Scientific Research

Controllable Anonymous Service Protocol Based on Non-Transferable Partially Blind Signature

Yong LI

Key Laboratory of Communication & Information Systems, Beijing Jiaotong University, Beijing Municipal Commission of Education, Beijing, China

Email: li.yong9@gmail.com

Abstract: Due to authentication and privacy protection requirements need to be satisfied simultaneously in some applications such as E-commerce, the definition of non-transferable partially blind signature and controllable anonymous service were proposed firstly. Using chameleon hash function and non-transferable partially blind signature as building block, the controllable anonymous service protocol is constructed. The new protocol is secure in the sense of anonymity, authenticity, unlinkability and non-transferability.

Keywords: authentication; digital signature; partially blind signature; non-transferability; privacy preserving

基于不可转移部分盲签名的可控匿名服务协议

李　勇

北京交通大学通信与信息系统北京市重点实验室，北京，中国，100044

Email: li.yong9@gmail.com

摘　要: 针对电子商务等领域需要同时提供用户认证和用户隐私保护的问题，本文首先定义不可转移部分盲签名，然后提出可控匿名服务的概念。以变色龙哈希函数和不可转移部分盲签名为构建模块，构造了一个具体的可控匿名服务协议。协议同时满足匿名性、认证、不可关联性、不可转移性。

关键词: 认证；数字签名；部分盲签名；不可转移性；隐私保护

1 引言

考虑电子商务中的一个场景[1]：消费者 Bob 想发给商家 Alice 购买某商品的订单，还要发给银行一个认证信息，如果 Alice 接受了订单，Bob 就可以通过银行进行转帐。但是 Bob 不想让银行看到订单的内容，同时也不想让 Alice 看到他的银行帐户信息。在实际应用中，一方面服务提供商、银行等机构要求认证用户信息的真实性、有效性；另一方面，用户需要在获得服务提供商提供的服务时，希望能够保护自己的隐私，比如用户可能并不希望服务提供商将自己的交易情况和个人信息建立关联。更进一步的，有时不仅需要保护用户的隐私，还需要保护服务提供商的权益，比如用户从服务提供商获得的服务不能转移给另一方使用。

这种认证与隐私保护间的矛盾与平衡问题是密码学和信息安全领域的重要研究内容。本文针对电子商务、数字版权保护等领域中既要保护消费者的隐私又要保护服务提供商的权益这类需求，提出可控匿名服务的概念，构造了一个实现可控匿名服务的具体方案，并给出其安全性分析。

资助信息：国家高技术研究发展计划(863 计划)项目(2009AA01Z423) 北京交通大学科技基金项目(2007XM006),北京交通大学红果园“双百”人才培育计划.

2 相关工作

2.1 双签名

安全电子交易（SET）规范中引入双签名的概念来处理交易中隐私保护问题[1]。双签名的工作机制是：对订单信息 m_1 和账户信息 m_2 分别产生消息摘要，合并两份摘要；计算合并结果的摘要值，然后签名者用私钥对摘要值签名（签名者必须把另一消息的摘要值包含在内，以便接收者验证双签名）。m_1 或 m_2 的接收方通过产生自己拥有的消息的摘要值，合并上另一消息的摘要值，并计算合并结果的摘要；若产生的结果与双签名解密后的结果匹配，则消息得到认证。消费者发出“购买请求”消息时，需要采用双签名算法，而商家验证双签名时，消费者的身份信息实际上通过

978-1-935068-10-5

消费者的公钥已经泄漏给了商家，虽然商家并不知道消费者账户信息。这不满足匿名性和不可关联性要求。

2.2 部分盲签名

盲签名可以使用户得到签名者的签名却不让签名者知道实际被签消息的内容，签名者也不能追踪签名[2]。利用这一特性，盲签名广泛应用于电子现金、电子选举系统中。然而，因为签名者无法控制盲签名，可能造成签名被非法使用以及在电子现金系统中数据库无限增长等问题。Abe 等在 1996 年亚洲密码学会议上提出了部分盲签名的概念[3]。在 2000 年美洲密码学会议上，Abe 等基于 Schnorr 签名方法提出了实际的签名算法并给出证明[4]。在部分盲签名方案中，签名者所签署的信息可以分为两部分，其中一部分对签名者公开(类似于传统的签名方案)，而另一部分则对签名者保密(类似于盲签名方案)。部分盲签名除了具有普通数字签名的不可伪造性之外，还具有部分盲性，即签名者拥有用户公开的全部信息，但对用户的秘密信息一无所知；不可关联性，即签名者仅从消息/签名对无法确定他是否对该消息签过名。

2.3 指定证实者签名

为了解决不可否认签名存在的缺点：若签名者主观上不愿意合作或客观上无法合作，他所产生的签名就不能被验证，Chaum 提出了指定证实者签名(designated confirmer signature)[5]。在这样的方案中，签名的确认或否认可以由一个称为证实者(confirmer)的第三方来完成。但除了签名者，其他任何人（包括证实者）仍然无法以签名者的名义产生（或伪造）有效的证实签名。进一步地，在必要的时候，证实者还可以将部分或全部指定证实者签名转化为普通的数字签名，从而使得任何人都可以验证这些签名的有效性。指定证实者签名的一个重要特性是：签名的接收方不能向任何第三方证实签名的有效性。

2.4 变色龙签名

变色龙签名最早由 Krawczyk 和 Rabin 在 1997 年提出[6]，它和普通签名的主要区别是所使用的特殊哈希函数：变色龙哈希函数（Chameleon Hash Function）。变色龙哈希函数是一种陷门单向哈希函数，可以阻止陷门信息拥有者之外任何人计算出哈希碰撞（对随机给定的输入）。因为这种特性，变色龙签名同时具备以下属性：

1) 不可否认性(Non-repudiation)：签名者不能否认自己生成的签名(因为他不能找到哈希碰撞)。

2) 不可转移性(Non-transferability)：签名接收者不能向任意第三方证实给定签名是对应某特定消息的有效签名(因为他可以用陷门哈希函数任意“打开”签名或者说伪造签名)。

因此，变色龙签名一方面提供签名方对所签消息的不可否认的承诺，另一方面，签名接收方也不可能提供给第三方关于消息的有效证据来证明签名的有效性。

3 不可转移部分盲签名

本节给出不可转移部分盲签名的定义。

定义 1 一个不可转移部分盲签名是四元组(G, S, U, V)：

1) 密钥生成算法 G 是概率多项式时间算法，输入安全参数 n，输出公/私钥对(pk, sk)。

2) 部分盲签名生成算法是签名者 S 和用户 U 间的交互协议，U 的公共输入包括公钥 pk、公共信息协商算法 Ag、信息 $info_u$。S 的公共输入包括公共信息协商算法 Ag、信息 $info_s$。S 的私有输入包括 sk，U 的私有输入包括消息 msg。停止时，S 的公共输出包含完成或未完成状态。若完成，S 的私有输出含有公共信息 info；U 的私有输出包含或⊥或(info, msg, sig)。

3) 验证算法 V 是多项式时间算法，输入(pk, info, msg, sig)，输出接受(accept)或拒绝(reject)。

不可转移部分盲签名的基本安全需求如下：

完备性：若 S 和 U 遵守签名协议，则以至少 $1-1/n^c$ 的概率，S 输出完毕和 $info=Ag(info_s, info_u)$，U 输出(info, msg, sig)，满足 V(pk, info, msg, sig)=accept，概率取遍 S、G 和 U 的内部掷币。

部分盲性：签名者对消息 msg 签名，知道公共信息 info 的内容，但不知道 msg 的内容。

不可伪造性：对任何不知道签名者私钥的实体，要伪造有效的签名是不可行的。

不可转移性：用户 U 不能把获得的签名转移给第三方使用。

注 1：签名算法中可以利用变色龙哈希函数来保证不可转移性。

4 可控匿名服务

本文称既能实现用户认证又可以保护用户隐私的服务为可控匿名服务，提供可控匿名服务的系统需要满足如下性质：

1) 匿名性：用户在获取服务时身份信息不会泄露。

2) 认证：用户可以向系统内其他机构证明自己的有效身份。

3) 不可关联性：系统不能将用户多次申请的服务与用户身份信息建立关联。

4) 不可转移性：用户获取服务所需的权限不能传给第三方。

其中第一、第三条性质重在保护用户的隐私，而第二、第四条性质则是保护服务提供商的权益，防止用户的权限任意扩散，即匿名服务是可控的。

4.1 可控匿名服务协议

协议参与方：银行 B（用户认证机构）、商家 M（服务提供方）、用户 U。设 g 是阶为 q 的群 G_q 的生成元，安全哈希函数 $H(\cdot):\{0,1\}^* \rightarrow G_q$，变色龙哈希函数 H_c，比如本协议可采用文献[7]中的变色龙哈希函数。$\{x_i,y_i=g^{x_i}\}(i\in\{B,M,U\})$是三方各自的私钥/公钥对，$(q,g,H,H_c)$可作为公共信息发布。设 m_1 表示用户的订单消息，m_2 表示用户的银行帐户消息。三方执行一轮协议对应的标识信息为 I。

协议描述如下：

1) 用户向商家发送订单信息 m_1 和 $H(m_1)$；

2) 商家验证 m_1 的完整性。随机选 $k,k_M\in Z_q^*$，计算 $r=g^k, s=x_M H(m_1\|r)+k, r_M=g^{k_M}$，把$(r,r_M)$发给用户。

3) 用户随机选 $t\in Z_q^*$，计算 $r_U=r_M g^t$,令 $m=m_2\|r_U$，$h=H(y_U,I), R=(g^t,y_U^t)$，$e=H_c(m\|R)=g^t h^m$，把 e 发给商家。

4) 商家计算签名 $s_M=se+k_M$，把 s_M 发给用户。

5) 用户计算 $s_U=s_M+t$，把$(r_U,s_U,m_2,r,h,R,H(m_1\|r))$发给银行。

6) 银行验证用户帐户信息 m_2 的完整性，然后验证商家签名的有效性：$g^{s_U}=(y_M^{H(m_1\|r)}r)^{Hc(m_2\|r_U\|R)}r_U$。

通过验证后，银行与用户间执行与上述 1-5 步类似的过程：

6.1) 随机选 $K,K_B\in Z_q^*$，计算 $R=g^K$, $S=x_B H(m_2\|R)+K$, $R_B=g^{K_B}$，把(R,R_B)发给用户。

6.2) 用户随机选 $T\in Z_q^*$，计算 $R_U=R_B g^T$，令 $m=m_1\|R_U$，$h=H(y_U,I), R=(g^t,y_U^t)$，$E=H_c(m\|R)=g^t h^m$，把 E 发给银行。

6.3) 银行计算签名 $S_B=SE+K_B$，把 S_B 发给用户。

6.4) 用户计算 $S_U=S_B+T$，把$(R_U, S_U, m_1, R, h, R, H(m_2\|R))$发给商家。

6.5) 商家验证订单信息 m_1 的完整性；然后验证银行签名的有效性：$g^{S_U}=(y_B^{H(m_2\|R)}R)^{Hc(m_1\|R_U\|R)}R_U$。

7) 验证通过，用户可获得订单 m_1 上的服务。

4.2 安全性分析

1) 正确性：银行对于商家的签名，易知下列等式满足：

$$g^{s_U}=g^{(s_M+t)}=g^{(se+k_M)}g^t=g^{se}r_M g^t=g^{se}r_U$$
$$=(g^{x_M H(m_1\|r)+k})^e r_U=(y_M^{H(m_1\|r)}r)^{Hc(m_2\|r_U\|R)}r_U。$$

类似的，商家对银行签名的验证等式也成立。

2) 部分盲性与匿名性：从上述协议执行过程分析，用户与商家第一次交互获得商家签名时，因采用的部分盲签名，商家只看到订单 m_1 的信息；用户与商家第二次交互发送银行签名时，商家得到 $H(m_2\|R)$，由哈希函数的安全性，商家仍然得不到用户的账户信息 m_2。因此，用户与商家交互到最终获取服务过程中，部分盲性和匿名性得到保证。类似的，用户与银行之间的交互，银行可验证用户帐户信息 m_2，银行不能从哈希值 $H(m_1\|r)$、$H_c(m_1\|R_U)$中获知用户订单 m_1 的信息，部分盲性满足。

3) 不可伪造性与认证：协议中的部分盲签名是基于离散对数问题的，可证明签名是不可伪造的。在协议第六步，用户通过帐户信息 m_2 向银行证明自己的合法帐户信息。

4) 不可关联性：若商家对同一用户 U 的不同订单信息 m_1、m_1'可以建立关联，即对相同的 m_2（同一用户 U），对随机数 $R\neq R'$，商家发现 $H(m_2\|R)=H(m_2\|R')$。这与 R、R'的随机性和哈希函数 H 的抗碰撞性矛盾。故商家不能将同一用户多次申请的订单服务与用户身份信息建立关联。另外，银行可以验证用户帐户的有效性，但银行无法推知用户订单信息，故银行也不能把用户身份与用户请求的订单服务建立关联。

5) 不可转移性：令 m=m2||rU（或 m=m1||RU），由变色龙哈希函数 Hc 的性质，用户用私钥 xU 作为陷门信息，用户可以计算哈希碰撞，即找到不同的 $m'\neq m$，$R'\neq R$，使得 $e'=Hc(m'\|R')=Hc(m\|R)=e$ (或 $E'=E$)。然后商家对 e 签名（银行对 E 签名），签名可通过第 6 步银行的验证（第 6.5 步商家的验证）。第三方无法区分签名是由用户有效的 m1(或 m2)生成、还是由用户利用私钥构造的信息生成，用户获取服务所需的权限因而不能传给第三方。不可转移性满足。

978-1-935068-10-5 © 2010 SciRes.

5 结束语

为解决电子商务等领域存在的用户认证与隐私保护之间的矛盾和平衡问题，本文首先定义不可转移部分盲签名，然后提出可控匿名服务的概念，并以变色龙哈希为工具，利用不可转移部分盲签名构造了一个具体的可控匿名服务协议，同时进行了协议安全性分析。文中提出的可控匿名服务协议，可以作为独立的研究领域，值得进一步研究。

References (参考文献)

[1] MasterCard, VISA. SET Secure Electronic Transaction Specification Book 1: Business Description(Version 1.0), 1997.

[2] D. Chaum. Blind signatures for untraceable payments. In: Proceedings of CRYPTO'82. Plenum Press,1983. 199−203.

[3] M.Abe and E.Fujisaki. How to date blind signatures. In: Kwangjo Kim and Tsutomu Matsumoto, editors. Proceedings of Advances in Cryptology-ASIACRYPT'96, LNCS 1163, Springer Verlag, 1996. 244−251

[4] M.Abe, T.Okamoto. Provably secure partially blind signatures. In: M. Bellare Ed. Proceedings of Advances in Cryptology-Crypto'2000, LNCS 1880, Springer Verlag, 2000. 271−299

[5] D. Chaum, Designated Confirmer Signatures, In: De Santis A, ed. Proceedings of the Advances in Cryptology-EUROCRYPT '94. LNCS 950, Springer-Verlag, Berlin, 1994. 86−89

[6] H. Krawczyk, T. Rabin. Chameleon hashing and signatures. Proceedings of NDSS 2000, 2000, 143−154

[7] Xiaofeng Chen, Fangguo Zhang, Haibo Tian, Baodian Wei, Kwangjo Kim. Key-Exposure Free Chameleon Hashing and Signatures Based on Discrete Logarithm Systems. Cryptology ePrint Archive, Report 2009/035, 2009.