ISSN 1000-9825 Journal of Software 软件学报 2000,11(10):1303~1306

一种椭圆曲线签名方案与基于身份的签名协议*

杨君辉[1] 戴宗铎[2] 杨栋毅[3] 刘宏伟[3]

[1](中国科学院软件研究所 北京 100080)

[2](中国科学技术大学研究生院信息安全国家重点实验室 北京 100039)

[3](北京兆日科技有限公司 北京 100089)

E-mail: yangdai@mimi.cnc.ac.cn

摘要 提出一种椭圆曲线数字签名算法.此方案比已有的椭圆曲线数字签名算法(elliptic curve digital signature algorithm,简称ECDSA)和Schnorr签名方案简单、有效.此外,还给出了基于身份蕴含公钥认证的椭圆曲线签名协议.

关键词 椭圆曲线,数字签名,离散对数.

中图法分类号 TP393

椭圆曲线密码是基于有限域上椭圆曲线有理点群的一种密码系统.它的安全性基于有限域上椭圆曲线离散对数问题(ECDLP),是一个困难问题.ECDLP比有限域上的离散对数问题(DLP)要困难得多.我们将分析RSA系统,对ElGamal密码和椭圆曲线密码所需要的计算量做个比较.记 $L_p(v,c)=\exp(c(\log p)^v(\log\log p)^{1-v})$. $L_p(v,c)$相对于参数$\log p$,当$v=0$时,是多项式关系;当$v=1$时,是指数关系;而当$0<v<1$时,则称为亚指数关系.众所熟知,对于模数为n的RSA系统,用数域筛法分解n的计算复杂性是$L_n(1/3,c)$,其中c是某个常数.同样,用数域筛法求有限域$GF(p)$上的离散对数的计算复杂性也是$L_p(1/3,c')$,其中c'是某个常数.而直至目前,已知求有限域上椭圆曲线的离散对数(ECDLP)的计算复杂性是$L_p(1,c)$.即攻击RSA和ElGamal系统存在亚指数算法,而攻击椭圆曲线密码是指数算法.因而,对于相同规模的参数,椭圆曲线密码每一比特密钥的强度要大得多.要得到同样强度的密码,椭圆曲线系统的参数规模要小得多.设n,N分别表示具有相同计算复杂性的椭圆曲线系统和ElGamal系统相应的有限域的规模,那么n,N有以下关系:

$$n=4.91N^{1/3}(\log(N\log 2))^{2/3}.$$

由这一公式可得到n,N的一组对应的数据(173,1024),(230,2048),(313,4096),即173比特的椭圆曲线系统相当于1024比特的ElGamal系统或RSA系统等等.可见,椭圆曲线系统的参数规模要小得多,而小的参数无论在实现上还是在应用上都具有较大的优越性.椭圆曲线密码的另一优点是椭圆曲线资源极丰富,一个有限域$GF(q)$中仅有一个乘法群,但其上彼此不同构的椭圆曲线的个数大于q.因而,椭圆曲线密码被普遍看好,被认为是新一代公钥密码系统.

本文由签名方程出发,推出一种椭圆曲线签名算法.该算法避免了Z_n中的求逆运算,比文献[1]中建议的椭圆曲线签名算法(elliptic curve digital signature algorithm,简称ECDSA)要简单,也比Schnorr签名方案简单.

1 椭圆曲线签名算法ECDSA及其变型

DSA是美国国家标准局制定的数字签名算法,它是建立在有限域乘法群上的.对于有限域上的椭圆曲线密

* 本文研究得到国家自然科学基金(Nos.69773015,69873043)资助,作者杨君辉,1942年生,研究员,主要研究领域为密码学.戴宗铎,女,1941年生,教授,博士生导师,主要研究领域为代数编码,密码学.杨栋毅,1963年生,博士,高级工程师,主要研究领域为信息安全系统,专用集成电路.刘宏伟,1968年生,博士,副教授,主要研究领域为信息安全系统,专用集成电路.

本文通讯联系人:杨君辉,北京 100080,中国科学院软件研究所

本文2000-05-31收到原稿,2000-06-30收到修改稿

© 中国科学院软件研究所 http://www.jos.org.cn

码系统,相应于 DSA,文献[1]建议采用椭圆曲线数字签名算法 ECDSA.下面给出此算法.

设系统参数是(F_q,E,P,n,h),其中F_q是有限域,E是F_q上的曲线,P是E上的一个有理点,称为基点,P的阶为素数n,E的有理点群的阶 Order$(E)=hn$.人们总是选择使 Order(E)几乎是素数,即h很小这样的曲线.当域的特征为 2 时,使得$h=2$或$h=4$;当域的特征为大素数时,$h=1$——找到这样的曲线不是很困难.系统的每一用户有一私钥k,公钥是$P_k=kP$.系统有一个 Hash 函数h.下面是 ECDSA 方案.

ECDSA

签名过程:

(1) A随机选择一个整数t,$1<t<n$,计算$tP=(x,y)$,$r=x \bmod n$;

(2) 计算$e=h(m)$;

(3) 计算$s=t^{-1}(e+rk) \bmod n$;

(4) m的签名为(s,r).

签名的验证:

(1) 计算$e=h(m)$;

(2) $u=s^{-1}e$,$v=s^{-1}r$;

(3) $(x_1,y_1)=uP+vP_k$,$r_1=x_1 \bmod n$;

(4) 如果$r=r_1$,则接受这个签名.

上面的签名方案与 ElGamal 以及 DSA 方案类似,在求s时需要计算Z_n中的逆元,这需要用扩展欧几里得算法以及多个整数除法与乘法,复不仅杂而且费时.人们利用以下称为签名方程的方法给出了 ElGamal 签名方案的多种变型.方程

$$u=wt+vk$$

称为签名方程.上述 ECDSA 签名方案就是(u,v,w)取$(e,-r,s)$得到的.ElGamal 数字签名方案的基本变型是取(e,r,s)的排列替代(u,v,w)而得到.

下面列出 6 种基本签名方程[2],它们定义了s和(r,t,k,e)的关系.

$$e=st+rk,$$

$$e=rt+sk,$$

$$s=et+rk,$$

$$s=rt+ek,$$

$$r=et+sk,$$

$$r=st+ek.$$

在下一节中,我们将由其中的一个签名方程出发,推导出一些椭圆曲线数字签名方案.

2　一些椭圆曲线数字签名方案

在这一节,我们由上面的第 3 个签名方程出发,推导出一些数字签名方案.

在上面的第 3 个签名方程$s=et+rk$中,我们用e^{-1}代替e,得到另一个方程:

$$s=e^{-1}t+rk.$$

在等式两边乘上e,得

$$se=t+rek.$$

由于$e=h(m)$对信息签名的发方和收方都是已知的,令$s'=se$,可以用(s',r)代替(s,r)作为信息m的签名.这时,签名方程变为

$$s=t+(re)k.$$

其中re是Z_n中乘法群的二元运算.如果我们将运算re换成域Z_n中加法群的运算$r+e$或二元扩域$GF(2^m)$加法群的运算$r\oplus e$(假设n的大小相当于m比特),它们的安全性应该是一样的,因为re,$r+e$以及$r\oplus e$之间有一种类似于"同构"的对应.下面用一个例子来加以说明.

© 中国科学院软件研究所 http://www.jos.org.cn

众所熟知,在ElGamal型的签名中,Hash函数不能省去,即$e=h(m)$不能用m代替,否则,就能伪造签名.请看下面的例子.

假设C已得到A对信息m的合法签名(s,r),采用的签名方程是$s=t+(mr)k$.C利用(m,s,r)能够得到$G=tP=sP-(mr)P_A$.C任选一整数a,计算$(t+a)P=G+aP=(x_1,y_1)$,$r_1=x_1=rr_0 \bmod n$.那么,令$s_1=s+a$,则(s_1,r_1)是信息mr_0^{-1}的合法签名,因为有$s_1=s+a=t+a+(mr)k=t+a+(mr_0^{-1}rr_0)k$.

我们知道,在$GF(n)$加法群中r_0的逆元是$-r_0$,在域$GF(2^m)$加法群中r_0的逆元是r_0.所以,不必再作推理,我们可以得到如下对应:

t	r_1	s_1	m	方程
$t+a$	rr_0	$s+a$	mr_0^{-1}	$s=t+(mr)k$
$t+a$	$r+r_0$	$s+a$	$m-r_0$	$s=t+(m+r)k$
$t+a$	$r\oplus r_0$	$s+a$	$m\oplus r_0$	$s=t+(m\oplus r)k$

因此,如果采用签名方程$s=t+(r+m)k$,则(s_1,r_1)是信息$m-r_0$的合法签名;如果采用的签名方程是$s=t+(r\oplus m)k$,则(s_1,r_1)是信息$m\oplus r_0$的合法签名.

这个例子用来说明二元运算mr,$m+r$以及$m\ominus r$有着对应关系,它们所对应的签名方程$s=t+(mr)k$,$s=t+(r+e)k$以及$s=t+(r\oplus m)k$中任何一个具有的弱点,另两个方程也必定相应地存在.在3种签名方案中,以第3个方案最为简单.这里,我们将此方案完整地叙述如下:设系统参数为$(GF(q),E,P,n,h)$,系统用户A的私钥是k,公钥是$P_A=kP$.

信息m的签名过程:

(1) A选择一个随机数t,$1<t<n$,计算$tP=(x,y)$,$r=x \bmod n$;

(2) 计算$e=h(m)$;

(3) 计算$s=t+(r\oplus r)k \bmod n$;

(4) (s,r)为信息m的签名.

签名的验证计算过程:

(1) $e=h(m)$;

(2) $u=e\oplus r \bmod n$;

(3) $(x_1,y_1)=sP-uP_k$,$r_1=x_1 \bmod n$;

(4) 如果$r=r_1$,则该签名为合法签名.

这一方案避免了$GF(n)^*$中的求逆运算,因而比ECDSA算法简单.我们知道,Schnorr签名方案的签名方程是$s=t+h(m,r)k$.计算$h(m)\oplus r$应比计算$h(m,r)$要简单些,所以,上述算法比Schnorr方案略快些.

3 基于身份的数字签名协议

一个数字签名认证系统如果有成千上万、甚至几十万、几百万用户,公钥的管理和存储就是一个大问题.下面,我们利用上述签名方案给出一个基于身份隐含认证的椭圆曲线数字签名认证系统方案.这种系统用户不需要存储公钥,公钥是在验证时依据用户身份信息重新计算出来的.但这种系统需依赖一个可信任的第三方.

它的做法是由第三方T,分配给每一个系统用户一个唯一的身份号I_A.T用一种安全的签名方案对I_A签名,产生用户A的私钥,并且秘密地传送给A.A用这个私钥进行信息签名.在验证时,验证方利用T的公钥以及A的身份I_A计算出A的公钥,再进行通常的认证.该协议由私钥产生,签名和认证这3部分构成.

设系统参数为$(GF(q),E,P,n,h)$.

私钥的生成:

(1) T选择一个秘密整数$k_T$$(1<k_T<n)$作为私钥,将$P_T=k_TP$作为公钥,是系统的公开参数.

(2) T分配每一位系统使用者一个身份号I_A.T选择一个随机数k_A^0,计算

$$P_A=k_A^0P=(x_0,y_0),\quad p_A=x_0 \bmod n;$$

© 中国科学院软件研究所 http://www.jos.org.cn

(3) 计算 $k_A=k_A^0+(p_A\oplus h(I_A))k_T$;

(4) T 将(P_A,k_A)秘密送给用户 A,k_A 是 A 的私钥,需保密;

(5) A 的公钥是 $k_AP=k_A^0P+(p_A\oplus h(I_A))P_T=P_A+(p_A\oplus h(I_A))P_T$.

签名过程:

(1) A 随机选择一个整数 t,计算 $tP=(x,y)$,$r=x \bmod n$;

(2) $e=h(m)$;

(3) $s=t\mid(e\oplus r)k_A$;

(4) (s,r)是信息 m 的签名,A 送出的信息是(m,s,r,I_A,P_A),其中 I_A,P_A 是常量.

验证签名过程:

(1) 设 $P_A=(x_0,y_0)$,$p_A=x_0P \bmod n$;

(2) 计算 A 的公钥 $G=P_A+(p_A\oplus h(I_A))P_T$;

(3) 计算 $e=h(m)$,$u=(e\oplus r) \bmod n$;

(4) 计算$(x_1,y_1)=sP-uG$,$r_1=x_1 \bmod n$;

(5) 比较 $r=r_1$?

4 结　论

本文由签名方程出发,推导出一个较为简单的椭圆曲线数字签名方案,并用这一方案给出了基于身份隐含(公钥)认证的椭圆曲线数字签名系统协议.

参考文献

1 Johson D, Menezes A. The elliptic curve digital signature algorithm. Technical Report, CORR 99-31, Canada: Department of Combinatorics and Optimization, University of Waterloo, 1999

2 Menezes A, Van Oorschot P C, Vanstone S. Handbook of Applied Cryptography. New York: CRC Press, 1996. 425～460

An Elliptic Curve Signature Scheme and an Identity-Based Signature Agreement

YANG Jun-hui[1]　DAI Zong-duo[2]　YANG Dong-yi[3]　LIU Hong-wei[3]

[1](*Institute of Software　The Chinese Academy of Sciences　Beijing*　100080)

[2](*State Key Laboratory of Information Security　Graduate School of University of Science and Tehnology of China　Beijing*　100039)

[3](*Beijing Sinosun Technology Co. Ltd　Beijing*　100089)

Abstract　In this paper, an elliptic curve signature scheme is proposed. This scheme is more efficient than ECDSA (elliptic curve digital signature algorithm) and Schnorr scheme. In addition, an implicitly-certified identity-based public key agreement is also provided.

Key words　Elliptic curve, digital signature, discrete logarithm.

© 中国科学院软件研究所 http://www.jos.org.cn