一类有限域丢番图方程的解及其应用①

陈持协[1], 王　标[1], 方颖珏[2], 巩小星[1]

[1](国际关系学院 信息科技系, 北京 100091)
[2](深圳大学 数学与计算科学学院, 深圳 518060)

摘　要:对一类有限域线性丢番图方程 $c\equiv x+by(\mathrm{mod}\ N)$进行了研究, 求出了其通解及域中有效解的对数, 并证明其能将部分曲线密码方案求解用户私钥的计算量降低为 N/z, z 为子群<-b>的最小非零元. 指出了 5 个应用该类型方程曲线密码方案, 最后以一个环 Z_n 上广义圆锥曲线多重数字签名方案私钥的求解为例进行说明.

关键词: 有限域; 丢番图方程; 通解; 曲线密码学; 私钥

Solution to a Class of Diophantine Equations over a Finite Field and Its Application

CHEN Chi-Xie[1], WANG Biao[1], FANG Ying-Jue[2], GONG Xiao-Xing[1]

[1](Department of Information and Technology, University of International Relations, Beijing 100091, China)
[2](College of Mathematics and Computational Science, Shenzhen University, Shenzhen 518060, China)

Abstract: This paper focuses on $c\equiv x+by(\mathrm{mod}\ N)$, the linear Diophantine equations over a finite field, and derives the general solution and the amount of solutions in the domain from the equations. Then demonstrates that this solution can partly reduce the amount of calculation which derive the signer's private key in some curve cryptography schemes to N/z (z is the smallest non-zero element of subgroup <-b>). Finally, lists five curve cryptography schemes that based on this type of equation, and takes the solution of the private key of a digital multi-signature scheme on the generalized conic curve over Z_n as an example to introduce the topic.

Key words: finite field; diophantine equation; general solution; curve cryptography; private key

丢番图方程(或称不定方程)是数论最古老、最重要的分支之一, 按照方程的形式可以分为 N 次方程、指数方程以及与其它学科融合产生的特殊形式方程, 如丢番图在密码学中的有限域形式.

1978 年 Manders[1]等人利用丢番图方程的困难性[2]证明 $ax^2+by-c=0$ 自然数解的判别属于 NP 完全问题以后, 丢番图方程在公钥密码体制中的应用备受研究人员关注, 如杨义先[3]、孙琦[4]等先后利用丢番图方程构造公钥密码方案, 李大兴[5]、曹珍富[6]等人亦进行了深入的研究. 之后, 随着曲线密码体制, 特别是椭圆曲线和圆锥曲线密码体制的广泛应用, 更多的方案被提出, 有限域丢番图方程在密码学领域得到进一步发展.

本文在前人研究的基础上, 求出一类有限域丢番图方程 $c\equiv x+by(\mathrm{mod}\,N)$ 的通解及其在域中有效解的对数. 进一步证明使用该类型方程构造的密码方案存在一定的安全问题, 并举例说明, 同时指出了 5 个应用此类型方程构造的签名方案. 研究结果对密码学中加密与签名方案的设计提出的几点新的要求, 以提高方案的安全性.

1　线性丢番图方程及其解的理论

由于线性丢番图内容较多, 在此仅指出其定义及对本文有意义的基本定理.

定义 1. 线性丢番图方程是指形为

$$a_1x_1+a_2x_2+\cdots+a_nx_n=c \tag{1}$$

的方程, 其中 $a_1, a_2, \ldots, a_n$ 和 c 为整形常量, $x_1, x_2, \ldots, x_n$ 为整形变量.

① 基金项目:中央高校基本科研业务费专项资金项目(3262015T48;KYF-2012-T09);北京市科技新星计划项目(XX2014B052);
大学生学术支持项目(3262014S190)
收稿时间:2015-03-17;收到修改稿时间:2015-05-07

根据线性丢番图方程解的理论, 有如下定理:

定理 1. 对线性丢番图方程(1), 记 $l=\gcd(a_1,a_2,\cdots,a_n)$, 当且仅当 $l\mid c$ 时, 方程有解. 且当 $l\mid c$ 时, 记 $A=(a_1,a_2,\cdots,a_n)^T$, $c'=c/l$, $D=(l,0,\cdots,0)^T$, U 是任一满足 $UA=D$ 的整形幺阵, 则方程(1)通解为

$$(x_1,x_2,\cdots,x_n)=(c',t_2,t_3,\cdots,t_n)*U$$

其中 $\gcd(a_1,a_2,\cdots,a_n)$ 表示 a_1, a_2, …, a_n 的最大公约数, $l\mid c$ 表示 c 能被 l 整除, t_2, …, t_n 是任意整数.

关于线性丢番图方程及其解的理论可参见文献[7,8].

2 一类有限域丢番图方程及其解的理论

定义 2. 有限域线性丢番图方程指形为:

$$c\equiv a_1x_1+a_2x_2+\cdots+a_nx_n(\mathrm{mod}\,N)$$

的方程, 其中 a_1, a_2, …, a_n, c 和 N 为整形常数, x_1, x_2, …, x_n 为整形变量.

本文主要针对其中 $a_1=1$, $n=2$ 的一类二元一次有限域线性丢番图方程的解进行分析.

即

$$c\equiv x+by(\mathrm{mod}\,N) \tag{2}$$

对方程(2), 有如下定理.

定理 2 有限域线性丢番图方程(2)有解, 且其解为

$$\begin{cases} x=c-(c-t)b \\ y=c-t \end{cases} \tag{3}$$

其中 t =0, 1, 2….

证明: 记 $l=\gcd(1,b)$, 则 $l=1$, $l\mid c$ 恒成立, 根据本文定理 1, 有

$$\begin{cases} x=\dfrac{uc+bt}{l}=uc+bt \\ y=\dfrac{vc-1\cdot t}{l}=vc-1\cdot t \end{cases}$$

其中 $t=0,1,2,\cdots$, u 和 v 为参数, 且 $u+bv=l=1$.

由欧几里得算法, 解得 u=1-b, v=1, 因此 x 和 y 的通解为式(3), 证毕.

根据有限群论的相关理论[9], 有以下定理.

定理3. 群 $(Z_n,+)$ 的子群 $\langle -b\rangle$, 其阶 $O\langle -b\rangle=\dfrac{N}{z}$, 则方程(2)中 x 有效解的个数为 $\dfrac{N}{z}$, 其中 z 为子群的最小非零元.

证明: 对于式(2), 其中 y 每增加 $O\langle -b\rangle$ 时, 有

$$\begin{aligned} &b(y+O\langle -b\rangle)(\mathrm{mod}\,N)\\ &=by+bO\langle -b\rangle(\mathrm{mod}\,N)\\ &=by+b\frac{N}{z}(\mathrm{mod}\,N)\\ &=by(\mathrm{mod}\,N) \end{aligned}$$

故 x 的周期为 $\dfrac{N}{z}$, 命题得证.

3 在曲线多重数字签名私钥求解中的应用

通过研究发现, 文献[10]-[14]所提出的数字签名方案, 都存在签名分量的构造式属于本文式子(2)所述方程类别, 攻击者可藉此降低求解签名者私钥的计算量, 使得上述文献所提方案存在安全隐患.

3.1 多重数字签名方案

1983 年 ITAKURA 等人[15]提出了多重数字签名, 以满足实际生活中多个用户同时对某一消息进行认证的需求. 之后, 多重数字签名方案由于其实用价值而备受研究人员关注, 基于不同数学难题的多重数字签名方案[16,17]被相继提出. 根据签名方式, 可分为有序多重数字签名和广播多重数字签名.

2009 年, 林松等人[10]提出了基于环 Z_n 上广义圆锥曲线的多重数字签名方案(记为 LWL 方案), 该方案为基于离散对数难题的广播多重数字签名方案, 可以抵抗 Pohlig–Hellman 攻击和 Wiener 攻击. 并且具有明文嵌入方便, 元素逆元求解速度快, 元素阶的计算及曲线上点乘运算比较容易等特点. 丁丽等人在文献[11]中指出该方案存在安全漏洞, 不能对抗内部成员攻击和流氓密钥攻击, 并提出改进方案(记为 DZQ 方案).

进一步研究发现, LWL 以及 DZQ 方案签名分量的构造式均属于定义 2 所述类型有限域丢番图方程, 根据定理 2 和定理 3, 攻击者只需穷举部分密钥空间即可获得签名者私钥, 方案的安全性被降低. 此外, 还有部分曲线公钥密码加密方案, 如文献[12]-[14]所提方案亦是同理, 在此不做赘述.

本文以 LWL 方案签名者私钥求解为例进行说明. 首先简要介绍环 Z_n 上广义圆锥曲线基础内容.

3.2 环 Zn 上广义圆锥曲线

Z_n 为一个模 n 的剩余类环, 环 Z_n 上广义圆锥曲线是指同余方程

$$y^2\equiv ax^2-bx-cxy(\mathrm{mod}\,n)$$

在 Z_n 上的解集, 一般记为 $R_n(a,b,c)$, 其中 $n=pq$, p, q 为两个不同的奇素数, 且有 $(a,n)=(b,n)=1$.

广义圆锥曲线 $R_n(a,b,c)$ 中，若满足 x^2+cx-a 在 F_p 和 F_q 上均不可约，且 $p+1=2r$，$q+1=2s$，其中 r，s 也为素数，则 $R_n(a,b,c)$ 中存在一个点 G，其阶 $N_n=lcm\{|R_p(a,b,c)|,|R_q(a,b,c)|\}=lcm\{p+1,q+1\}=2rs$，符号 $lcm\{a,b\}$ 表示 a 和 b 的最小公倍数，且 $(R_n(a,b,c),\oplus)$ 中任一元的阶整除 N_n. 广义圆锥曲线密码体制的理论参见文献[18].

3.3 LWL 多重数字签名方案

以下仅简要介绍其签名验证过程，详见文[10].

假设有 k 个签名者参与签名，记每个签名者 U_i 的私钥为 d_i，对应的公钥为 $Q_i=d_iG(\mathrm{mod}\,n)$，$G$ 为曲线基点，$H(m)$ 是待签名消息 m 的单向 hash 值. 公开 n，G，Q_i，保密用户私钥 d_i.

签名过程:

① 签名者随机选取整数 $k_i\in Z_{N_n}^*$，计算 $C_i=k_iG=(x_i,y_i)$ 和 $\delta_i=k_i-d_iH(m)(\mathrm{mod}\,N_n)$，将 (C_i,δ_i) 作为签名发给收集者;

②收集者收到每个签名者对 m 的签名 (C_i,δ_i) 后，计算 $C=\sum_{i=1}^{k}C_i(\mathrm{mod}\,n)$ 和 $\delta=\sum_{i=1}^{k}\delta_i(\mathrm{mod}\,N_n)$，若 $C\neq 0$，$\delta\neq 0$ 则 (C,δ) 为消息 m 的多重数字签名，否则让各签名者重新签名.

验证过程:

验证方根据签名者公钥以及收到的签名，计算 $Q=\sum_{i=1}^{k}Q_i(\mathrm{mod}\,n)$，$C^*=\delta G\oplus H(m)Q$，验证 C^* 与 C 是否相等.

3.4 对 LWL 方案求解签名者私钥

上述 LWL 方案中，签名分量 δ_i 的构造式为

$$\delta_i=k_i-d_iH(m)(\mathrm{mod}\,N_n) \tag{4}$$

对于攻击者，δ_i 和 $H(m)$ 已知，k_i 和 d_i 未知，攻击者要求解签名者私钥 d_i，根据定理 2，且其解为

$$\begin{cases} d_i=\delta_i-t_i \\ k_i=\delta_i+(\delta_i-t_i)H(m) \end{cases}$$

其中 $t_i=0,1,2\cdots$.

又由定理 3 可知，攻击者求解签名者私钥最多需要 $\frac{N_n}{z}$ 次有限数域上的一阶多项式运算(时间损耗较少)，及 $\frac{N_n}{z}+z$ 次广义圆锥曲线上的倍点运算，其中 z 为子群 $\langle H(m)\rangle$ 的最小非零元. 若无上述定理，攻击者至少需要计算 $\frac{N_n}{z}$ 次广义圆锥曲线上的倍点运算.

例 1　对 LWL 方案求解用户私钥数值模拟.

取曲线 $R_{65}(2,1,0)$：$y^2\equiv 2x^2-x(\mathrm{mod}\,65)$，则有 $p=5$，$q=13$，$r=(p+1)/2=3$，$s=(q+1)/2=7$，$N_n=2rs=42$，并选取基点 $G=P(2)=(32,64)$;

签名者 U_1 选取私钥 $d_1=5$，公钥 $Q_1=d_1G=5P(2)=P(3)$，对消息 m 的 hash 值 $0<H(m)=15<N_n$ 签名如下:

① 随机选取 $0<k_1=4<N_n$，计算 $k_1G=4P(2)=(51,56)$，则 $51\equiv 9(\mathrm{mod}\,42)$，$56=14(\mathrm{mod}\,42)$;

②计算 $\delta_1=k_1-d_1H(m)=4-5\times 15=13(\mathrm{mod}\,42)$.

则 U_1 对消息 $H(m)$ 的签名为(9, 14, 13).

攻击者根据消息 $H(m)=15$ 的签名(9, 14, 13)，代入式(4)有

$$13=k_1-15*d_1(\mathrm{mod}\,42) \tag{5}$$

又知子群 $\langle 15\rangle$ 的最小非零元为 3，则攻击者只需按顺序求解 42/3=14 对(d_1, k_1)的值，如下表 1 所示.

表 1　方程(5)求解结果

(d_1, k_1)				
(1,28)	(2,1)	(3,16)	(4,31)	(5,4)
(6,19)	(7,34)	(8,7)	(9,22)	(10,37)
(11,10)	(12,25)	(13,40)	(14,13)	(15,28)

由上表可见，第 15 对解(15,28)中，k_1=28 已重复. 通过 $k_1G=k_1P(2)=(51,56)$，得 k_1=4，根据 k_1 的周期 14，可得 d_1 的取值: 5, 19, 33，接着验证 $d_1G=d_1P(2)=P(3)$，即得用户私钥 d_1=5.

4　结论与展望

本文主要研究了一类有限域丢番图方程 $c\equiv x+by(\mathrm{mod}\,N)$ 的解集，求得其通解为:

$$\begin{cases} x=c-(c-t)b \\ y=c-t \end{cases}$$

其中 $t=0,1,2,\cdots$. 且其在域内的整数解的有效对数为 $\frac{N}{z}$，z 为子群 $\langle -b\rangle$ 的最小非零元.

该类方程常被应用于曲线公钥密码体制的数字签名及多重数字签名方案中，运用上述结果可以降低这些方案中求解用户私钥的计算量，计算量降低为 $\frac{N}{z}$，是穷举全局私钥计算量的 $\frac{1}{z}$. 文中指出 5 个应用该类型方程曲线密码方案，并以 LWL 方案的私钥求解进行说明，具体数值模拟和求解过程见于例 1.

本文研究结果对密码学中加密与签名方案的设计提出一点新的要求, 以提高方案的安全性:

①对于加密与签名方案中, 加密及签名分量的构造式应尽量避免使用(2)式类型, 而采用更加复杂的 $c \equiv ax + by(\mathrm{mod}\, N)$ 类型式;

②若由于计算量及方案复杂度所限必须使用(2)式类型构造分量, 则在应用时, 应选取最小非零元尽可能小的 b, 对 hash 值, 可采用加 salt 进行改变.

对更具有一般性且应用更加广泛的一类有限域丢番图方程 $c \equiv ax + by(\mathrm{mod}\, N)$, 甚至多元以及高阶方程的研究, 需要进一步结合丢番图方程的理论、数论基础知识和密码学基本原理进行, 对有限域丢番图方程解的理论以及密码学中数字签名方案的安全性提高, 具有一定的价值和意义.

参考文献

1 Manders K, Adleman L. NP-complete decision problems for binary quadratics. Journal of Computer and System Sciences, 1978,16(2): 168–184.

2 Adleman L, Manders K. Diophantine complexity. IEEE 17th Annual IEEE Symposium on Foundations of Computer Science. IEEE, New York, 1976: 81–88.

3 杨义先,李世群,罗群.丢番图公钥密码体制.通信学报,1989, 2:78–80.

4 孙琦.用丢番图方程构作公开钥密码.四川大学学报(自然科学版),1991,1:15–18.

5 李大兴,赵霖.攻破“丢番图公钥密码体制”.通信学报,1990, 1:93–96,83.

6 曹珍富.破译一类丢番图型公钥密码体制.自然杂志,1992, 2:151.

7 Mordell LJ. Diophantine Equations. New York: Academic Press, 1969:22–52.

8 曹珍富.丢番图方程引论.哈尔滨:哈尔滨工业大学出版社, 1989.

9 王萼芳.有限群论基础.北京:清华大学出版社,2002.

10 Lin S, Wang B, Li Z. Digital multi-signature on the generalized conic curve over Zn. Computers and Security, 2009, 28(1-2): 100–104.

11 丁丽,周渊,钱海峰.广义圆锥曲线的多方签名的安全分析与设计.北京工业大学学报,2010,(5):646–650.

12 Chen TS, Huang KH, Chung YF. Digital multi-signature scheme based on the Elliptic Curve cryptosystem. Journal of Computer Science and Technology, 2004, 19(4):570-inside back cover.

13 肖龙,王标,孙琦.基于环 Zn 上的圆锥曲线数字签名和多重数字签名.西安交通大学学报,2006,6:648–650,718.

14 周艳,江明明.环 Zn 上广义圆锥曲线的广播多重数字签名.计算机与现代化,2010,3:125–127,132.

15 Itakura K, Nakamura KA. Public key cryptosystem suitable for digital multisignatures. NEC Research and Development, 1983, 71:1–8.

16 Boyd C. Digital Multisignatures. Cryptography and Coding. Oxford:Oxford University Press, 1989: 241–246.

17 Harn L, Kiesler T. New scheme for digital multisignature. Electronics Letters, 1989, 25(15): 1002–1003.

18 孙琦,朱文余,王标.环上广义圆锥曲线和公钥密码体系.四川大学学报:自然科学版,2007,44(2):213–220.