文章编号: 1005-0523(2007)02-0139-04

一种基于离散对数问题的存根代理盲签名方案

刘二根, 左黎明

(华东交通大学 基础科学学院, 江西 南昌 330013)

摘要: 数字签名用来保证原始数据完整性和有效性, 一个数字签名方案包括数字签名生成算法和数字签名验证算法. 简短地介绍了盲签名、代理签名的基本思想和基本性质, 并给出如何通过非对称密码算法的思想来实现这些签名方案, 提出并详细介绍了基于离散对数问题的有存根的(免责声明)代理盲签名方案, 讨论了基于离散对数问题的密码学算法的可能攻击方法, 在此基础上给出了协议实现时的一些有益的建议.

关键词: 数字签名; 盲签名; 代理签名; 代理盲签名方案; 离散对数问题;

中图分类号: O156.1; TP393.08

文献标识号: A

1 引言

随着计算机技术和网络通讯技术的发展, 电子政务、电子商务得以广泛的开展, 而且成为时代的趋势, 网络安全问题日渐成为网络应用的核心问题, 要在互联网上安全地传输信契约、合同、信件、帐单、订单等数据, 必须依赖一些网络安全协议, 而协议需要我们用数字签名(Digital Signature)来代替以往的手写签名. 数字签名的目的是提供一种手段, 使得一个实体把他的身份与某个信息捆绑在一起. 一个消息的数字签名实际上是一个数, 它依赖于仅仅签名者知道的某个秘密, 也依赖于被签名信息本身. 所以, 数字签名可以被看成是一种证明签名者身份和所签署内容真实性的一段信息. 一般而言, 作为数字签名算法, 它必须满足以下三点:

(1) 不可否认性: 签名者事后不能否认自己的签名;

(2) 不可伪造性: 任何他人不能伪造签名;

(3) 可鉴别性: 当双方为签名真伪发生争执时, 可以由第三方解决争端.

签名算法的分类:

(1) 按照数字签名的目的可分成: 普通数字签名

和特殊目的的数字签名(如不可否认签名、盲签名、群签名、代理签名、一次性签名等). 前者由签名算法(Digital Signature Generation Algorithm)和验证算法(Digital Signature Verification Algorithm)组成. 而后者还需要一些附加的内容:

(2) 按照验证方法可分成: 在验证时需要输入被签名信息和在验证中自动恢复被签名信息两类;

(3) 按照是否使用随机数可分成: 确定的和随机的两种签名算法.

一个完整的数字签名体制一般记为: (M, S, K, SIG, VER) , 其中 M 表示消息集合, S 表示签名集合, K 表示密钥集合, SIG 表示签名算法集合, VER 表示签名验证算法集合. 历史上出现过许多签名方案, 比较著名的数字签名算法有 RSA 签名方案、Rabin 签名方案、ElGamal 签名方案、DSS 签名方案、Lamport 签名方案、Bos-Chaum 一次性签名方案等, 大部分数字签名方案主要是基于两大难题: (1) 大数分解问题; (2) 有限域上离散对数问题.

2 盲签名与代理签名

收稿日期: 2007-01-11

基金项目: 江西省自然科学基金资助项目(0611009)

作者简介: 刘二根(1965-), 男, 江西吉水人, 教授.

2.1 盲签名的一般表述

关于盲签名,学术界对其精确定义有很多不同的说法,但是其本质是相同的,用通俗语言描述是:如果A要B对信息 m 进行签名,但是又让B知道信息 m 或者只能让B知道部分信息.盲签名可以分为:完全盲签名和部分盲签名.大多数情况下我们讨论盲签名方案的是完全盲签名方案,完全盲签名的一般过程:

Step1: A取出信息 m ,并生成一个随机数,该随机数称为盲化因子(blinding factor),利用该随机数隐藏原信息 m ,得到隐藏后信息 m' ;

Step2: A将 m' 发送给B;

Step3: B对 m' 签名,将签名结果发送给A;

Step4: A除去盲化因子,得到B对 m 的签名.

由以上过程我们可以看出,签名过程中存在A欺诈B的可能,主要原因是信息 m 可能含有对B不利的内容,因此针对此问题,出现了许多新的盲签名协议.

2.2 一种基于离散对数问题的盲签名协议

A要求B对信息 m 进行盲签名,盲签由签名者B开始,签名者B最终没有得到关于信息 m 的签名信息.签名中选择大素数 p , p 满足: $p-1$ 的大的素数因子 q 为大素数, $q|(p-1)$,且在 Z_p^* 上离散对数问题是难解问题. g 是 Z_p^* 的 q 阶元, $g^q=1 \pmod p$.若选取私钥 x ,则令公钥为 $y=g^x \pmod p$,公开 p, q, g .协议描述如下:

B $\rightarrow$ A: 任取 $k \in Z_q^*$, 计算 $\bar{k}=g^k \pmod p$, 将 $\bar{k}$ 发送给A;

A $\rightarrow$ B: 任取 $a, b \in Z_q^*$, 计算 $r=\bar{k}^a g^b \pmod p$, $\tilde{m}=am\bar{k}r^{-1} \pmod q$, 将 $\tilde{m}$ 发送给B;

B $\rightarrow$ A: 利用自己的私钥 x 对 $\tilde{m}$ 进行签名, 计算 $\tilde{s}=(x\bar{k}+k\tilde{m}) \pmod q$, 将 $\tilde{s}$ 发送给A;

A: 计算 $s=(\tilde{s}\bar{k}^{-1}+bm) \pmod q$, 则 (r, s) 是对 m 的签名.

验证算法如下: 验证 $g^s \equiv y^r r^m \pmod p$. 若成立, 则接受 (r, s) 是对 m 的签名. 否则拒绝.

协议正确性证明如下:

$$s=(\tilde{s}\bar{k}^{-1}+bm) \pmod q=(x\bar{k}r^{-1}+k\tilde{m}\bar{k}^{-1}+bm) \pmod q;$$

$$s=(xr+kam\bar{k}r^{-1}\bar{k}^{-1}+bm) \pmod q=(xr+kam+bm) \pmod q;$$

$$g^s=g^{(xr+kam+bm) \pmod q} \pmod p=g^{xr} g^{kam+bm} \pmod p=y^r r^m \pmod p.$$

2.3 代理数字签名的概念与基本性质

2.3.1 代理数字签名的基本概念

设A、B是数字签名机制 (M, S, K, SIG, VER) 的

两个用户, 他们的密钥对分别为 $(x_A, y_A), (x_B, y_B)$. 如果有以下条件成立:

(1) A利用他的密钥 x_A 计算出一个数 σ , 并且将 σ 秘密地交给B;

(2) 任何人(包括B)在试图求出 x_A 时, σ 都不会对它有任何帮助;

(3) B可以用 σ 和 x_B 生成一个新的签名密钥 $\sigma_{A \rightarrow B}$;

(4) 存在一个公开的验证算法 $ver_{A \rightarrow B}$, 使得对任何 $s \in S$ 和 $m \in M$, 都有以下成立: $ver_{A \rightarrow B}(y_A, s, m) = True \leftrightarrow s = sig(\sigma_{A \rightarrow B}, m)$;

(5) 任何人在试图求出 x_A, x_B, σ 和 $\sigma_{A \rightarrow B}$ 时, 任何数字签名 $sig(\sigma_{A \rightarrow B}, m)$ 都不会对他产生任何帮助.

那么我们称用户A将他的(部分)数字签名权力委托给了用户B, 并且称A为B的原始签名人, 称B为A的代理签名人, 称 σ 为委托密钥, 称 $\sigma_{A \rightarrow B}$ 为代理签名密钥, 称以 $\sigma_{A \rightarrow B}$ 作为签名密钥对消息 $m \in M$ 生成的数字签名 $sig(\sigma_{A \rightarrow B}, m)$ 为A的代理签名(Proxy Signature), 能够生成代理签名的数字签名体制被称为代理签名体制. 以上定义可见于文献[8].

2.3.2 代理数字签名的基本性质

(1) 原始签名的不可伪造性: 除了原始签名人外, 任何其他(包括代理签名人)都不可能伪造原始签名人的数字签名.

(2) 代理签名的不可伪造性: 除了代理签名人外, 其他任何人(包括原始签名人)都不能生成有效的该代理签名人的代理签名.

(3) 代理签名的可区别性: 任何一个代理签名都与原始签名人的数字签名有明显不同, 不同签名人之间的代理签名有明显不同, 防止互相推诿抵赖.

(4) 不可抵赖性: 任何签名人(包括代理签名人和原始签名人)均不能对其签名加以否认.

(5) 身份证实性(代理签名人的可区别性): 原始签名人可以根据代理签名知道代理签名人的身份, 防止其滥用其代理权利.

(6) 密钥依赖性: 代理签名密钥依赖于原始签名人的密钥.

在文献[8]中分别给出了基于离散对数问题和大数分解问题的两种不同代理数字签名方案.

3 代理盲签名机制与协议

3.1 代理盲签名概述

从代理签名的定义我们知道, 对于原始签名人

而言,他事先并不知道他的代理签名人要对什么样文件信息进行数字签名,因此从一定意义上而言,代理签名具有盲签名的一些特点,即原始签名人并不知道要签名的文件内容.但是代理签名与盲签名也有不同的特点,代理签名人可以知道要签名的文件内容,并对其进行签名.由此过程可以看出,代理签名人可以与其它恶意攻击者对原始签名人进行串谋攻击.有些情况下,对于代理签名人,也必须对其隐瞒要签名的文件内容,因此我们提出了代理盲签名.代理盲签名仍然属于代理签名的框架,但是必须增加一些内容,进行扩充.

盲签名有可以被欺骗的弱点,对于盲签名,我们必须作出一些限制,比如:需签名文件与签名人无利益关系.若A要求B对信息 m 进行盲签名,那么A必须明确的用自己的私钥对公开保证签名人权益的免责声明进行签名,免责声明可能类似于以下的一段信息:需签名文件与签名人无利益关系,否则,签名文件无效.并把经过A签名的免责声明加到盲签名文件中去,以后验证盲签名的同时,也要能验证免责声明签名.在此基础上,我们就可利用代理签名机制建立代理盲签名协议.

3.2 基于离散对数问题的代理盲签名协议

选择大素数 p , p 满足: $p-1$ 的大的素数因子 q 为大素数, $q|(p-1)$,且在 Z_p^* 上离散对数问题是难解问题. g 是 Z_p^* 的 q 阶元, $g^q=1 \pmod p$.若选取私钥 x ,则令公钥为 $y=g^x \pmod p$,公开 p, q, g .设A、B、C是数字签名机制(M, S, K, SIG, VER)的三个用户,他们的密钥对分别为 (x_A, y_A) 、 (x_B, y_B) 、 (x_C, y_C) .A为B的原始签名人,B为A的代理签名人, σ 为委托密钥, $\tilde{\sigma}$ 为代理签名密钥, $y_{\tilde{\sigma}}=g^{\tilde{\sigma}} \pmod p$ 为代理签名公钥, m 为需签名文件信息, $\tilde{m}$ 为B对于C的免责声明信息, $h(x)$ 为一种散列算法, $\parallel$ 表示连接运算.C要求B对消息 m 利用 $\tilde{\sigma}$ 进行盲签名.

(1) A对B的委托过程

A:随机选取一个数 $t \in Z_q^*$,计算 $T=g^t \pmod p$, $\tilde{h}=h(T, y_A)$, $;\sigma=\tilde{h}x_A+tT \pmod q$;

A $\rightarrow$ B: $(\sigma, T, \tilde{h})$;

B:验证等式 $g^{\sigma}=y_A T^t \pmod p$,成立则计算 $\tilde{\sigma}=\sigma+x_B y_B \pmod q$;

(2) 对免责声明信息 $\tilde{m}$ 的签名过程

B $\rightarrow$ C:随机选取一个数 $v \in Z_q^*$,计算 $\tilde{v}=g^v \pmod p$, $\tilde{h}=h(\tilde{m}, \tilde{v})$,将 $(\tilde{m}, \tilde{v}, \tilde{h})$ 发送给C;

C:选择两个随机数,计算 $w=g^a \pmod p$, $r=\tilde{v}^a g^b \pmod p$;

C:计算 $\tilde{w}=g^w \tilde{h} \pmod p$, $e=h(\tilde{w})$, $\tilde{m}=am\tilde{v}^{-1} \pmod q$, $\tilde{e}=h(e \parallel \tilde{m})$;

C:计算 $\tilde{s}=\tilde{h}e x_c+a \pmod p$,以 $(e, \tilde{e}, \tilde{s})$ 作为生成的免责声明信息的签名;

C $\rightarrow$ B: $((e, \tilde{e}, \tilde{s}), \tilde{m})$,将免责声明签名和要B进行盲签的经过处理的文件信息发给B;

(3) 对免责声明信息的签名验证过程

B:计算 $\tilde{e}'=h(e \parallel \tilde{m})$,验证 $\tilde{e}' \equiv \tilde{e}$,计算 $w=g^s y_c^{-e\tilde{h}} \pmod p$, $\tilde{w}=g^w \tilde{h} \pmod p$, $e'=h(\tilde{w})$,验证 $e' \equiv e$;

以上过程的正确性由下式证明: $g^s y_c^{-e\tilde{h}} = g^{\tilde{h}e x_c + a - x_c e\tilde{h}} = g^a = w \pmod p$

(4) 代理盲签名的生成过程

B $\rightarrow$ C:利用代理签名密钥 $\tilde{\sigma}$ 对 $\tilde{m}$ 进行签名,计算 $S=(\tilde{\sigma} + v\tilde{m}) \pmod q$,将 $\tilde{s}$ 发送给C;

C:计算 $s=(\tilde{s}r^{-1} + bm) \pmod q$,则 (r, s, T) 是对 m 的签名.

(5) 代理盲签名的验证过程

验证 $g^s \equiv y_{\tilde{\sigma}} r^m \pmod p$.若成立,则接受 (r, s, T) 是对 m 的签名.否则拒绝.

以上过程的正确性由下式证明:

$$g^s = g^{\tilde{s}r^{-1} + bm} = g^{(\tilde{\sigma} + v\tilde{m})r^{-1} + bm} = g^{\tilde{\sigma}r + v\tilde{m}r^{-1} + bm} = g^{\tilde{\sigma}r + v\tilde{m}r^{-1} + bm} = y_{\tilde{\sigma}} r^{(v\tilde{m} + b)m} = y_{\tilde{\sigma}} r^m \pmod p$$

3.3 协议分析

(1)免责声明的有效性:在构造免责声明的过程中,参与运算的数据包括了C需要B进行盲签名的文件信息 $\tilde{m}$,因此保证了免责声明与被盲签文件信息的相关性.同时由于C的签名是有效的,最终保证免责声明的有效性.当信息 $\tilde{m}$ 最终被发现与B的利益有关,B可以利用该签名来否认盲签文件信息的有效性.

(2)代理签名的不可伪造性:由于只有B才能生成 $\tilde{\sigma}$,所以除B以外(包括A),任何人不可能伪造签名.

(3)代理签名的可区分性:最终的签名为 (r, s, T) 由三部分组成,一部分是普通的签名信息 s ,一部分是某个数 r ,另一个部分是由被代理人产生的数 T ,只要代理人、被代理人的私钥不同或者被代理人开始选的随机数不同, r, s, T 不会同时相同.

(4)不可抵赖性:由代理签名的不可伪造性和代理签名的可区分性可以知道,B对签名是不能抵赖的.

(5)身份证实性和密钥依赖性显然是.

(6)可注销性:只要被代理人宣称 T 失效,则所

有与之相关的签名均失效.

4 与协议相关的一些问题

由于我们的协议主要是基于离散对数问题的难解性,因此对于协议中的参数必须认真考虑其取值,目前针对离散对数问题的攻击方法有以下几种:

- (1) Pohlig-hellman 离散对数算法;
- (2) Pollard-p 离散对数算法;
- (3) 基于有限循环群理论的离散对数算法;
- (4) Shark 离散对数算法:这是一种非常有效的方法,速度很快,需要的存储也少.

这些算法主要是针对离散对数问题中 $(p-1)$ 只有小素数因子或者 p 本身不够大进行的,因此在使用时,建议取 $p > 2^{512}$ 、 $q > 2^{140}$,且 p, q 均为素数,另外协议中用到的随机数尽量与 q 同长度,同时需要保证 q 与 $\sqrt{p}$ 必须差比较大的数量等级.关于散列函数和算法的选择,考虑到目前MD5和SHA-1被攻破,虽然很难评估其对协议本身的影响,但是我们可以选择能够产生512位长度散列值的算法来增强其安全性.

参考文献:

- [1] Cryptography and Network Security: Principles and Practice, Second Edition. William Stallings Prentice [M] Hall, Inc. 1999.
- [2] Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition [M] John Wiley & Sons, Inc. 1996.
- [3] Laih Chi - Sung, Kuo Wen - Chung. New signature scheme based on factoring and discrete logarithms. IEICE [J]. Trans. Fundamentals, 1997, E80-A(1): 46-53.
- [4] Lee W B, Chang C C. Efficient group signature scheme based on the discrete [J]. logarithm. IEE Proc. Comput. Digital Tech., 1998, 145(1): 15-18.
- [5] Nyberg K, Rueppel R A. Message Recovery for Signature Schemes Based on The Discrete Logarithm [J] Problem, Designs, Codes and Cryptography, 1996(7): 61-81.
- [6] Wenbo Mao. Modern Cryptography: Theory and Practice [M]. 北京: 电子工业出版社, 2004.
- [7] 卢开澄. 计算机密码学—计算机网络中的数据保密与安全 [M]. 第3版. 北京: 清华大学出版社, 2003.
- [8] 杨义先, 孙伟, 等. 现代密码学新理论 [M]. 北京: 科学出版社, 2002.

A Proxy Blind Signature Scheme Based on The Discrete Logarithm Problem

LIU Er-gen, ZUO Li-ming

(School of Natural Science, East China Jiaotong Uni., Nanchang 330013, China)

Abstract: A digital signature is used to ensure completeness and effectiveness of some original data. A digital signature scheme consists of a signature generation algorithm and an associated verification algorithm. This paper provides a brief introduction to the basic ideas behind blind and proxy signatures, and shows how these signatures can be realized through reversible public-key encryption techniques. describes in detail a proxy blind signature scheme based on The Discrete Logarithm Problem. Finally, we discuss some techniques based on the intractability of the discrete logarithm problem. Based on above it shows some profit advise which agreement achieving.

Key words: digital signature; blind signature; proxy signature; proxy blind signature scheme; Discrete Logarithm Problem