无随机预言模型的盲签名 *

王静然, 钱海峰
(华东师范大学 计算机科学与技术系, 上海 200241)

摘 要: 近些年来,盲签名的研究取得了很多的成果,但也存在着计算过程复杂、传输效率低、交互次数频繁等问题。基于 Boneh 等人提出的签名,首先给出一个不包含随机预言模型的盲签名方案。不包括随机预言机,盲签名就是一个可实现的安全的标准方案,而考虑到交互次数问题,该方案还可以引入公共参考串(common reference string, CRS)来完成签名方的非交互零知识证明,使得盲签名算法仅包含两次交互,实现了轮优先 round optimal,在此基础上也可以实现盲签名算法的并发执行。该盲签名算法构造简单且计算复杂度较低,因此比现有的盲签名方案更加有效,节省了传输带宽,提高了传输效率。

关键词: 盲签名; 随机预言机; 盲性; 不可伪造性
中图分类号: TP399 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1837-03
doi:10.3969/j.issn.1001-3695.2010.05.065

Blind signature without random oracles

WANG Jing-ran, QIAN Hai-feng
(*Dept. of Computer Science, East China Normal University, Shanghai* 200241, *China*)

Abstract: In recent years, the studies of blind signatures achieved a lot of results, but there still are many problems. Boneh and Boyen gave a new signature, derived the blind signature scheme from their idea. This paper first gave a blind signature without random oracles, with this property, the scheme was secure in standard model. Then, used common reference string to do non-interactive zero knowledge proof, made the blind signature into only two moves to achieve round optimal, and the concurrency operation of blind signature could be reach by this. For the algorithm is simple and not complicated, the blind signature is more efficient than the existing secure blind signature schemes, so save transmission bandwidth and improves transfer efficiency.

Key words: blind signature; random oracle; blindness; unforgeability

0 引言

盲签名是电子签名方案的扩展。签名者被要求对某个消息进行签名,但他却不能知道此消息或者任何与此消息有关的事情。当要求签名的人需要对个人消息进行保护的时候,比如说在电子现金或电子选举中,盲签名就会被使用到。

盲签名方案定义最早在 1982 年由 Chaum[1] 提出,第一个盲签名的构造是基于 RSA 难解问题。后来,Juels 等人[2] 和 Pointcheval 等人[3] 给出了盲签名安全性的形式化证明。构造盲签名方案有两种基本的方法,一个是基于 RSA 算法,如文献[1,4];另外是基于双线性映射问题,如文献[5~7]。考虑到盲因子的添加和去除,基于双线性映射问题的方案来构造盲签名要更常用些,并且它的计算复杂度也小于基于因子分解的 RSA 问题。因此,尽管第一个盲签名方案是基于 RSA 问题的,近些年的盲签名算法的构造一般都是选择了双线性映射。而在众多的双线性盲签名方案中,采用 Water 签名方案的 Okamoto 方案是近些年提出的比较优秀的方案,它在签名方案的传输方式、对签名消息的盲化和去盲,以及对请求签名者身份的证明都比较有效和成功,但此方案在消息的传输上仍然存在着计算复杂和传输消息较长的缺陷。

大部分安全的盲签名方案都使用了随机预言机[6~8],但是,随机预言模型是不能用在标准模型中的,而且在算法实现上也很困难。于是很多不包含随机预言机的盲签名方案在近些年也被陆续地提出来,如文献[9,10]。文献[10]的解决方法远远比包含随机预言机的盲签名低效,而且它的构造也很复杂,包含许多次签名者和使用者的信息交互。Okamoto 的盲签名方案要相对好些,但是在签名者和使用者的信息交互上仍然需要占用很大的带宽,大大增加了传输消耗,降低了传输效率。另外,还有一个新的构造盲签名方案的方法被提出来,它使用公共参考串(common reference string, CRS)来取代随机预言机。

近年来,由于对安全性和计算复杂性以及算法效率方面的考虑,盲签名方案的构造变得越来越复杂,如文献[5,10]。消息签名者和使用者之间的交互次数越来越多,算法的计算也很繁琐。如何减少交互和精简运算复杂度,从而节省传输带宽、提高运算效率仍然是需要研究的问题。

本文首先提出了一个不是轮优先的无随机预言机的盲签名方案。没有随机预言机,算法构造简单,实现也是可行的。此盲签名方案还可以修改为使用 CRS 完成非交互零知识证明,避免签名双方的多次交互,实现轮优先这个属性,因此解决

收稿日期: 2009-09-17; **修回日期**: 2009-10-27 **基金项目**: 国家自然科学基金资助项目(60873217,60703004);国家教育部博士点基金资助(20070269005)

作者简介: 王静然(1984-),女,安徽淮北人,硕士,主要研究方向为信息安全、密码学(wujunshi41@163.com);钱海峰(1977-),男,副教授,博士,主要研究方向为信息安全、密码学.

了上面提到的两个研究问题。在此基础上,进行一些小修改,本文的方案也可以满足协议执行的并发性。

1　预备知识

1.1　双线性映射(bilinear map)

令 G 是序为 p 的加法循环群, g 是 G 的生成元, 且 G_1 也是一个序为 p 的乘法循环群。

如果对于所有 $u,v\in G$ 和 $a,b\in\{0,\cdots,p-1\}$,都有 $e(u^a,v^b)=e(u,v)^{ab}$,且 $e(g,g)\neq 1$,那么就说函数 $e:G\times G\to G_1$ 是双线性的。

1.2　Boneh-Boyen signature(BBS)问题

Boneh 等人[11]构造了一个算法,Qian[12]证明了它,并把它改为一个不包含随机预言机的安全模型,本文的盲签名方案的安全性则基于这个 BBS 问题,给出其定义。

定义 1　BBS 问题。令 $K:(\mathrm{CRS},\tau)\leftarrow K(1^\lambda)$ 是如上所述的双线性映射,随机选择 $x,u_0,u_1\in\{0,\cdots,p-1\}$,有 $X=g^x$, $U_0=g^{u_0}$, $U_1=g^{U_1}$ 和 $y=e(g,g)^x=e(X,g)$,这里把 x,X 作为私钥, U_0,U_1,y 作为公钥。

当输入消息 m,算法随机选择 $r\in\{0,\cdots,p-1\}$,计算 $\sigma_1=X(U_0U_1^m)^r$, $\sigma_2=g^r$,输出 $\sigma=(\sigma_1,\sigma_2)$。

在不知道私钥的情况下,根据输出 σ 求解 m 是不可解的。

1.3　证据不可区分性证明(*WIP*)

构造 WIP(witness-indistinguishable proof)的方法很多,如文献[13,14],其主要是实现两个功能:

a)验证者不能得到任何有关证据(witness)的信息。保证盲签名方案里对消息 m 盲化。

b)无论在验证前还是验证后,被验证者不能对证据进行更改。保证 c 一定是由 t 和 m 生成。

本文给出一个比较简单的方法,从而不对盲签名算法复杂度造成影响。

(a)使用者首先随机选择 $\alpha,\beta\leftarrow^r\{0,\cdots,p-1\}$,计算 $y=g^{-\alpha}U_1^{-\beta}$,然后把 y 同 c 一起发给签度。

(b)签名者随机选择 $\alpha\leftarrow^r\{0,\cdots,p-1\}$ 发给使用者。

(c)使用者计算 $T=t+a\alpha,S=m+\alpha\beta$ 并把 T、S 发给签名者。

(d)签名者验证等式 $c=g^TU_1^Sy^a$ 是否成立,如果成立,则 WIP 执行成功,盲签名算法继续进行,否则算法终止。

1.4　公共参考串(*CRS*)

在公共参考字符串(common reference string, CRS)中,假设交互的双方都可以访问一个公共的字符串,并且协议的双方在交互的过程中都不可以知道产生这个字符串的陷门,这个陷门是在安全性证明中被模拟器所获得。在实际使用中,一个可信任的第三方可以通过 CRS 生成算法 $K:(\mathrm{CRS},\tau)\leftarrow K(1^\lambda)$ 产生一个 CRS,然后丢掉陷门 τ。公共参考字符串 CRS 是公开的,交互的双方都可以得到它,在下面的盲签名方案里面,可以把签名使用者要证明的信息包含在这个公共参考串中,以实现非交互的零知识证明。

1.5　盲签名定义

定义 2　盲签名。一个盲签名方案包含两个交互方签名者和使用者(S, U)和一组算法(KeyGen, Sign, Vrfy)。

a)KeyGen 是一个概率多项式算法,以安全参数 1^k 作为输入,输出一对公钥和私钥(pk, sk)。

b)S 和 U 是一对多项式交互概率图灵机,输入是公钥 pk, sk 是 S 私有的,而消息 m 是 U 拥有的并通过算法获得 S 对其的签名。

在算法 Sign 中, U 首先把消息 m 盲化为 m',再把它发给签名者 S。S 对消息 m'进行签名,得到结果 σ'并把它发给使用者 U。U 最后对签名去盲化,生成针对消息 m 的签名 σ。算法 Sign 最终输出(σ,m)或者 fail。

c)Vrfy 也是一个多项式时间算法,它的输入是(pk ,m, σ),经验证,如果 σ 是消息 m 的签名,那么它输出 accept,否则输出 reject。

1.6　安全性定义

盲签名的安全性包含以下两点:

a)盲性(blindness)。签名者对所签名的消息是盲的,即签名者不知道签名的消息的内容,即使公布消息及其签名,签名者也无法追踪签名和消息的对应关系。

定义 3　盲性。如果任何 PPT 算法 S 在下面攻击中成功的概率是可以忽略的,那么盲签名算法就满足盲性:

(a)S 输出公钥 pk 和一对相同长度的消息 m_0、m_1。

(b)随机选择一个比特 b,S 与两个诚实的使用者进行交互, $U_b=U_{pk}(m_b)$, $U_{\bar b}=U_{pk}(m_{\bar b})$, 当交互算法执行完后,签名 σ_0, σ_1 定义为:如果任何一个使用者 U_b 或 $U_{\bar b}$ 终止了,那么(σ_0, σ_1)=($\perp$,$\perp$);否则,令 σ_0(或 σ_1)是 U_0(或 U_1)的输出。

(c) 最后,S 输出一个比特 b'。

定义 S 成功的概率是 $Adv_S^{\mathrm{blind}}=Pr[b'=b]-\frac{1}{2}$。

b)不可伪造性(unforgebility)。除去签名者自己以外,任何人(包括合法的 U)都不可能伪造出合法的签名。

定义 4　不可伪造性。对任意攻击者 F 如果满足下面实验得到的成功概率是可忽略的,那么盲签名方案就是不可伪造的:

(a)密钥生成算法 KeyGen 生成(pk, sk),F 可以得到公钥 pk。

(b)F 可以和诚实的签名者执行多项式次盲签名算法,得到 n 个签名 $\sigma_0,\cdots,\sigma_n$。

(c)最后 F 输出一组消息和与其对应的签名(m_1,σ_1),…,(m_{n+1},σ_{n+1})。

定义 F 成功的概率是:

$$Adv_F^{\mathrm{unforg}}=Pr[\forall 1\leqslant i\leqslant n+1,\mathrm{Vrfy}(pk,(m_i,\sigma_i))=1]$$

2　盲签名方案

如图 1 所示,本文的方案包含两个交互方签名者和使用者(S,U)和一组算法(KeyGen, Sign, Vrfy)。

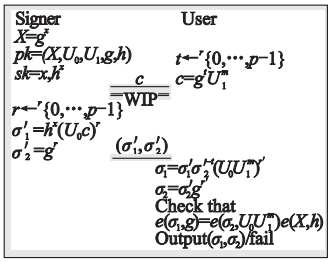

图1　盲签名方案

1)密钥产生算法 KeyGen　令 G,G_1 是序为 p 的双线性群, $e:G\times G\to G_1$ 是对应的双线性映射,算法随机选择 $g,h\in G$ 和 $x\in\{0,\cdots,p-1\}$,然后选择 $U_0,U_1\in G$。输出一对公钥 $pk=$

(X,U_0,U_1,g,h)和私钥 $sk=x,h^x$。其中 $X=g^x$。

2)签名算法 Sign　U 通过下面的步骤获得对消息 m 的签名:

a)U 随机选择 $t\leftarrow^r\{0,\cdots,p-1\}$,计算 $c=g^tU_1^m$ 并把 c 发给签名者 S。

b)为了证明 U 没有欺骗签名者,S 和 U 之间要执行一个 WIP*,具体证明方法如上所述,如果这个证明失败了,那么 U 会在这里终止算法。另外,这个 WIP 是非常短而有效的,而本文的安全性证明不依赖于这个算法,所以可以仅仅把它当做一个黑盒子来处理。

c)S 在和 U 执行 WIP 验证成功后,随机选择 $r\leftarrow^r\{0,\cdots p-1\}$,并使用密钥 sk 计算 $\sigma'_1=h^x(U_0c)^r$ 和 $\sigma'_2=g^r$,然后把签名 (σ'_1,σ'_2)发给 U。

d)U 首先验证签名$(\sigma'_1\sigma'_2)$, 如果不成功,那么终止算法,否则,U 随机选择 $r'\leftarrow^r\{0,\cdots,p-1\}$ 计算 $\sigma_1=\sigma'_1\sigma'^{-t}_2(U_0U_1^m)^{r'}$ 和 $\sigma_2=\sigma'^{-t}_2g^{r'}$,产生对应消息 m 的真正签名 $(\sigma_1\sigma_2)$。

3)要验证对应消息 m 的签名$(\sigma_1\sigma_2)$　只需要检查等式 $e(\sigma_1,g)=e(\sigma_2,U_0U_1^m)e(X,h)$ 是否成立,如果成立,输出 $\sigma=(\sigma_1,\sigma_2)$;否则输出 fail。

注:在此方案的基础上,WIP 的任务是完成使用者对 c 一定是由 t 和 m 生成的证明,而改成以 CRS 为基础的非交互式零知识证明,则是通过可信任第三方的帮助,使得盲签名算法只包含两次交互,从而实现轮优先。本文在上文对 CRS 的使用作了说明,Hazay[15] 的论文给出了非交互零知识证明的更详细的构造方法。

3　盲签名方案性能分析

对应上文给出的盲签名方案,本章首先给出其安全性证明,即盲性和不可伪造性的证明,然后在 3.2 节中对运算复杂度等方面与其他盲签名方案进行比较。

3.1　安全性分析

3.1.1　盲性

证明　假设存在一个攻击者 S^*,对 $i=0,1$,S^* 作为一个不可信的签名者与一个诚实的使用者 U 执行盲签名算法,获得数据 pk_i,sk_i,m_i,σ_i,攻击算法执行完后,S^* 输出 b 实现对 i 的猜测,如果猜测成功,那么算法成功,否则失败。后面将通过几个实验来讨论 S^* 成功的可能不会大于 $1/2+\varepsilon$。其中 ε 是个可忽略的概率。

1)实验 G_0　S^* 仅仅执行盲签名算法获得数据 pk_i,sk_i,m_i,σ_i,此时 S^* 猜测 b 成功的概率是 1/2。

2)实验 G_1　S^* 在获得 c_i 时尝试对 b 进行猜测,由于 t_i 是随机选取的,而本文盲签名中使用者的信息证明 WIP 是安全的黑盒子,所以 S^* 无法比实验 U_0 中获得更多的可用的消息。

3)实验 G_1　S^* 在获得 U 最终给出的签名 σ 时尝试对 σ' 与 σ 对应关系的猜测,这一步,由于 U 在给出最终的签名前对 σ'去盲化并作了一个随机处理,r'是随机选取的,这就保证了这一步签名中 S^* 得不到更多的信息。

从以上三步实验可以看出, 无论 pk_i,sk_i,m_i,σ_i 是什么,随机值 r,r'都是存在的,因此每一次盲签名算法的执行,pk_i,sk_i,m_i,σ_i 都会存在相同的对应关系,也就是说,攻击者 S^* 是无法用比随便猜测 b 的值更大的概率来完成攻击实验的,所以本文的盲签名方案可以满足盲性。

3.1.2　不可伪造性

本文的盲签名方案的签名部分是基于 BBS 问题的,通过图 1 可以很容易看出,如果存在一个攻击者 U^* 可以成功伪造一个签名实现对盲签名方案的攻击,那么 BBS 问题就是不安全的,也即本文的盲签名方案是满足不可伪造性的。

证明　首先,假设有攻击者 U^* 可以与诚实的签名者 S 进行交互, 在只允许不超过 n 次执行盲签名算法的基础上最后产生 $n+1$ 个合法的签名$(m_1,\sigma_1),(m_2,\sigma_2),\cdots,(m_{n+1},\sigma_{n+1})$。

由于攻击者 U^* 是不诚实的,那么在与签名者交互的过程中,则可以保留一个存储数据的表格,对应地存储 $m_i,t_i,c_i,\sigma'_i,r'_i,\sigma_i$,这样在 n 次的询问后,可以得到多于 $n+1$ 次的表格数据,于是可以成功地通过盲签名算法的逆运算得到 $n+1$ 个满足 BBS 问题的(m_i,σ_i),而其中至少一个不是通过询问盲签名算法方案得到的,这样就完成了对 BBS 问题的攻击。

3.2　效率分析

下面将从所使用的难解问题是否包含随机预言机、是否是轮优先的,签名算法、验证算法复杂度是否可以并行实现等方面与已有的盲签名算法进行比较。表 1 中列出了几个算法的对比。其中用 h 表示哈希算法,用 m 表示标量乘,用 e 表示指数算法,p 表示双线性算法。为了方便比较,本文还把 Okamoto 里面的 Σ_protocol 部分不列入复杂度计算里面。从表 1 可以看出,本文的盲签名算法是不包含随机预言机的轮优先的方案,在算法的实现、效率、复杂度等方面都有了相应的提高,对本文开头提出的问题给出了解决方案。

表 1　几个盲签名算法的比较

盲签名方案	包含随机预言机	轮数	签名算法	验证算法	是否可以并行
SH[6]	是	4	$8m+2p+h$	$m+p$	否
OT[9]	否	5	$12e+5m+p$	$m+p$	是
Ours	否	2	$8e+5m+p$	$p+m+e$	是

4　结束语

盲签名是对普通签名方案的扩充,在电子现金支付和电子选举等情况中起着重要的作用。本文基于 BBS 问题提出了一种新的不包含随机预言模型的盲签名方案,与已有的盲签名相比较,该方案计算复杂度相对较低,需要传输信息比较少,在引入非交互式零知识证明之后,还实现了轮优先这一属性。因此在算法构造和实现上都实现了对当前盲签名方案的改进。

参考文献:

[1] CHAUM D. Blind signatures for untraceable payments[C]// Proc of Crypto Advances in Cryptology. [S.l.]: Prenum Publishing Corporation, 1982:199-204.

[2] JUELS A, LUBY M, OSTROVSKY R. Security of blind digital signatures[C]//Proc of the 17th Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 1997: 150-164.

[3] POINTCHEVAL D, STERN J. Provably secure blind signature schemes[C]//Proc of International Conference on the Theory Applications of Cryptology and Information Security: Advances in Cryptology. London: Springer-Verlag, 1996.

[4] CHIEN H, TSENG Yuh-min. RSA-based partially blind signature with low computation[C]// Proc of the 8th IEEE International Conference on Parallel and Distributed Systems. 2001: 385-389.

(下转第 1844 页)

信任度的服务组合优化算法。该方法的核心是在确保 QoS 可信的基础上实现服务组合的优化。针对目前 QoS 计算大多基于性能计算的情况,本文提出了兼顾性能指标和可信指标的 QoS 计算方法,区分了 QoS 数据的不同来源,强调了信任级别的概念,并根据社会交往的方式明确了直接经验和间接经验在可信计算中的权重,从而计算出实际的 QoS 属性值,最后通过服务组合优化算法得到满足用户需求的服务组合方案。实验结果表明,本文的方法在很大程度上保证了 QoS 的可信性,性能 QoS 和信任 QoS 两个方面都取得了较好的效果。

未来的工作笔者将集中于计算方法的优化,进一步提高算法的效率,同时对服务之间的关联性进行研究,探讨服务组合过程中各服务的依赖关系。

参考文献:

[1] 胡春华, 吴敏, 刘国平. Web 服务工作流中基于信任关系的 QoS 调度[J]. 计算机学报, 2009, 32(1):42-53.

[2] NARAYANAN S, MCLLRAITH A. Simulation, verification and automated composition of Web services[C]// Proc of the 11th International World Wide Web Conference (WWW2002). 2002:77-88.

[3] HAMADI R, BENATALLAH B. A Petri net-based model for Web service composition[C]// Proc of Australasian Database Conference. 2003:191-200.

[4] ZHANF R, ARPINAR B, ALEMAN-MEZA B. Automatic composition of semantic Web services[C]// Proc of International Conference on Web Services. 2003:38-41.

[5] 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.

[6] TIAN M, GRAMM A, RITTER H, *et al*. Efficient selection and monitoring of QoS-aware Web services with the Ws-QoS framework [C]// Proc of the IEEE International Conference on Web Intelligence (WI 2004). New York: IEEE Press, 2004:152-158.

[7] SHUPING R. A model for Web services discovery with QoS[C]// Proc of ACM SIGCOM Exchanges. 2003:1-10.

[8] JURCA R, BINDER W, FALTINGS B. Reliable QoS monitoring based on client feedback[C]// Proc of the 16th International World Wide Web Conference (WWW 2007). 2007:1003-1011.

[9] 李研, 周明辉, 李瑞超,等. 一种考虑 QoS 可信性的服务选择方法[J]. 软件学报, 2008, 19(10): 2620-2627.

[10] 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 Envoronmental and Gspatial Science and Engineeing (EG'08). 2008:220-225.

[11] TEACY W T L, CHALKIADAKIS G, ROGERS A, *et al*. Sequential decision making with untrustworthy service providers[C]// Proc of 7th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2008). 2008:755-762.

[12] 郭慧鹏, 怀进鹏, 邓婷,等. 一种可信的自适应服务组合机制[J]. 软件学报, 2008, 31(8): 1434-1444.

[13] 郭得科, 任彦, 陈洪辉,等. 一种 QoS 有保障的 Web 服务分布式发现模型[J]. 软件学报, 2006, 17(11):2324-2334.

[14] QIU Z Y, ZHAO X P, CAI C, *et al*. Towards the theoretical foundation of choreography[C]// Proc of the 16th International World Wide Web Conference (WWW 2007). 2007:973-982.

[15] 林闯, 田立勤, 王元卓. 可信网络中用户行为可信的研究[J]. 计算机研究与发展, 2008, 45(12): 2033-2043.

[16] ERI T. SOA 概念、技术与设计[M]. 王满红, 陈荣华,译. 北京: 机械工业出版社, 2007.

(上接第 1839 页)

[5] KIAYIAS A, Zhou Hong-sheng. Concurrent blind signatures without random oracles[C]// Lecture Notes in Computer Science. Berlin: Springer, 2006:49-62.

[6] SONG Han, CHANG E. A pairing-based blind signature scheme with message recoverfy[J]. International Journal of Information Technology,2005,2(4): 303-308.

[7] GJOSTEEN K, KRAKMO L. Round-optimal blind signatures from waters signatures[C]// Lecture Notes in Computer Science. Berlin: Springer, 2008: 112-126.

[8] BELLARE M, NAMPREMPRE C, POINTCHEVAL D, *et al*. The power of RSA inversion oracles and the security of Chaum's RSA-based blind signature scheme[C]// Proc of Lecture Notes in Computer Science. Berlin: Springer, 2002: 319-338.

[9] OKAMOTO T. Efficient blind and partially blind signatures without random oracles[C]// Lecture Notes in Computer Science. Berlin: Springer, 2006: 80-99.

[10] CAMENISCH J, KOPROWSKI M, WARINSCHI B. Efficient blind signatures without random oracles[C]// Lecture Notes in Computer Science. 2004. Berlin: Springer, 2005: 134-148.

[11] BONEH D, BOYEN X. Efficient selective-ID secure identity based encryption without random oracles[C]// Proc of Lecture Notes in Computer Science. Berlin: Springer, 2004: 223-238.

[12] QIAN Hai-feng. Random-oracle-free signatures and sequential aggregate signatures with short keys[Z].

[13] FEIGE U, SHAMIR A. Zero knowledge proofs of knowledge in two rounds[C]// Lecture Notes in Computer Science. Berlin: Springer-Verlag, 1990: 526-544.

[14] DWORK C, NAORI M. Zaps and their applications. foundations of computer science[C]// Proc of the 41st Annual Symposium. 2002: 283-293.

[15] HAZAY C, KATZ J, KOO C, *et al*. Concurrently-secure blind signatures without random oracles or setup assumptions[C]// Lecture Notes in Computer Science. Berlin: Springer, 2007: 323-341.

[16] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Information Theory Society, 1976, 22(6): 644-654.

[17] RIVEST R, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2):120-126.

[18] GOLDWASSER S,MICALI S, RIVEST R. A digital signature scheme secure against adaptive chosen message attacks[J]. SIAM Journal on Computing, 1988, 17(2):281-308.

[19] BONEH D, LYNN B, SHACHAM H. Short signatures from the weil pairing[C]// Lecture Notes in Computer Science. Berlin: Springer, 2001: 297-319.

[20] LI Yong, CHEN Hui-yan. Efficient identity-based signature scheme with partial message recoverfy [EB/OL]. (2007-02-10) http://www2.computer.org/portal/web/csdl/doi/10.1109/SNPD.