# 一个新型的盲签名方案

吉 延,许 爽,沈 虹
(西安工业学院 计算机系,陕西 西安 710032)

**摘 要**:将XML数字签名规范引用到盲ElGamal签名算法当中,提出一套新型的盲签名方案,并给出了实现的基本思路。该方案具备XML数字签名和盲ElGamal签名各自的优点,安全性很高,具有良好的应用价值和前景,对盲签名的研究提供了一种新的有意义的参考方向。

**关键词**:盲签名;ElGamal;XML
**中图分类号**:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)08-0219-03

# A New Blind Signature Scheme

JI Yan,XU Shuang,SHEN Hong
(Xi'an Institute of Technology ,Xi'an 710032,China)

**Abstract**: A new blind signature scheme is proposed combining the concept of XML blind signature scheme based on ElGamal public key system, and proposes a simple realizable scheme, which has the merits of ElGamal blind signature and XML, and has high security and many valuable applications. Therefore, a new kind of research orientation associated on blind signature is shown.

**Key words**: blind signature; ElGamal; XML

## 0 引 言

数字签名是一项重要的计算机网络安全技术,它的基本作用是保证传送的信息不被窜改和伪造,并确认签名人的身份。盲签名是一种特殊的数字签名。1983年,Chuam首先提出了盲签名的概念[1]。

XML[2]是W3C(World Wide Web Consortium,国际互联网协会)于1998年2月提出的一个基于文本的描述结构化数据的可扩展标识语言规范,它和HTML(HypeText Markup Language,超文本标识语言)同是SGML(Standard Generalized Markup Language,标准通用标识语言)的一个子集。随着XML网络应用的不断发展,对网络信息安全性要求也越来越高,同时对一些重要信息还要求签名确认,因此XML与数字签名的结合被提到议事日程。

## 1 盲签名与盲ElGamal签名方案

### 1.1 盲签名

盲签名是指签名人并不知道所签文件或消息的具体内容,而文件或消息的拥有者又可以从签名人在盲化文件或消息上的签名得到签名人关于真实文件或消息的签名[1]。基于盲签名的特点,盲签名技术在电子货币、电子投票、电子支付等应用中的匿名性方面起着重要作用,国内外学者就此进行了许多相关研究并取得了成果[3~5]。

### 1.2 基于ElGamal的盲签名方案

在盲消息签名方案中,签名者仅对盲消息m'进行签名,并不知道真实消息m的具体内容,且该类签名的特征是:sig(m)=sig(m')或sig(m)含sig(m')中的部分数据。签名者只要保留关于盲消息m'的签名,便可确认自己关于m的签名[6]。举例说明:Alice想获取Bob对消息m的签名,$x$和$y=\alpha^x \bmod p$为Bob的私钥和公钥,$p$为大素数,$\alpha$为$Z_{p-1}$的生成元。

步骤1 Alice:选择随机选择盲因子$h \in Z_{p-1}$,计算$\beta=\alpha^h \bmod p$,$m'=mh \bmod (p-1)$,将$(\beta,m')$送给Bob;

步骤2 Bob:选择随机数$k \in Z_{p-1}$,计算$\gamma=\beta^k \bmod p$,$s=x\cdot\gamma+m'\cdot k \bmod (p-1)$,并将$(\gamma,s)$发回给Alice;

步骤3 Alice:sig(m)=$(\gamma,s)$,验证方程$\alpha^s=\gamma^m\cdot y^\gamma \bmod p$,成立则接受此签名。

## 2 XML数字签名规范

2001年8月20日由IETF(Internet Engineering Task Force)和W3C共同组建的XML Signature工作组公布了XML数字签名的推荐版本(Proposed ecommendation)。W3C将XML数字签名规范解释为:定义一种与XML语法兼容的数字签名语法描述规范,描述数字签名本身及签名的生成、校验过程[7]。作为一个安全有效的数字签名方

收稿日期:2005-11-27
作者简介:吉 延(1979-),男,陕西延安人,硕士研究生,研究方向为Web应用程序安全性;沈 虹,教授,研究方向为电子政务、网络安全。

案,该规范提供了数字签名的完整性(Integrity)、签名确认(Authentication)和不可抵赖性(None-repudiation)。

以下给出XML数字签名的数据模型框架。

(1)<Signature>
(2) <SignedInfo>
(3) <CanonicalizationMethod/>
(4) <SignatureMethod/>
(5) <Reference(URI=?)>
(6) <Transforms/>
(7) <DigestMethod/>
(8) <DigestValue/>
(9) </Reference>
(10) </SignedInfo>
(11) <SignatureValue/>
(12) <KeyInfo/>
(13) <Object/>
(14) </Signature>

## 3 一种基于ElGamal的XML盲签名方案

### 3.1 XML技术、盲ElGamal签名结合的可能性与意义

#### 3.1.1 XML技术的优势

XML的优势在于:良好的数据格式,可扩展性,高度结构化,便于网络传输。XML允许各种不同专业开发与自己特定领域相关的标记语言,这就使得该领域的人可以交换数据和信息,而不用担心接收端是否有特定的软件来浏览数据。XML的扩展性和灵活性允许它描述不同种类应用软件中的数据,且能集成不同来源的数据,这给数据的建立提供了极大的方便;同时由于基于XML的数据是自我描述的,数据不需要内部描述就能被交换和处理。XML被发送给客户端后,用户可以使用不同的方法处理数据,也能以多种方式显示,这一切都为开发灵活、高效的Web应用软件奠定了基础。由于XML是一个开放的基于文本的格式,可与HTML一样使用HTTP进行传递,不需要对现存的网络作任何改变。XML的压缩性也很好,不会给网络传输增加太大的负担。XML的内容和样式是分开的,服务器在将内容传给客户的同时也将与之关联的样式发送过来,这样大大减少了服务器与客户的交互,从而减轻了服务器的压力。XML的标记含义丰富,与其内容紧密相连,明确地标志所标记的内容,因而使得检索行为更加简单,检索结果也更有意义。XML较之HTML有着诸多优点,在网络信息交换方面充分体现了它的强大优势,迅速成为网络数据表示和信息交换的标准。于是,XML对其传输的信息的安全性要求愈来愈高,XML本身的安全性显得力不从心,而基于ElGamal公钥加密体制的盲ElGamal签名可以充分保证信息的安全性。同时盲ElGamal签名还提供了签名的盲性和签名人的匿名性,必将使XML技术在电子货币、电子投票、电子支付等应用中发挥作用。由此可见,盲ElGamal签名与XML技术的结合满足了XML对信息安全性的要求,而且给XML带来了全新的应用方向。

#### 3.1.2 盲ElGamal签名的特性

假设 $u,v$ 是定义在两个不同概率空间的随机变量,其概率分布分别为 $P(u)$、$P(v)$,联合分布为 $P(u,v)$,如果在多项式时间内无法区分概率分布 $P(u,v)$ 与 $P(u)*P(v)$,则称 $u,v$ 是不可联系的。

在盲签名方案中,即使签名人存储盲消息m'及其签名sign(m')或其他有关数据,待(m,sign(m))公开后签名人也无法找出(m',sign(m'))和(m, sign(m))之间的联系,即(m', sign (m'))和(m,sign(m))是不可联系的,进而也就无法追踪到消息m,则称为强盲签名方案;若签名人可以将二者联系,则称为弱盲签名方案。

在上面提到的盲ElGamal签名方案中,如果签名者保留sig (m') 及其它有关数据,待sig(m)公开后,计算 $h' = m'\cdot m - 1$,再验证 $\alpha h' = \beta$,从而可恢复原签名过程。所以盲ElGamal签名方案属于弱盲签名方案,它适合于大多数电子货币和电子投票系统的设计。XML与盲ElGamal签名的结合扩展了盲ElGamal签名应用的范围,必将引发人们对盲签名研究更多的关注。

#### 3.1.3 XML技术、盲ElGamal签名的结合

XML技术、盲ElGamal签名的结合既保留了XML技术、盲ElGamal签名各自的优势,又补充了各自的不足,因而具有良好的应用价值和前景,主要体现在电子货币、电子投票等方面。在XML技术、盲签名的结合中,XML数字签名规范是骨架,盲ElGamal签名则是灵魂。

### 3.2 基本思路

(1) 盲化消息。依据盲ElGamal签名方案将消息m盲化生成m'。

(2) 建立签名。依据XML数字签名规范建立签名,包括建立<Reference/>元素、建立 <SignedInfo/> 元素、建立<Signature/>元素,消息接收者Bob将建立了<Signature/>元素的XML文档传给发送者Alice。接收者Bob在建立<Signature/>元素的过程中依据盲ElGamal签名方案生成sig(m')。

(3) 验证签名。XML数字签名方案的验证分为两部分:引用确认(Reference Validation) 和签名确认(Signature Validation)。前者确认被签署对象没有被做任何修改;后者保证签署人身份的真实性(注意:这里是"身份"的真实性确认,消息对于Bob来说仍是盲的)。发送者Alice获取Bob发来的( $\gamma$, $s$ ) 作为对消息m的签名,并利用Bob的公钥验证其签名有效性。

### 3.3 一个基于ElGamal的XML盲签名

(1) 盲化消息。

a. Alice选择 $h$,利用Bob的公开密钥 $y$,做 $\beta = \alpha^h \bmod p$; $m' = mh \bmod (p-1)$;

b. Alice将m'封装入XML文档,或提供m'的URI;

c. Alice将包含m'或m'的URI的XML文档发送给

Bob。

(2) 建立签名。

a. Bob 建立<Reference/>元素:

①Bob 对 m'按照<Transforms/>进行转换;

②Bob 根据<DigestMethod/>对①的结果进行摘要算法计算,并将结果存入<DigestValue/>;

③Bob 建立<Reference/>,内容包括<Transforms/>、<DigestMethod/>和<DigestValue/>。

b. Bob 建立<SignedInfo/> 元素,内容包括<CanonicalizationMethod/>、<SignatureMethod/>、<Reference/>。

c. Bob 建立<Signature/>元素。

①Bob 根据<CanonicalizationMethod/>将<SignedInfo/>元素规范化;

②Bob 利用自己的私有密钥 $x$,做 $\gamma = \beta^k \bmod p$, $s = x \cdot \gamma + m' \cdot k \bmod (p-1)$, 并规范化 $s$;

③Bob 根据<SignatureMethod/>操作<SignedInfo/>元素和 $s$,将结果存入<SignatureValue/>;

④Bob 建立<Signature/> 元素,包括<CanonicalizationMethod/>、<SignedInfo/>、<SignatureValue/>;

⑤Bob 可将自己的公钥 $y$ 放入<KeyInfo/>,也可不放入。

d. Bob 将建立了<Signature/>元素的 XML 文档传给 Alice。

(3) 验证签名。

a. 引用确认:

①Alice 对 m'按照<Transforms/>进行转换;

②Alice 根据<DigestMethod/>对上一步的结果进行摘要算法计算,并将结果与<DigestValue/>内容对比,相同则进行下一步;否则,认为消息被中途窜改,签名无效,拒绝接受。

b. 签名确认:

①Alice 根据<CanonicalizationMethod/>将<SignedInfo/>元素和 $s$ 规范化;

②Alice 根据<SignatureMethod/>操作<SignedInfo/>元素和 $s$,将结果与<SignatureValue/>内容对比,相同则进行下一步;否则签名人身份被否认,签名无效,拒绝接受;

③Alice 获得 Bob 的公开密钥 $y$(可以从<KeyInfo/>得到);

④Alice 做 $\alpha^s = \gamma^m \cdot y^\gamma \bmod p$,验证其签名$(\gamma, s)$的有效性。

### 3.4 安全性分析

安全用 XML 数字签名规范、ElGamal 公钥体制和盲签名等多重方法来保证。

(1) XML 数字签名规范本身提供了较强的安全性保证。例如,<SignatureMethod/>元素位于<SignedInfo>内部,增加了安全性;经过引用确认和签名确认两重验证,在保证签名信息的完整性、不可抵赖性的同时,提高了安全性。

(2) ElGamal 公开密钥体制的安全性。公开密钥体制的安全性依赖于一种特殊的数学函数——单项陷门函数的性质。ElGamal 算法,其安全性依赖于计算有限域上离散对数这一难题。具体地说,主要依赖于 $p$ 和 $\alpha$,若选取不当则签名容易伪造,应保证 $\alpha$ 对于 $p-1$ 的大素数因子不可约[8]。

(3) 盲签名的匿名性使签名人隐私得到了充分保护;盲性使被签名对象不被签名人泄漏,这些都加强了安全性。

## 4 结束语

基于 ElGamal 公钥体制的 XML 盲签名技术兼具了 XML 数字签名规范和盲 ElGamal 签名的优点,所以具有良好的应用价值和背景。盲 ElGamal 签名已经在电子公文、电子货币、电子投票中得到应用。而它与 XML 技术的结合必将使盲签名技术得到更广泛、更深层的应用,如应用于 XML 格式的邮件系统中[9]。最后,XML 部分盲签名、XML 代理多重盲签名都是今后值得关注的研究方向。

**参考文献:**


[1] Chaum D. Blind Signature Systems[A]. Proceedings of CRYPTO'83[C]. New York:Plenum Press,1984.

[2] W3C. Extensible Markup Language(XML) 1.0[EB/OL]. http://www.w3.org/TR/1998/REC-xml-19980210, 1998.

[3] Chaum D. Blind Signature for Untraceable Payments[A]. Advances in Cryptology. Proc. CRYPTO'82[C]. New York: Plenum Press,1983.199-203.

[4] Abe M, Fujisaki E. How to Date Blind Signature[A]. Proceedings of Advances in Cryptology - Asiacrypt 96[C]. LNCS,Kyongju,Korea:Springer,1996.244-246.

[5] Chamenisch J L. Blind Signatures Based on the Discrete Logarithm Problem[A]. Rump Session of Eurocrypt'94[C]. Heidelberg,Germany:[s.n.],1995.

[6] 洪泽勤,曾俊杰,钟　旭,等.基于 ElGamal 的强盲签名方案[J].信息工程大学学报,2004,5(4):18-19.

[7] Canonical XML W3C Recommendation[EB/OL] http://www.w3.org/TR/2001/REC-xml-c14n-2001-03-15.

[8] 李方伟,李维科.一种基于 ElGamal 体制的盲签名方案[J].重庆邮电学院学报,2004,16(6):1-2.

[9] 王　晨,沈　虹.基于 XML 技术的邮件格式化[J].西安工业学院学报, 2005,25(3):250-251.