盲代理重签名方案[J]. 电子与信息学报,2010,(05):1219 – 1223.

[14] Paterson K G and Schuldt J. Efficient identity – based signatures secure in the standard model. ACISP 2006, Melbourne, Australia, 2006: 207 – 222.

[15] 胡小明,杨寅春,刘琰. 一种基于标准模型的盲代理重签名方案的安全性分析和改进[J]. 小型微型计算机系统,2011,(10):2008 – 2011.

[16] 咎亚洲,刘文芬,魏江宏,等. 适用于无线传感器网络的动态 ID 认证方案[J]. 密码学报,2014,(05):422 – 436.