文章编号:1001 - 9081(2006)06 - 1346 - 02

代理多重签名和指定接收人的代理多重签名方案

张丙娟,余梅生,邹建艳
(燕山大学 信息科学与工程学院,河北 秦皇岛 066004)
(zhangbingjuan2005@126.com)

摘 要:设计了一种基于椭圆曲线离散对数问题(Elliptic Curre Discrete Logarithm Problem, ECDLP)的代理多重签名方案,该方案不仅满足了代理多重签名的所有安全要求,而且避免了签名生成和签名验证过程中费时的求逆运算。在此方案的基础上提出了一种新的指定接收人的代理多重签名方案,并对其安全性进行了分析。

关键词:椭圆曲线离散对数问题;代理多重签名;指定接收人签名
中图分类号: TP309.7 **文献标识码**:A

Proxy multi-signature and designated-receiver proxy multi-signature schemes

ZHANG Bing-juan, YU Mei-sheng, ZOU Jian-yan
(*College of Information Science and Engineering, Yanshan Unversity, Qinghuangdao Hebei* 066004, *China*)

Abstract: Proxy multi-signature scheme was first designed on ECDLP. This scheme can not only satisfy all the security requirements, but also avoid wasting time on inversion operations of its signature generation and verification. Then a new designated-receiver proxy signature scheme was proposed, and its security was analyzed.

Key words: ECDLP; proxy multi-signature scheme; designated-receiver proxy signature scheme

0 引言

1996 年,M Mambao 等人提出了代理数字签名问题[1],并提出了基于素数域的各种代理签名方案,为密码学和数字签名的研究与应用开辟了一个新的领域。文献[2]提出了一类新的代理签名方案——代理多重签名(在一个代理多重签名方案中,一个代理人可以同时代表多个原始签名人的利益在一个文件上签字)。该方案在电子商务和网络安全通信方面有广泛的应用前景。一般情况下的代理多签名方案都是基于群的离散对数问题,基于椭圆曲线离散对数问题的研究成果很少。

椭圆曲线密码体制因为其安全性高、密钥长度短和带宽要求低等优势,受到了越来越多的关注,将成为以后公钥密码体制的主流方向。在安全性相当的情况下,椭圆曲线密码系统比其他一些密码系统(例如:基于整数分解的 RSA、基于离散对数问题的 ELGamal、DSA 等)更加高效。在一个有限域上可以有非常多的曲线适合建立密码系统,从这点而言,椭圆曲线在安全性保障和发展前景上比其他系统更有优势。

指定接收者签名[3,4]是指只有指定的接受者才能验证,而其他的接收者不能验证的签名。在实际应用中,原始签名者除了要求有代理者外还希望能指定一个签名的接受人,代理签名人只能对发给该接收人的信息代理原始签名人签名,而对除此之外的其他信息代理签名人则不能代理原始签名人签名。这种方案适用于许多特定的场合,具有理论和实际的意义,能有效地防止代理签名人滥用代理签名的权利而给原始签名人的权益造成危害。在本文中我们将椭圆曲线密码体制和指定接收者签名的思想结合起来,形成了一种新的指定接收人的签名方案。

1 有限域上的椭圆曲线密码体制[5]

椭圆曲线密码是一种基于椭圆曲线离散对数问题的公钥密码,1985 年由 N Koblitz 和 V Miller 分别提出,之后人们对其进行了大量研究,并形成了系统的密码体制。

1)选取定义在有限域 F_q 上的一条安全曲线 E,使得 E 上的 F_{q^-} 有理点群的阶被一个大素数 n 整除,保证椭圆曲线上有理点群上的离散对数问题是难解的。

2)选取一个基点 $P = (x_P, y_P) \in E$,P 的阶为 n,即有 $nP = O$,O 表示一个无穷远点。基点 P 公开。

3)设 A,B,C 为系统的三个用户,A 的私钥为 $x_A \in_R Z_n^*$,$P_A = x_A P \in E$,P_A 作为 A 的公钥,同样 B 选取私钥为 $x_B \in_R Z_n^*$,$P_B = x_B P \in E$,P_B 作为 B 的公钥,C 选取私钥为 $x_C \in_R Z_n^*$,$P_C = x_C P \in E$,P_C 作为 C 的公钥,公钥 P_A, P_B, P_C 在系统内公开。

2 代理多重签名方案

设 E 是定义在有限域 F 上的一条曲线,用 $\#E$ 表示 E 中元素的个数,并设 n 是 $\#E$ 的一个大素因子,$P \in E$ 是 E 中一个阶为 n 的点。将 E、n、P 公开。假设 $A_1, A_2, \cdots, B$ 是 $n+1$ 个用户,其中 A_i 为原始签名人,B 为代理签名人。

1)初始化过程

A_i 的私钥为 x_i,对应的公钥 $P_i = x_i P$,私钥 x_i 保密,公钥 P_i 公开,其中 $1 \leqslant i \leqslant n$,以下相同;

B 的私钥为 x_B,对应的公钥 $P_B = x_B P$,私钥 x_B 保密,公钥 P_B 公开;

2)数字签名权利的委托过程

原始签名人 A_i 为了将其权利委托给代理签名人 B,又不

收稿日期:2005 - 12 - 16;**修订日期**:2006 - 02 - 27

作者简介:张丙娟(1980 -),女,山东德州人,硕士研究生,主要研究方向:信息安全、数字签名; 余梅生(1943 -),男,教授,主要研究方向:信息安全与通信保密; 邹建艳(1981 -),女,山东青岛人,硕士研究生,主要研究方向:信息安全、数字签名.

暴露自己的私钥 x_i 同时指名代理签名的验证人 C,A_i 首先选取随机数 k_i,并计算 k_iP。即 $Q_i = k_iP = (x_{0i}, y_{0i})$,其中 $x_{0i}, y_{0i} \in F$。然后 A_i 计算:

$r_i = x_{0i} \bmod n$;

$e_1 = H(m_W)$,m_W 包括代理人 B 的身份、代理权限以及代理签名的有效时间;

$\sigma_i = (x_i e_1 + r_i k_i) \bmod n$;

最后 A 将 (Q_i, σ_i, m_W) 秘密的发送给 B,以下称 (Q_i, σ_i, m_W) 为 A_i 将其签名权委托给 B 的委托信息。

代理签名人 B 收到一组委托信息 (Q_i, σ_i, m_W) 后,先计算 $Q_i = (x_i, y_i)$, $r_i = x_{0i} \bmod n$。然后验证以下等式是否成立:

$\sigma_i P = e_1 P_i + r_i Q_i$

其中,P 是 E 的基点,为系统的公开参数,P_i 为原始签名人的公钥。如果等式不成立,代理签名人必须拒绝接受委托信息 (Q_i, σ, m_W),认为 (Q_i, σ_i, m_W) 来自不合法的原始签名人 A_i,如果等式成立,则说明 (Q_i, σ_i, m_W) 来自原始签名人 A_i。

3) 代理签名的产成过程

对于某个消息 m,代理签名人 B 进行以下计算:

$\sigma' = \sum_{i=1}^{n} \sigma_i + x_B \bmod n; e_2 = H(m, m_W)$;

B 随机选取 $k, 0 < k < n$,计算 kP 记 $kP = (x, y)$ 其中 x、$y \in F$ 然后计算:

$r = x \bmod n; s = (e_2\sigma' + k) \bmod n$;

则 $((m, r, s), Q_1, Q_2, \cdots, Q_n, m_W)$ 构成了代理签名人 B 对消息 m 的代理签名。

4) 代理签名的验证过程

接受人收到代理签名 $((m, r, s), Q_1, Q_2, \cdots, Q_n, m_W)$ 后计算:

$sP - e_2(e_1 \sum_{i=1}^{n} P_i + \sum_{i=1}^{n} r_i Q_i + P_B)$,设 $sP - e_2(e_1 \sum_{i=1}^{n} P_i + \sum_{i=1}^{n} r_i Q_i + P_B) = (x, y)$;如果 $x \bmod n \equiv r$,则代理签名 $(m, r, s), Q_1, Q_2, \cdots, Q_n, m_W)$ 得到验证。证明过程如下:

$$
\begin{aligned}
&sP - e_2(e_1 \sum_{i=1}^{n} P_i + \sum_{i=1}^{n} r_i Q_i + P_B) \\
&\quad = (s - e_2(e_1 \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} r_i k_i + k_B))P \\
&\quad = (s - e_2(\sum_{i=1}^{n} (e_1 x_i + r_i k_i) + k_B))P \\
&\quad = (s - e_2(\sum_{i=1}^{n} \sigma_i + k_B))P \\
&\quad = (s - e\sigma')P = kP = (x, y)
\end{aligned}
$$

可见,对验证人来说只要证实 $x \bmod n \equiv r$ 就可说明代理签名的正确性。

此代理多重签名体制所满足的基本性质:

1) 基本的不可伪造性。在这个签名方案中由于 x_i 是保密的,任何人(包括代理签名人 B) 都不能生成原始签名人 A_i 的普通数字签名。

2) 代理多签名的不可伪造性。代理密钥 $\sigma' = \sum_{i=1}^{n} \sigma_i + x_B \bmod n$,所以任何人(包括每一个原始签名人) 都不能生成有效的代理多重签名。

3) 代理签名的可区分性。在代理签名中包含有代表代理签名人身份及权限的 m_W,所以该代理多重签名与原始签名人的普通多重签名有明显的区别,而且不同代理签名人生成的代理多重签名之间也有明显的区别。

4) 不可抵赖性。代理签名 $((m, r, s), Q_1, Q_2, \cdots, Q_n, m_W)$ 的正确性验证需要原始签名人的公钥和代理签名人的公钥,而且签名中包含有代理签名者的身份,所以任何签名人(包括原始签名人和代理签名人) 在生成一个代理多重签名后,不能再对其否认。

5) 身份证实性。在这个签名中每一个原始签名人都可以确定相应的代理签名人的身份。

6) 密钥的依赖性。代理密钥 $\sigma' = \sum_{i=1}^{n} \sigma_i + x_B \bmod n$,依赖与每个原始签名人的秘密密钥和代理签名人的秘密密钥。

7) 可注销性。任何一个原始签名人都可以注销他委托给代理签名人的签名权利。

同时,在该代理方案中,B 不可能无限制地代表 A_i 对消息进行签名,并且有代理时效的限制。若 B 将代理权转移给第三者 D,D 也不可能代表 A_i 对消息进行签名,因 A_i 的授权消息 m_W 包含了代理者的身份等消息,并且 m_W 受单向 hash 函数保护。因此该方案是安全的签名方案。

3　一种指定接收人的代理多重签名方案

假设 $A_1, A_2, \cdots, B, C$ 是 $n+2$ 个用户,其中 A_i 为原始签名人,B 为代理签名人,C 为代理签名的验证人。椭圆曲线参数选择同上。

1) 初始化过程

A_i 的私钥为 x_i,对应的公钥 $P_i = x_i P$,私钥 x_i 保密,公钥 P_i 公开,其中 $1 \leqslant i \leqslant n$,以下相同;

B 的私钥为 x_B,对应的公钥 $P_B = x_B P$,私钥 x_B 保密,公钥 P_B 公开;

C 的私钥为 x_C,对应的公钥 $P_C = x_C P$,私钥 x_C 保密,公钥 P_C 公开;

2) 数字签名权利的委托过程

原始签名人 A_i 将其权利委托给代理签名人 B,同时指名代理签名的验证人 C。A_i 首先选取随机数 k_i,并计算 k_iP。即 $Q_i = k_iP = (x_{0i}, y_{0i})$,其中 $x_{0i}, y_{0i} \in F$。然后 A_i 计算:

$r_i = x_{0i} \bmod n$;

$e_1 = H(P_C, m_W)$,m_W 包括代理人 B 的身份,验证人 C 的身份,代理权限,以及代理签名的有效时间,P_C 为验证者 C 的公钥;

$\sigma_i = (x_i e_1 + r_i k_i) \bmod n$;

最后 A 将委托信息 $(Q_i, \sigma_i, m_W, P_C)$ 秘密的发送给 B。

代理签名人 B 收到一组委托信息 $(Q_i, \sigma_i, m_W, P_C)$ 后,先计算 $Q_i = (x_{0i}, y_{0i})$, $r_i = x_{0i} \bmod n$。然后验证以下等式是否成立:

$\sigma_i P = e_1 P_i + r_i Q_i$

如果等式不成立,代理签名人必须拒绝接受委托信息 (Q_i, σ, m_W, P_C),认为 $(Q_i, \sigma_i, m_W, P_C)$ 来自不合法的原始签名人 A_i,如果等式成立,则说明 $(Q_i, \sigma_i, m_W, P_C)$ 来自原始签名人 A_i。

3) 代理签名的产成过程

对于某个消息 m,代理签名人 B 进行以下计算:

$\sigma' = \sum_{i=1}^{n} \sigma_i + x_B \bmod n; e_2 = H(m, P_C, m_W)$

B 随机选取 $k, 0 < k < n$,计算 kP_C 记 $kP_C = (x, y)$ 其中 x、$y \in F$ 然后计算:

$r = x \bmod n; s = (e_2\sigma' + k) \bmod n$

则 $((m, r, s), Q_1, Q_2, \cdots, Q_n, m_W)$ 构成了代理签名人 B 对消息 m 的代理签名。

(下转第 1350 页)

3）本地 OCSP 响应器取出客户端请求中的“id-pkix-service-locator”扩展项内容，利用 MD5 算法计算相应的 Hash 值 H，再将包含 H 的 DNS 查询以记录类型为“A”的形式发送到根 DNS-OCSP 服务器，其中，记录类型“A”表示一个主机的 IP 地址记录。

4）根 DNS-OCSP 服务器从收到的 DNS 查询取出问题证书的权威 OCSP 响应器信息，再解析该权威 OCSP 响应器的 IP 地址。如果能成功解析则将权威 OCSP 响应器的 IP 地址返回给本地 OCSP 响应器，否则返回错误信息给本地 OCSP 响应器。

5）如果本地 OCSP 响应器收到的是正确的权威 OCSP 响应器的 IP 地址，则新生成一个 OCSP 请求再发送到权威 OCSP 响应器。然后权威 OCSP 响应器生成数字签名或未数字签名的响应返回到本地 OCSP 响应器，本地 OCSP 响应器再将响应返回到客户端，流程结束。

6）如果本地 OCSP 响应器收到的是错误信息，则生成“unknown”响应返回到客户端，流程结束。

5 结语

本文提出的 DNS-OCSP 结合 DNS 的 referral 工作原理，使客户端只要求知道一个本地 OCSP 响应器的地址，而不需知道所有权威 OCSP 响应器的地址，也能查询任何一个权威 OCSP 响应器，这样，就可构建一种统一的证书验证模式，使不同 CA 的证书验证成为可能。并且，本系统建立在 DNS 基础上，所以具有较强的扩展性。

但本系统还存在两个主要问题有待进一步研究：

1）因为从本地 OCSP 响应器到根 DNS-OCSP 服务器的 DNS 查询未加密，也未数字签名。这样就存在 DOS 攻击的可能。攻击者可能在返回给本地响应器的响应中包含错误权威响应器的 IP 地址，造成证书状态查询时返回“unknown”信息，从而阻止正常的证书验证。

2）与 CRL 相比，CRL 仅需在发布时进行一次数字签名，而 DNS-OCSP 对每一个返回“good”或“revoked”状态的响应均需要数字签名，这样 DNS-OCSP 响应器负载将随 OCSP 请求的增加而成比例上升，所以系统的负载平衡也是需要考虑的问题。

参考文献：

[1] HOUSLEY R, POLK W, FORD W, *et al*. Internet x.509 public key infrastructure: Certificate and certificate revocation list(crl) profile[S]. RFC3280, IETF, http://www.ietf.org/rfc/rfc3280.txt?number=3280, April 2002.

[2] HOUSLEY R, FORD W, POLK W, *et al*. Internet x.509 public key infrastructure certificate and crl profile[S]. RFC2459, IETF, http://www.ietf.org/rfc/rfc2459.txt, January 1999.

[3] MYERS M, ANKNEY R, MALPANI A, *et al*. Online Certificate Status Protocol, version 2.[EB/OL] http://tools.ietf.org/wg/pkix/draft-ietf-pkix-ocspv2/draft-ietf-pkix-ocspv2-02.txt, March 2001.

[4] E-Soft Inc. Secure server survey[EB/OL]. http://www.securityspace.com/s_survey/sdata/200508/certca.html, August 2005.

[5] VeriSign Inc. Verisign international server ca-class 3 crl[EB/OL]. http://crl.verisign.com/Class3InternationalServer.crl, July 2005.

[6] GeoTrust Inc. Equifax secure certificate authoritycrl[EB/OL]. http://crl.geotrust.com/crls/secureca.crl, July 2005.

[7] Thawte Consulting Ltd. Thawte server ca crl[EB/OL]. https://www.thawte.com/cgi/lifecycle/ThawteServerCA.crl, July 2005.

[8] Entrust Inc. Entrust SSL Web Server Certificate Practice Statement[EB/OL]. http://www.entrust.com/ssl-certificates/CPS/pdf/webcps112803.pdf, November 2003.

（上接第 1347 页）

4）代理签名的验证过程

指定的验证人 C 收到代理签名$((m,r,s),Q_1,Q_2,\cdots,Q_n,m_W)$后计算：

$x_C(sP-e_2(e_1\sum_{i=1}^{n}P_i+\sum_{i=1}^{n}r_iQ_i+P_B))$，设 $x_C(sP-e_2(e_1\sum_{i=1}^{n}P_i+\sum_{i=1}^{n}r_iQ_i+P_B))=(x,y)$；如果 $x \bmod n \equiv r$，则代理签名$(m,r,s),Q_1,Q_2,\cdots,Q_n,m_W)$得到验证。验证过程的正确性可证明如下：

$$
\begin{aligned}
&x_C(sP-e_2(e_1\sum_{i=1}^{n}P_i+\sum_{i=1}^{n}r_iQ_i+P_B))\\
&=x_C(s-e_2(e_1\sum_{i=1}^{n}x_i+\sum_{i=1}^{n}r_ik_i+k_B))P\\
&=x_C(s-e_2(\sum_{i=1}^{n}(e_1x_i+r_ik_i)+k_B))P\\
&=x_C(s-e_2(\sum_{i=1}^{n}\sigma+k_B))P\\
&=x_C(s-e\sigma')P=x_CkP=(x,y)
\end{aligned}
$$

可见，对验证人来说只要证实 $x \bmod n \equiv r$ 就可说明代理签名的正确性。

这个指定接收人的代理多重签名方案除了满足同上的性质外，还满足用户机密性，即只有指定的接受人 C 才可以验证签名的正确性，因此也只有 C 才可以向第三方证明签名的有效性。除 C 外任何第三方不能从签名中得到原始签名人 A_i 或代理签名人 B 的身份。

4 结语

在我们所提出的方案中，没有求逆运算和指数运算，所以复杂度比较低，从而提高了签名生成和验证过程的速度。根据 ECDLP 的难解性和哈希函数的单向性可知该方案安全性比较高。由于 x_i,x_B,x_C 是保密的，所以对攻击者而言 σ 和 σ' 是不可求的，而且在这两个签名方案中 s 的运算法则同 Schnorr 签名方案中 s 的运算法则，所以综合上述安全因素，攻击是不可能的。

参考文献：

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature for delegating signing operation[A]. Proceedings of 3rd ACM Conference on Computer and Communication Security[C]. New Delhi: ACM, 1996.48-57.

[2] YI LJ, BAI GQ, XIAO GZ. Proxy Multi-Signature: A New Type of Proxy Signature Schemes[J]. Acta ElectronicaSinica, 2001, 29(4): 1-2.

[3] 曹珍富，李建中，李继国. 一个新的具有指定接受者(t, n)门限签名加密方案[J]. 通信学报，2003，24(5)：8-13.

[4] 张彰，蔡勉，肖国镇. 一个高效的门限共享验证签名方案及其应用[J]. 通信学报，2003，24(5)：134-139.

[5] ANSI X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature(ECDSA)[S].