DOI:10. 19431/j. cnki. 1673-0062. 2023. 04. 011

一种抗弱曲线故障攻击的 SM2 数字签名算法设计

钱垂昇,曾玖贞,王　彦*

(南华大学 电气工程学院,湖南 衡阳 421001)

摘　要:SM2 数字签名算法是中国版的椭圆曲线数字签名算法,尽管该算法的设计在数学理论是安全的,但在算法的具体实现时却容易遭受物理攻击。因此,加强 SM2 数字签名算法在实现过程中的抗攻击性具有重要意义。本文基于故障感染思想提出了一个针对 SM2 数字签名算法的抗故障攻击策略,通过改变算法中的标量运算操作,使得算法遭受攻击后故障将在签名过程中扩散,从而破坏攻击者利用错误签名快速检索签名私钥的条件。实验结果表明,此防御策略不仅可以抵御弱曲线故障攻击,还可以防御弱曲线故障和二次故障注入的结合攻击。此外,本文还将椭圆曲线算法中常用点检测抗故障攻击策略和本文提出的故障感染防御策略都在现场可编程逻辑列阵上实现,对两种策略的硬件面积开销、单次签名时间开销进行比较,结果显示,本文提出的策略在硬件性能上比基于点检测的策略更优越。

关键词:SM2 数字签名算法;弱椭圆曲线;现场可编程逻辑列阵实现;抗故障攻击
中图分类号:TN918　　**文献标志码**:A
文章编号:1673-0062(2023)04-0083-07

Design of SM2 Digital Signature Algorithm Against Weak Curve Fault Attack

QIAN Chuisheng, ZENG Jiuzhen, WANG Yan*
(School of Electrical Engineering, University of South China, Hengyang, Hunan 421001, China)

Abstract: The SM2 digital signature algorithm is the Chinese version of the Elliptic Curve Digital Signature Algorithm (ECDSA). Although the design of the algorithm is mathematically safe, it is vulnerable to physical attacks when the algorithm is implemented. Therefore, it is of great significance to strengthen the attack resistance of SM2 digital signature algorithm in the implementation process. Based on the idea of fault infection, this paper proposes an anti-fault attack strategy for SM2 digital signature algorithm, which changes

收稿日期:2023-02-12
基金项目:湖南省教育厅科学研究一般项目(20C1619)
作者简介:钱垂昇(1997—),男,硕士研究生,主要从事网络信息安全方面的研究。E-mail:18773929871@163. com。
*通信作者:王　彦(1971—),男,教授,博士,主要从事智能信息处理和智能控制方面的研究。E-mail:wangyan5406@163. com

the scalar operation in the algorithm so that the fault will spread in the signing process after the algorithm is attacked, thereby destroying the conditions for attackers to quickly retrieve the signature private key by using incorrect signatures. Experimental results show that the proposed defense strategy can not only resist weak curve fault attacks but also defend against combined attacks of weak curve faults and secondary fault injection. In addition, we also implement the common point detection anti-fault attack strategy in elliptic curve algorithm and the fault infection prevention strategy proposed on Field Programmable Logic Array (FPGA) and compare the hardware area overhead and single signature time overhead of the two strategies, and the results show that the proposed strategy is superior to the point detection-based strategy in hardware performance.

key words: SM2 digital signature algorithm; weak elliptic curve; FPGA implementation; against fault attack

0　引　言

随着数字化的进程全面推进,信息安全也越来越受到公众关注,加密技术则是当前解决信息安全问题的主要技术手段。密码算法作为加密技术的核心,一般分为加密解密、签名验签、密钥交换三种类型,其中数字签名算法(digital signature algorithm,DSA)用于确保信息传输过程中数据的真实性、完整性以及不可抵赖性[1]。自 1976 年 Whitfield Diffie 和 Martin Hellman 首次提出数字签名的概念,至今已经出现了许多优秀的数字签名算法。在众多数字签名算法中,椭圆曲线数字签名算法(elliptic curve digital signature algorithm, ECDSA)凭借同等安全水平下密钥更短、签名速度更快等优点而被广泛应用。SM2 数字签名算法(SM2 digital signature algorithm,SM2-DSA)是中国版的 ECDSA,虽然两者的安全性都依托于椭圆曲线离散对数难题(elliptic curve discrete logarithm problem,ECDLP),但 SM2-DSA 的安全性要高于 ECDSA[2]。尽管理论上 SM2-DSA 和 ECDSA 都是安全的,但如果在算法实现的物理设备中引入故障注入攻击,就极有可能导致设备的安全性失效。

故障注入攻击是指在密码设备注入特定故障,使得设备输出故障信息,最终通过分析故障信息得到设备中使用的密钥。文献[3-6]中介绍了几种针对椭圆曲线密码系统(elliptic curve cryptography,ECC)的故障注入攻击方案。其中,弱曲线故障攻击利用故障注入将算法运行中使用的安全椭圆曲线变成另一条不安全的弱椭圆曲线,并通过 Pohlig-Hellman 算法和 Pollard Rho 算法破解弱椭圆曲线上的 ECDLP,从而获取算法中的私钥[6]。为了提高密码算法在实际应用中的安全性,研究人员又进行了许多抗故障攻击的防御策略研究。

对于在 ECC 算法而言,有效点检测是最常用的故障攻击防御策略。在算法运行时,一旦中间状态点被注入故障,该点就会脱离原来的椭圆曲线,从而影响之后一系列的点运算,所以可以在输出结果前对标量运算生成的点进行检测,如果生成的点不在原来的椭圆曲线上,则拒绝输出结果。文献[7]针对 ECDSA 提出了双重随机点检测策略,以防御弱曲线故障攻击。该防御策略在点检测的基础上加入了随机延迟和双重检测机制,解决了简单点检测策略在二次故障注入下失效的问题。文献[8]中将低成本的故障检测与恢复机制和坐标轴随机化技术相结合,提出了一个可以同时防御差分功耗攻击和差分故障攻击的低成本方案。当受到差分故障注入攻击时,可以利用蒙哥马利阶算法中间变量关系的不变性检测到故障,然后将标量运算跳回到上一个有效状态,从而保证故障注入失效的同时不会影响最终的正确结果。除了有效点验证思想,故障感染思想也是抗故障攻击研究的重点。文献[9]中介绍了一种基于故障感染的故障防御策略,以抵抗针对 SM2-DSA 的基格故障攻击。该策略通过故障在签名生成过程中的传播将格攻击所需要的条件破坏掉,从而保证即使发生关键信息泄露,也能够抵御格攻击。

目前对 SM2-DSA 的抗故障攻击研究主要集

中在基格故障攻击和差分故障攻击,关于弱曲线故障攻击的防御研究还比较少。本文基于故障感染思想提出一个新的故障攻击防御策略,以获得一种抗弱曲线故障攻击的改良版 SM2-DSA,利用故障的传播,破坏签名过程中所使用的随机标量值与签名私钥之间的关系,从而保证即使攻击者破解了弱椭圆曲线上的 ECDLP 也无法获得签名私钥。并通过现场可编程逻辑阵列(filed programmable gate array,FPGA)实现了改良后的算法硬件电路设计,对电路的防御效果进行测试。为了更好地验证防御策略的有效性,设计了一种硬件木马,用来模拟针对硬件电路的随机故障注入。同时还设计了一个基于简单点检测防御策略的算法硬件电路作为对比实验,分析对比了两种防御策略的性能和硬件实现上的开销。

1　SM2 数字签名算法基础

1.1　椭圆曲线基本理论

本文中对 SM2-DSA 的分析都是基于素数域 F_p 下的椭圆曲线 $E(a,b)$,其 Weierstrass 方程定义如下所示:

$$E:y^2 = x^3 + ax + b \bmod p \tag{1}$$

其中 $a,b \in F_p$,且满足 $4a^3+27b^2 \neq 0 \bmod p$。椭圆曲线 $E(a,b)$ 上的所有点和素数域 F_p 上的无穷远点 O 构成一个椭圆曲线群 $E(F_p)$,而 $E(F_p)$ 上的标量运算 $kP=P+P+\cdots+P$ 为椭圆密码算法的核心。其中点 $P(x_P,y_P)$ 为 $E(F_p)$ 上除无穷远点 O 外的任意一个点,$k \in \{1,\cdots,p-1\}$。标量运算由点加和倍点两种点运算组成,两种基本点运算的公式如下:

设 $(x_3,y_3)=(x_1,y_1)+(x_2,y_2)$,则:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \tag{2}$$

其中

$$\lambda = \begin{cases} \dfrac{3x^2 + a}{2y_1}, x_1 = x_2, y_1 = y_2 \\ \dfrac{y_2 - y_1}{x_2 - x_1}, \text{其他} \end{cases} \tag{3}$$

此外,对于 $E(F_p)$ 上所有的点 $P(x_P,y_P)$ 还满足:$P+O=P$;$-P=P(x_P,p-y_P)$。

标量运算之所以成为椭圆密码算法的核心,是因为由其衍生出的 ECDLP 为算法提供了数学理论安全。ECDLP 定义为:在 $E(F_p)$ 上有一个非无穷远点 P,且点 P 的阶为 n。存在一个整数 $k \in [1,\cdots,n-1]$,使得 $Q=kP$,那么 k 就称为以 P 为底 Q 的离散对数。假设知道 P 与 Q,求解满足条件的 k,则称为椭圆离散对数难题。当前求解 ECDLP 最好的方法就是 Pohlig-Hellman 算法和 Pollard Rho 算法的结合算法,但其破解 ECDLP 的时间复杂度仍是指数级 $O(\sqrt{q})$,其中 q 为 n 的最大素因子。而在密码算法所选取的椭圆曲线点,其阶 n 本身就是一个大素数。所以一般情况下,即使是最好的算法,也无法在有限时间内破解算法中的 ECDLP。

1.2　SM2 数字签名算法

SM2-DSA 作为中国政府发布的改良版 ECDSA,其签名生成过程与签名时使用的标准椭圆曲线与 ECDSA 都有所不同。在进行签名前,SM2-DSA 需要先进行预计算生成用户杂凑值 Z_A:

$$Z_A = H_v(A_{\text{ENTL}} \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A) \tag{4}$$

式中:H_v 为 SM3 杂凑函数;ID_A 为签名方 A 的标识符;A_{ENTL} 是由 ID_A 的比特位长度转换成的两字节值。SM2-DSA 的签名生成过程如算法 1 所示。

1)算法 1:SM2 数字签名算法

输入:素数域特征 p,椭圆曲线参数 (a,b),基点 $G(x_G,y_G)$ 以及基点的阶 n,待签名信息 M,用户杂凑值 Z_A,签名私钥 d_A。

输出:签名对 (r,s)。

1:$e=H_v(Z_A \| M)$;

2:选择一个随机整数 $k \in [1,n-1]$;

3:标量运算 $Q(x_1,y_1)=kG$;

4:计算 $r=e+x_1 \bmod n$。如果 $r=0$ 或 $r+k=n$,跳回第 2 步;

5:计算 $s=(1+d_A)^{-1}(k-rd_A) \bmod n$。如果 $s=0$,跳回第 2 步;

6:输出签名对 (r,s)。

SM2-DSA 硬件实现的整体架构如图 1 所示,自上而下划分为密码协议层、椭圆曲线点运算层、模运算层。本文采用了蒙哥马利阶算法实现标量运算模块,不仅适合在硬件上实现,同时也可以抵御简单功耗攻击,其具体过程如算法 2 所示[10]。同时,基于加法器实现了模运算中最重要的模乘运算,使得整个硬件设计更加地轻量化。

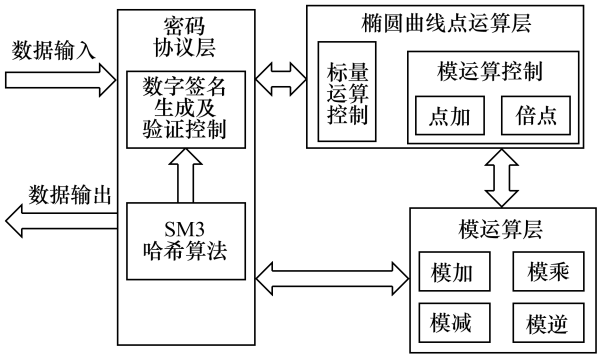

图 1　SM2-DSA 硬件架构

Fig. 1　SM2-DSA hardware architecture

2)算法 2:蒙哥马利阶算法

输入:椭圆曲线上的点 $P(x_P,y_P)$,标量值 $k=(k_{n-1},\cdots,k_1,k_0)$。

输出:$Q(x_Q,y_Q)=kP$。

1:计算 $Q_0=P,Q_1=2P$;

2:从 $i=n-2$ 到 $i=0$ 遍历 k_i;

2.1:如果 $k_i=1,Q_0=Q_0+Q_1,Q_1=2Q_1$;

2.2:否则,$Q_1=Q_0+Q_1,Q_0=2Q_0$;

3:遍历结束,输出 Q_0。

2　针对 SM2 数字签名算法的抗弱曲线故障攻击防御策略

2.1　弱曲线故障攻击 SM2 数字签名算法

攻击者在 SM2-DSA 执行签名生成时,向椭圆曲线参数 a 的坐标值注入一段连续随机故障。这使得算法 1 中的第 3 步标量运算落在一条弱椭圆曲线上,并导致算法输出一个错误签名对。攻击者再根据错误签名对和二次剩余定理得到弱椭圆曲线参数和标量运算结果 Q'的坐标,进而可以破解弱椭圆曲线上的 ECDLP,得到随机标量值 k'满足 $Q'=k'G'$。但 k'并不是签名过程使用的真实随机标量 k,二者的关系如式(5)所示。

$$k=k'+in',i=0,1,2,\cdots,\left[\frac{n}{n'}\right] \tag{5}$$

式中:n 为标准椭圆曲线上基点 G 的阶;n'为弱椭圆曲线上基点 G'的阶。

根据算法 1 第 6 步中签名 s 的生成公式,可以推导出私钥 d_A 的表达式,其如式(6)所示。显然,签名对(r,s)是已知的,所以只需要将式(5)代入表达式中,则可以求出私钥的所有可能值。通常 n 与 n'之间相差较小,所以私钥 d_A 的可能值个数也就很少。由于公钥 P_A 与私钥 d_A 之间满足关系:$P_A=d_AG$,则可以根据这个关系快速筛选出正确的私钥值。

$$d_A=(k-s)(r+s)^{-1}\bmod n \tag{6}$$

综上,通过上述方法就可以破解出签名私钥 d_A 的值。除了对参数 a 进行故障注入外,还可以对基点 G 的坐标值进行故障注入也可以得到相同的效果,具体的分析过程参见文献[6]。

2.2　基于点检测的防御策略

根据弱曲线故障攻击的攻击原理,遭受攻击后签名算法将在一条非标准椭圆曲线上运行,所以点检测是防御这种攻击最常用的手段。基于点检测思想,对 SM2-DSA 的签名过程进行改进,在签名对(r,s)输出前增加一步点检测操作。具体来说,由于公私钥对(P_A,d_A)是在标准椭圆曲线上预先生成的,所以正常情况下根据式(6)可以得到如下等式:

$$P_A==(k-s)(r+s)^{-1}G \tag{7}$$

如果等式(7)成立,说明签名对生成和公私钥对生成使用的是同一条标准椭圆曲线,即代表签名过程中未遭受弱曲线故障攻击,可以正常输出签名对。否则,就代表签名过程中遭受到攻击,算法将拒绝输出签名对。点检测-SM2-DSA 的详细过程如算法 3 所示。

算法 3:点检测-SM2 数字签名算法。

输入:素数域特征 p,椭圆曲线参数(a,b),基点 $G(x_G,y_G)$以及基点的阶 n,待签名信息 M,用户杂凑值 Z_A,签名私钥 d_A,签名公钥 P_A。

输出:签名对(r,s)。

1:$e=H_v(Z_A\parallel M)$;

2:选择一个随机整数 $k\in[1,n-1]$;

3:标量运算 $Q(x_1,y_1)=kG$;

4:计算 $r=e+x_1 \bmod n$。如果 $r=0$ 或 $r+k=n$,跳回第 2 步;

5:计算 $s=(1+d_A)^{-1}(k-rd_A)\bmod n$。如果 $s=0$,跳回第 2 步;

6:标量运算 $D=(k-s)(r+s)^{-1}G$;

7:判断 $D==P_A$ 是否成立:

7.1:如果成立,则正常输出签名对(r,s);

7.2:否则,清除签名对,拒绝输出;

8:结束签名。

从上述算法过程可以看出,基于点检测策略改进后的 SM2-DSA 相比于原版的算法,主要多出了一个标量运算操作。此外,算法最终是通过一个条件来判断是否正常输出签名对。而在实际的应用中,这样的判断操作很容易因为二次故障注

入而被跳过[7]。一旦跳过条件判断将使得签名对直接输出,就意味着点检测机制已经失效。

2.3　基于故障感染的防御策略

从 2.1 节中关于 SM2-DSA 的弱曲线故障攻击的描述中可以知道,虽然攻击没有直接针对私钥 d_A,但是通过破解 ECDLP 可以得到弱椭圆曲线上的随机标量值 k'。再利用 k'与签名中使用的真实随机标量值 k 之间的关系、真实随机标量值 k 与私钥 d_A 之间的关系,可以快速检索出正确私钥。基于故障感染思想,对原 SM2-DSA 进行改进,改进后的 SM2-DSA 遭受故障攻击后会在签名过程中不断的传播故障,最终将快速检索私钥 d_A 的建立条件破坏掉,从而使得攻击者即使破解出 k'的值也无法在有限的时间内检索出正确的私钥值。改进后的签名过程如算法 4 所示。

算法 4:故障感染-SM2 数字签名算法。

输入:素数域特征 p,椭圆曲线参数(a,b),基点 $G(x_G,y_G)$以及基点的阶 n,待签名信息 M,用户杂凑值 Z_A,签名私钥 d_A,签名公钥 P_A。

输出:签名对(r,s)。

1:$e=H_v(Z_A \parallel M)$;

2:选择一个随机整数 $k\in[1,n-1]$;

3:标量运算 $T(x_T,y_T)=kG+d_AG$;

4:计算 $D(x_D,y_D)=T-P_A$;

5:计算 $r=e+x_D \bmod n$。如果 $r=0$ 或 $r+k=n$,跳回第 2 步;

6:计算 $s=(1+d_A)^{-1}(k-rd_A) \bmod n$。如果 $s=0$,跳回第 2 步;

7:输出签名对(r,s)。

当算法正常运行时,签名过程中使用的椭圆曲线和生成公私钥对所使用的是同一条标准椭圆曲线。根据公私钥之间的关系,算法中的第 3、4 步相当于式(8)。将式(8)代替第 3、4 步,此时的签名过程与原版 SM2-DSA 的签名过程是一样的,输出的即为正确的签名对。

$$D(x_D,y_D)=kG+d_AG-d_AG=kG。\tag{8}$$

如果算法运行时遭受到弱曲线故障攻击,则算法 4 中第 3 步的标量运算就会在一条故障椭圆曲线上执行,这就意味着 T 和 P_A 不在同一椭圆曲线上。那么即使此时算法中的第 4 步在实际计算中依旧使用了式(2)和式(3)所示的运算法则,但最终的运算结果 $D'(x_{D'},y_{D'})$已经不是故障椭圆曲线上的点。如果攻击者想继续利用弱曲线的特性进行故障分析,那么就只能恢复故障曲线上的点 $T'(x_{T'},y_{T'})$的坐标,然后通过破解 ECDLP 找到满足 $T'(x_{T'},y_{T'})=k'_TG'$的随机标量值 k'_T。假设攻击者成功破解 ECDLP 并得到的 k'_T的值。但是由算法 4 中第 3 步的标量运算可知,k'_T与真实随机标量值 k、私钥 d_A 都有关系,具体表现如式(9)所示。其中 n'为故障椭圆曲线上基点 G'的阶,n 为标准椭圆曲线上基点 G 的阶,真实随机标量值 k 和私钥值 d_A 是两个未知的随机数。通过式(9)变换可以得到真实随机标量值的表达式 $k=k'_T+in'-d_A$,或是私钥的表达式 $d_A=k'_T+in'-k$。无论是计算真实随机标量值 k 还是私钥值 d_A,表达式的右边都有一个未知的随机数。在这种情况下,没有比穷举法更快的方式可以检索到唯一正确的随机标量值 k 或私钥值 d_A。目前签名中所使用的随机标量值 k 和私钥值 d_A 一般都是 256 bit 的大数,而想要通过穷举法在有限的时间内完成一次对某个 256 bit 未知数的检索,以目前的计算水平是无法做到的。并且从表达式来看,即使在最好的情况下(即表达式中 $i=0$ 时)也要进行一次检索。而在最坏的情况下,要进行 $2\left[\frac{n}{n'}\right]+1$ 次检索才能达到目的。所以基于故障感染策略改进后的 SM2-DSA,即使在遭受弱曲线故障攻击后故障曲线上的 ECDLP 被破解的情况下,攻击者也无法获取签名私钥 d_A。

$$k'_T+in'=k+d_A,i=0,1,2,3,\cdots,2\left[\frac{n}{n'}\right]。\tag{9}$$

实际上,算法 4 中第 3 步的两次标量运算可以合并为一次标量运算 $T(x_T,y_T)=(k+d_A)G$。即相比于原版的 SM2-DSA,基于故障感染策略改进后的 SM2-DSA 在签名过程中只多了一次点加运算。并且,相对于点检测策略容易因二次故障注入而跳过输出前的判断操作,最终造成防御失效来说,故障感染策略并没有这样明显的缺陷。

3　实验分析

本文中共设置了三组对比实验,包括无防御策略组、点检测防御组、故障感染防御组。每一组都使用 Verilog 硬件语言完成电路设计,然后用 Modelsim 工具进行电路功能仿真验证,最后基于 FPGA 芯片对三组电路进行综合实现和性能评估。整个实验都在 3.2 GHz、4 核 CPU 的个人电脑上进行。实验中所有 SM2-DSA 电路在进行仿真验证时都采用同一条官方推荐的 256 bit 标准椭圆曲线[11]。

硬件木马是攻击者在芯片设计或制造时植入的微小电路,当该电路在某种条件下被激活就会导致芯片功能发生改变或芯片的内部信息泄露[12]。基于这种特性,硬件木马可以很好和针对硬件的故障攻击相结合,基于故障攻击的硬件木马结构如图 2 所示。实验中设计的硬件木马激活后有两种状态,第一种状态下可以向椭圆曲线参数注入起始位置随机的、连续 L bit 的翻转故障,第二种状态下可以向椭圆曲线参数注入指定起始位置的、连续 L bit 的特定翻转故障(L=1、2、4、8、16)。通过在首次故障注入后再屏蔽签名输出前的判断操作来模拟点检测 SM2-DSA 电路上的二次故障注入,同时在故障感染 SM2-DSA 电路上采用首次故障注入后随机激活硬件木马,再注入一次故障来模拟二次故障注入。

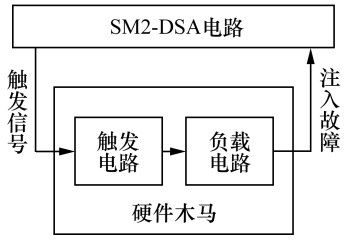

图 2　基于故障攻击的硬件木马示意图

Fig. 2　Schematic diagram of a hardware Trojan based on a fault attack

根据弱曲线故障攻击的攻击原理可知,并不是故障攻击后得到的每一条故障曲线都是弱椭圆曲线。只有当故障曲线上基点 $G'(x_{G'},y_{G'})$ 的阶 n' 具有一个较小的最大素因子 q 时,才能保证故障曲线上的 ECDLP 被成功破解。以当前的计算水平,当最大素因子 q 满足 $0.886\sqrt{q}<2^{100}$ 时,该椭圆曲线就可以被定义为弱椭圆曲线[13]。考虑到本实验中电脑的实际算力,先对无防御策略 SM2-DSA 电路进行多次故障注入模拟,然后恢复出故障曲线参数并对故障曲线上基点 $G'(x_{G'},y_{G'})$ 的阶 n' 进行分析,选取出满足最大素因子 q 的比特长度 $l_q<70$ 的故障曲线。将这些故障曲线对应的故障注入位置和翻转情况一一记录,然后根据所记录的情况,用硬件木马电路的第二种激活状态对点检测 SM2-DSA 电路和故障感染 SM2-DSA 电路注入特定故障,使得故障注入后的签名过程使用上述对应的 $l_q<70$ 的故障曲线。对三组电路进行的弱曲线故障攻击的情况如表 1 所示,其中 l_q 为故障攻击后得到故障曲线上基点的阶的最大素因子的比特长度,“-”代表在无防御策略的 SM2-DSA 电路上并未进行弱曲线故障注入与二次故障注入结合攻击的实验。从表 1 中可以看出,无任何防御策略的原始 SM2-DSA 电路易遭受弱曲线故障攻击威胁。虽然点检测 SM2-DSA 电路可以防御单次的弱曲线故障攻击,但如果攻击者通过二次故障注入跳过输出前的判断操作,则点检测 SM2-DSA 电路对弱曲线故障攻击的防御就会失效。而对于故障感染 SM2-DSA 电路,无论是单次的弱曲线故障攻击还是与二次故障注入结合的弱曲线故障攻击,都可以成功防御。

表 1　三组 SM2-DSA 电路上弱曲线故障攻击情况

Table 1　Weak curve fault attack on three sets of SM2-DSA circuits

l_q	弱曲线故障攻击			弱曲线故障攻击+二次故障注入攻击		
	无防御策略组	点检测防御组	故障感染防御组	无防御策略组	点检测防御组	故障感染防御组
46	攻击成功	攻击失败	攻击失败	-	攻击成功	攻击失败
52	攻击成功	攻击失败	攻击失败	-	攻击成功	攻击失败
53	攻击成功	攻击失败	攻击失败	-	攻击成功	攻击失败
56	攻击成功	攻击失败	攻击失败	-	攻击成功	攻击失败
59	攻击成功	攻击失败	攻击失败	-	攻击成功	攻击失败
61	攻击成功	攻击失败	攻击失败	-	攻击成功	攻击失败
63	攻击成功	攻击失败	攻击失败	-	攻击成功	攻击失败

实验最后在 Vivado 平台上基于 Xilinx Kintex-7 系列的 xc7k325 芯片对三组电路进行综合实现。设计点检测 SM2-DSA 电路时,将点检测操作中的标量运算和签名生成中的标量运算复用了同一个

标量运算器。从表 2 可以看出,相对于无防御策略的 SM2-DSA 电路,点检测 SM2-DSA 在面积开销上额外多出了 15.7% 的查找表(look-up table,LUT)和 13.1% 的触发器(flip-flop,FF),但在时间上点检测 SM2-DSA 电路却额外多出了 94.0% 的开销,而故障感染 SM2-DSA 在签名过程中只比原版算法多出了一个点加操作,所以硬件实现后,故障感染 SM2-DSA 电路在面积开销上比无防御策略的 SM2-DSA 电路额外多出了 7.4% 的 LUT 和 3.4% 的触发器,在时间上额外多出了 0.84% 的开销。

综上所述,基于故障感染的改良版 SM2-DSA 电路不仅可以防御弱曲线故障攻击,还可以防御弱曲线故障与二次故障注入的结合攻击。同时其在硬件的面积开销和时间开销上也比一般的点检测 SM2-DSA 电路表现地更出色。

表 2　本文三组 SM2-DSA 电路基于 FPGA 硬件实现的性能比较

Table 2　Performance comparison of three sets of SM2-DSA circuits based on FPGA hardware implementations

实验组	时钟频率/MHz	LUT	flip-flop	单次签名生成时间/ms
无防御策略组	100	20 232	8 039	3.418
点检测防御组	100	23 419	9 093	6.631
故障感染防御组	100	21 728	8 313	3.447

4　结　论

本文针对 SM2-DSA 算法提出了一个基于故障感染思想的抗弱曲线故障攻击的防御策略,根据该防御策略对 SM2-DSA 硬件电路进行改进,并在改进后的电路上模拟故障注入攻击仿真实验。仿真结果表明,基于故障感染的策略可以同时抵御弱曲线故障攻击和二次故障注入攻击。此外,基于故障感染策略的电路和基于一般点检测策略的电路、无防御策略的电路一同在 Kintex-7 FPGA 上进行性能分析,分析结果表明,故障感染防御策略不仅在硬件额外面积开销上比一般点检测策略少了大约一半,在单次签名生成时间上也只增加了 0.84%,远低于点检测策略增加的 94.0%。

参考文献:

[1] 程朝辉. 数字签名技术概览[J]. 信息安全与通信保密,2020(7):48-62.

[2] 孙荣燕,蔡昌曙,等. 国密 SM2 数字签名算法与 ECDSA 算法对比分析研究[J]. 网络安全技术与应用,2013(2):60-62.

[3] RUSSON A. Differential fault attack on montgomery ladder and in the presence of scalar Randomization[C]//Progress in Cryptology-INDOCRYPT 2021:22nd International Conference on Cryptology in India. Jaipur,India:Springer International Publishing,2021:287-310.

[4] CAO W Q,SHI H S,CHEN H,et al. Lattice-based weak curve fault attack on ECDSA[C]//ICT Systems Security and Privacy Protection:36th IFIP TC 11 International Conference,SEC 2021. Cham,Switzerland:Springer International Publishing,2021:146-161.

[5] TAKAHASHI A,TIBOUCHI M. Degenerate fault attacks on elliptic curve parameters in OpenSSL[C]//2019 IEEE European Symposium on Security and Privacy (Euro S & P). Stockholm,Sweden:IEEE,2019:371-386.

[6] QIAN C S,WANG Y,WANG M H,et al. Security analysis of SM2 signature algorithm based on fault attack[C]//Second International Symposium on Computer Technology and Information Science (ISCTIS 2022). Guilin,China:SPIE,2022,12474:1247402.

[7] 张宇. 基于 ECDSA 的故障攻击研究[D]. 西安:西安电子科技大学,2014:29-34.

[8] 喻潇. 抗旁路攻击的双域 ECC 标量乘电路研究与设计[D]. 南京:南京航空航天大学,2020:58-60.

[9] CAO W Q,FENG J Y,ZHU S F,et al. Practical lattice-based fault attack and countermeasure on SM2 signature algorithm[C]//Information and Communications Security:17th International Conference,ICICS 2015. Beijing,China:Springer International Publishing,2016:62-70.

[10] CHAKRABORTY A,BHATTACHARYA S,DIXIT T H,et al. Template attack on SPA and FA resistant implementation of montgomery ladder[J]. IET information security,2016,10(5):245-251.

[11] IT security techniques. Digital signatures with appendix Part 3:Discrete logarithm based mechanisms:ISO/IEC 14888-3:2006[S]. Geneva,Switzerland:ISO (International Organization for Standardization),2018:155.

[12] 黄钊,王泉,杨鹏飞. 硬件木马:关键问题研究进展及新动向[J]. 计算机学报,2019,42(5):993-1017.

[13] MARTÍNEZ V G,GONZALEZ-MANIANO L,MUÑOZ A M,et al. Secure elliptic curves in cryptogrophy[J]. Computer and network security essentials,2018(1):283-298.