doi:10.11959/j.issn.1000-436x.2017158

基于 0.1π 旋转相位 Grover 算法的 ECC 电压毛刺攻击算法

王潮[1]，曹琳[1]，贾徽徽[2]，胡凤[1]
（1. 上海大学通信与信息工程学院特种光纤与光接入网重点实验室，上海 200072；2. 公安部第三研究所，上海 200031）

摘 要：将 Grover 算法应用到对公钥密码的故障攻击中，提出一种基于固定相位旋转 Grover 量子算法，当旋转相位为 0.1π 时，仿真实验搜索成功率提高到 99.23%。进一步与故障攻击结合，提出基于 0.1π 旋转相位 Grover 算法的椭圆曲线密码电压毛刺攻击算法，仿真实验以 100%的概率攻击了 NIST 公布的 Koblitz 安全曲线 K-163，其计算复杂度呈指数级降低。这是除 Shor 算法之外量子计算对公钥密码的一种新的有效攻击途径，有助于拓展量子计算对其他公钥密码体制的攻击。

关键词：量子搜索算法；Grover 算法；相位匹配；量子计算；电压毛刺攻击
中图分类号：TP309.7 **文献标识码**：A

ECC fault attack algorithm based on Grover's quantum search algorithm with 0.1π phase rotation

WANG Chao[1], CAO Lin[1], JIA Hui-hui[2], HU Feng[1]
(1. Key Lab of Specialty Fiber Optics and Optical Access Network,
School of Communication and Information EngineeringShanghai University, Shanghai 200072, China;
2. The Third Research Institute of Ministry of Public Security, Shanghai 200031, China)

Abstract: The Grover's algorithm was used for fault attack against the public key cryptography. A fixed phase rotation based Grover's algorithm was proposed, and the probability of success achieved 99.23% with 0.1π phase rotation. Combined with the fault attack further, ECC (elliptic curve cryptography) voltage burr attack algorithm based on Grover algorithm with 0.1π phase rotation was proposed. Then a safety Koblitz curve, K-163, published successfully attacked by NIST on binary domain in simulation and the success rate was 100%. The complexity of the attack greatly reduces on the exponential. It was a new effective way, except the Shor's algorithm, to attack public key cryptography by quantum computing, and it contributed to extend the attack ways to the other public key cryptography.

Key words: quantum search algorithm, Grover's algorithm, phase matching, quantum computing, voltage burr attack

1 引言

现有 2 种量子计算机：当前无法实用化的通用量子计算机和商用化专用量子计算机 D-Wave。

近几年，美国、英国、欧盟以及 Google、IBM 等均在自主研发通用量子计算机技术，如 Google 量子霸权、IBM Q 等项目。若量子比特数达到 50，则可匹敌当前最强的超级计算机。另外，首家商用化专用型量子计算机公司 D-Wave 已达千位级量子比特，展现了惊人的指数级空间加速潜力，同 Lockheed Martin、Google、Los Alamos、Temporal Defense Systems（TDS）等长期合作，应用于航天航空、人工智能、网络安全等领域。

因此，基于量子算法进行有效密码攻击也是量子计算由实验室迈向实践的重要一步。

ECC(elliptic curve cryptography)是目前安全强度最高的公钥密码，由 Koblitz 和 Miller 在 1985 年提出，其安全性是建立在有限域上椭圆曲线离散对数计算困难性的基础之上的，由于目前还没有发现亚指数级的破译算法，因此，在实际应用中，ECC

收稿日期：2017-02-15；**修回日期**：2017-06-01
基金项目：国家自然科学基金资助项目（No.61572304, No.61272096, No.61332019）
Foundation Item: The National Natural Science Foundation of China (No.61572304, No.61272096, No.61332019)

的安全强度还比较高。ECC 已经逐渐被加入到标准组织如 ANSI(American National Standards Institute)、IEEE(Institute of Electrical and Electronic Engineers)、ISO(International Standards Organization)和 NIST (National Institute of Standards and Technology)发布的标准中，并广泛应用到无线通信、智能卡、嵌入式系统等环境中。

2002 年，Chris Monico 与 Notre Dame 大学数学研究中心的数学家采用 Pollard rho 算法，成功完成了 Certicom 的 ECC-109 bit 大素数域的挑战。2004 年 4 月 8 日，Chris Monico 带领 Texas Tech 大学的数学家成功完成了 Certicom 的 ECC-109 bit 二进制域的挑战。但在此之后，根据滑铁卢大学和 CertiCom 公司等业内研究，近年对 ECC 并没有新的破译进展。

各种研究表明，一般数学分析对 ECC 几乎构不成威胁，对 ECC 的攻击主要是基于非数学难题方法的攻击，如侧信道攻击[1,2]。1997 年，Boneh 等[3]首次提出了故障攻击（fault attack）方法。2000 年，Biehl 等[4]成功实现了对 ECC 的差分故障攻击（DFA, differential fault attack）。2008 年，滑铁卢大学的 Dominguez-Oviedo 等[5]提出了一种基于故障攻击（fault-based attack）的新方法来攻击椭圆曲线标量乘法（ECSM）算法，使 NIST 公布的除 K-283 以外的安全曲线的安全性都受到了威胁，算法攻击成功的概率达到了 0.99。2006 年，赵彦光等[6]对基于 ECC 算法的专用密码芯片进行了功耗分析。2012 年，张金中等[7]给出了一种能够解决“零块失效”问题的改进故障分析方法，实验表明 15 次故障注入便可恢复 192 bit 完整密钥。

从理论上说，量子 Shor 算法可用于攻击公钥密码 RSA 和 ECC。但是，量子器件发展缓慢，短期内尚难以达到破译 1 024 bit RSA 所需的 2 000 qubit[8]。

而量子算法中的 Grover 算法优势在于对无序数据库快速有效的搜索，相当于降为一半长度密钥的穷尽搜索，但计算复杂度仍然是指数级的，虽然普适性强，但对公钥密码的威胁不致命。因此，本文考虑在公钥密码的非数学攻击方法中引入量子计算加速，并将其应用到对 ECC 的攻击中。实验表明，新算法使攻击复杂度指数级降低。目前，已有将 Grover 算法用于侧信道攻击中扫描式攻击的研究[9]。

不过，Grover 算法并不是完美的，经典 Grover 算法仅在数据库的总态数无穷大时才接近于 100%，当数据库规模偏小时，其搜索成功率并不高。

1999 年，Biham 等[10]提出了一种 Grover 量子搜索算法。2000 年，Biham 等[11]将 Hadamard 变换替换为任意酉变换，对 Grover 搜索的方法做了进一步研究。2005 年，Grover[12]提出了固定点量子搜索。2007 年，Younes[13]提出了基于固定相位旋转的 Grover 算法，该算法在现有的幅度放大算法中，把旋转相位从原来的 π 改为 1.825π，从而将算法最低成功概率提高到了 98%。2011 年，Dhawan 等[14]对 Grover 算法的 2 种数据编码方法进行了比较，发现 Perkowski 的编码方法比 Hogg 的效率要高，更容易降低 Oracle 量子成本。

1999 年，Long 等[15]研究发现，Grover 量子搜索算法若保证有一半的成功率，被搜索数据库大小应为 $O\left(\frac{1}{\delta^2}\right)$。2004 年，Long 等[16]从 Grover 算法的几何可视化入手，分析一次 Grover 变换后的弧度，给出了 Grover 改进算法。该算法首先使用 Grover 变换迭代 $J=\left[\frac{\frac{\pi}{2}-\beta}{2\beta}\right]$ 次，其中，$\beta=\arcsin\left(\frac{1}{\sqrt{N}}\right)$，[]表示取整。然后根据相位匹配条件，将相位取反替换成一个与数据库的大小 $\sqrt{N}$ 有关的相位旋转，此相位旋转角度比 π 略小，为 $\Phi=\theta=2\arcsin\left[\sin\left(\frac{\pi}{4J+6}\right)\sqrt{N}\right]$，经过改进的算法搜索成功率可以达到 100%。

2007 年，Li 等[17]通过对 π 的取值来寻找新的相位匹配条件，很好地解决了当目标解 M 和数据库大小 N 之间相对大小关系不同时，普通 Grover 算法失效的问题。

本文算法是在文献[16]的成果上改进而来，采用了固定相位旋转方法，从而能够将其应用到 ECC 的故障攻击中，实现量子算法对公钥密码的故障攻击。本文从实际应用出发，详细分析了实际应用中固定相位旋转的改进 Grover 算法的迭代次数和成功率，并给出了仿真结果，改进 Grover 算法的仿真实验搜索成功率为 99.23%，将其应用到故障攻击中后，对 ECC 的攻击成功率为 100%。

2　Grover 量子搜索算法的基本原理

对于一个含有 $N=2^n$ 个元素的搜索问题，假设搜索问题有 M 个解，搜索问题的一个特殊的例子可以表示为：x 是 0~N−1 的整数，若 x 是搜索问题的解，则 $f(x)=1$，若 x 不是搜索问题的解，则 $f(x)=0$。Grover 算法的搜索过程如图 1 所示，其中，输入端包含了一个 n qubit 寄存器和一个有若干量子比特的 Oracle 工作空间。从图 1 可以看出，算法一共需要执行 $O(\sqrt{N})$ 次搜索过程，每一次搜索过程称为一次 Grover 迭代。

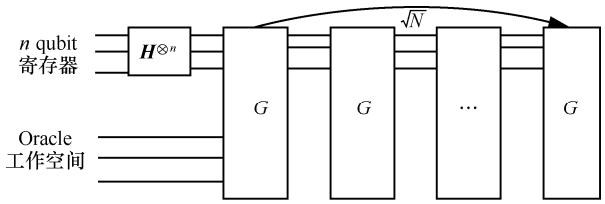

图 1　Grover 算法的搜索过程

设 Grover 算法初始态是 $|0\rangle^{\otimes n}$，经过 Hadamard 变换得到均衡叠加态为

$$|\phi\rangle=\frac{1}{N^{\frac{1}{2}}}\sum_{x=0}^{N-1}|x\rangle \tag{1}$$

如图 2 所示，能实现 Grover 迭代的量子线路总共分为以下 4 步。

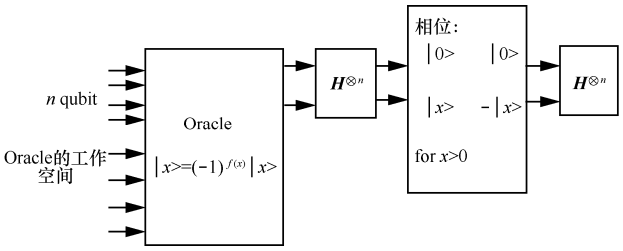

图 2　迭代路线

Step1　使用 Oracle 算子 O，对目标态进行取反，分别检验每个元素是否为搜索问题的解。计算规则为

$$|x\rangle\to(-1)^{f(x)}|x\rangle \tag{2}$$

Step2　应用 Hadamard 变换操作 $\boldsymbol{H}^{\otimes n}$（$\boldsymbol{H}^{\otimes n}=\boldsymbol{H}\otimes\boldsymbol{H}\otimes\cdots\otimes\boldsymbol{H}$）。

$$\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{3}$$

其中，$\boldsymbol{H}^{\otimes n}$ 即为 $\boldsymbol{H}$ 的 n 次 Kronecker 直积。

Step3　条件相移，使 $|0\rangle$ 以外的每个基态都获得 π 的相移，对应的酉算子为

$$2|0\rangle\langle 0|-\boldsymbol{I} \tag{4}$$

Step4　对 Step3 的结果施加 Hadamard 变换 $\boldsymbol{H}^{\otimes n}$。

Step 2~Step 4 的作用效果可以等效为

$$U=2|\phi\rangle\langle\phi|-\boldsymbol{I} \tag{5}$$

Grover 迭代可写为

$$G=UO=(2|\phi\rangle\langle\phi|-\boldsymbol{I})O \tag{6}$$

Oracle 实质为一个酉算子，其作用为 $|x\rangle|b\rangle\xrightarrow{\text{Oracle}}|x\rangle|b\oplus f(x)\rangle$，其中，$|x\rangle$ 是一个指标寄存器，Oracle 的量子比特 $|b\rangle$ 是单量子比特，当 $f(x)=1$ 时会反转；否则不变。在 Grover 量子搜索算法中 Oracle 作用为

$$|x\rangle\left|\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\right\rangle\xrightarrow{\text{Oracle}}(-1)^{f(x)}|x\rangle\left|\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\right\rangle$$

因为在量子搜索过程中，Oracle 量子比特 $|b\rangle$ 状态一直保持不变，因此可以定义 Oracle 作用为 $|x\rangle\xrightarrow{\text{Oracle}}(-1)^{f(x)}|x\rangle$。

一次 Grover 迭代中，$(2|\phi\rangle\langle\phi|-\boldsymbol{I})$ 和 O 的作用是量子态在二维空间中的 2 次变换，Grover 迭代可视为在由开始向量 $|\phi\rangle$ 和目标解组成的均匀叠加态张成的二维空间中旋转。Grover 算法的几何可视化如图 3 所示。量子计算机的初态可以重新表示为

$$|\phi\rangle=\sqrt{\frac{m}{N}}|s\rangle+\sqrt{\frac{N-m}{N}}|t\rangle \tag{7}$$

其中，

$$|t\rangle=\frac{1}{\sqrt{N-m}}\sum_{x}^{2}|x\rangle \tag{8}$$

$$|s\rangle=\frac{1}{\sqrt{m}}\sum_{x}^{1}|x\rangle \tag{9}$$

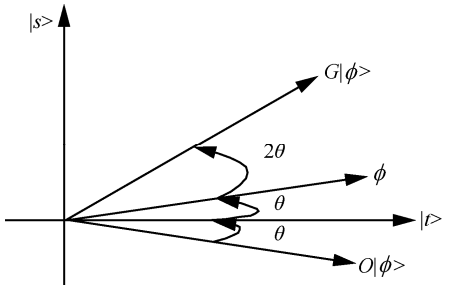

图 3　Grover 算法的几何可视化

从图3可以看出，量子计算机的初态是由$|t\rangle$和$|s\rangle$张成的空间，运算O的作用是将定义在二维空间中的初态$|\phi\rangle$对$|t\rangle$进行一次反射，类似地，$2|\phi\rangle\langle\phi|-1$是定义在二维空间中的向量对$|\phi\rangle$的一次发射。2次反射的积是一次旋转，因此，一次$G$迭代的作用将$|\phi\rangle$变为

$$G|\phi\rangle=\cos 3\theta|t\rangle+\sin 3\theta|s\rangle \tag{10}$$

反复进行G迭代，就能以很高的概率搜索到目标解$|s\rangle$的位置。

3 基于固定旋转相位的Grover算法的ECC电压毛刺攻击算法设计

3.1 基于固定相位旋转的改进Grover算法

根据经典Grover算法中相位旋转的角度不同，固定相位旋转Grover算法便可演化出多种不同的Grover算法。当旋转相位为π时，等价于经典Grover算法[18,19]；当取0.5π时，等价于Younes的局部扩散算法[20]；当取1.825π时，等价于Younes的固定相位算法[21]。

文献[16]研究结果显示，在三维空间中，迭代算子G每作用一次，就会使相位旋转大小为$4\arcsin\left(\sin\left(\frac{\alpha}{2}\right)\sin\theta\right)$，且标记态向量可以表示为(0, 0, 1)，初始态向量可表示为(0, 0, −1)[22]。若要成功概率最大，迭代步数应为

$$R=\left\lfloor\frac{\pi}{4\arcsin\left(\sin\left(\frac{\alpha}{2}\right)\sin\theta\right)}\right\rfloor \tag{11}$$

由于$\sin\theta=\sqrt{\frac{M}{N}}$，由数学知识可知，当$\theta$很小时，$\sin\theta\approx\theta$，所以当$M\ll N$时，可得

$$R\approx\left\lfloor\frac{\pi}{4\sin\left(\frac{\alpha}{2}\right)\sqrt{\frac{M}{N}}}\right\rfloor=O\left(\sqrt{\frac{M}{N}}\right) \tag{12}$$

当旋转相位α取不同值时，基于固定相位旋转的Grover算法可演化出其他几种Grover算法。

1) 旋转相位$\alpha=\pi$

$$R=\left\lfloor\frac{\pi}{4\arcsin\left(\sin\left(\frac{\alpha}{2}\right)\sin\theta\right)}\right\rfloor\approx\left\lfloor\frac{\pi}{4}\sqrt{\frac{N}{M}}\right\rfloor \tag{13}$$

此时的Grover算法等价于经典Grover算法[18,19]。

2) 旋转相位$\alpha=\frac{\pi}{2}$或$\alpha=\frac{3\pi}{2}$

$$R=\left\lfloor\frac{\pi}{4\arcsin\left(\sin\left(\frac{\alpha}{2}\right)\sin\theta\right)}\right\rfloor\approx\left\lfloor\frac{\pi}{2\sqrt{2}}\sqrt{\frac{N}{M}}\right\rfloor \tag{14}$$

此时的Grover算法等价于Younes局部扩散算法[20]。

3) 旋转相位$\alpha=1.825\pi$或$\alpha=0.175\pi$

$$R=\left\lfloor\frac{\pi}{4\arcsin\left(\sin\left(\frac{\alpha}{2}\right)\sin\theta\right)}\right\rfloor\approx\left\lfloor\frac{1.825\pi}{2\sin\theta}\right\rfloor \tag{15}$$

此时的Grover算法等价于Younes的固定相位算法[21]。

4) 把旋转相位降为$\alpha=0.1\pi$

$$R=\left\lfloor\frac{\pi}{4\arcsin\left(\sin\left(\frac{\alpha}{2}\right)\sin\theta\right)}\right\rfloor\approx\left\lfloor5\sqrt{\frac{N}{M}}\right\rfloor \tag{16}$$

根据以上研究，以π为中心，本文主要考虑旋转角度小于π的情况。随着相位旋转角取值变小，虽然在相同的数量级$\sqrt{\frac{N}{M}}$下所需的迭代步数变多，但Grover算法获得目标态的成功概率与旋转角度的变化关系较为复杂。

因此，基于文献[16]对旋转相位的研究，本文将在0.1π～π旋转相位的范围内进行分析，选取适当的旋转相位，使Grover搜索成功概率接近100%。

3.2 基于Grover固定旋转相位改进的ECC电压毛刺攻击算法

故障攻击[1,2]的故障注入可以为非正常工作电压、电辐射、非正常工作周期等，这种错误是临时性的，只会影响当前数据而不会对芯片造成损坏。本文主要研究电压毛刺攻击。电压毛刺攻击的毛刺既可以在时钟信号上进行叠加得来，也可以是来自外部短暂的电磁脉冲。在编程过程中，通过异或运算对加入的电压进行模拟。

下面将对电压毛刺攻击基于ECC密码体制的加密芯片、基于固定旋转相位的改进Grover算法的搜索密钥算法及其迭代过程进行介绍。

1) 使用电压毛刺技术攻击基于ECC密码体制的加密芯片，具体算法设计如下。

首先，设密钥 k 长度为 l，点乘运算时从低位开始加入异或运算，相当于加入了电压毛刺攻击，并持续 $l-m$ 次点加—倍点循环。电压毛刺加入位置也可从高位开始或随机选择开始位置，但要对随机选择的位置进行标记，防止密钥位的重复计算，影响攻击效率。密钥由 k 变为错误的 k'，k' 中有 $l-m$ 位为 0，剩余 m 位为正确密钥值，此时执行点乘算法得到错误的 Q'。

其次，此时密钥的低 $l-m$ 位为 0 已经确定，高 m 位可取值 0 或 1。列出全部 l 位所有可能值构成密钥空间 $\{k'_m\}$，$\{k'_m\}$ 的范围为

$$\{k'_m\}=\left(\left(\underbrace{11\cdots1}_{m}\underbrace{00\cdots0}_{l-m}\right)\sim\left(\underbrace{00\cdots0}_{m}\underbrace{00\cdots0}_{l-m}\right)\right) \tag{17}$$

然后，将密钥空间 $\{k'_m\}$ 中的值进行逐一的点乘运算，得到结果 $\{Q'_m\}$。此时 $\{Q'_m\}$ 与 $\{k'_m\}$ 中的值是一一对应的。将 $\{Q'_m\}$ 中的值与 Q' 进行对比，找出结果相同时 Q'_m 所对应的 k'_m，其中，k'_m 的前 m 位为正确密钥值。

最后，重复上述过程，直到找出密钥完整值，再与 k 进行比较。

对上述电压毛刺故障攻击得到的 m 位正确密钥值与 l−m 位 0 值构成临时密钥空间 $\{k'_m\}$（大小为 N=2m），建立数据库 A，再通过基于固定旋转相位的改进 Grover 量子算法可快速搜索出临时密钥 k。

2) 基于固定旋转相位的改进 Grover 算法搜索密钥算法步骤如下。

Step 1　准备 2 个量子寄存器。在第一个寄存器存放 m qubit，在第二个寄存器存放 1 qubit。

Step 2　制造 m qubit 的均匀叠加态 s。

将 Grover 量子搜索算法的第一个寄存器 m qubit 初始化为 $|0\rangle^{\otimes m}$，第二个寄存器中的 1 qubit 初始化为 $|1\rangle$。对第一个量子寄存器中的每一个量子比特都进行 Hadmard 变换，有

$$|s\geqslant \boldsymbol{H}^{\otimes m}|0\rangle^{\otimes m}=\frac{1}{2^{\frac{m}{2}}}\sum_{x=0}^{2^m-1}|x\rangle \tag{18}$$

上述操作实现了 m qubit 的均匀叠加，从而得到了状态 s。

Step 3　由式(16)执行 $5\sqrt{2^m}$ 次 Grover 迭代。

首先，利用 $\{k'_m\}$ 中的密钥值分别进行点乘运算，得到 $\{Q'_m\}$。定义 Oracle 为 $F(x)$，满足

$$\begin{cases}F(x)=0, & Q'\neq Q'_m\\ F(x)=1, & Q'=Q'_m\end{cases} \tag{19}$$

通过 Oracle 就可以标记正确的 Q'，进而找出对应 m 位正确密钥。

基于固定旋转相位的改进 Grover 算法的迭代包括以下 4 个步骤。

① Oracle 标记目标解时相位旋转角度记为 θ，算符为

$$\boldsymbol{I}_x=\boldsymbol{I}+(\mathrm{e}^{\mathrm{i}\theta}-1)|x\rangle\langle x| \tag{20}$$

② 应用 Hadamard 变换 $\boldsymbol{H}^{\otimes m}$。

③ 条件相移，$|0\rangle$ 以外的每个基态相位旋转角度记为 ϕ，算符为

$$\boldsymbol{I}_0=\boldsymbol{I}+(\mathrm{e}^{\mathrm{i}\phi}-1)|0\rangle\langle 0| \tag{21}$$

④ 对上一步的结果施加 Hadamard 变换 $\boldsymbol{H}^{\otimes m}$。

这里令 $\theta=\phi=0.1\pi$，酉变换的作用是将目标态的几率振幅进行放大，从而降低非目标态的几率振幅。经过多次 Grover 迭代后，就可以使目标态振幅达到最大，最后，能在测量时以较高的概率输出问题的目标解。

Step 4　输出一个 k'。此时，k' 中含有 m 位正确的密钥值。

完成一次搜索后，再将密钥位由高到低，重复执行上述过程，直至推测出全部密钥。

4　基于固定旋转相位的 Grover 算法的 ECC 电压毛刺攻击算法的仿真结果

4.1　基于固定相位旋转的改进 Grover 算法实验分析

在对固定相位旋转的改进 Grover 算法的仿真模拟中，本文取数据库状态总数 N=10^3，通过改变 α 的值，得到 4 种算法的搜索成功概率对比，如图 4 所示，在仿真过程中，通过变化旋转相位，对比不同旋转相位条件下得到的搜索成功率，发现当旋转相位为 0.1π 时，成功率接近 100%。而且，从图 4 中可以看出，目标态数为状态总数的一半时，相比于其他算法，旋转相位为 0.1π 的 Grover 算法的搜索成功概率会远高于经典 Grover 算法的搜索成功概率，可见缩小旋转相位对目标态的成功搜索概率的提升是非常大的。

图 5 为 4 种算法迭代次数的对比，由图 5 可以看出，旋转相位为 0.1π 的 Grover 算法迭代步数最大达到了 159，经典 Grover 算法最大的迭代步数却只有 24。

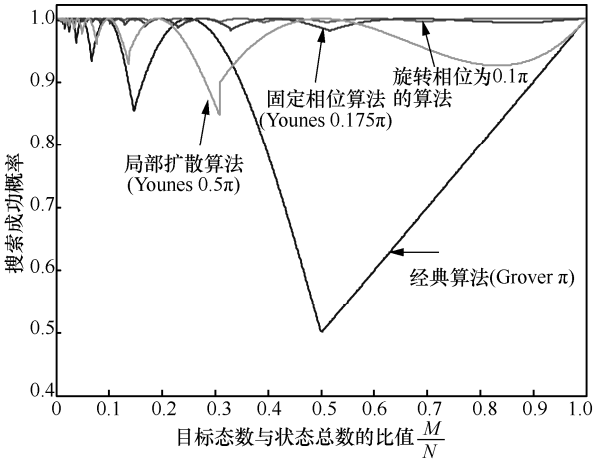

图 4 4 种 Grover 算法的搜索成功概率对比

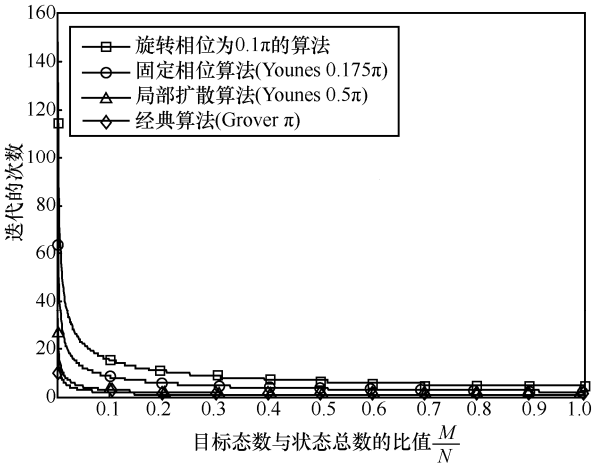

图 5 4 种 Grover 算法的迭代次数对比

根据仿真实验输出数据结果，当状态总数 N=10^3 且 $0<\frac{M}{N}\leqslant 1$ 时，4 种算法的性能对比如表 1 所示，$P_{\min}$ 为搜索成功的概率最小值，$\left(\frac{M}{N}\right)_{P=P_{\min}}$ 为当搜索成功概率取最小值时的 $\frac{M}{N}$ 值，$R_{\max}$ 为最大迭代数。

表 1 给出了 4 种不同 Grover 算法的搜索成功率对比结果，显然，经典 Grover 算法的搜索成功概率最低，仅为 50%，且最大迭代次数最少，即搜索消耗时间相对较少；旋转相位 $\alpha=0.1\pi$ 的改进 Grover 算法的搜索成功概率是最高的，达到了 99.23%，尽管其最大迭代步数最大，但是与其他算法相比，其算法实现的复杂度的数量级相同，均为 $\sqrt{\frac{N}{M}}$。

表 1 4 种 Grover 算法的性能指标对比

性能指标	Grover 算法（$\alpha=0.1\pi$）	Younes 固定相位算法（$\alpha=1.825\pi$）	Younes 局部扩散算法（$\alpha=0.5\pi$）	经典 Grover 算法
$P_{\min}$	0.992 3	0.980 7	0.847 6	0.500 0
$\left(\frac{N}{N}\right)_{P=P_{\min}}$	0.511 8	0.514 1	0.307 9	0.500 0
$R_{\max}$	159	90	35	24

因此，本文选用 $\alpha=0.1\pi$ 的 Grover 算法来进行 ECC 的攻击实验。

4.2 基于 0.1π 旋转相位的 Grover 算法的 ECC 电压毛刺攻击算法对 K-163 安全曲线的攻击实验

实验环境为 Intel(R) Core(TM) i5-3230M，CPU 为 2.60 GHz，内存为 4 GB，编程环境为 Microsoft Visual Studio C++ 2010，仿真环境为 Matlab 2010，攻击流程如图 6 所示。

实验的对象为 NIST 推荐的在二进制域上的一条 Koblitz 安全曲线，即 K-163。

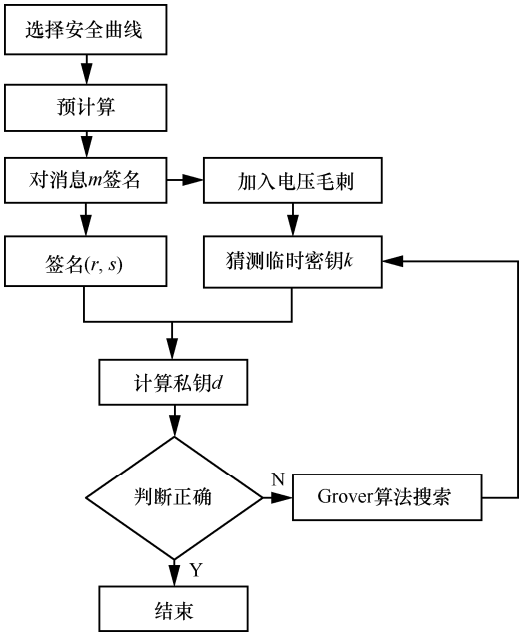

图 6 基于改进 Grover 算法的椭圆曲线密码（ECC）电压毛刺攻击流程攻击流程

NIST 推荐的在二进制域上的 Koblitz 曲线 K-163 的参数如下

K-163: m=163, $f(z)=z^{163}+z^7+z^6+z^3+1$, a=1, b=1, h=2

n=0x00000004000000000000000020108A2E0CC0D99F8A5EF

x=0x00000002FE13C0537BBC11ACAA07D793

DE4E6D5E5C94EEE8

y=0x0000000289070FB05D38FF58321F2E800536D538CCDAA3D9

其中，m 是表示二进制域 F_{2^m} 的扩展次数，$f(z)$表示次数为 m 的约减多项式，a、b 表示椭圆曲线 $y^2+xy=x^3+ax^2+b$ 的系数，n 表示基点 P 的阶，h 表示余因子，x、y 表示 P 的 x 和 y 坐标。

随机获取 128 bit 密钥为

k=0xF74AC3B11234567855AC435962FE9AE2

图 7 横坐标为密钥的位数，共 128 bit，纵坐标为电压阈值大小。通过分析电压阈值数据得出，纵坐标数值大于 0.5 读出位值为 1，小于或等于 0.5 读出位值为 0。

最后得出 128 bit 的猜测密钥为

k'=11110111010010111100001110110001000100001101000101011001111000010101011010110001000001101011001011000101111111010011010111000 01

与原密钥相同，攻击成功。

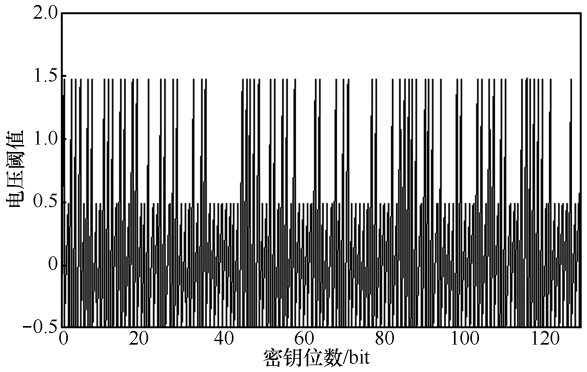

图 7　针对 K-163 安全曲线的攻击仿真

4.3　攻击 K-163 安全曲线实验复杂度分析

对美国 NIST 公布的 1 条 Koblitz 安全曲线 K-163 进行攻击时，为了方便对结果进行分析，在曲线域的范围内随机取一些常见的密钥长度 k。

由于 ECC 点乘算法每一次循环时间非常短，当 m 取值过大或过小时，电压毛刺持续时间在实际操作中不易控制，因此，m 取值应尽量适中。表 2 中列举一次攻击得到的正确密钥数分别为 8、16、32、64 bit。计算复杂度。

通过表 2 可得出以下结论。

1) 相对于穷举攻击，电压毛刺攻击 ECC 算法计算复杂度由 $O(2^l)$降到 $O(\frac{l}{m}\times 2^m)$，可以从指数级上大幅降低计算复杂度。对于不同的安全曲线，密钥长度越长，攻击复杂度也就越高。

2) 通过比较原始的 ECC 算法电压毛刺故障攻击与加入 Grover 算法后的攻击，算法的复杂度由 $O(2^m)$降为 $O\left(2^{\frac{2m}{3}}\right)$，密钥长度越长，算法的优越性也越明显。对于旋转相位为 0.1π 的改进 Grover 算法故障攻击整体算法，当密钥长度为 l 时，若每次执行 Grover 过程能够得到 m bit 正确密钥，则攻击的计算复杂度将由 $O(2^l)$降为 $O(5\times 2^{\frac{2m}{3}})$，从指数级上大大降低了复杂度。

5　结束语

侧信道攻击是针对密码设备实现过程中泄露出来的物理效应进行攻击，存在计算复杂度较高、资源冗杂等问题，而 Grover 算法对公钥密码的穷举分析仅相当于降低一半密钥，缺乏攻击的致命性。针对各自的特点，本文将这两者结合，介绍了几种基于固定相位旋转的改进的 Grover 算法，研究了一种搜索成功率几乎为 100%的基于 0.1π 旋转相位的 Grover 算法，并对其进行了数字仿真模拟，结果显示搜索成功率为 99.23%。然后，将其运用于 ECC 电压毛刺故障攻击中，又提出了基于 0.1π 相位旋转的 Grover 量子搜索算法的 ECC 电压毛刺攻击算法，最大化提高了搜索正确密钥的成功概率，即对长度为 l 的密钥，若每次执行 Grover 过程得到 m bit 正确密钥，则攻击的计算复杂度将由 $O(2^l)$降为 $O(5\times 2^{\frac{2m}{3}})$，从指数级上大大降低了复杂度，有效提升量子计算对密码攻击的普适性和致命性。同时进行了攻击仿真实验，成功地攻击了 NIST 公布的二进制域上的一条 Koblitz 安全曲线 K-163，攻击成功率为 100%。

针对 ECC，本文有效实现了基于 Grover 算法的

表 2　　K-163 安全曲线，密钥 k 的长度 l=128 bit，攻击的计算复杂度对比

功击类型	复杂度			
	m=8	m=16	m=32	m=64
原电压毛刺攻击	$O(2^{12})$	$O(2^{19})$	$O(2^{34})$	$O(2^{65})$
加入 Grover 算法	$O(5\times 2^{8})$	$O(5\times 2^{11})$	$O(5\times 2^{18})$	$O(5\times 2^{33})$

故障攻击，提出使用量子计算对公钥密码的一种新的有效的攻击途径，有助于拓展量子计算对其他公钥密码体制的攻击，同时，对其他公钥密码体制侧信道攻击也有普适性。该研究领域目前在国内外基本处于空白状态，下一步研究可以攻击多条安全曲线，进一步验证算法的有效性和实用性，然后可以考虑将量子算法应用到对公钥密码的其他攻击中，找到更好的攻击方法。量子算法的应用，给密码安全性提出了更高的要求，因此，需要针对量子算法的特点尽快设计抗量子攻击的安全有效密码，保证各行业的安全。

参考文献：

[1] ZHANG F, GUO S Z, ZHAO X J. A framework for the analysis and evaluation of algebraic fault attacks on lightweight block ciphers[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(5): 1039-1054.

[2] ZHAO X J, GUO S, ZHANG F. Algebraic fault analysis on GOST for key recovery and reverse engineering[C]//2014 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). 2014:29-39.

[3] BIHAM E, SHAMIR A.Differential fault analysis of secret key cryptosystem[J]. Springer Berlin Heidelberg, 1997, 1294:513-525.

[4] BIEHL I, MEYER B, MULLER V. Differential fault attacks on elliptic curve cryptosystems[C]//CRYPTO 2000, LNCS 1880. 2000: 131-146.

[5] DOMINGUE-VIEDO A, HASAN MA, ANSARI B. Fault-based attack on Montgomery's ladder ECSM algorithm[J]. Journal of Cryptology, 2011,24(2):346-374.

[6] 赵彦光, 白国强, 陈弘毅, 等. ECC 专用密码芯片的功耗分析研究[J]. 计算机工程与应用, 2006, 42(16): 25-28.
ZHAO Y G, BAI G Q, CHEN H Y, et al. Study of power analysis attack to ECC in ASIC chip[J]. Computer Engineering and Applications, 2006, 42(16): 25-28.

[7] 张金中, 寇应展, 王韬, 等. 针对滑动窗口算法的椭圆曲线密码故障分析[J]. 通信学报, 2012, 33(1): 71-78
ZHANG J Z, KOU Y Z, WANG T, et al. Fault analysis on elliptic curve cryptosystems with sliding window method[J]. Journal on Communications, 2012, 33(1): 71-78.

[8] 王潮, 王云江, 胡风. 量子计算机的商业化进展以及对信息安全的挑战[J]. 网络与信息安全学报, 2016, 2(3): 17-27.
WANG C, WANG Y J, HU F. Shaping the fature of commercial quantum computer and the challenge for information security[J]. Chinese Journal Network and Information Security, 2016, 2(3): 17-27.

[9] 陈宇航, 贾徽徽, 姜丽莹. 基于 Grover 算法的 ECC 扫描式攻击[J]. 信息网络安全, 2016(2):28-32.
CHEN Y H, JIA H H, JIANG L Y. ECC scanning attack based on Grover algorithm[J]. Net Info Security, 2016(2):28-32.

[10] BIHAM E, BIHAM O. Grover's quantum search algorithm for an arbitrary initial amplitude distribution[J]. Physical Review A, 1999, 60(4): 2742-2745.

[11] BIHAM E, BIHAM O. Analysis of generalized Grover quantum search algorithms using recursion equations[J]. Physical Review A, 2001, 63(1): 5348-5353.

[12] GROVER J K. Fixed-point quantum search[J]. Physical Review Letters, 2005, 95(15): 1-4.

[13] YOUNES A. Fixed phase quantum search algorithm[J]. Applied Mathematics & Informationences, 2007, 7(1):93-98.

[14] DHAWAN S, PERKOWSKI M. Comparison of influence of two data-encoding methods for Grover algorithm on quantum costs[C]// The 41st IEEE International Symposium on Multiple-Valued Logic. 2011: 176-181.

[15] LONG G L, LI Y S, ZHANG W L. Dominant gate imperfection in Grover's quantum search algorithm[J]. Physical Review A, 2000, 61(042305):1-5.

[16] LONG G L, LI Y S, XIAO L. Phase matching in quantum searching and the improved Grover algorithm[J]. Nuclear Physics Review, 2004, 21(2):114-116.

[17] LI P C, LI S Y. Phase matching in Grover's algorithm[J]. Physics Letters A, 2007, 366(1-2): 42-46.

[18] YOUNES A, ROWE J, MILLER J. Quantum search algorithm with more reliable behaviour using partial diffusion[C]//The 7th International Conference on Quantum Communication, Measurement and Computing. 2004.

[19] GROVER L K. Quantum mechanics helps in searching for a needle in a haystack[J]. Physical Review Letters, 1997, 79(2):325-328.

[20] GROVER L K. A fast quantum mechanical algorithm for database search[C]//The 28th Annual ACM Symposium on the Theory of Computing. 1996: 212-219.

[21] BULGER D, BAEITOMPA W P, WOOD G R. Implementing pure adaptive search with Grover's quantum algorithm[J]. Journal of Optimization Theory and Applications, 2003, 116(3): 517-529.

[22] LONG G L, LI Y S, ZHANG W L. Phase matching in quantum searching[J]. Physics Letters A, 1999, 262(1): 27-34.

作者简介：

王潮（1971-），男，江苏镇江人，博士，上海大学教授，主要研究方向为无线传感器网络、网络信息安全与椭圆曲线密码学、量子计算与量子攻击密码分析。

曹琳（1991-），女，山东临沂人，上海大学硕士生，主要研究方向为量子计算与量子攻击密码分析。

贾徽徽（1987-），男，山东临沂人，公安部第三研究所工程师，主要研究方向为网络与信息安全、智能卡安全、量子攻击密码分析。

胡风（1991-），男，浙江温州人，上海大学博士生，主要研究方向为信息安全、量子计算密码、社会网络。