DWNAF:带门限的动态窗口的NAF标量乘法

史 量 徐 明
(上海海事大学信息工程学院 上海 201306)

摘 要 为了提高水声信道传输数据的安全性,针对非对称加密对节点性能要求较高的问题,提出了一种带门限的动态窗口的NAF标量乘法(DWNAF)。该方法通过"门限"对经典的窗口法的窗口大小进行动态控制,优化了预处理过程,有效降低了预计算和标量乘计算的开销。实验表明,在预计算量相同的情况下,DWNAF的点加次数仅为RWNAF的25%。在安全性方面,DWNAF采用窗口法、平衡能量法与masking方法相结合的方式,能有效抵御SPA,DPA及其变种RPA和ZPA等常见的边信道攻击。

关键词 水下声传感器网络,边信道攻击,数据安全,NAF
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.10.030

DWNAF:A Dynamic Window NAF Scalar Multiplication with Threshold

SHI Liang XU Ming
(School of Information Engineering,Shanghai Maritime University,Shanghai 201306,China)

Abstract In order to improve the safety of the data transmission in underwater acoustic channel,in view of the fact that asymmetric encryption requires high performance of nodes,a dynamic window NAF scalar multiplication with a threshold (DWNAF) was proposed for underwater acoustic sensor networks. The method is based on the classic width-ω NAF method through a "threshold" for dynamic control,and it can optimize the pretreatment process and effectively reduce the pre-calculation in scalar multiplication. Experimental results show that under the same pre-calculation,the point-add in DWNAF is only 25% of that in RWNAF. In security,DWNAF adopts the combination of window method,energy balance method and masking method,which can effectively resist the common side channel attacks such as SPA,DPA and its variants RPA and ZPA.

Keywords Underwater acoustic sensor network,Side channel attack,Data security,NAF

1 引言

随着水下声传感器在众多领域(尤其是军事领域)的广泛应用,保证水下数据传输的安全性越来越受到人们的重视。相对于陆上无线传感器,水下声传感器及其信道具有高时延、低传输带宽、储存及计算能力低下以及能源不易被更换(在一般情况下能源往往不可能被更换)等特点。基于上述特点,本文提出用椭圆曲线密码系统来加密数据。

通常情况下,虽然公钥密码体制由于密钥空间和运算消耗都比较大而被认为不适用于传感器等单片机环境中,但椭圆曲线密码系统具有安全性高、计算开销小、存储空间小和带宽要求低的特点,目前被广泛用于智能芯片卡的加密中。2004年Malan D J[12]首次在Mica2传感器上成功实现了基于椭圆曲线密码系统的密钥交换,为本文研究的可行性提供了实验基础。但椭圆曲线密码系统极易受到边信道攻击。目前人类的深潜记录是由法国深海实验室创造的330m[14],而一般水下声传感器节点都部署在浅海(水深小于500m的海域),所以水下声传感器节点完全可能遭受边信道攻击。

NAF(Non-Adjacent Form)标量乘法是一种能显著提高椭圆曲线密码系统运算效率的标量乘法。相比于普通二进制编码,它以增加一次倍点的代价平均减少了1/3的点加次数。但NAF本身并不抵御边信道攻击,并且椭圆曲线的标量乘计算也是相对复杂和耗能的,所以许多算法计算都致力于提高NAF标量乘法的计算效率和安全性。

本文提出一种带门限的动态窗口的NAF标量乘算法(DWNAF),它提高了传统NAF标量乘法加密算法的效率,并且能有效抵御SPA,DPA及其变种ZPA和RPA等常见的

到稿日期:2016-11-16 返修日期:2017-02-09 本文受国家自然科学基金项目(61202370),上海市教委科研创新项目(14YZ110),中国博士后科学基金资助项目(2014M561512)资助。

史 量(1992-),男,硕士,主要研究方向为椭圆曲线密码学与边信道攻击,E-mail:lukesscn@gmail.com;徐 明(1977-),男,博士,副教授,CCF会员,主要研究方向为水声传感器网络、网络安全与隐私保护、智能信息处理。

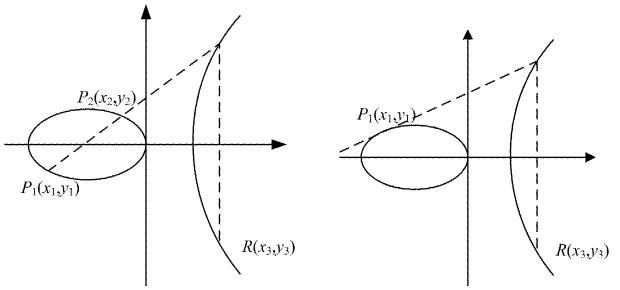
边信道攻击;同时提出最小能量消耗定理和最大预计算利用率定理对算法进行佐证,进一步证明了算法的可行性。

2 基础知识与相关工作

2.1 基础知识

2.1.1 椭圆曲线密码系统

Koblitz[1]和 Miller[2]于 1985 年提出将椭圆曲线应用于公钥密码体制。由于基于椭圆曲线的离散对数问题的求解难于标准的离散对数问题的求解,因此在安全性相同的情况下,基于椭圆曲线的密钥长度要短于标准的离散对数密钥。椭圆曲线具有点加和倍点两种运算法则,椭圆曲线 E 上的两个点相加可以得到 E 上第三个点,椭圆曲线的点加及倍点的几何意义如图 1 所示。



(a)椭圆曲线点加的几何示意图 ($R=P_1+P_2$)　　(b)椭圆曲线倍点的几何示意图 ($R=2P_1$)

图 1 椭圆曲线运算的几何意义示意图[3]

2.1.2 NAF 标量乘法

椭圆曲线的标量乘法就是椭圆曲线上一个点 G 与一个随机的大整数 k 的乘积,即:

$$Q=kG=G+G+\cdots+G+G$$

椭圆曲线标量乘法是椭圆曲线密码系统中最关键(也是消耗资源和能量最多)的步骤。由于在雅可比坐标下,倍点的运算消耗小于点加的运算消耗,因此通常做法是将 k 做一个转换以减少其中的点加次数。NAF[4]是其中效率最高的方法,它将二进制进行了转换,以增加一位二进制位的代价平均可使 2/3 的位数为 0,因此极大地减少了点加次数。

为了提高 NAF 标量乘法的效率,一种比较常见的方法是窗口法[5]。窗口法将 NAF 处理的二进制位划分成若干个块。在计算时只需预计算每块的可能值,然后调用预计算的值,在某些情况下即可极大地减少计算量。但在一些情况下预计算往往会造成存储空间的浪费,本文 2.3 节将重点介绍这一问题。

2.1.3 边信道攻击

P. Kocher[6]于 1996 年提出可以通过边信道泄露的信息,如运算过程中各部分所用时间、消耗能源不同等,分析出保密信息的攻击方法。使得一些在数学理论上安全的加密手段也有被破解的可能。

能量分析攻击对基于椭圆曲线的密码系统构成了严重威胁,能量分析攻击大致分为简单能量分析(SPA)[6]、差分能量分析(DPA)[9]及其变种修正能量分析(RPA)[9]和零值点攻击(ZPA)[9],对于每种攻击,存在不同的抵御方法。

针对 SPA,主要对抗方法有平衡能量法(混淆法)[8]和窗口法[7]。结合两种方法可有效抵御 SPA。

针对 DPA 及其变种 RPA 和 ZPA,对抗方法有随机化基点坐标法[9]、随机化曲线法[9]和指数分裂法[9]。本算法采用基于指数分裂法的 masking 方法[5],其比指数分裂法更简单,且可以达到抵御 RPA 和 ZPA 的效果。

2.2 椭圆曲线密码系统应用于水声信道中的可行性

Malan D J 于 2004 年首次在 Misa2 传感器上成功实现了基于椭圆曲线密码系统的密钥交换[12],之后出现了大量在无线传感器中的椭圆曲线应用研究,但目前在陆上无线传感器应用中并不流行使用椭圆曲线密码系统,下文将解释具体原因。文献[10]指出水下声传感器的硬件设计与经典陆上无线传感器(Mica2,MicaDot2,Telos)类似,因此可以将陆上传感器的处理时延和能量消耗作为参考。文献[11]给出了 160 位椭圆曲线密码系统和 1024 位 RSA 密码系统,分别对在 Mica2,MicaDot2 和 TelosB 传感器上的签名过程产生的能耗和时延进行了比较,如表 1 所列。

表 1 1024 位 RSA 与 160 位 ECC 在 MicaDot2,Mica2 及 TelosB 上的开销比较[11]

传感器	密码系统	密钥生成过程消耗	密钥验证过程消耗
MicaDot2	RSA-1024	363.50mWs 22.03s	14.19mWs 1.12s
	ECC-160	27.23mWs 1.65s	53.96mWs 3.27s
Mica2	RSA-1024	359.87mWs 12.04s	14.05mWs 0.47s
	ECC-160	26.96mWs 0.89s	53.42mWs 1.77s
TelosB	RSA-1024	68.97mWs 5.66s	2.70mWs 0.022s
	ECC-160	6.26mWs 0.52s	12.41mWs 1.02s

由于椭圆曲线密码系统的安全性高,160 位椭圆曲线密码系统与 1024 位 RSA 密码系统的安全性相当。从表 1 可以看出,椭圆曲线密码系统在签名过程中的能量和时间消耗仅为 RSA 密码系统的 7.6%,验证过程是 RSA 密码系统的 5 倍,总的来说其相对 RSA 密码系统有较大的优势。对于无线传感器,椭圆曲线密码系统的能耗在可接受范围之内,但秒数量级的时延无法应用于时效性要求较高的无线传感器网络。这也是椭圆曲线密码系统在无线传感器领域未得到广泛应用的原因。

但水声信道及其协议均能容忍高时延,所以秒数量级的处理时延相对其传输时延并不算多。基于椭圆曲线密码系统的其他特性,本文将椭圆曲线密码系统运用于水下声传感器中。

2.3 现有 NAF 标量乘算法存在的问题

在 NAF 标量乘法中,计算最复杂且功耗最大的过程就是标量乘计算,而带有预计算的 NAF 标量乘法大大减少了计算标量乘法时点加的次数。但无论是 Width-ω NAF[7](基于固定窗口的 NAF 标量乘法)、RWNAF[15](基于固定窗口改进后的 NAF 标量乘法),还是 FWNAF[7](基于 Moller 碎

片窗口技术的标量乘法),都需要进行至少$(2^{\omega}-1)/2$次预计算,若采用平衡能量法抵御 SPA(简单能量分析),那么预计算的次数就需要翻倍(需要计算符号为负的情况,以避免点减时的求逆操作)。即使是对预计算量进行过优化的 RWNAF 算法,其预计算利用率依旧非常低,表 2 列出了窗口宽度为 4 的 RWNAF 的计算结果示例。

表 2　窗口宽度为 4 的 RWNAF 的计算结果示例

表示方法	表示结果
二进制	1,0,1,0,1,0,1,0,0,1,0,1,0,1,0,1,1,0,1,0
RWNAF(ω=4)	1,0,0,0,−5,0,0,0,−5,0,0,0,−11,0,0,0,5,0,0,0,11

如表 2 所列,窗口宽度为 4,需要进行 15 次预计算,然而编码中仅仅用到了−5P,−11P,11P 和 5P 4 个预计算点,利用率只有 26%。

根据实验统计可知,一个 128 位的密钥在ω=4 的情况下用 RWNAF 进行编码后的平均预计算利用率可以达到 87.3391%,但随着窗口的增加,利用率会急剧减少(ω=6 时,预计算利用率为 56.2321%;而 ω=7 时,预计算利用率仅为 29.3082%),所以单纯通过窗口大小来进行预计算存在极大的浪费,对于存储能力较低的传感器节点而言,无疑增加了传感器节点的存储负担。为了解决这一问题,本文提出一种带门限的动态窗口的 NAF 标量乘法,有效减少了预计算数量,提高了预计算利用率。

3　带门限的动态窗口的 NAF 标量乘法

本文提出 3 个算法,其中算法 1 与算法 2 为 DWNAF 生成算法和 DWNAF 标量乘算法,在传感器中运行。算法 3 为最大窗口大小适应算法,为算法 2 中 ω 的生成提供依据,在实际运用中当传感器出厂时即可预先输入结果,或查表获得结果。

3.1　DWNAF 生成算法

与传统基于窗口的 NAF 标量乘法不同的是,本文提出门限这一概念,放弃以窗口大小来决定预计算点的数量,使得算法不必进行 $2^{\omega}-1$ 次预计算(为了抵御 SPA 而采用混淆法,NAF 标量乘算法对负值也会进行预计算),只需进行 g 次预计算即可。例如门限大小 g=3 时,DWNAF 只需预计算 3P,−3P,−P 这 3 个点即可,大大减少了预计算次数,增加了预计算利用率。DWNAF 生成算法的伪代码如下。

算法 1　DWNAF 生成算法

```
1. Function DWNAF_gene(k,ω,g)
2.   If k mod 2=0
     //如果 k 为偶数,将 k 加 1 变为奇数
3.       k←k+1
4.   End If
5.   r←0,i←0
6.   While k>1
7.       r_i←ω
8.       Is_opt←False
9.       Start_add←False
         //初始当前窗口为最大窗口
10.      While r_i>1
11.        u[i]←(k mod 2^(r_1+2))−2^ω
12.        If |u[i]|<g //符合门限,判断是否最优
13.            If Is_opt=False
14.                Start_add←True
15.                  r_i←r_i+1
16.            Else
17.                k←(k−u[i])/ 2^r_1
18.                d[r]←u[i]
19.                Break
20.            End If
21.        Else//超出门限且在减少状态,当前窗口大小减半
22.            If Start_add=False
23.                r_i←r_i/ 2
24.            Else
25.                Is_opt←True
26.                r_i←r_i−1
27.            End If
28.        End If
29.      r←r+r_i
30.      i←i+1
31.      d[r]←1//将最高位设为 1
32.  For d_e In d //将其余位数补 0
33.      If d_e=Null
34.          d_e← 0
35.      End If
36.  Return
```

算法的基本思想是:先从最大窗口大小开始计算,若得到的值大于门限值,则将窗口大小除以 2,再判断门限是否最优,即让窗口大小加 1,若当前窗口大小加 1 后刚好超出门限,则可判断当前门限最优。这样可以保证 DWNAF 生成的每一位都是小于门限值的数,同时又不像 RWNAF 那样死板,通常 DWNAF 的计算量明显小于 RWNAF 的计算量。

3.2　DWNAF 标量乘算法

DWNAF 标量乘算法通过 masking 方法有效抵御了 DPA 及其变种 RPA 和 ZPA 攻击,并且通过混淆法(将先求逆再点加计算变成直接点加计算)与窗口法相结合,有效防止了 SPA 攻击,保证了密钥的安全性。算法借鉴了 RWNAF 只预计算奇数点的方法,同时又采用门限的方法大大减少了预计算量,节省了存储空间,提高了算法效率。

算法 2　DWNAF 标量乘算法

```
1. Function DWNAF_multi(k,g)
2.   ω= Max_window(n,g)//根据最大窗口大小适应算法可以使平
     均点加次数达到最小极限,实际应用中可通过查表得到
3.   R←random()
4.   result←DWNAF_gene(k,ω,g)
5.   pre-compute:3P…gP,−P,−3P,−Gp
6.   Q←result[result.length−1]P+R
     //这里采用 masking 方法可有效抵御 DPA 及其变种 RPA,ZPA
     攻击
```

```
7.  For i←result.length−2
8.      Q←ECDBL(Q)
9.      If result[i] != 0
        //这里 result[i]可正可负,并且都从预计算表中取值,有效抵御 SPA 攻击
10.         Q←ECADD(Q,result[i]P)
11.     End If
12. If k%2=0
13.     Q←Q−P
        //如果 k 为偶数那么减去 P 还原
14. End If
15. Return Q−R
```

算法的基本思想是:根据最大窗口大小适应算法得到 ω,并且通过 DWNAF 生成算法得到 DWNAF 处理后的序列结果。将结果通过 masking 方法进行处理和预计算,之后进行标量乘运算,最后对 masking 方法处理后的结果进行还原。

3.3 最大窗口大小适应算法

本节主要讨论算法 2 中 ω 与 g 的取值问题,在以往基于窗口的 NAF 标量乘法中,ω 的取值往往与节点的计算与储存能力有关。由于 DWNAF 加入了门限的概念,使得门限 g 的取值与节点储存能力直接相关,但 ω 的取值与节点储存能力的相关性不大。

显然,在算法 1 中,当 g 确定时,随着 ω 的取值增大,最终标量乘的点加次数会逐渐减少。但事实上,随着 ω 增大会增加预处理的计算量,所以 ω 不可能无限增大。根据 3.4.1 节提出的最小能量消耗定理,证明了在 n 位密钥中当 k 确定时随着 ω 增加平均点加次数存在极限。所以本节提出最大窗口大小适应算法以求出最恰当的 ω。

算法 3 最大窗口大小适应算法

```
1. Function Max_window(n,g)
2.  ω←2//窗口初始值从 2 开始
3.  While former_add−current_add<0.5
    //根据最小能量消耗定理,当能量消耗量之差小于 0.5 次点加时忽略不计
4.    S_add←0
5.    i←1
6.    While i≤N //N 是样本数,在实验中取 10000
7.        test=random(n)
          //随机生成 n 位二进制数
8.        Result=GDWNAF_gene(test,ω,g)
9.        S_add←S_add+Result.n_add
10.       Add←S_add/i //统计平均点加数
11.       former_add←Add
12.       ω←ω+1
13. Return ω,Add
```

算法的基本思想是:根据定理 1,在大量的样本空间下,计算窗口大小为 ω 的平均点加数,并与窗口大小为 $\omega-1$ 的平均点加数进行比较。当它们的差小于 0.5 时,最大窗口适应成功。

3.4 最小能量消耗定理与最大预计算利用率定理

作为算法 3 的理论基础,本节详细介绍了最小能量消耗定理,并对其进行了数学证明;又根据最小能量消耗定理提出推论,即最大预计算利用率定理,并进行了数学证明。

3.4.1 最小能量消耗定理

定理 1 当 k 与 g 确定时,$\exists$ 正整数 n_0 使得 $\forall\omega>n_0$ 时的能量消耗量与 $\omega=n_0$ 的能量消耗量之差可以忽略不计(一般小于 0.5 次点加的能量),可以近似看作 $\omega=n_0$ 时标量乘法达到最小能量消耗量。

证明:根据算法 1 可知:$u[i]\leftarrow(k \bmod 2^{r_1+1})-2^{r_1}$ 且 $r_1\in[2,\omega]$,得 $|u[i]|\leqslant 2^{\omega}$。又 $-g\leqslant u[i]\leqslant g$ 时,$n_{add}\leftarrow n_{add}+1$。综上,当 $\frac{g}{2^{\omega}}$ 越小,进行点加操作的概率 P_{add} 越小。因此,当 k 与 g 确定时,ω 越大,P_{add} 越小。不妨设点加次数与 ω 存在函数关系 $N_{add}(\omega)=n_{add}$,当 $\omega\in N^*$ 时,N_{add} 为数列,记作 $\{N_{add}\}$,且元素 $n_{add}>0$,得:数列 $\{N_{add}\}$ 存在下界 $l>0$。又易知函数 N_{add} 单调递减,得:给定任意 $e>0$,$\exists\omega\in N^*$ 使得 $|N_{add}(\omega)-1|<e$。因此,$\{N_{add}\}$ 存在极限。定理得证。

3.4.2 最大预计算利用率定理

定理 2 当 k 与 g 确定时,$\exists$ 正整数 n_0,使得当 $\omega=n_0$ 时,算法预计算利用率最大。

证明:若 $d[r]\neq 0$,则 $u[i]\in[-g,g]$。其概率 $P=\prod_{j=0}^{n-1}\frac{2^j g}{2^{\omega}}=\frac{2^{\frac{n(n-1)}{2}}\times g^n}{2^{\omega}}$。又根据算法 3 以及定理 1 可知:当 n 确定时,ω 是自变量为 g 的单调递增函数,根据复合函数的性质,2^{ω} 也为自变量为 g 的单调递增函数,记作 $Fun(g)$,得:$p_G=\frac{2n^{\frac{n(n-1)}{2}}g^{n-1}Fun(g)-2^{\frac{n(n-1)}{2}}g^nFun'(g)}{Fun^2(g)}$。令 $p_G=0$,得到方程:$nFun(g)=gFun'(g)$。根据定理 1 及导数相关定理易知 $nFun(g)>0$ 且 $Fun'(g)>0$,所以一定存在 $g>0$ 使得方程成立,即 p_G 存在最大值。又因预计算利用率与 p_G 正相关,综上,当 k 与 g 确定时,$\exists$ 正整数 n_0,使得当 $\omega=n_0$ 时,算法预计算利用率最大。定理得证。

4 DWNAF 算法的性能及安全性分析

4.1 实验环境搭建

本实验在 Ubuntu 系统下搭建 TinyOS 环境,所有代码用 nesC 编写,最大限度地模拟单片机的情况,如表 3 所列。采用的随机样本是由逆转法[13]生成的伪随机数,与真实随机情况近似,保证了数据的客观有效。

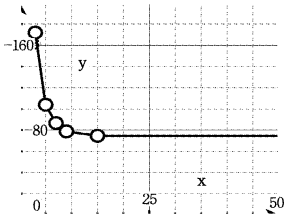
表 3 实验环境

操作系统	Ubuntu 14.04 &TinyOS 2.1.1
使用语言	nesC 1.3.3
运行内存	2GB

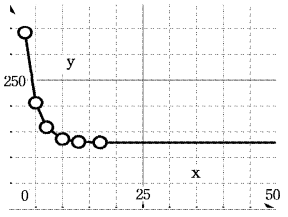
4.2　定理相关实验结果及性能分析

4.2.1　最小能量消耗定理实验结果及性能分析

大量的实验结果(1000 例不同的情况生成的密钥)均符合上述定理结论,本文仅举其中两例进行分析(图 2 中 x 轴为最大窗口大小 ω,y 轴为点加次数)。从图 2 可以看出,点加数随最大窗口数的增加单调递减,最后会趋于一个固定的值。并且当 ω 大于某个值 n_0 时,其变化量会变得非常小,几乎可以忽略。



(a)当门限 $g=63$ 时随着 ω 增加点加的减小次数(512 位密钥)



(b)当门限 $g=63$ 时随着 ω 增加点加的减小次数(1024 位密钥)

图 2　最小能耗定理举例

4.2.2　最大预计算利用率定理实验结果及性能分析

大量的实验结果(1000 例不同的情况生成的密钥)均符合上述定理结论,本文仅举一例进行说明。如图 3 所示,预计算利用率一开始会快速单调递增,当 $\omega=6$ 时预计算利用率达到最大值,之后会缓慢单调递减,最终趋于平稳。

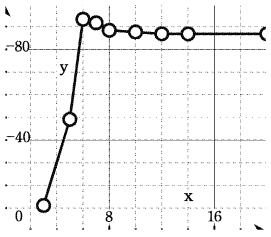


图 3　当门限 $g=63$ 时随着 ω 增加预计算利用率的变化曲线(1024 位密钥)

4.3　算法相关实验结果及性能分析

4.3.1　DWNAF 生成算法的效率分析

由于本算法是在结果中加入门限进行过滤,因此相对于以往的 NAF 生成算法可能会产生一些额外的计算量。为了减少这些额外消耗,本算法通过使用优化算法找出适合的窗口大小,在性能上相比顺序查找有所提升。根据最小能量消耗定理,密钥长度小于 1024 位时,通常最大窗口不会超过 16。实验证明,按照算法 1 中的优化查找算法得到的平均查找长度仅为 3～5,虽然这会导致多余的能量消耗,但是相比复杂的 NAF 标量乘法,这些额外能量消耗几乎可以忽略。

在一般情况下,预处理的能量消耗与之后标量乘的能量消耗相比是微乎其微的。本算法虽然会延长预处理的时间,但其运用于高时延的水声信道中的传输时延是秒数量级的,所以传感器内部的毫秒数量级的处理时延对整体的影响并不大。在水下环境中,传感器的能源一般是很难甚至不可能被更换的,因此在这种情况下以时间换取能源是非常可行的。

4.3.2　DWNAF 标量乘法的效率分析

根据最小能量消耗定理和最大预计算利用率定理,可以证明本算法无论是在效率还是预计算利用率上均能达到比较高的水准。本节主要通过实验数据来对比 RWNAF 和 FWNAF 以说明 DWNAF 的性能。

如表 4 所列,样本分别用标准 NAF,RWNAF,FWNAF,DWNAF 进行编码,样本分为 4 组,4 组的密钥长度分别为 128 位、256 位、512 位、1024 位,每组样本为 100000 个随机生成的密钥。表 4 中的统计数据均由此取平均得到,所以是真实可信并具有代表性的。

表 4　各项 NAF 标量乘法性能比较

算法	密钥长度/bit	预计算空间	运算量	预计算利用率/%
NAF	128	1	43.4373A+128.6736D	99.9999
RWNAF($\omega=4$)	128	15	33A+129D	87.3391
FWNAF($\omega=4.875$)	128	15	30.0150A+129.5566D	84.6257
DWNAF($g=5$)	128	5	29.6711A+129.0048D	98.3027
DWNAF($g=7$)	128	7	26.8875A+128.9991D	96.8661
NAF	256	1	86.1839A+256.6563D	99.9999
RWNAF($\omega=5$)	256	31	52A+256D	80.1095
FWNAF($\omega=5.875$)	256	31	48.2822A+257.9561D	77.6712
DWNAF($g=7$)	256	7	52.5704A+257.5652D	99.9806
DWNAF($g=15$)	256	15	43.9587A+257.3252D	93.8464
NAF	512	1	171.4391A+512.6639D	99.9999
RWNAF($\omega=6$)	512	63	87A+517D	74.1873
FWNAF($\omega=6.875$)	512	63	80.7952A+514.4471D	71.5687
DWNAF($g=15$)	512	15	86.6382A+513.3318D	99.5933
DWNAF($g=31$)	512	31	74.4705A+513.7079D	90.2411
NAF	1024	1	324.0902A+1024.5784D	99.9999
RWNAF($\omega=7$)	1024	127	148A+1030D	68.5221
FWNAF($\omega=7.875$)	1024	127	138.9695A+1026.9282D	54.2550
DWNAF($g=31$)	1024	31	147.6773A+1025.8498D	99.1961
DWNAF($g=63$)	1024	63	129.3665A+1026.0506D	87.1049

通过表 4 的性能比较可以看出,在相同点加数的情况下,DWNAF 的预计算量仅为 FWNAF 的 30%,为 RWNAF 的 25%。其预计算利用率比 FWNAF 提高了 15%左右,比 RWNAF 提高了 12%左右。

如图 4 所示,其中 x 轴为密钥位数,y 轴为预计算个数,z 轴为点加次数,最下面的曲面代表 DWNAF,中间曲面代表 FWNAF,最上面的曲面代表 RWNAF。对于 RWNAF 和 FWNAF,由于预计算次数只能是 $2^{\omega}-1$,因此应该形成若干条射线,但为了方便比较,本节通过拉格朗日插值将其拟合成光滑曲面。从图 4 中可以看出,在预计算量相同的情况下,FWNAF 所需的点加次数略优于 RWNAF,而 DWNAF 的点加次数仅为 RWNAF 的 25%,大大节约了能源。

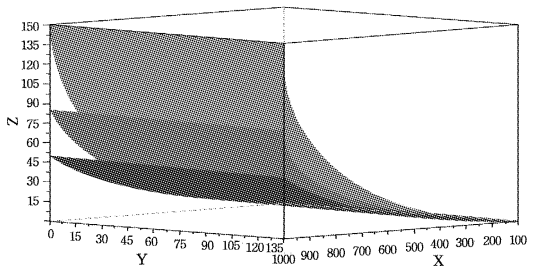


图 4 RWNAF,FWNAF 以及 DWNAF 所测得的数据点进行拟合后形成的 3D 图

4.4 算法安全性分析

4.4.1 抵御 SPA 攻击

SPA 利用指令执行期间点加和倍点所需的能量不同的特点,通过监听能量变化分析出密钥信息。DWNAF 采用窗口法和平衡能量法的双重保护来抵御 SPA 攻击。由于窗口法引入了预计算,使得 SPA 无法区别椭圆曲线上点的大小,所以攻击者很难通过单纯的波形得到相关的密钥信息。

在没有采用平衡能量法的普通 NAF 标量乘法中,由于点是有正负的,因此当计算负值时,需要进行求逆运算,这时产生的能量曲线会有明显区别。

DWNAF 将负点进行预计算,所以在计算标量乘法时只有倍点和点加运算,没有求逆运算。这样消除了点加与点减运算能量波形的区别,以此抵御了 SPA 攻击。

4.4.2 抵御 DPA 攻击及其变种 RPA 和 ZPA 攻击

DWNAF 采用 masking 方法对基点 P 进行处理,在标量乘加密运算时在基点 P 上加上一个随机数,使得攻击者即使截取到能量曲线也无法获得密钥的有效信息,有效抵御了 DPA 攻击及其变种 RPA 和 ZPA 攻击。

结束语 DWNAF 作为一种高效的基于窗口的 NAF 标量乘算法,运算效率高,解决了基于窗口的 NAF 标量乘法需要大量预计算的问题;并且采用平衡能量法和 masking 方法有效防止了 SPA,DPA 及其变种 ZPA 和 RPA。其缺点是生成算法在运算时的时间消耗相比 RWNAF 和 FWNAF 更大,但在水声信道下,由于信道时延非常大,其产生的时间成本一般并不影响传感器性能,并且相比于 NAF 标量乘法的复杂运算,生成算法的运算能量消耗基本可以忽略。

由于实验设备有限,本文并没有给出真实情况的时延及能量消耗,但仿真的数据表明本算法相比其他基于椭圆曲线密码系统的标量乘法更适用于水声信道,相信 DWNAF 会成为未来水下声传感器安全领域的新思路。

参 考 文 献

[1] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation,1987,48:203-209.

[2] MILLER V S. Use of elliptic curves in cryptography, Advances in Cryptology[C]//Proceedings of Crypto'85. Lecture Notes in Computer Science,1986:417-426 .

[3] WANG Y. The design and implementation of ECC to against SCA on smart card[D]. Beijing: Beijing Jiaotong University, 2009. (in Chinese)
王阳. 智能卡上抗边通道攻击的椭圆曲线密码算法的设计与实现[D]. 北京:北京交通大学,2009.

[4] 维基百科. Non-adjacent form[OL]. (2016-05-11) [2016-10-04]. https://en. wikipedia. org/wiki/Non-adjacent_form.

[5] KOYAMA K,TSURUOKA Y. Speeding up elliptic cryptosystems by using a signed binary window method, Advances in Cryptology[C]// Proceedings of Crypto'92. Lecture Notes in Computer Science,1993:345-357.

[6] KOEHER P. Timing attacks on Implementations of Diffie-Hellman,RSA,DSS,and other system[C]//CRYPTO 96. Springer-Verlag,1996:104-113.

[7] OKEYA K,TAKAGI T. A More Flexible Countermeasure against Side Channel Attacks Using Window Method[C]// International Workshop on Cryptographic Hardware & Embedded Systems-ches. Cologne,Germany,2003:397-410.

[8] WANG M,WU Z. Algrithm of NAF scalar multiplication on ECC against SPA[J]. Journal on Communications,2012(S1): 228-232. (in Chinese)
王敏,吴震. 抗 SPA 攻击的椭圆曲线 NAF 标量乘实现算法[J]. 通信学报,2012(S1):228-232.

[9] HIDEYO M,ATSUKO M,HIROAKI M. Efficient Countermeasures against RPA, DPA, and SPA[C]// Lecture Notes in Computer Science. 2004:343-356.

[10] WANG J,CHEN J F,ZHANG L J,et al. Underwater sensor networks[J]. Technical Acoustics,2009,28(1):89-94. (in Chinese)
王静,陈建峰,张立杰,等. 水下无线传感器网络[J]. 声学技术,2009,28(1):89-94.

[11] PANAGIOTIS T,ZAHARIADIS T,HELEN L,et al. Analyzing energy and time overhead of security mechanisms in Wireless Sensor Networks[C]// 15th International Conference on Systems,Signals and Image Processing(IWSSIP). 2008:137-140.

[12] MALAN D J,WELSH M,SMITH M D. A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography[C]// IEEE International Conference on Sensor and Ad Hoc Communications and Networks. 2004:71-80.

[13] TORAL R,CHAKRABARTI A. Generation of Gaussian distributed random numbers by using a numerical inversion method [J]. Computer Physics Communications,1993,74(3):327-334.

[14] LI R P. The development status and trends of ocean engineering technology[J]. Ship Economy & Trade,2002,42(1):1-5. (in Chinese)
李润培. 海洋工程技术发展现状及趋势[J]. 船舶经济贸易,2002,42(1):1-5.

[15] ZHANG T,FAN M Y,WANG G W. Protection against Power Analysis Attack for ECC on Smartcard[J]. Computer Engineering,2007,33(14):125-127. (in Chinese)
张涛,范明钰,王光卫,等. Smartcard 上椭圆曲线密码算法的能量攻击和防御[J]. 计算机工程,2007,33(14):125-127.