

密码算法功耗分析仿真平台 操作手册



武汉大学
WUHAN UNIVERSITY

目录

一、CPA-XX 攻击:	1
1.激活攻击界面	1
2.攻击界面设置	8
3.攻击参数设置	12
二、文件合并	17
三、加密和解密:	23
1.激活攻击界面	23
2.加解密设置	23
附: 攻击步骤	26
1.No-Count 和 Pipeline	26
2.Random	26
3.Mask	27

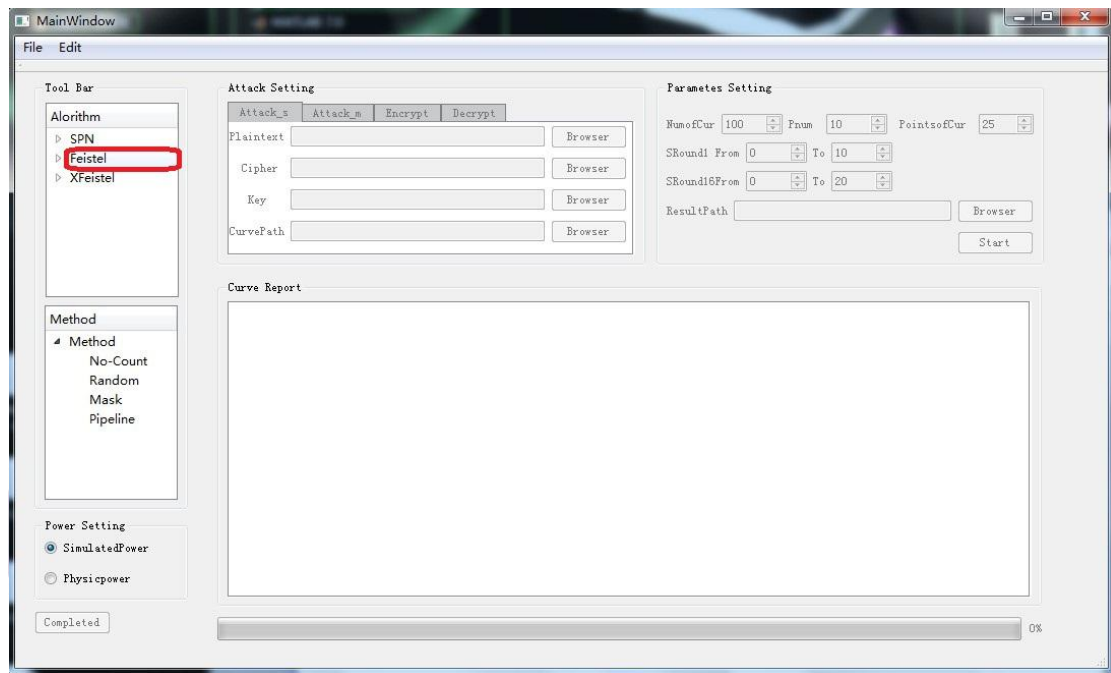


武汉大学
WUHAN UNIVERSITY

一、CPA-XX 攻击:

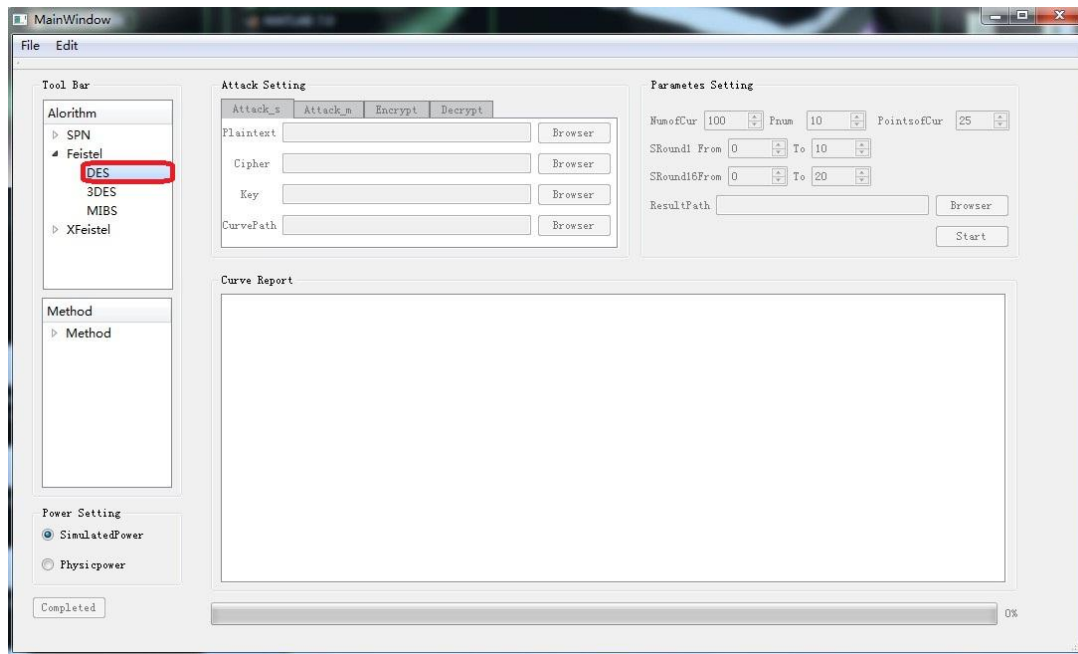
1.激活攻击界面

(1)选择攻击的算法结构，例如单击 **Feistel**



有三种算法结构，SPN、Feistel、XFeistel。

(2)选择攻击的算法，例如双击 DES

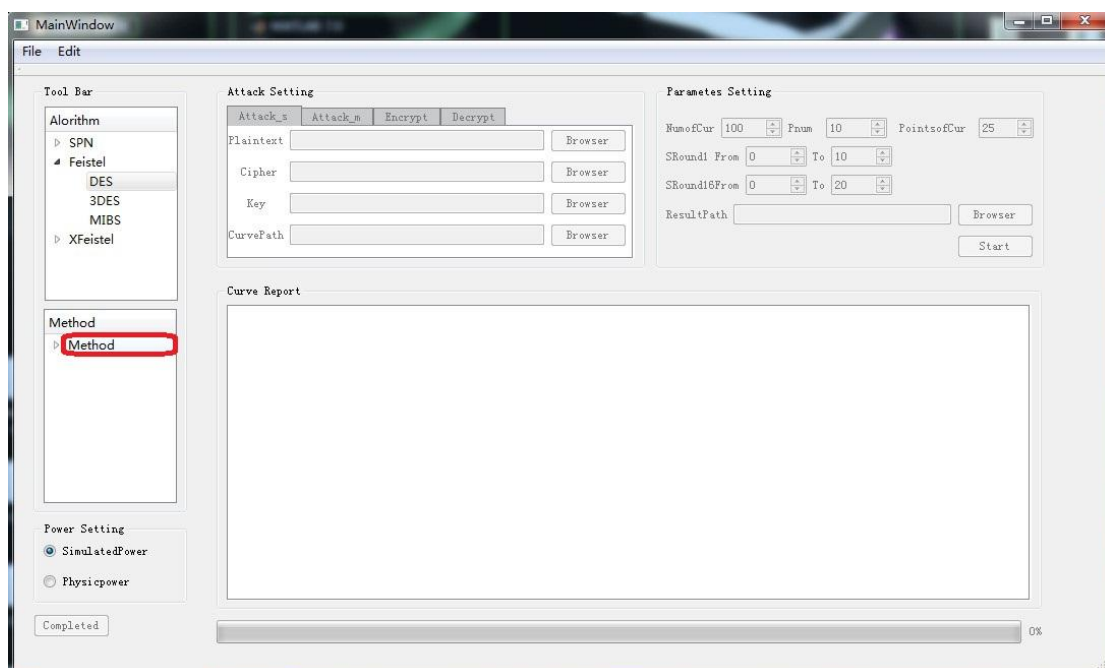


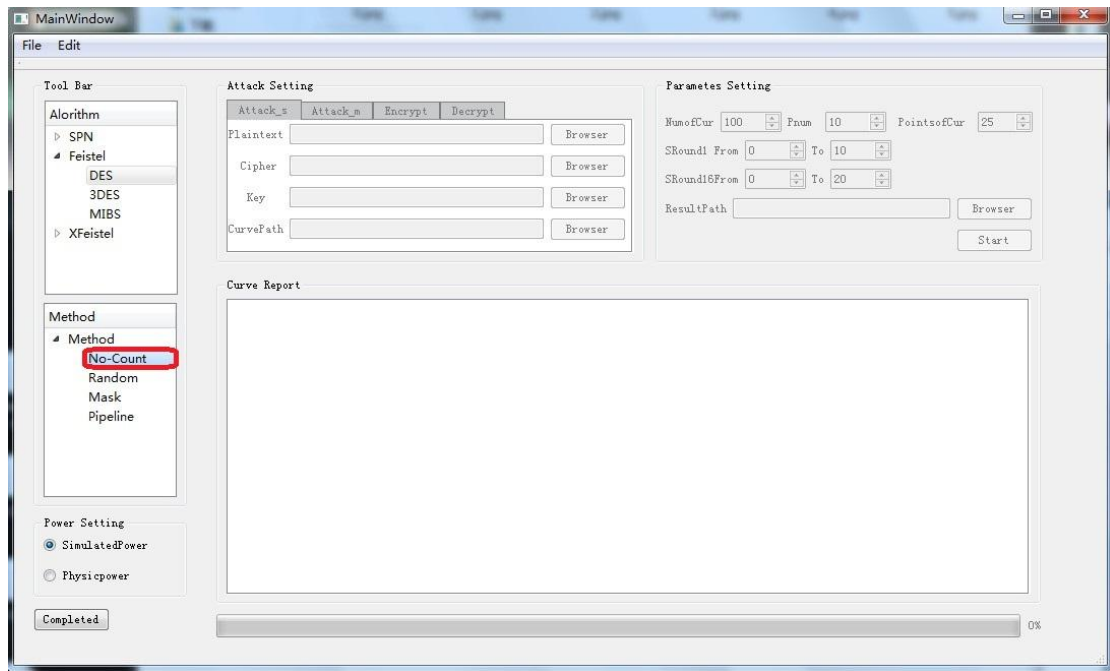
SPN 结构的算法包括 AES 和 Print。

Feistel 结构的算法包括 DES, 3DES 和 MIBS。

XFeistel 结构的算法包括 SMS4。

(3)选择攻击方法，单击 Method，双击对抗方法

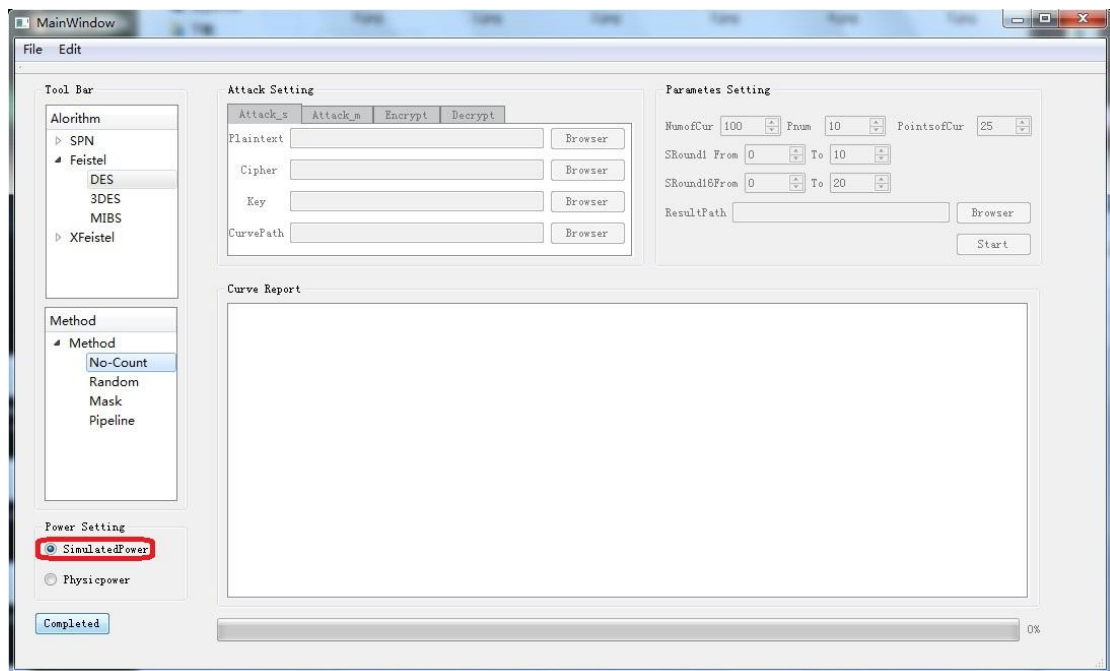




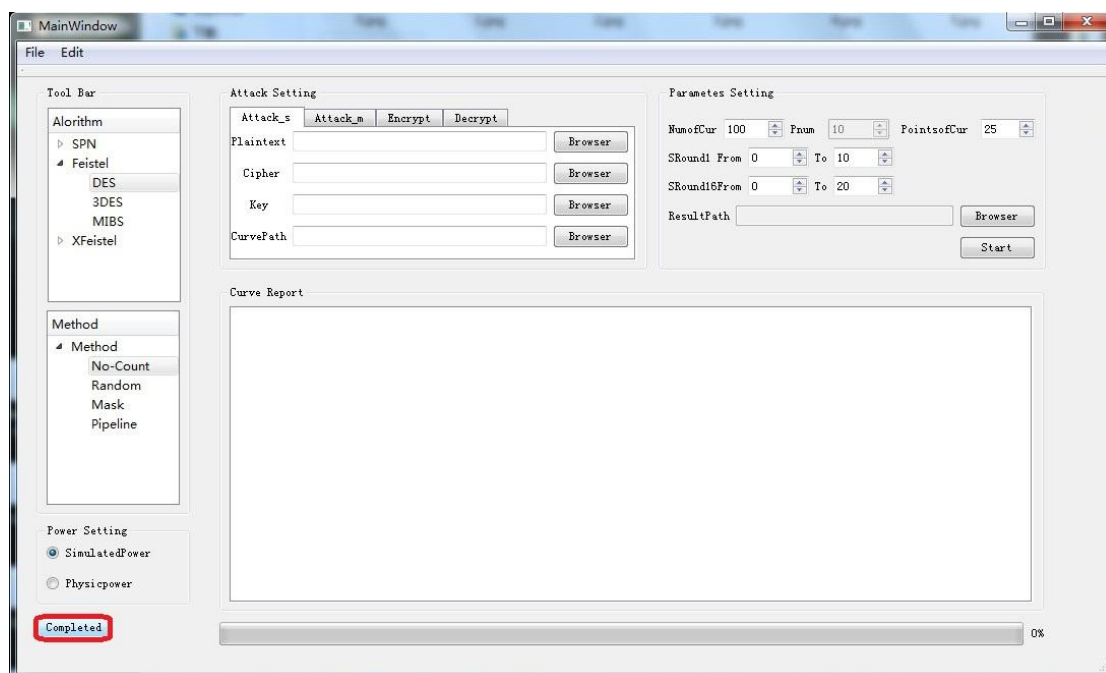
攻击方法为 CPA，对抗方法包括 No-Count(无对抗),Random(随机时间片),Mask(掩码),Pipeline(流水)



(4)选择功耗设置，仿真功耗或实采功耗



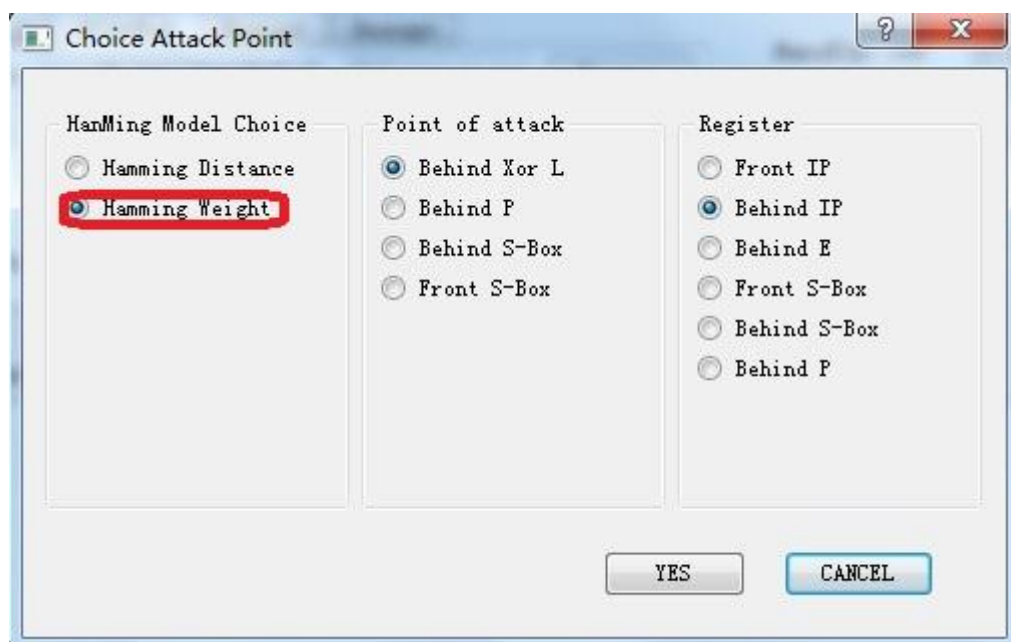
(5)单击 **Completed** 进入攻击点设置



(6)攻击点设置

若对抗方法选择的是 No-Count, Random 或 Pipeline 则需要选择能量模型和攻击点，例如单击 **Hamming Weight**。若为 Mask 则跳过步骤

(6)直接进行步骤(7)。



①能量模型包括汉明距离模型和汉明重量模型。

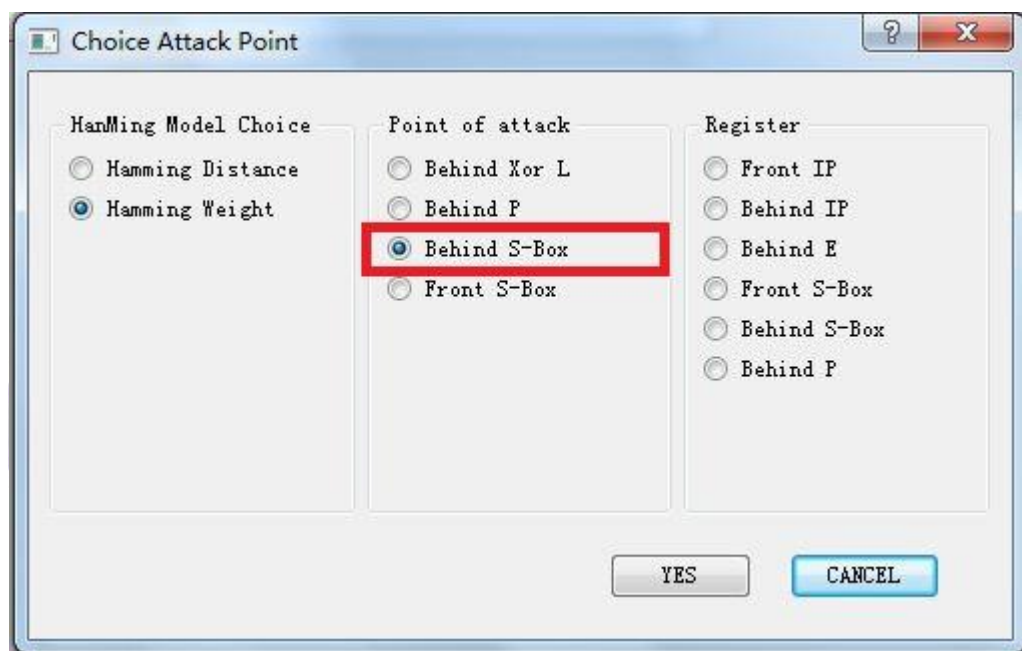
②选择攻击点，例如单击 Behind S-Box

Behind Xor L:异或输出

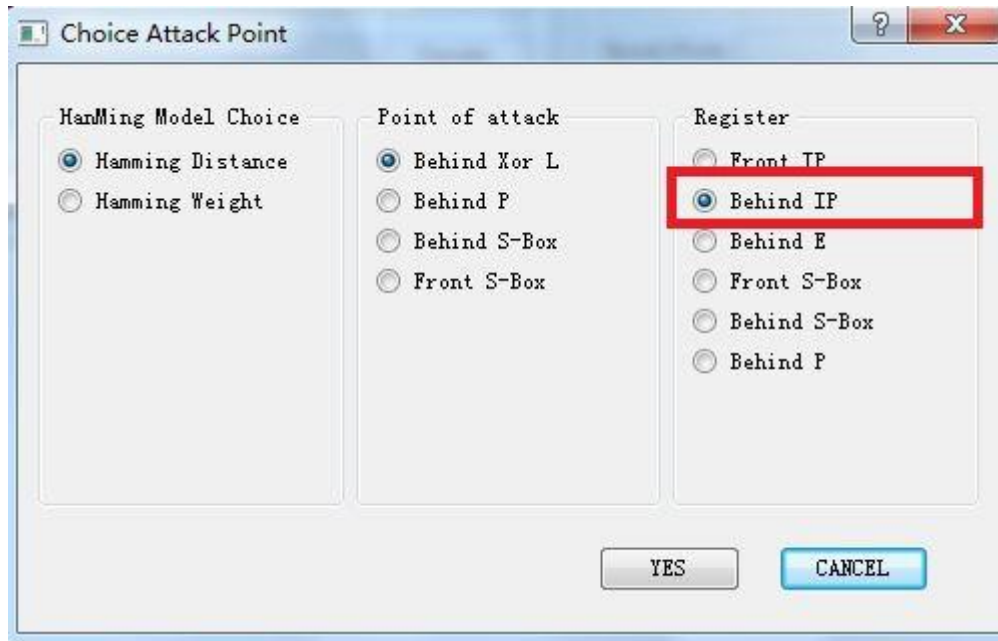
Behind P:P 置换输出

Behind S-Box:S-Box 输入

Front S-Box:S-Box 输出



③若选择汉明距离模型还需设置 Register。由于汉明距离模型是用攻击点状态和其之前的一个状态异或，所以 Register 中存储的状态应设置在攻击点之后。



Front IP: IP 置换输入

Behind IP: IP 置换输出

Behind E: E 扩展输入

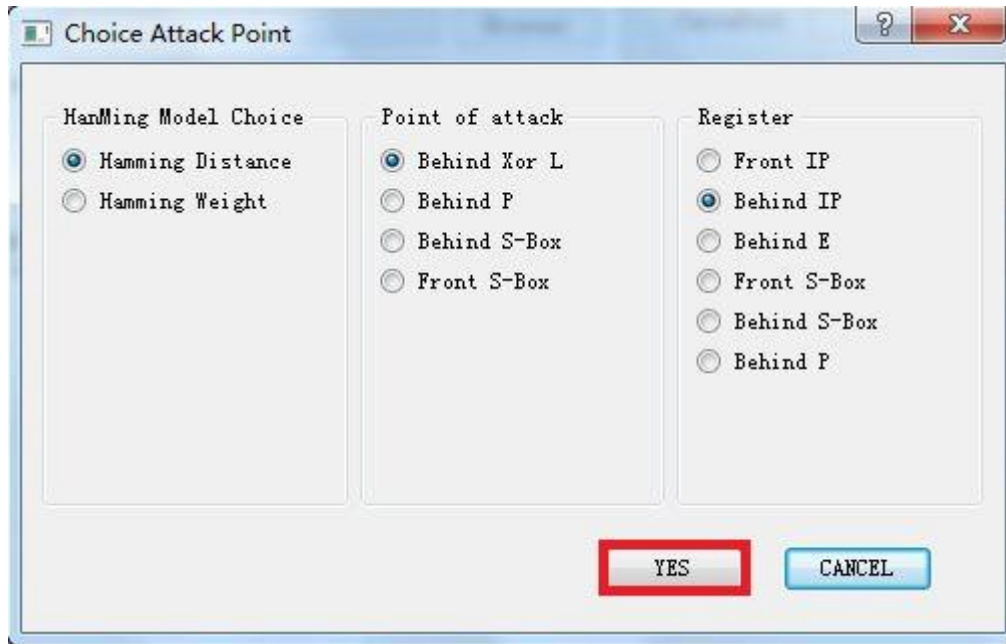
Behind E: E 扩展输出

Front S-Box: S-Box 输入

Behind S-Box: S-Box 输出

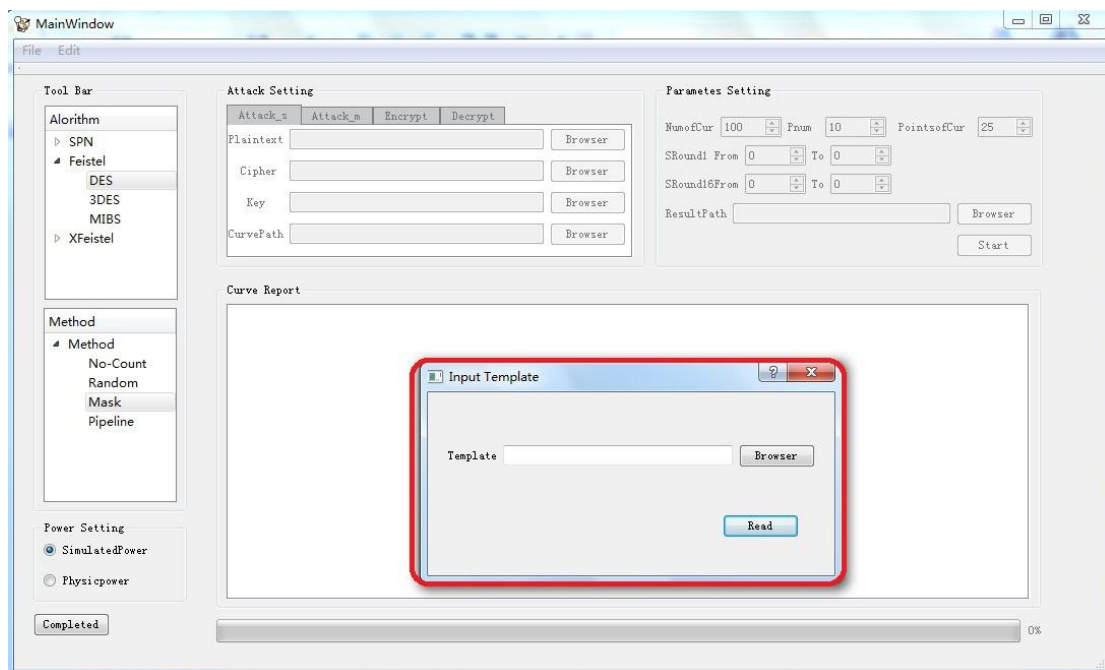
Behind P: P 置换输出

④单击 YES 后进行第 8 步 Attack Setting。

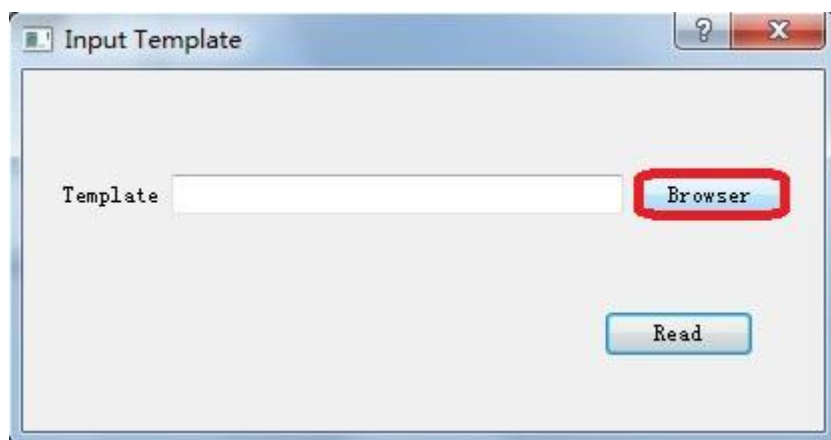


若使用默认设置则无需进行上述操作，直接跳过上述步骤单击 YES。

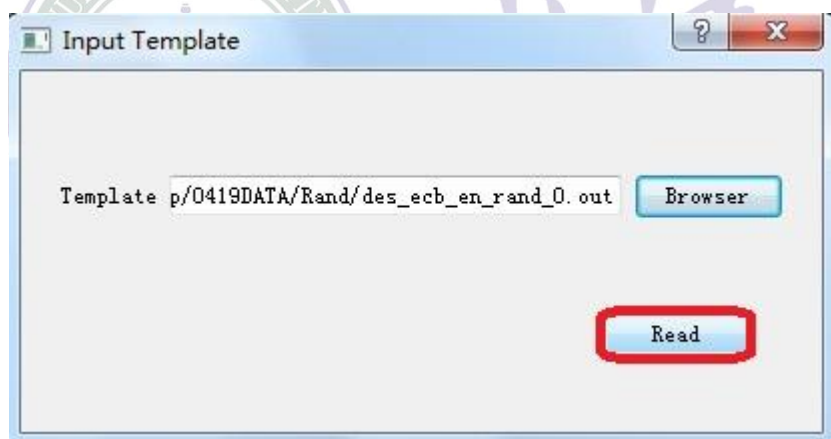
(7)若 Method 选择的是 Mask，由于 Mask 采用的是模板攻击，所有不需要设置能量模型和攻击点但要读入模板文件。若为其它方法则跳过步骤(7)至步骤(8)。



①单击 **Browser** 按钮选择模板文件路径

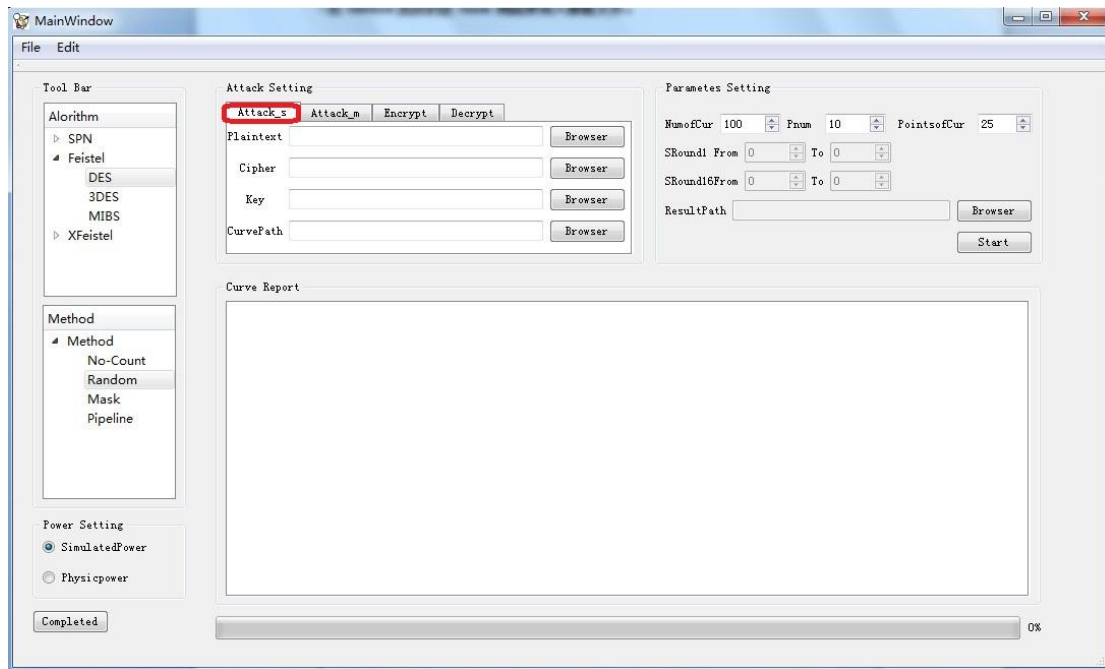


②单击 **Read** 按钮读入模板文件



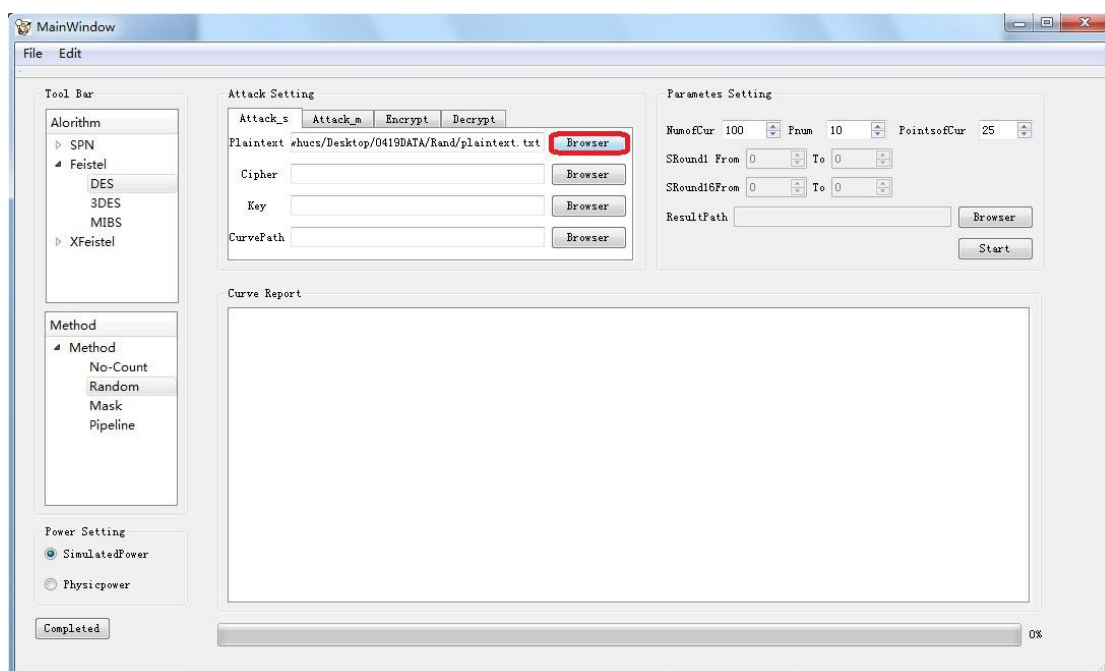
2.攻击界面设置

(1)进行攻击设置，若功耗文件为单个文件则选 **Attack_s**，若为多个文件则选 **Attack_m**

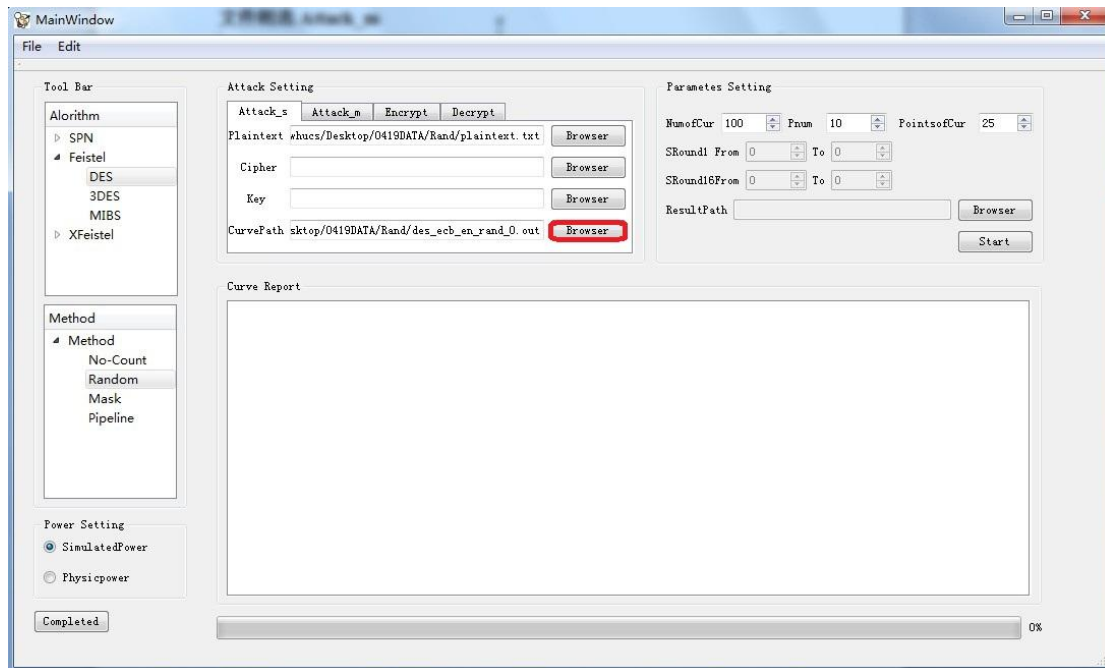


Attack_s 使用单个功耗文件攻击 ,Attack_m 多个功耗文攻击(且功耗文件的标号前必须有下列划线才行, 如 des_ecb_en_ran_0),CurvePath 必选 Plaintext 和 Cipher 二者至少选一个 若选 Plaintext 则攻第一轮, 若选 Cipher 则攻第十六轮,若同时选则同时攻第一轮和第十六轮 Key 可选, 若选择可将攻击结果进行验证

(2)选择明文路径

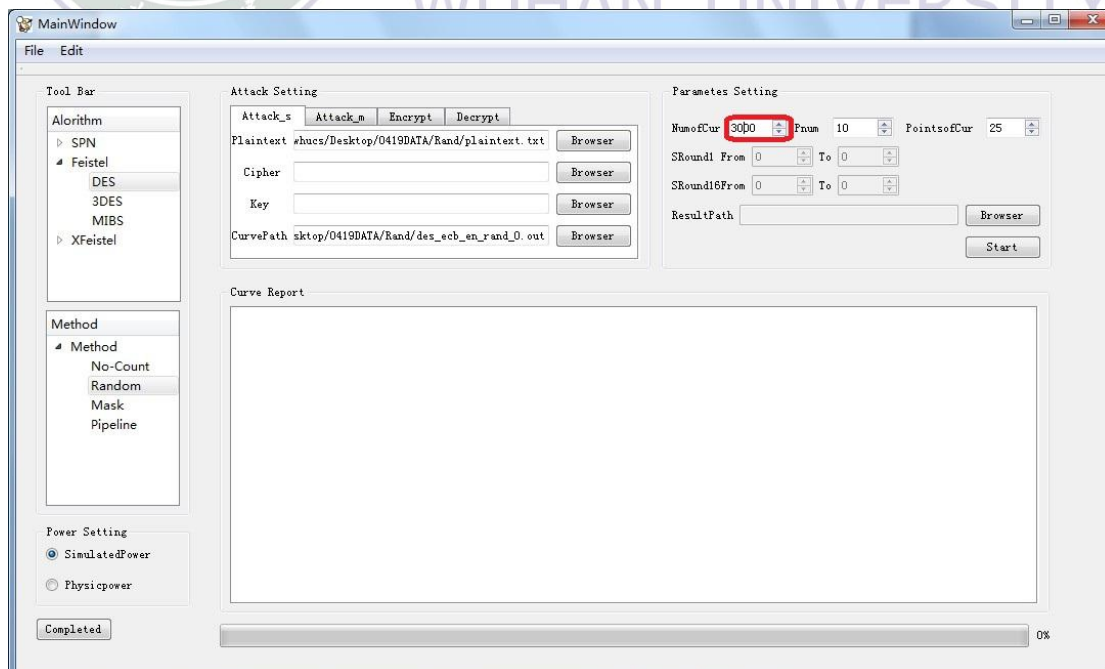


(3)选择密钥路径

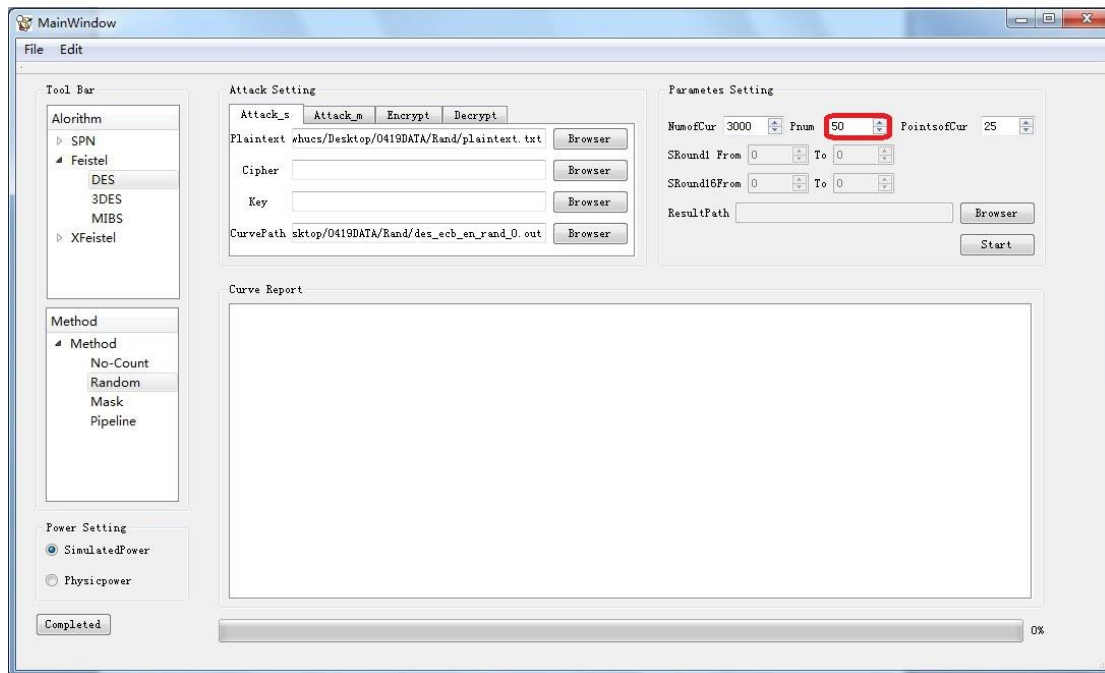


3.攻击参数设置

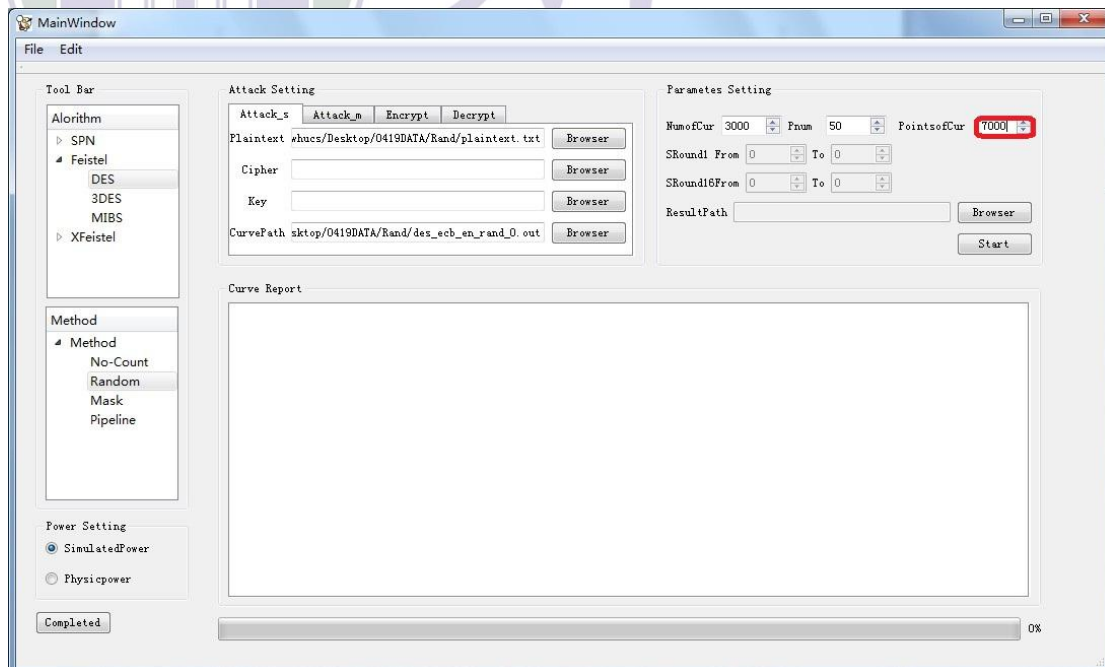
(1)设置功耗曲线条数 Num of Cur



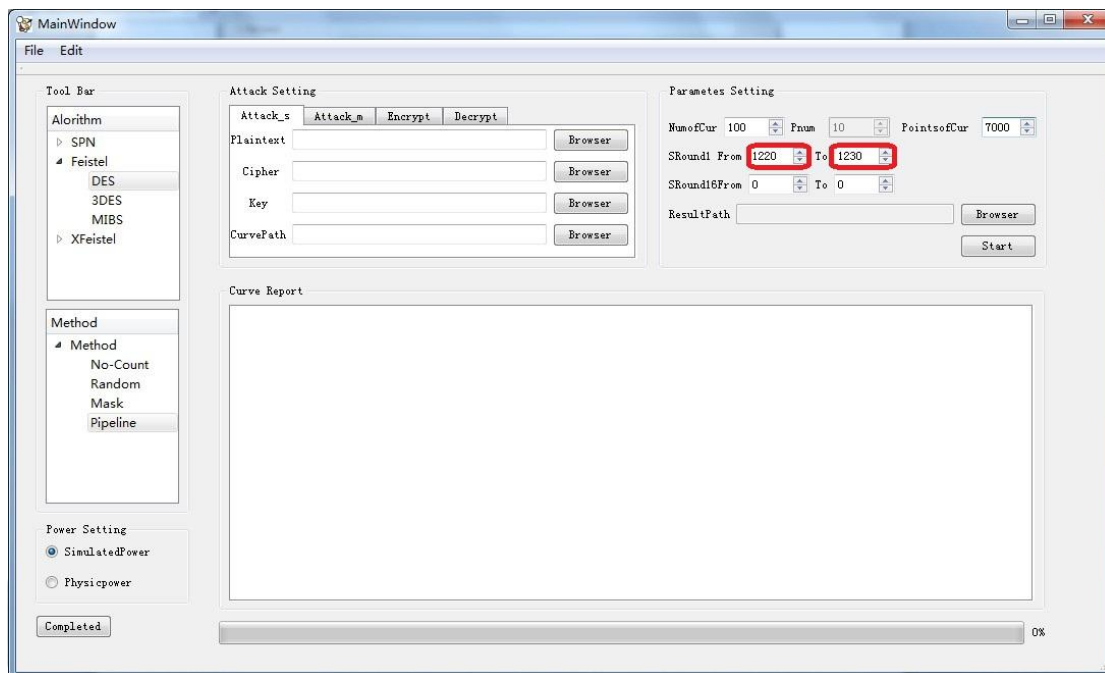
(2)选择每个周期采集的点数 Pnum



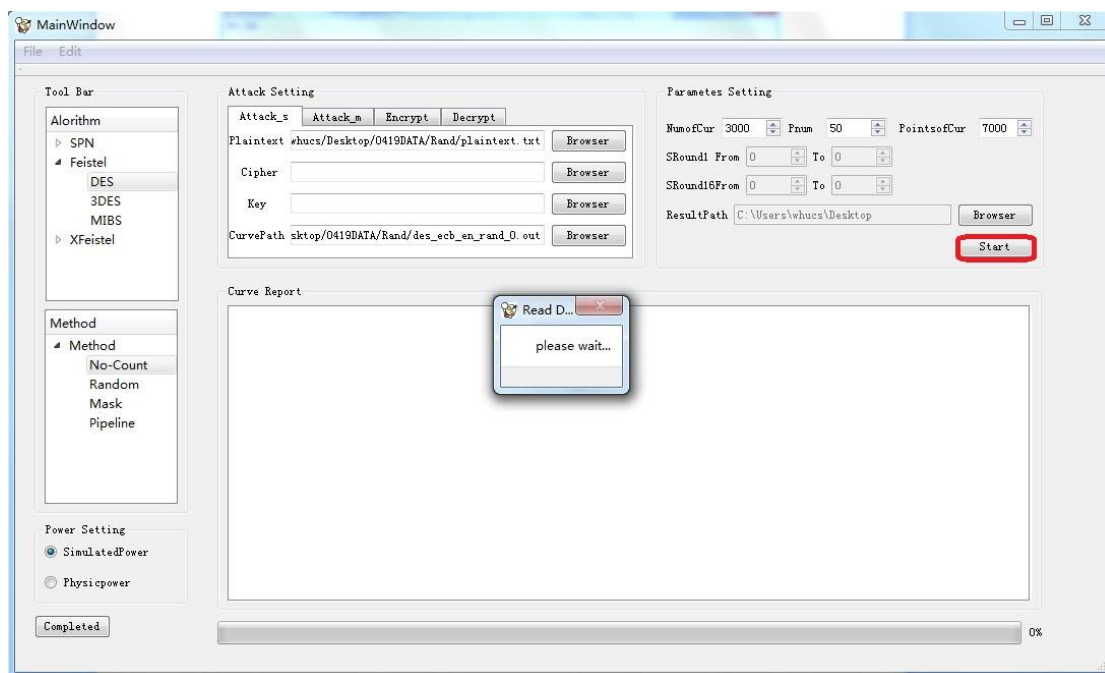
(3)设置每条功耗曲线的点数 Points of Cur



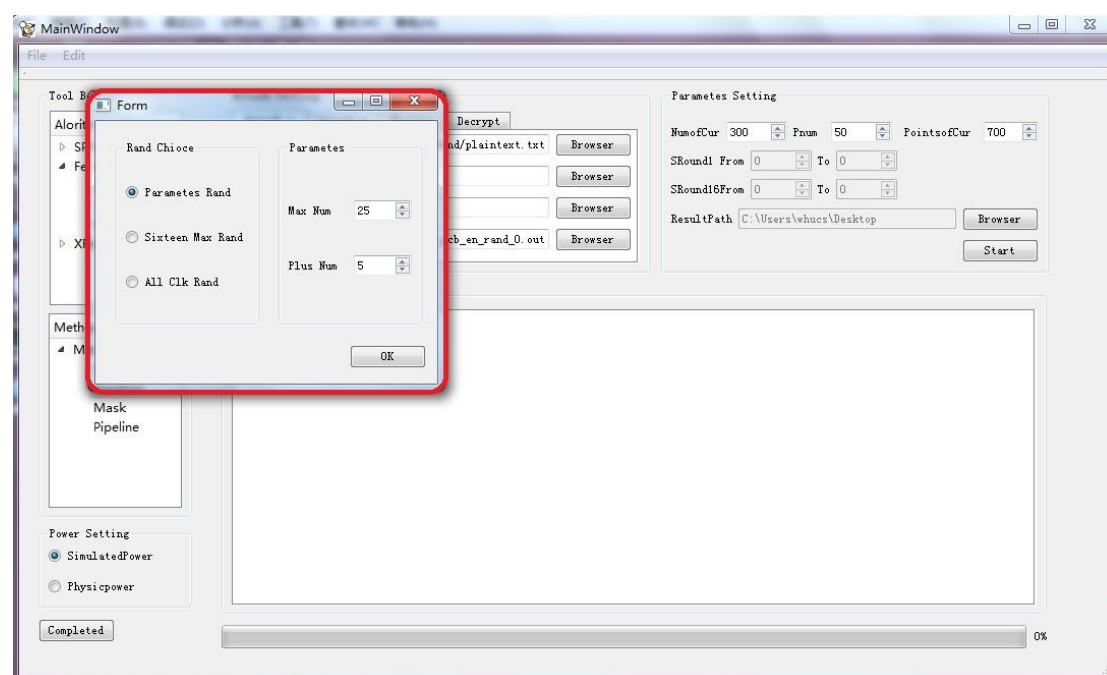
(4)若已知攻击点在功耗曲线中对应的位置，则可设置 **SRound1**
From、**To** 和 **SRound16From**、**To** 的值以减少攻击时间，**To** 值应小于 **Points of Cur**，否则无须设置。



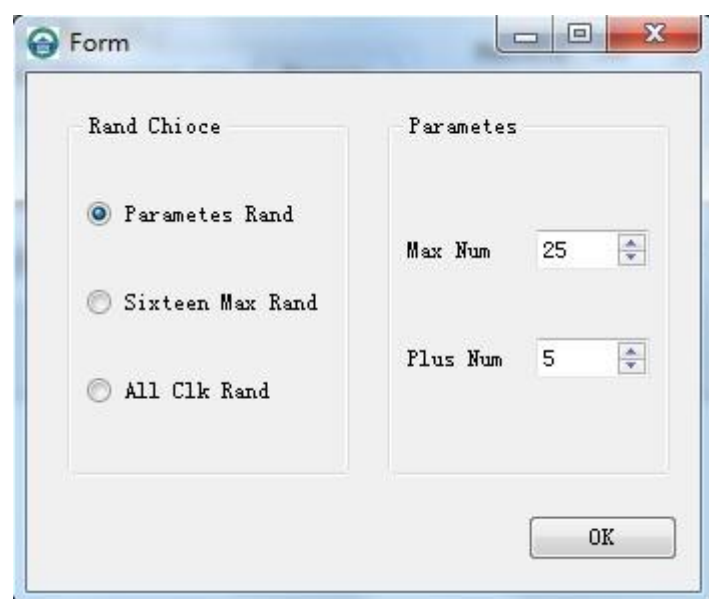
(5)单击 **Start** 开始攻击



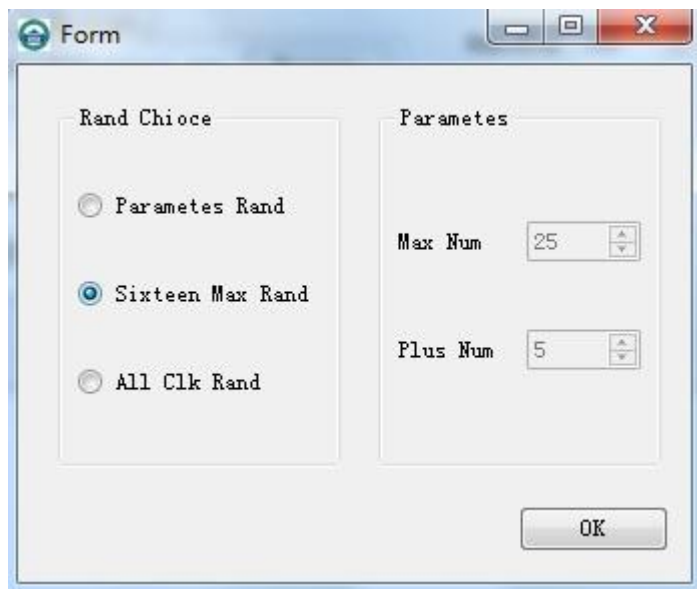
若 Method 选择的为 Random 单击 Start 后会弹出一个参数设置框



①Parametes Rand 需要设置右边的 Parametes, Max Num 设置选取的峰值的数量, Plus Num 设置多少个相邻峰值相加, 这两个值的设置依赖于数据。

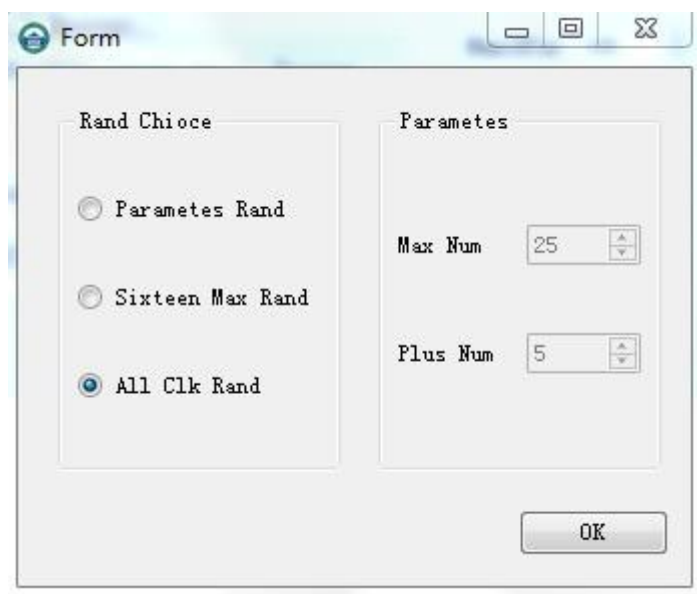


②Sixteen Max Rand 不需要设置右边的 Parametes，仅在所有功耗值中取前 16 个最大峰值依次作为第一轮到第十六轮的峰值。



The screenshot shows a Windows-style dialog box titled "Form". It has two main sections: "Rand Chioce" on the left and "Parametes" on the right. In the "Rand Chioce" section, there are three radio buttons: "Parameters Rand", "Sixteen Max Rand" (which is selected), and "All Clk Rand". In the "Parametes" section, there are two numeric input fields: "Max Num" with the value 25 and "Plus Num" with the value 5. An "OK" button is located at the bottom right of the dialog box.

③All Clk Rand 不需要设置右边的 Parametes，仅仅将所有时钟周期内的 power 相加。

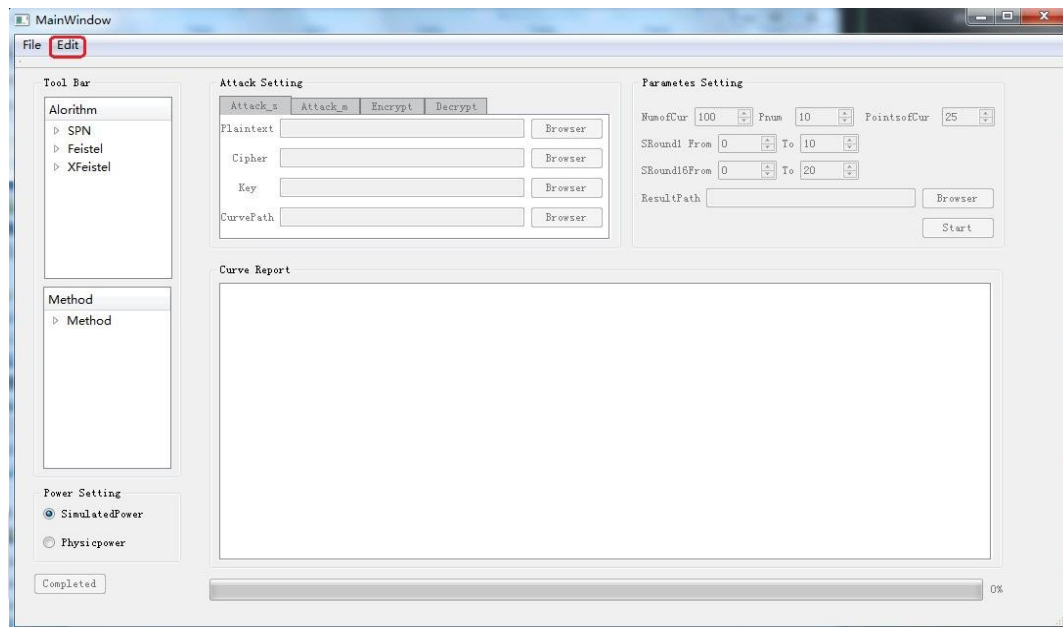


This screenshot is identical to the one above, showing the "Form" dialog box. However, in this instance, the "All Clk Rand" radio button in the "Rand Chioce" section is selected, while "Parameters Rand" and "Sixteen Max Rand" are unselected. The "Parametes" section remains unchanged with "Max Num" set to 25 and "Plus Num" set to 5. The "OK" button is still at the bottom right.

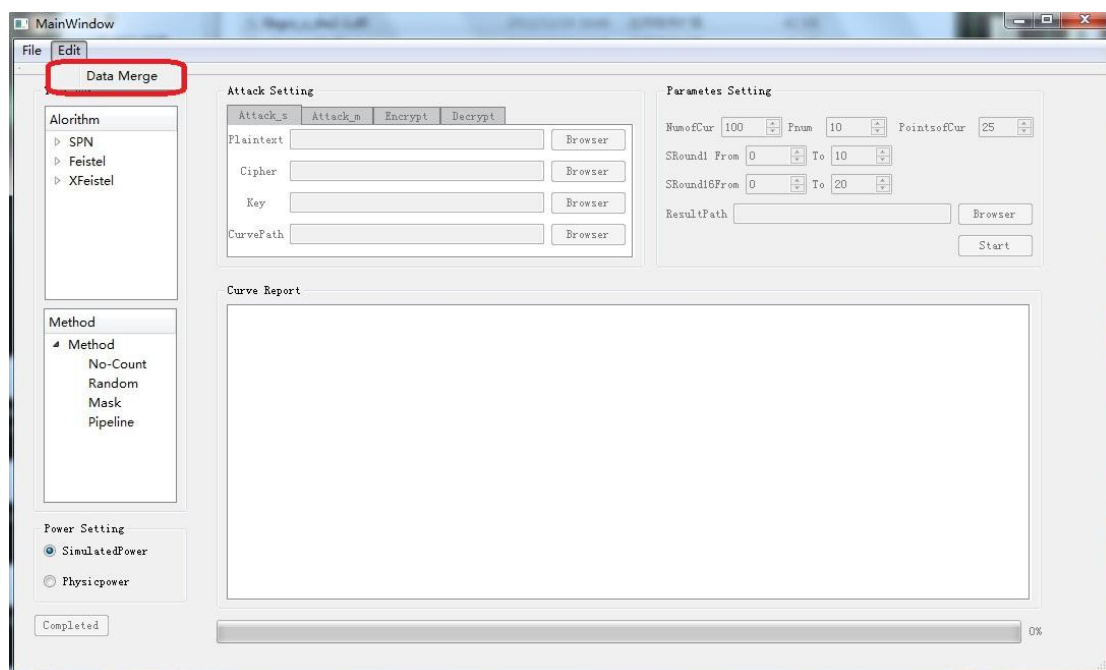
二、文件合并:

由于只有 random 有 multi 的功耗文件，所以本功能只针对 random。

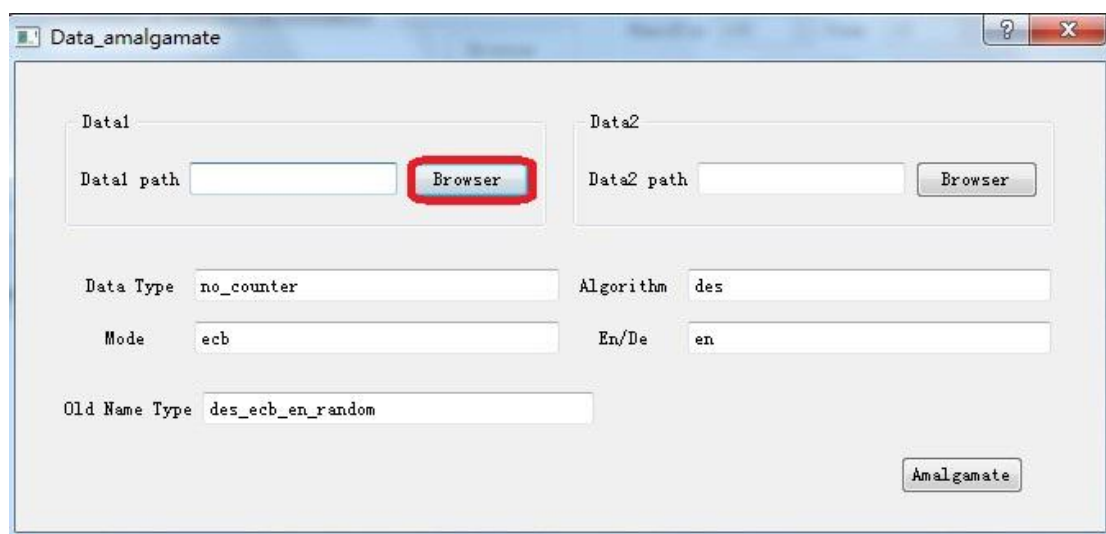
1.单击菜单栏的 Edit



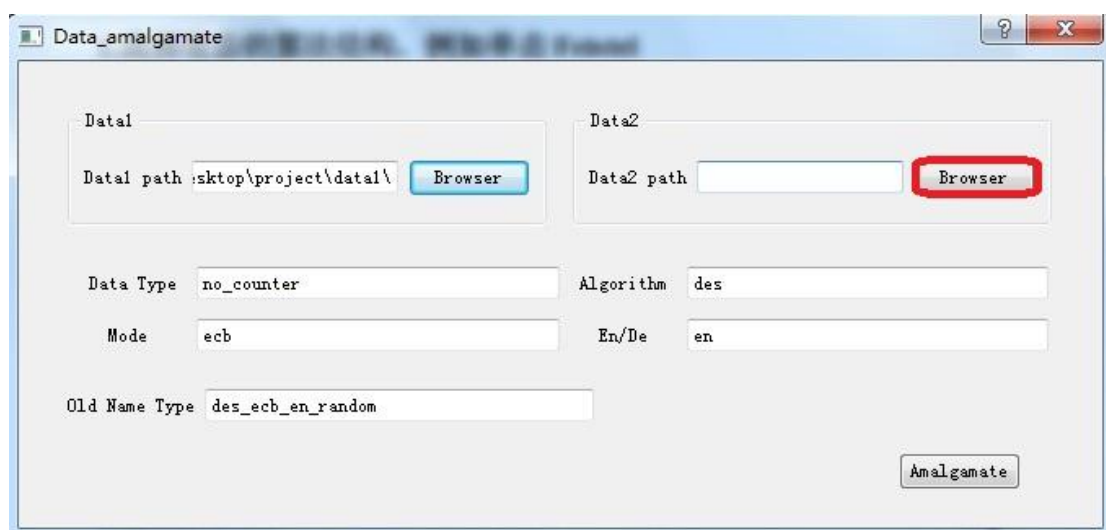
2.单击 Data Merge



3.单击 **Browser**，选择第一组功耗文件目录



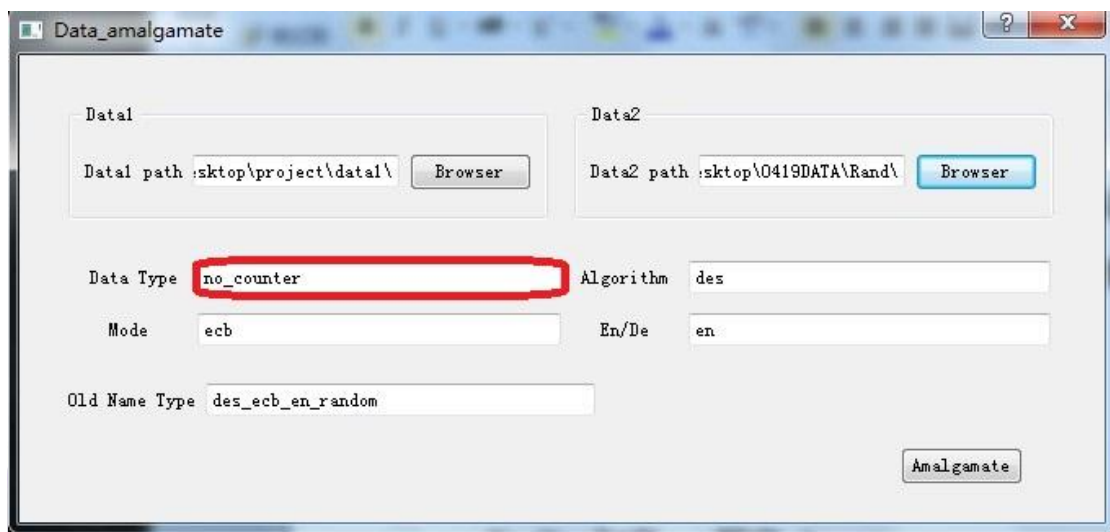
4.单击 **Browser**，选择第二组功耗文件目录，该目录中的文件夹不能为空白文件夹。若 **Data1 path** 的文件夹为空，则将 **Data2 path** 中的功耗文件重命名后存于 **Data1 path**;若 **Data1 path** 的文件夹不为空，则将 **Data2 path** 中的功耗文件重命名后追加于 **Data1 path** 中的功耗文件后。



5.在文本框中填写功耗文件名前缀，只能用英文和下划线。

合并后的功耗文件命名格式为：

Algorithm_Mode_En/DE_Data Type_编号.out

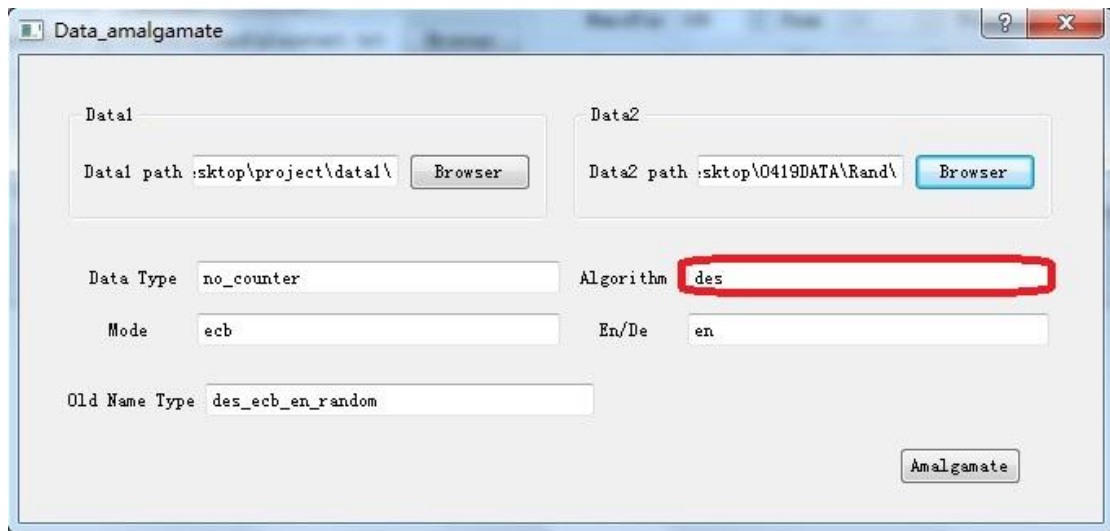


Data Type(对抗方式)命名规则：

- ①若无对抗 no_counter
- ②若为随机时延则填入 ran
- ③若为掩码则填入 mask
- ④若为流水则填入 pipeline

Algorithm:算法

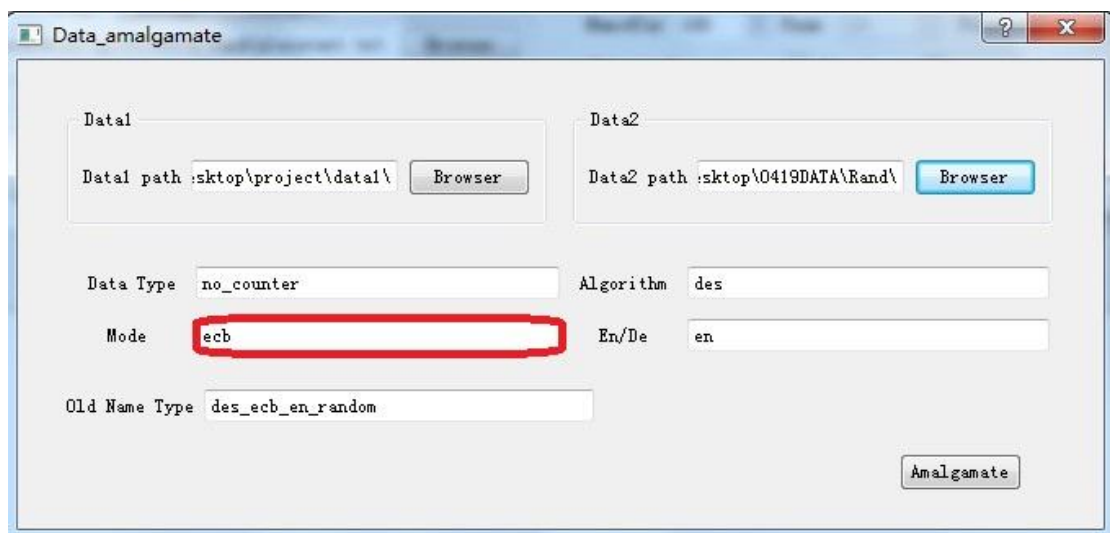
包括 des,3des,mibs,aes,print,sms4



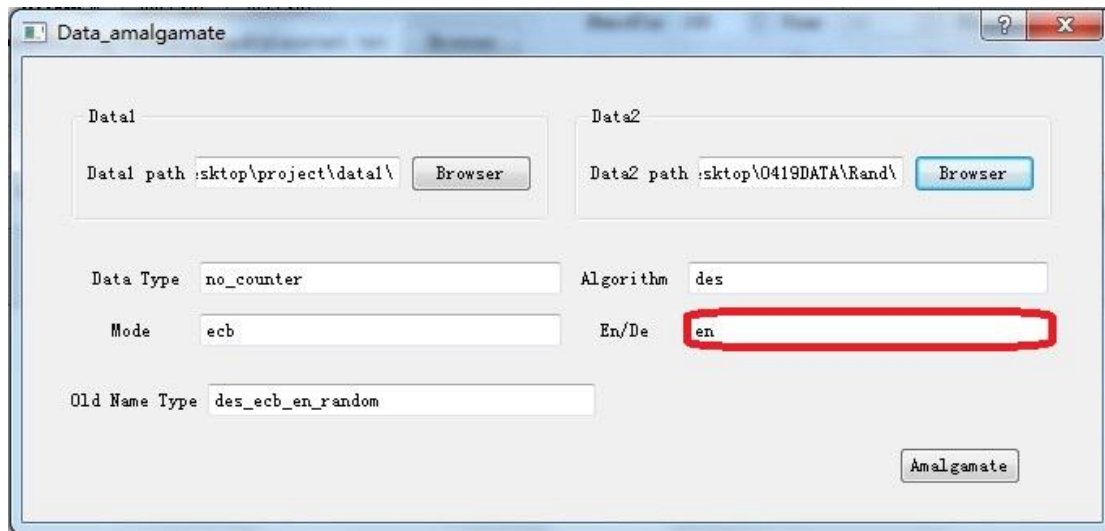
Mode:模式

DES 有四种工作模式:

- ①ecb 表示电子密码本模式
- ②cbc 表示加密分组链接模式
- ③cfb 表示加密反馈模式
- ④ofb 表示输出反馈模式。

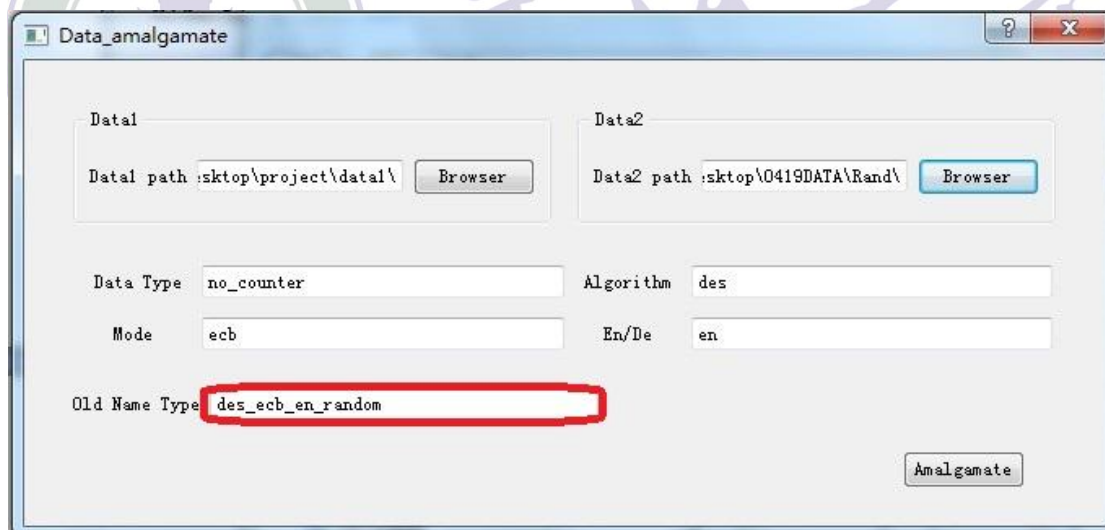


En/De:加密填入 **en**，解密填入 **de**。

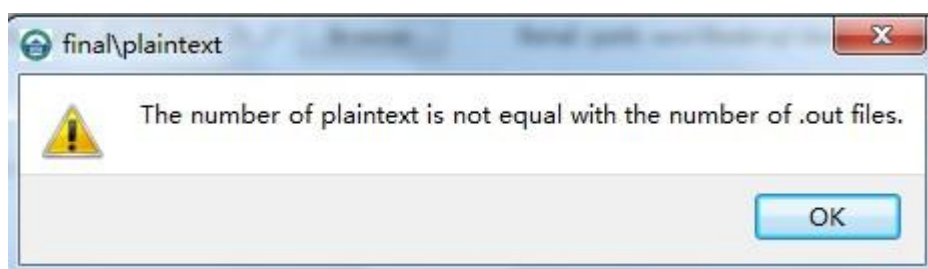


Old Name Type:填入 **Data2 path** 中功耗文件名除编号外的旧前缀名。

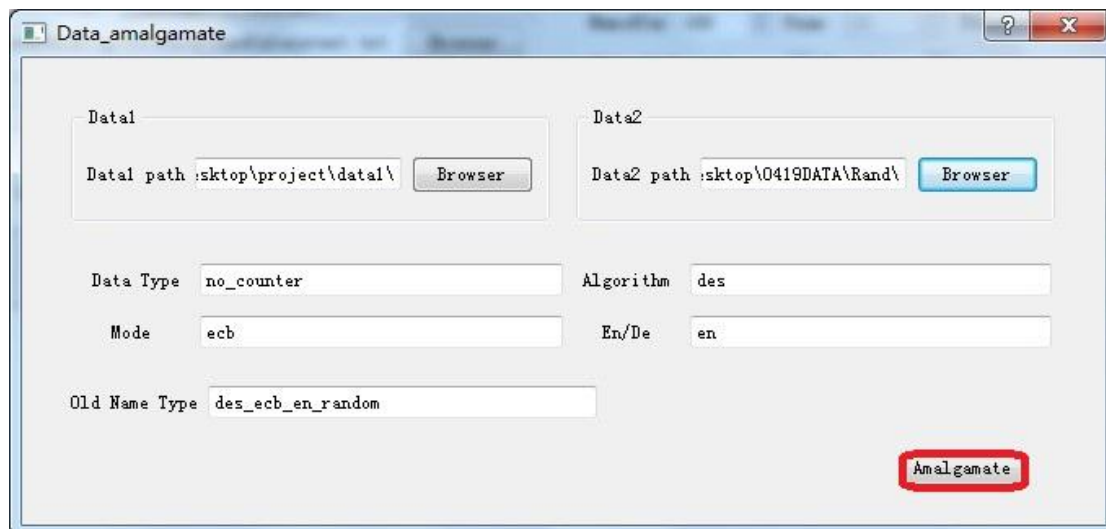
如 **Data2 path** 中文件名为 **des_ecb_en_random1.out** 时，填入 **des_ecb_en_random**。



功耗文件夹需有明文或密文文件，且明文或密文条数必须和功耗曲线条数相等，否则会有警告



6. 单击 Amalgamate 进行合并



例:

① Data1 path 中 50 个功耗文件, des_ecb_en_ran_0...des_ecb_en_ran_49
Data2 path 中 100 个功耗文件, des_ecb_en_random0...des_ecb_en_random99
Data Type: ran, Algorithm: des, Mode: ebc, En/De: en, Old Name Type:
des_ecb_en_random
合并后 150 个重命名的功耗文件存于 Data1 path 中, 先存放的是原 Data1 path 中的功耗文件, 存放顺序为:
des_ecb_en_ran_0...des_ecb_en_ran_49, des_ecb_en_ran_50...des_ecb_en_ran_149

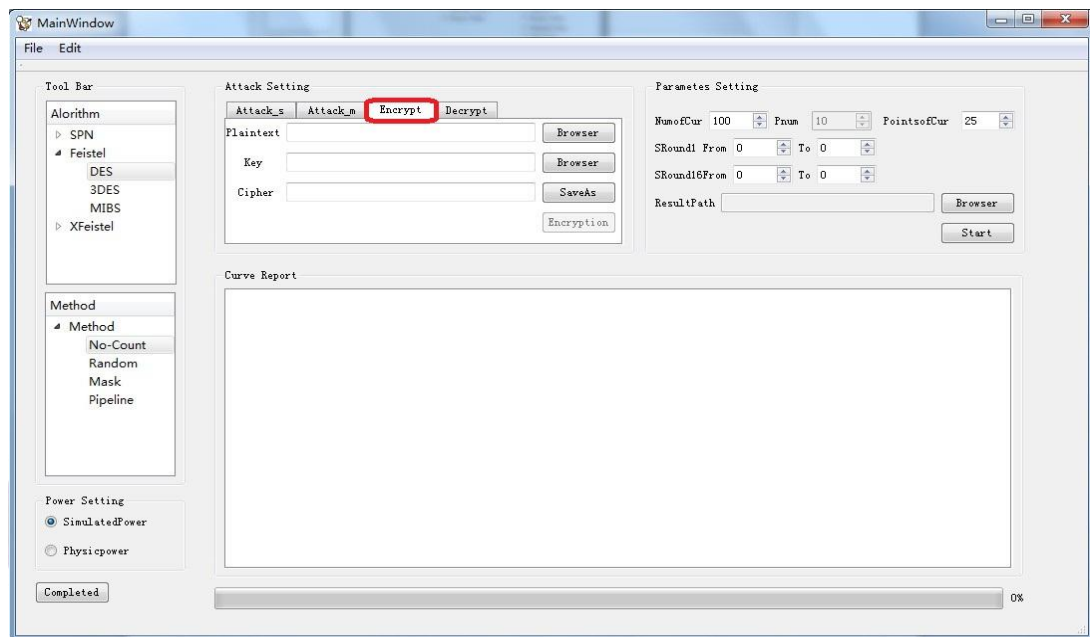
② Data1 path 为空文件夹
Data2 path 中 100 个功耗, des_ecb_en_random0...des_ecb_en_random99
Data Type: ran, Algorithm: des, Mode: ebc, En/De: en, Old Name Type:
des_ecb_en_random
合并后 100 个重命名的功耗文件存于 Data1 path 中, 存放顺序为:
des_ecb_en_ran_0...des_ecb_en_ran_99

三、加密和解密：

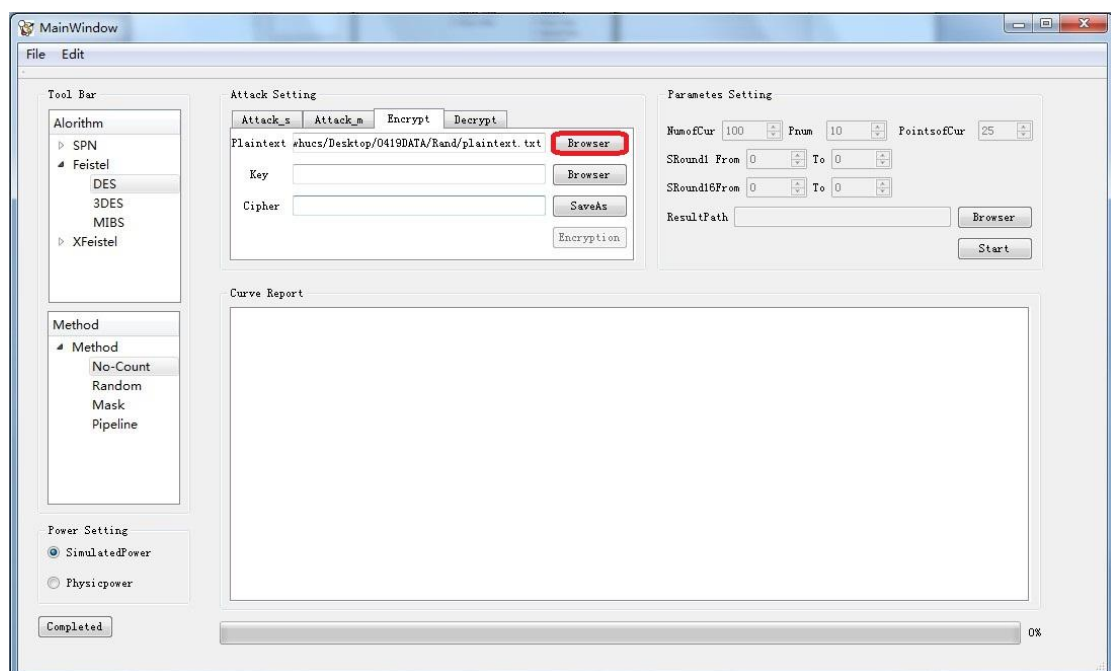
1.激活攻击界面，可参照第二部分的操作

2.加解密设置

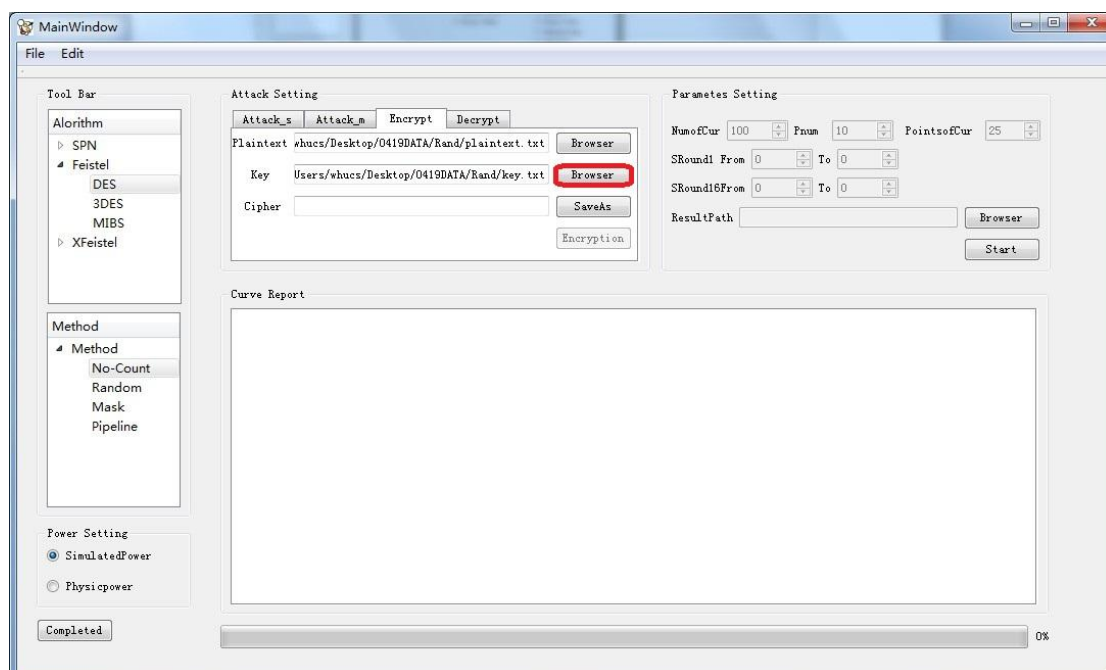
(1)加密单击 **Encrypt**，解密单击 **Decrypt**



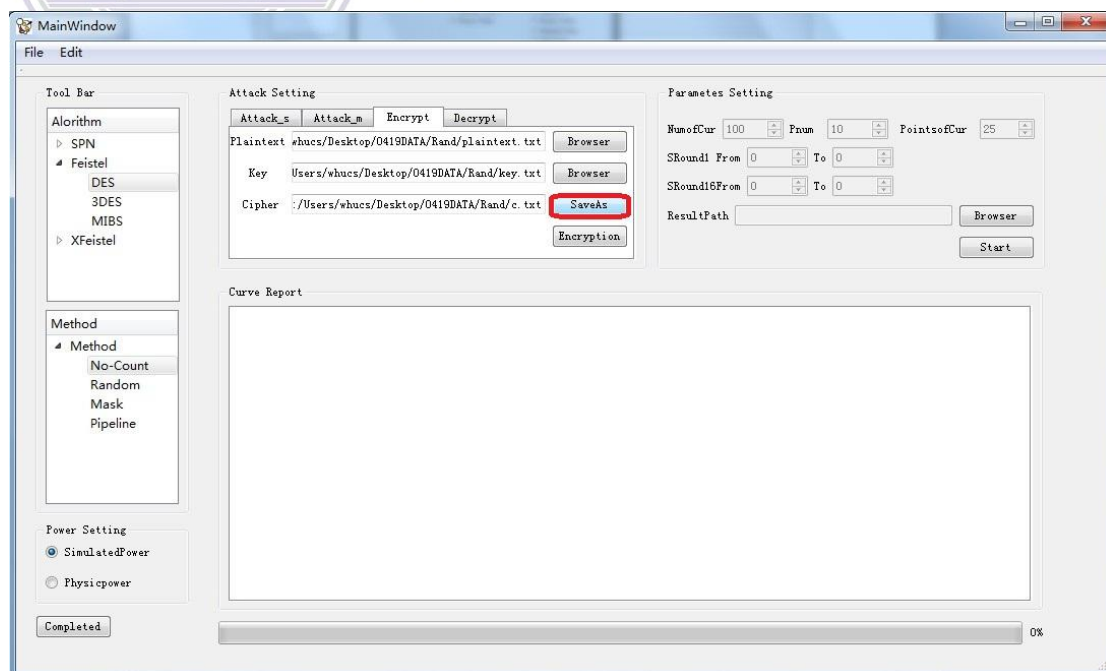
(2)加密选择明文路径，解密选择明文路径



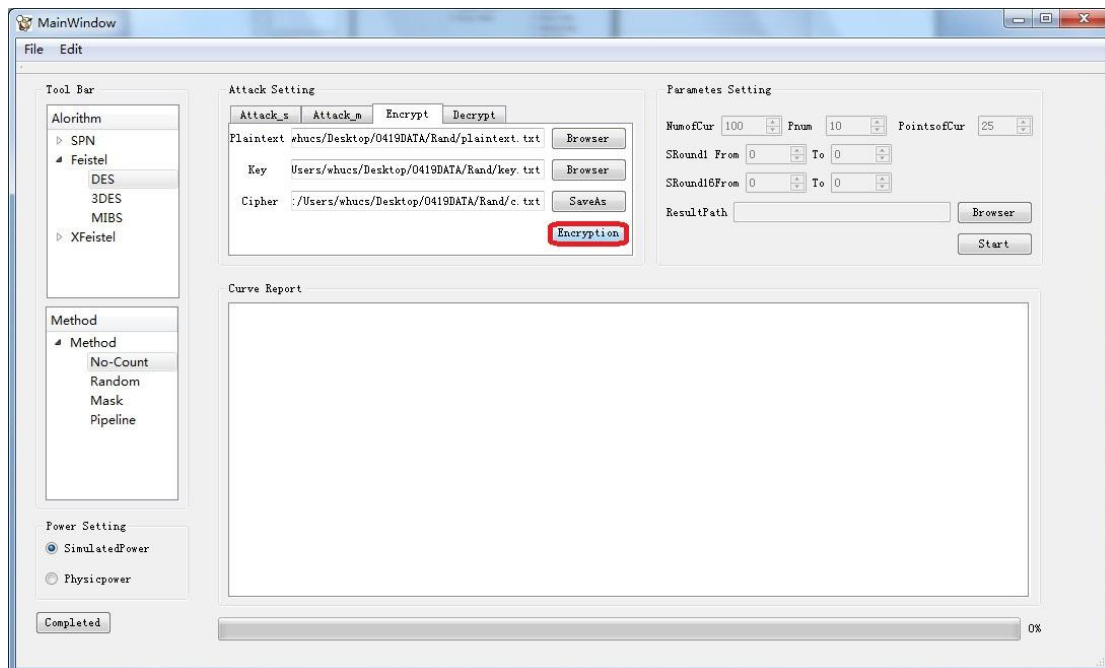
(3)选择密钥路径



(4)选择密文或明文保存路径



(5)单击 **Encryption** 进行加密，解密则单击 **Decryption**



武汉大学
WUHAN UNIVERSITY

附：攻击步骤

1.No-Count 和 Pipeline

(1)激活攻击界面

- ①选择密码算法结构
- ②选择密码算法
- ③选择攻击方法
- ④选择功耗设置
- ⑤单击 Completed

(2)攻击设置

- ①单击 Attack_s
- ②选择明文或密文、密钥和功耗文件路径

(3)参数设置

- ①设置 NumofCur
- ②设置 Pnum
- ③设置 PointsofCur
- ④设置 SRound1 From 、To，SRound16 From、To，可略过该步

(4)单击 Start 开始攻击

2.Random

- (1)若功耗文件为多个文件且功耗文件名中的编号前无下划线，则需要

进行重命名，参照第三部分的文件合并，否则跳过该步。

(2)激活攻击界面，参照 No-Count 和 Pipeline 相应步骤

(3)攻击设置

①若功耗文件为单个文件单击 Attack_s，若为多个文件单击 Attack_m

②选择明文或密文、密钥和功耗文件路径

(4)参数设置，参照 No-Count 和 Pipeline 相应步骤

(5)单击 Start 开始攻击

3.Mask

(1)激活攻击界面，参照 No-Count 和 Pipeline 相应步骤

(2)读入功耗模板，参照 二(7) 中的操作

(3)攻击设置，参照 No-Count 和 Pipeline 相应步骤

(4)参数设置，参照 No-Count 和 Pipeline 相应步骤

(5)单击 Start 开始攻击



武汉大学

WUHAN UNIVERSITY