马少华,张　兴,韩　冬,等. 基于 ECDSA 优化算法的智能农业无线传感器节点的网络安全认证[J]. 江苏农业科学,2015,43(4):389 – 392.
doi:10.15889/j.issn.1002 – 1302.2015.04.137

基于 ECDSA 优化算法的智能农业无线传感器节点的网络安全认证

马少华, 张　兴, 韩　冬, 史　伟
(辽宁工业大学电子与信息工程学院,辽宁锦州 121001)

摘要:为满足应用于监测大棚种植基本环境的无线传感器节点认证的需求,在传感器 IRIS 节点上实现了基于椭圆曲线加密体制的数字签名算法(ECDSA),并在 ECDSA 程序中嵌入 7 种针对提高 ECDSA 性能的优化算法,通过开/关的方式,比较各优化算法的空间复杂度(消耗 ROM/RAM 空间)和时间复杂度(初始化所需时间、签名产生所需时间、认证所需时间)。通过试验测试和综合比较分析,提出了适合应用于大棚种植监测的无线传感器节点认证方案。

关键词:智能农业;无线传感器节点;网络安全认证;椭圆曲线数字签名算法;优化
中图分类号: S126　　**文献标志码:** A　　**文章编号:**1002 – 1302(2015)04 – 0389 – 03

现代设施农业是适应市场化、集约化、国际化大生产的新型现代农业产业形态,是传统农业向现代高效农业转变过程的必然选择,设施农业发展状况在一定程度上反映了农业现代化水平[1-2]。大棚种植是设施农业中一个重要组成部分,具有利用适宜作物生长的环境温湿度和光合作用来控制植物生长的优点。由 Eko 节点构成的智能农业传感网能够收集对农作物影响非常大的土壤温湿度、光照等信息,通过无线多跳的 ZigBee +4G 方式传送到种植园主的手机上,方便其了解农作物生长的环境状况,以便采取有效措施促进生产。目前,智能农业传感网已应用于国内外的种植园和果蔬大棚中,对农作物的生长管理、产品产量和质量提高具有显著效果,它的精度高、灵活性强、可靠性高、经济性好等优点使其在设施农业领域具有非常好的应用前景[3]。但是,如果智能农业传感网发给种植园主的是虚假信息或是被篡改的不真实信息,那么智能农业传感网非但不能对生产起促进作用,反而会耽误灌溉、施肥等有效时机,或使农作物的生长环境变得更糟。智能农业传感网的安全保障就变得至关重要。通过分析可知,只要保证农业传感信息的来源可靠和在传输过程中不被篡改就足够了,而无需对这些信息进行保密。当前的问题是对称加密算法在信息加密方面非常有效,而在认证方面无法保证邻居之间对密钥的安全建立;非对称加密算法的开销非常大,不适合资源非常有限的无线传感器网络。ECC 算法的实施有效解决了这一问题,但尚未见在 Eko 节点的 IRIS 平台上实施[4-5]。

为满足应用于大棚种植的无线传感器网络中节点认证的需求,本研究实现了在传感器 IRIS 平台上运行基于椭圆曲线加密体制的数字签名算法(ECDSA);并加入 7 种优化算法,通过对它们测试、比较和分析,提出了一个适于大棚种植的节点认证方案,从而使签名和认证时间大大缩短,并确保该方案适用于资源有限的由 Eko 节点构成的智能农业传感网。

1　软硬件平台

1.1　硬件平台

现在得到应用的 Eko 节点为 Crossbow 公司产品,目前,该公司的 WSN 方面的产品已被 MEMSIC 公司收购。Eko 传感器节点基于 IRIS 平台,其 ROM 空间为 128 k 字节,RAM 空间为 8 k 字节;通信模块位于 ISM 免费频段 2.4 GHz,并支持 IEEE 802.15.4 协议,数据的传输率为 250 kb/s,最大可视传输距离超过了 1 000 m(最大可视传输距离指无障碍情况下的通信,2008 年,在北京北海两岸布置 IRIS 节点测试得到最大可视距离);处理器芯片采用是低功耗的 ATmega1281,其性能有利于进行数字签名中的大量复杂运算。

1.2　软件平台

Eko 节点使用的是无线传感器平台所特有的开源操作系统 TinyOS,由 nesC 编程语言编写。TinyOS 是一款基于事件驱动型的操作系统,其特点是能很有效地调度各种组件,从而高效地完成各项系统功能。

2　ECDSA 及其优化算法

2.1　ECC 简介

椭圆加密算法(ECC)的数学基础是利用椭圆曲线上的有理点构成 Abel 加法群上椭圆离散对数的计算困难性,是目前公钥加密体制中对 1 bit 所提供加密强度最高的加密算法。ECC 仅需使用 160 bits 的密钥长度就可获得等同于 RSA 加密算法采用密钥长度为 1 024 bits 的安全强度[4-6]。本研究采用 160 bit 的椭圆加密算法算法。

2.2　数字签名原理

所谓数字签名,就是只有消息的发送方才能产生的别人

收稿日期:2015 – 01 – 07
基金项目:国家自然科学基金(编号:61272214);辽宁省博士科研启动基金(编号:20121045);辽宁省高等学校杰出青年学者成长计划(编号:LJQ2014066)。
作者简介:马少华(1988—),男,江苏大丰人,硕士研究生,从事物联网信息安全研究。E – mail:756918512@qq.com。
通信作者:张　兴,副教授,研究生导师,从事网络体系架构与协议、信息安全等研究。E – mail:zhang_xing@emails.bjut.edu.cn。

无法伪造的一段数字串,这段数字串同时也是对信息的发送方发送信息真实性的一个有效证明。数字签名一般通信过程如图 1 所示。(1)节点 A 通过自己的私钥和数字签名生成算法对消息 M 进行签名,得到签名 S,并附在消息 M 上。(2)节点 B 收到来自节点 A 的消息后,通过节点 A 的公钥和数字签名认证算法对收到的消息进行认证,根据返回的签名有效值来判断消息的真伪。

2.3　ECDSA 数字签名方案

ECDSA 数字签名方案是 ECC 和 DSA 的结合。整个签名过程与 DSA 类似,所不同的是签名、认证中采用的算法是 ECC,最后的签名 S 为(r,s)(图 1)。ECDSA 数字签名生成算法和签名认证算法如下。(1)数字签名生成算法:记 $P=(x,y)$。节点 A 选取一随机整数 k 满足 $1\leqslant k<n$ 和 $gcd(k,n)=1$,计算 $r\equiv x \bmod n$;$s\equiv k^{-1}(M+kr) \bmod n$。则节点 A 对消息 M 的签名 $S=(r,s)$。(2)数字签名认证算法:节点 A 的任意邻居 B 依次计算 $c\equiv s^{-1} \bmod n$;$u_1\equiv Mc \bmod n$;$u_2=rc \bmod n$;$u_1G+u_2P=(x,y)$;$r'\equiv x \bmod n$。若 $r'=r$,则认证成功,认定节点 A 发送的信息可信。反之,认证失败,认定信息 M 非节点 A 发送或被篡改。

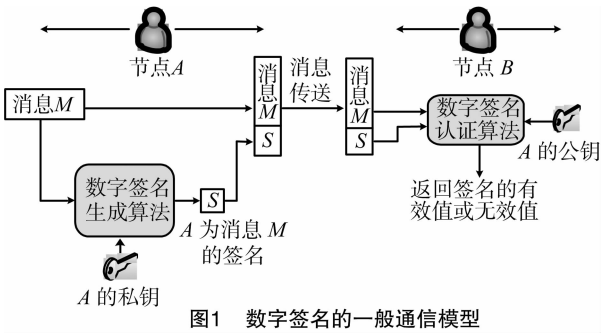


图1　数字签名的一般通信模型

2.4　ECDSA 的 7 种优化算法

ECDSA 可划分为 ECC 算法模块和数字签名模块。其中 ECC 模块由大整数运算和椭圆曲线类组成,数字签名模块由数字签名的产生和认证组成。本研究选取 4 种优化大整数运算的算法(巴雷特减法算法[7]、混合乘法算法[8]、混合平方算法[9]、曲线优化算法[8])、2 种优化椭圆曲线的算法(射影平面坐标系[8]、滑动窗口[8])和 1 种优化签名认证的算法(夏米尔技巧优化算法[9])。由于本研究侧重于对各优化算法在 IRIS 节点上的性能分析,各优化算法具体知识可详见参考文献[8-9]。

3　ECDSA 及 7 种优化算法的实现

3.1　ECDSA 的实现

本研究设定消息长度为 52 b,为提高测试结果的准确性,每个程序测试 10 次,试验结果取 10 次测试结果的算术平均值。测试结果见表 1,ECDSA 所占用的 ROM 和 RAM 在IRIS 节点的承受范围之内,初始化所需的时间也较短,但签名生成所需时间和签名认证所需时间较长,特别是签名认证所需时间超过了 1 min。

表 1　ECDSA 在 IRIS 节点上的测试结果

节点类型	所需空间(byte)		所需时间(s)		
	ROM	RAM	初始化	签名生成	签名认证
IRIS	16 860	817	0.000 1	31.954 4	64.225 5

3.2　优化算法的测试

本研究对上述 7 种优化算法通过开关的方式来测试其在 IRIS 节点上所耗的 ROM/RAM 空间、初始化所需时间、签名产生时间和认证所需时间。

3.2.1　主要程序代码

```
##NN
CFLAGS + = -DBARRETT_REDUCTION #巴雷特减法
CFLAGS + = -DHYBRID_MULT #混合乘法
CFLAGS + = -DHYBRID_SQR #混合平方法
CFLAGS + = -DCURVE_OPT #曲线优化算法
##ECC
CFLAGS + = -DPROJECTIVE #射影平面坐标系
CFLAGS + = -DSLIDING_WIN #滑动窗口优化算法
##ECDSA
CFLAGS + = -DSHAMIR_TRICK #夏米尔技巧
```

3.2.2　7 种优化算法的测试结果分析　由图 2-a 中虚线可知,初始化时间值较大的有巴雷特减法算法、滑动窗口算法、夏米尔技巧优化算法,其他算法初始化时间几乎为零。这是因为巴雷特减法算法、滑动窗口算法、夏米尔技巧优化算法需要进行预运算。而由实线发现,滑动窗口算法对初始化时间影响最大,几乎降低了 50% 的时间。因此,滑动窗口算法对初始化时间影响最大。

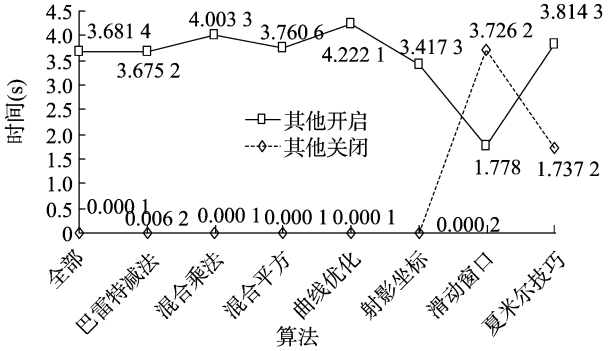
由图 2-b、图 2-c 可知,射影平面坐标系优化算法对减少签名的产生和认证所需时间影响最大。由图 2-b、图 2-c 中虚线可知,射影平面坐标系优化算法对产生签名和签名认证的效率提高 3 倍以上;结果表明,关闭射影平面坐标系优化算法会降低产生签名和签名认证的效率 8 倍以上。虽然射影平面坐标系优化算法很有效,但也是消耗 ROM 空间最多的算法。

夏米尔技巧优化算法也是提高签名认证效率较好的算法。由图 2-c 中虚线可知,夏米尔技巧优化算法对签名认证效率提高了 2 倍,但所需的 ROM、RAM 空间分别增加了 548、634 b;而实线可知,关闭夏米尔技巧优化算法后,签名认证效率降低 160%,但减少了 2 204 b 的 ROM 空间,而 RAM 值几乎没有减少,是因为当关闭夏米尔技巧优化时,滑动窗口算法被用于签名认证。

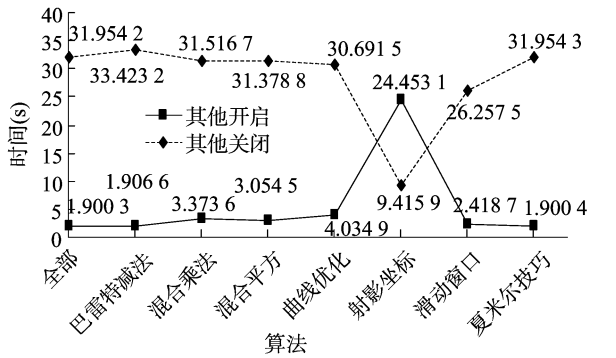
由图 2-b、图 2-c 和图 3 中虚线可知,滑动窗口算法对产生签名的效率和签名认证的效率提高了 1.2 倍,但 RAM 值剧增了 2.5 倍;由图 2-b、图 2-c 和图 3 中实线可知,关闭滑动窗口算法对产生签名的效率和签名认证的效率降低了 130%,但节省了 632b 的 RAM 空间。

由图 2-b、图 2-c 虚线可知,混合乘法、混合平方法和曲线优化算法对提高产生签名和签名认证的效率不大。而从图 2-b、图 2-c 实线发现,以上 3 种优化算法分别对产生签名的效率提高了 1.8、1.6、2.1 倍;对签名认证的效率分别提高了 1.8、1.5、2.0 倍。这是因为在产生签名和签名认证的运算中最耗时的运算为求逆运算,只有在开启射影平面坐标优化算法取缔求逆运算的情况下,才会使产生签名和签名认证运算中最耗时的运算变为模乘运算,这样才会使以上 3 种优化算法的优化效果明显。

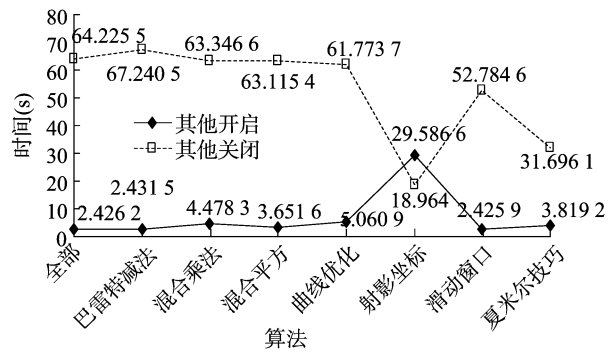
由上述分析可知,从消耗 RAM 空间的角度看,滑动窗口算法 > 夏米尔技巧算法 > 巴雷特减法 > 混合乘法 = 混合平



a. 7 种优化算法初始化所耗时间

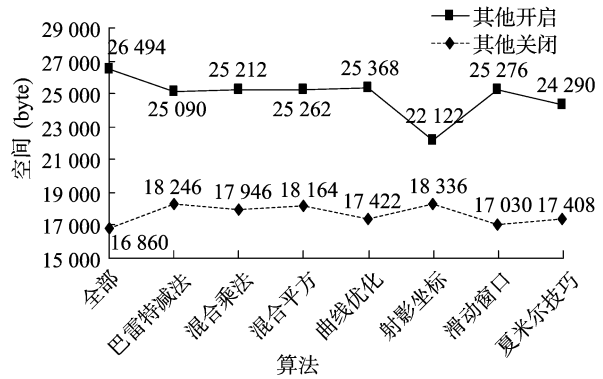


b. 7 种优化算法签名所耗时间

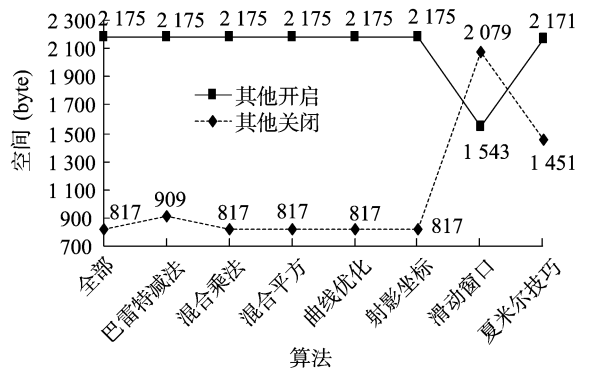


c. 7 种优化算法签名认证所耗时间

图2　7 种优化算法的时间复杂度



a. 7 种优化算法占用的 ROM 比较



b. 7 种优化算法占用的RAM比较

图3　7 种优化算法的空间复杂度

表 2　各方案在 IRIS 节点上测试结果

类别	空间复杂度(byte)		时间复杂度(s)		
	ROM	RAM	初始化时间	签名时间	认证时间
方案 1	21 594	817	0	2.424 9	4.861 9
方案 2	23 022	909	0.006 5	2.418 4	4.856 9

方法 = 曲线优化算法 = 射影平面坐标法;从消耗 ROM 空间的角度看,射影平面坐标法 > 巴雷特减法≈ 混合平方法 > 混合乘法 > 曲线优化算法≈夏米尔技巧算法 > 滑动窗口算法;从签名效率角度看,射影平面坐标法 > 曲线优化算法 > 混合乘法 > 混合平方法 > 滑动窗口算法 > 夏米尔技巧算法 > 巴雷特减法(图 3)。

4　适合大棚种植的 ECDSA 方案

由于 IRIS 节点中 RAM 资源稀少,根据上述分析,切实可行方案有如下 2 种:方案一为选用混合平方法、混合乘法、曲线优化算法和射影平面坐标法;方案二为选用混合平方法、混合乘法、曲线优化算法、射影平面坐标法和巴雷特减法。2 个方案的测试结果见表 2。其中,方案一中 RAM 值为 817 b,时间复杂度为 7.286 8 s;方案二 RAM 值为 909 b,时间复杂度为 7.2818 s。比较结果显示,方案一较方案二 RAM 值小 92 b,而时间复杂度大 0.005 s。综合大棚种植的特点,方案一是更为可取的方案选项。因此,适合大棚种植的 ECDSA 方案为混合平方法 + 混合乘法 + 曲线优化算法 + 射影平面坐标法。

5　结论

本研究主要创新点有 2 个方面:(1)将基于 ECC 加密算法的数字签名算法(ECDSA)在 IRIS 节点上实现,并测试 ECDSA 消耗的 ROM/RAM 空间、初始化时间、产生签名时间和签名认证时间;(2)通过开/关的方式,测试 7 种 ECDSA 的优化算法的 ROM/RAM 空间、初始化时间、产生签名时间和签名认证时间,并从空间复杂度(ROM/RAM 空间)和时间复杂度(初始化所耗时间、产生签名所耗时间、签名认证所耗时间)比较各优化算法。通过测试与比较分析,提出了适合应用于大棚种植监测的无线传感器节点认证方案。

参考文献:

[1]戴起伟,曹　静,凡　燕,等. 面向现代设施农业应用的物联网技术模式设计[J]. 江苏农业学报,2012,28(5):1173 - 1180.

[2]戴起伟,凡　燕,曹　静,等. 物联网技术与江苏智能农业产业发展[J]. 江苏农业科学,2011,39(5):1 - 3.

[3]肖　婷,庄义庆,糜　林,等. 物联网传感技术在大棚草莓生产中的应用[J]. 江苏农业学报,2014,30(5):1185 - 1187.

翟　哲,李伟凯,李长凯,等. EMD 在叶绿素光谱信号去噪中的应用[J]. 江苏农业科学,2015,43(4):392 – 396.
doi:10.15889/j.issn.1002 – 1302.2015.04.138

EMD 在叶绿素光谱信号去噪中的应用

翟　哲, 李伟凯, 李长凯, 裴　玉
(黑龙江八一农垦大学信息技术学院,黑龙江大庆 163319)

摘要:基于每个 IMF 自关联函数的特征,提出了一种新的 EMD 去噪方法。以检测苗期玉米叶片叶绿素含量为例,首先对原光谱信号采用 SNV + Detrending 方法进行预处理,然后利用该方法对预处理后的信号进行去噪,并与小波去噪方法和 EMD 融合小波去噪方法进行对比,最后应用偏最小二乘回归方法进行校正模型的建立。结果表明:将该方法应用到实际近红外光谱信号去噪中,其预测集决定系数(r^2)达到 0.984,残差均方根 *RMSE* 为 0.075,证明该方法在近红外光谱处理过程中具有很好的去噪效果,建立的校正模型具有较高的鲁棒性和推广性。

关键词:经验模态分解;自适应;近红外光谱;叶绿素
中图分类号: S126　　**文献标志码**: A　　**文章编号**:1002 – 1302(2015)04 – 0392 – 05

随着计算机科学技术的飞速发展,近红外光谱技术在仪器分析领域受到了有关专家的高度重视[1]。近红外光谱技术之所以能迅速发展并在各个行业都有广泛的应用,是因为它有很多的优越性[2]。但是由于外界环境的影响,近红外光谱仪所采集到的光谱信号,除了包含自身信息外,在测量中还不可避免地得到许多无关的噪声信号[3]。因此在使用化学计量方法建立校正模型时,消除光谱数据无关噪声在光谱数据分析中变得十分关键和必要。本研究将改进经验模态分解(empirical mode decomposition,EMD)方法引入到近红外光谱信号去噪中,旨在探索近红外光谱信号去噪的新方法。

1　基本思想

EMD 方法就是把 1 个非线性非平稳的信号分解为有限个本征模函数(intrinsic mode function,IMF)分量和 1 个趋势项[4],原始信号 $x(t)$ 可表示为:

$$x(t)=\sum_{i=1}^{n}c_i(t)+r_n(t)。\tag{1}$$

式中:$c_i(t)$ 为第 i 个 IMF 分量;$r_n(t)$ 为筛选到最后剩下的趋势信息;t 为时间;n 为分解的 IMF 个数。各个 IMF 分量都代表信号从高频到低频的分量,通常情况下阶数较小的 IMF 代表高频分量和噪声信号,阶数较大的 IMF 代表低频分量,受噪声影响较小。

EMD 其实就是把信号的极值特征尺度作为度量而进行筛选的过程,信号从最小特征尺度实行筛选,因此得到周期最短的 IMF[5-6]。之后再进行逐层筛选,最终获得周期尺度渐次增大的多个 IMF,此过程亦显示出了多分辨辨识的滤波全程。这个途径是依据信号分解的 IMF 分量建构滤波函数,所以能极大保持信号固有的非线性、非平稳特征。

假设 $x(t)$ 为含噪信号,则经过 EMD 算法的分解后其高通滤波表达如下:

$$x_{hp}(t)=\sum_{i=1}^{k}c_i(t),(1<k<n)。\tag{2}$$

带通滤波表达如下:

$$x_{dp}(t)=\sum_{i=h}^{k}c_i(t),(1<h<k<n)。\tag{3}$$

低通滤波表达如下:

$$x_{lp}(t)=\sum_{i=k}^{n}c_i(t)+r_n(t),(1<k<n)。\tag{4}$$

但是,噪声同信号在 IMF 分量内叠混,可以用 EMD 阈值去噪的方法[7]。其中在阈值选择方面,根据 Donoho 等给出的小波去噪中的阈值[8],其中小波去噪软阈值为:

$$y_{soft}(t)=\begin{cases}sng[x(t)]\cdot[|x(t)|-\delta], & |x(t)|>\delta\\ 0, & |x(t)|\leqslant\delta\end{cases}。\tag{5}$$

式中:δ 为通用阈值。

在第 j 层选取 $\delta=\sigma_j\sqrt{2\ln N}$。

式中:N 为信号的长度;σ_j 为噪声在第 j 层的标准差,可利用 $\sigma_j=media/0.6745$ 进行估计,*media* 为第 j 层上小波系数的绝

收稿日期:2014 – 05 – 25
基金项目:黑龙江八一农垦大学研究生创新科研项目(编号:YJSCX2013 – 16BYND)。
作者简介:翟　哲(1988—),男,黑龙江庆安人,硕士研究生,主要从事数据处理研究。E – mail:zhai_zhe@163.com。
通信作者:李伟凯,博士,教授,博士生导师,主要从事光电检测研究。Tel:(0459)6819009;E – mail:bynd@263.net.cn。

[4]张　兴,何泾沙,韦　潜. 无线传感器网络中节点移动场景下的密钥管理方法[J]. 东南大学学报:自然科学版,2011,41(2):227 – 232.
[5]张　兴,何泾沙,韦　潜,等. 无线传感器网络中移动场景下的安全路由重构[J]. 北京工业大学学报,2012,38(9):1377 – 1383.
[6]蔡　冰,叶　玲. 基于 ECC 数字签名的实现及优化[J]. 计算机工程,2009,35(19):161 – 163.
[7]Menezes A J,van Oorschot P C,Vanstone S A. Handbook of Applied cryptography[M]. boca raton:crc press,1996:603 – 604.
[8]Gura N,Patel A,Wander A. Comparing elliptic curve cryptography and RSA on 8 – bit CPUs[C]//Proceedings of the 2004 Workshop in Cryptographic Hardware and Embedded Systems. 2004:119 – 132.
[9]Hankerson D,Menezes A,Vanstone S. Guide to elliptic curve cryptography[M]. Berlin:Springer,2004:75 – 152.