文章编号:2095-6134(2015)05-0695-06

基于 Nand Flash 物理特性的签名私钥产生方法及其应用*

贾世杰[1,2,3], 夏鲁宁[1,2†], 闻 楠[4]

(1 中国科学院数据与通信保护研究教育中心, 北京 100093; 2 中国科学院信息工程研究所, 北京 10093;
3 中国科学院大学, 北京 100049; 4 北京江南天安科技有限公司, 北京 100083)

(2014 年 8 月 29 日收稿; 2015 年 1 月 14 日收修改稿)

Jia S J, Xia L N, Wen N. Signature private key generation method based on the physical properties of Nand Flash and its applications[J]. Journal of University of Chinese Academy of Sciences, 2015,32(5):695-700.

摘 要 Nand Flash 是消费类电子设备常用的非易失性存储器件. 利用 Nand Flash 芯片生产过程中所确定的物理特性,能够提取每芯片唯一的数字指纹信息. 本文基于这种特性提出利用 Nand Flash 芯片的数字指纹产生 SM2 签名私钥的方法. 这种方法提取的 SM2 签名私钥与 Nand Flash 器件具有可验证的紧耦合特征. 本方法与具体的数字签名算法无关,可以应用在任何需要对存储器件或电子设备本身进行基于数字签名的身份鉴别的场合之中.

关键词 Nand Flash; SM2; 随机数; 数字签名

中图分类号:TP309 **文献标志码**:A **doi**:10.7523/j.issn.2095-6134.2015.05.017

Signature private key generation method based on the physical properties of Nand Flash and its applications

JIA Shijie[1,2,3], XIA Luning[1,2], WEN Nan[4]

(1 *Data Assurance and Communication Security Center, Chinese Academy of Sciences, Beijing* 100093, *China*;
2 *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*;
3 *University of Chinese Academy of Sciences, Beijing* 100049, *China*;
4 *Beijing Jiang Nan Tian An Technology Company, LTD, Beijing* 100083, *China*)

Abstract More and more consumer electronic devices are equipped with Nand Flash as nonvolatile memory device. Unique digital fingerprint information can be extracted from each Nand Flash chip by using the physical properties of Nand Flash, which are determined in the production process. We propose a new method, based on the physical properties of Nand Flash, to produce private keys for SM2 signature scheme, which is verifiably tight coupled to the Nand Flash device. Notably, this method is irrelevant to the specific digital signature schemes, and it is applicable to any occasion where digital signature scheme is used for identification of the storage devices or electronic devices.

Key words Nand Flash; SM2; random number; digital signature

* 国家科技支撑计划(2013BAH15F03)资助

† 通信作者,E-mail:xialuning@iie.ac.cn

Nand Flash 是一种非易失性(在断电情况下仍能保存信息)的存储器件,已经广泛地应用于各种消费类电子产品中. 智能手机、数码相机等所使用的 SD 卡、TF 卡,日常所用的 U 盘,以及逐渐普及的固态硬盘等都是以 Nand Flash 作为存储器件的数据存储装置.

在特定安全需求下,需要对存储器件或电子设备本身进行身份鉴别,以确定器件或设备的真实性. 例如现在电子病历成为医疗纠纷案件的焦点,需要基于电子签名来构建电子病历的可信生态环境,为避免电子病历受到患方的质疑,需对存储电子病历的设备进行身份鉴别.

基于非对称算法的数字签名技术是一种强鉴别手段,相比于口令、指纹等鉴别机制具备更高的安全强度,网上银行、移动支付等对安全性要求较高的应用领域均不同程度地采用数字签名身份鉴别机制. 基于 SM2 椭圆曲线密码算法的数字签名是中国自主的数字签名算法,在国家密码管理局的推动下正在逐渐应用于国内各行各业. SM2 的私钥本质上就是一个随机数,因此在产生 SM2 签名公私钥对时,对于私钥的产生通常就是使用随机数产生的方法. 使用软件伪随机数发生器产生私钥是不安全的,通常在电子设备的电路中有专门的随机数产生芯片,用以产生签名私钥或其他随机数[1]. 专门的随机数芯片能够以较高速率产生大量随机数,但它也增加了芯片的成本.

本文引入一种基于 Nand Flash 的硬件物理特性的签名私钥产生方法,它与每个芯片自身的物理特性相关,这种物理特性是在芯片生产过程中所确定的,我们将其称作 Nand Flash 芯片的数字指纹. 即便相同型号的芯片,其数字指纹也是不同的,即数字指纹具备芯片唯一性.

相比于专用随机数芯片,这种方法产生的数据量有限,虽无法达到较高速率,但产生签名私钥大多数情况下是对时间非敏感且频度不大的应用,例如医院用于存储患者电子病历的电子设备,因此完全可以基于 Nand Flash 数字指纹信息产生每个 Nand Flash 芯片唯一的签名私钥. 此外,对于仅需少量随机数的非时间敏感应用,也可以此作为物理随机源之一. 由于数字指纹与 Nand Flash 器件具有紧耦合性,因此使用这种方法获得的签名私钥也与器件具有紧耦合性. 这种紧耦合性是可以通过计算相关系数来验证的.

1 Nand Flash 介绍

1.1 Nand Flash 存储单元

闪存主要有 2 种类型,Nand Flash 和 Nor Flash[2]. Nor Flash 的成本相对较高,读写数据时不容易出错,比较适合应用于存储少量的代码. Nand flash 成本相对较低,数据读写相对更容易出错,所以一般都需要有软件或者硬件的数据校验,称为 ECC. Nand Flash 存储容量大、价格低廉、速度快,经过 ECC 后读写错误率在可控范围内,因此常被用来存储大量的数据. 在使用 Nand Flash 作为非易失存储器件的嵌入式系统中,Nand Flash 相当于 PC 上硬盘的角色.

Nand Flash 利用双栅极结构的晶体管来存储数据[3]. 如图 1 所示,施加在控制栅极(Control Gate)上电压的不同决定了是向浮置栅极(Floating Gate)充入电荷还是使其释放电荷. 浮置栅极是由夹在两层二氧化硅材料之间的氮化物构成的,中间的氮化物就是可以存储电荷的电荷势阱,栅极与硅衬底之间有二氧化硅绝缘层,用来保护浮置栅极中的电荷不会泄漏. 数据是 0 还是 1,以栅极与源极(Source)之间的电压是否超过一个特定的阈值来表示[3]. 对 Nand Flash 进行编程(写)操作时,会在控制栅极上施加正向的大电压,利用 F-N 隧道效应,将 Nand Flash 存储单元所存储的数值由逻辑‘1’变为逻辑‘0’. 对 Nand Flash 进行擦除操作时,会在 Nand Flash 存储单元的控制栅极上施加一个反向的电压,同样利用 F-N 隧道效应,将 Nand Flash 存储单元所存储的数值由逻辑‘0’变为逻辑‘1’.

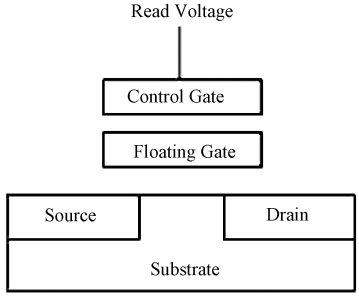

图 1 Nand Flash 存储单元

Fig. 1 Nand Flash memory cell

1.2 Nand Flash 组织结构

如图 2 所示,Nand Flash 的若干个存储单元

的晶体管的栅极通过“字线”连接,构成一页(Page),相邻的多页构成一块(Block). 相邻晶体管的漏极和源极头尾相连,最高端接位线,最低端与高电压的源极相连. 通过位线相连的同一块上的 2 个存储单元属于不同的页.

块和页是 Nand Flash 中的基本单位,一个块包含多页(常见的为 32 页或者 64 页),一页包含多个字节(常见的为 512 Bytes 或者 2K Bytes)[3]. 对 Nand Flash 的读和编程操作是以页为单位的,而对 Nand Flash 的擦除操作是以块为单位的. 一个 Nand Flash 芯片中含有上千个块(常见的有 8 192块或 4 096 块等)[4].

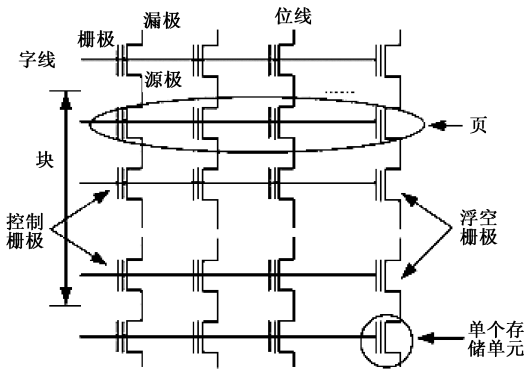

图 2　Nand Flash 的组织结构

Fig. 2　Array organization of Nand Flash

1.3　Nand Flash 的编程操作影响

基于上述 Nand Flash 的组织结构,由于属于不同页的存储单元在物理结构上是相邻的,因此对 1 页的存储单元进行编程操作时,会对其相邻页存储单元晶体管的浮置栅极与源极之间的电压产生间接的影响,即产生间接的控制门电压. 对 1 页经过多次编程操作后,这种影响会导致其相邻页的存储单元发生位翻转现象,即存储单元所存储的信息由逻辑‘1’变为逻辑‘0’.

随着 Nand Flash 容量的增大,单位面积内的存储单元数也越来越多,所以各个存储单元在单位面积和其栅极与硅衬底之间的二氧化硅绝缘层厚度的微小差异,就会对其编程操作造成影响[5],导致不同的存储单元产生位翻转现象的时间也不一样. 本文利用 Nand Flash 的此物理特性提取随机数,作为 Nand Flash 的数字指纹.

2　Nand Flash 数字指纹提取及 SM2 私钥产生方法

2.1　数字指纹提取

根据上文所述,由于各存储单元在单位面积及栅极与硅衬底之间的二氧化硅绝缘层厚度等物理特性方面存在差异,导致对相邻页的重复编程造成的控制门电压变化影响的忍耐能力不同,因此可利用此物理特性对 Nand Flash 进行数字指纹信息提取[5].

首先对 Nand Flash 的 1 块进行擦除操作,使该块内所有页所存储的信息均变为逻辑‘1’,A 页和 B 页是此块内物理上相邻的 2 页. 然后对该块内的 A 页进行重复编程操作,每次对 A 页编程操作之后,对 B 页进行读操作,观察 B 页上各存储单元是否发生了位翻转现象(即存储的信息由逻辑‘1’变为了逻辑‘0’). 若 B 页上某存储单元发生了位翻转现象,记录此时对 A 页的编程次数;若对 A 页若干次编程操作后,B 页上的某存储单元未发生位翻转,则记编程次数为 0. 将 B 页的各个存储单元发生位翻转现象时对应的 A 页的重复编程数组合起来,构成此 Nand Flash 的一个数字指纹信息. 算法伪代码如下:

```
EraseBlock(TheBlock)
for Cycle = 0... 10000 do
  ProgramAllZeroes(PageA)
  bits = ReadPage(PageB)
  for b = 1... BitsPerPage do
    if bits[b] = = 0 then
      Signature[b] = Cycle
    end if
  end for
end for
```

由于电子噪声的影响,对同一 Nand Flash 的相同的块和页进行 2 次数字指纹信息提取操作所提取的指纹信息不会完全一样[6],但是两组指纹信息有很大的相关性. 我们定义(X,Y)为两组数字指纹信息对,根据公式 $P(X,Y)=\frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma_X\sigma_Y}$ 计算其相关系数[6]. 根据计算的相关系数大小,可以判断两组数字指纹信息是否取自同一 Nand Flash 芯片的同一块和页. 这也是“数字指纹”的含义所在——判断 2 次提

取的指纹是否来自同一 Nand Flash 芯片的同块同页不是根据数值的精确比对来确定的,而是通过对比两次提取的数据之间的相关性而确定的,这与指纹识别技术的原理非常类似.

2.2 产生 SM2 私钥

根据 GM/T 0003—2012《SM2 椭圆曲线公钥密码算法》以及 GM/T 0009—2012《SM2 密码算法使用规范》,对一个有效的 F_q($q=p$ 且 p 为大于 3 的素数,或 $q=2^m$)上椭圆曲线系统参数的集合,要求用随机数发生器产生整数 $d\in[1,n-2]$(n 为所选取椭圆曲线基点 G 的阶,$n>2^{191}$ 且 $n>4p^{1/2}$),并推荐使用 256 位的椭圆曲线.

Nand Flash 数字指纹的数据量远远大于 256 位,按照每页 512 字节计算,即每页 4 Kbits,每个 bit 的数字指纹信息用 2 个字节表示(因为对相邻页的重复编程次数需在 4 500 到 5 000 次之间),所以对一页提取的数字指纹为 8 K 字节. 图 3 为对某页提取的指纹信息的前 450 字节.

```
00 00 00 00 1D F0 00 00 23 74 00 00 00 00 00 00 14 EA 00 00 00 00 00 00 00 00 00 25 B3
00 00 00 00 00 00 00 0E 05 00 00 00 00 00 00 00 00 00 00 00 23 10 16 12 00 00 00 00 00 00 00 00
00 00 1D CB 00 00 00 00 00 00 24 26 00 00 00 00 00 00 00 00 00 00 20 3D 00 00 18 DB 00 00 00 00
00 00 00 00 00 00 1A C0 00 00 1E 42 00 00 00 00 1E 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 1E 87 00 00 00 00 00 00 25 BA 25 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 15 DE 1C 68 1E 52 00 00 24 AE 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 22 45 00 00 00 00 00 00 00 00 25 F4 00 00 00 00 00 00 00 00 00 00
1E 77 00 00 00 00 00 00 00 00 00 18 B0 00 00 21 EE 17 07 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 0E 00 00 00 00 00 00 00 00 26 02 00 00 00 00 00 00
00 00 26 88 00 00 00 00 00 00 00 00 00 00 00 21 C4 1A 49 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 16 68 00 00 00 00 00 00 00 00 00 1F 66 00 00 00 00 00 00 00 00 00 00 00 00 00 16 66
21 9F 00 00 00 00 00 00 00 00 00 00 00 00 20 94 00 00 00 00 00 00 00 00 26 92 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 95 1A EF 00 00
0B 26 21 F9 00 00 00 00 00 00 00 00 00 00 00 21 5C 00 00 1D 2B 22 8E 00 00 1D 76 00 00 00 00
00 00 00 00 00 00 1E FB 00 00 1E 36 00 00 19 E0 00 00 00 00 00 00 1C 94 00 00 00 00 0F FA
```

图 3 数字指纹信息的前 450 字节

Fig. 3 The first 450 bytes of the digital fingerprint information

从 8 K 字节中生成 256 位最简单的方法就是直接截取数字指纹的前 256 位作为 SM2 签名私钥. 但从图 3 中可以看出,数字指纹是一个稀疏向量,直接截取前 256 位这样会提取出多个 0,不适合作为 SM2 签名私钥. 消除 0 元的方法可以直接剔除 0 位,还可以将数字指纹分为 256 位的级联分组,将部分或全部分组进行模二加的结果作为签名私钥. 采用后一种方法将图 3 所示的数据样本进行 SM2 私钥提取,得到以下 32 个字节:16 AD 36 7E 03 20 26 67 0B 7A 29 A0 25 43 23 07 3B 2A 0D BE 13 E4 13 D6 1F 31 27 07 14 96 27 4A. 这个数据的随机性仍然是不好的,因此仍不适合直接作为私钥使用. 为了增强随机性,本文采用 SM3 密码杂凑算法,即将数字指纹进行散列计算,将计算结果作为私钥.

由于电子噪声的存在,对同一芯片的相同位置提取的多组数字指纹值很难完全相同,所以用于生成 SM2 私钥的数字指纹必须存储下来,以备未来验证使用. 基于安全性考虑,存储的位置将不能被格式化操作所覆盖,这也有多种选择:可以将数字指纹信息保存在 Nand Flash 的隐藏扇区中[7],或保存在人为标记的坏块中(仍可正常进行编程和写操作). Nand Flash 控制器电路(可编程)会禁止外界对这些位置的读写请求[8],但 Nand Flash 控制器自身可以对其进行读写[9]. 而对于 SM2 私钥,可以不作存储,需要时由 Nand Flash 控制器进行 SM3 计算后获得.

Single-Level Cell(SLC)型 Nand Flash 页的写操作寿命是 100 万次左右,因此当验证私钥的次数(即对同一芯片的固定一页进行数字指纹信息提取的次数)超过一定阈值后,相关性会有所下降. 可在每一页的 OOB 区域记录对该页验证私钥的次数,当超过阈值后,选取另外一页进行数字指纹信息提取,并对提取的数字指纹信息进行秘密存储和 SM3 计算,从而更换新的 SM2 私钥. SM2 私钥产生流程如图 4 所示.

3 实验

3.1 实验环境

我们在图 5 的 Nand Flash 开发板上实现了对 Nand Flash 的数字指纹信息的提取. 硬件环境为:控制器为 STM32F103,该控制器是基于 ARM 的 32 位的 Cortex-M3 的 CPU,最高工作频率 72 MHz. Nand Flash 为三星公司生产的 K9K8G08,该型号 Nand Flash 共有 8 192 个块,每块含 64 页,每

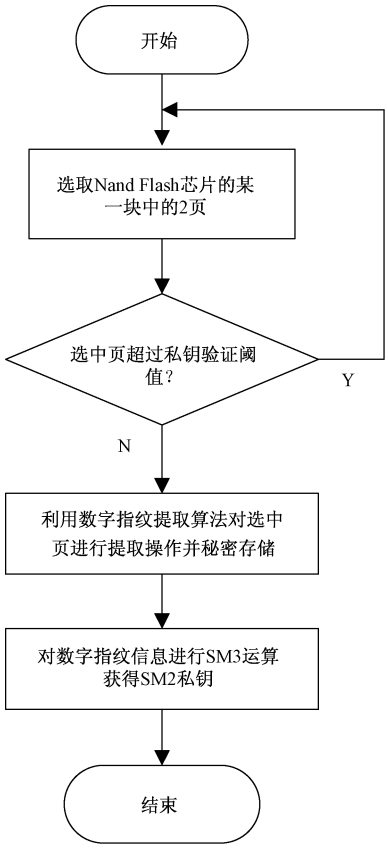

图 4　SM2 私钥产生流程图

Fig. 4　Flow diagram of SM2 private key generation

页 2 Kbytes,容量为 1 GBytes. 本实验选取 2 个 K9K8G08 芯片作对比,分别记作 Chip1 和 Chip2. 软件环境为:64 位的 win7 操作系统,keil uVision V4. 7,C 语言开发环境.

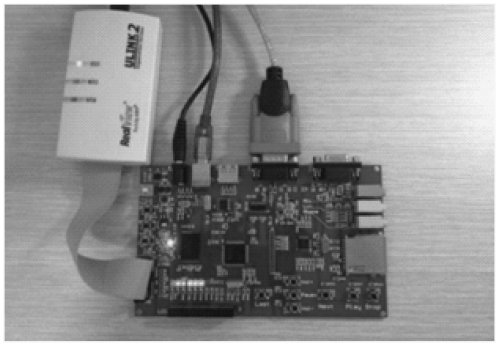

图 5　Nand Flash 开发板

Fig. 5　Nand Flash test board

3. 2　数字指纹相关性实验

首先验证数字指纹的相关性,这种相关性确保数字指纹与 Nand Flash 器件的紧耦合,进而确保由数字指纹生成的 SM2 私钥与 Nand Flash 器件紧耦合. 根据 2. 1 提取数字指纹信息的算法,选取 Chip1 的第 1 800 块进行擦除操作,并对此块的第 1 页进行重复编程操作,每次编程操作后读此块的第 2 页,观察记录第 2 页的位翻转情况. 进行两组实验,将提取到的数字指纹信息记为 Trail1. 1 和 Trail1. 2.

再选取 Chip1 的第 1 900 块进行擦除操作,并对此块的第 4 页进行重复编程操作,每次编程操作后读此块的第 5 页,观察记录第 5 页的位翻转情况. 同样进行 2 组实验,将提取到的数字指纹信息记为 Trail2. 1 和 Trail2. 2. 将从 Chip1 获得的 4 组数据通过 Matlab 软件计算两两的相关系数,计算结果如表 1 所示(* 表示重复部分,省略).

表 1　Chip1 4 组数据的相关系数

Table 1　Correlation coefficients of four groups of data from chip1

	Trail1. 1	Trail1. 2	Trail2. 1	Trail2. 2
Trail1. 1	1	0. 815 8	0. 027 3	0. 028 4
Trail1. 2	*	1	0. 012 2	0. 006 7
Trail2. 1	*	*	1	0. 805 5
Trail2. 2	*	*	*	1

分析上述数据可以看出,对 Chip1 的同一块和页提取的设备指纹有很大的相关性,相关系数均在 0. 8 以上;对 Chip1 的不同块和页提取的设备指纹的相关性很小,相关系数均在 0. 1 以下. 再次选取 Chip1 不同的块和页,重复上面的对比实验,所得的实验结果相同.

为验证不同芯片之间的实验结果,根据 2. 1 提取数字指纹信息的算法,选取 Chip2 的第 1 800 块进行擦除操作,并对此块的第 1 页进行重复编程操作,每次编程操作后读此块的第 2 页,观察记录第 2 页的位翻转情况. 进行 2 组实验,将提取到的数字指纹信息记为 Trail3. 1 和 Trail3. 2. 将从 Chip1 与 Chip2 获得的各 2 组数据通过 Matlab 软件计算两两的相关系数,计算结果如表 2 所示(* 表示重复部分,省略).

表 2　两芯片间数据的相关系数

Table 2　Correlation coefficients of data from two chips

	Trail1. 1	Trail1. 2	Trail3. 1	Trail3. 2
Trail1. 1	1	0. 815 8	0. 015 6	0. 021 6
Trail1. 2	*	1	0. 007 9	0. 012 4
Trail3. 1	*	*	1	0. 826 7
Trail3. 2	*	*	*	1

分析上述数据可以看出,对同一芯片的同一块和页提取的设备指纹有很大的相关性,相关系数均在0.8以上;对不同芯片的块和页提取的设备指纹的相关性很小,相关系数均在0.1以下.再次选取2芯片的不同的块和页,重复上面的对比实验,所得的实验结果相同.

通过实验测得,对1页的重复编程次数在4 500次以上时,所提取的指纹信息与选取其他块和页所提取的指纹信息就已经有很大的区分度;重复编程次数超过5 000次后,不同指纹信息的区分度增长幅度不大,所以本实验用16 bits存储对每个存储单元所提取的指纹信息,在10 s左右即可获得8 KBytes字节的数字指纹信息.

通过上述方法,当用户需要验证SM2私钥与Nand Flash器件的耦合关系时,可以重复针对相同页的实验获得参考数字指纹,并与已存储的数字指纹进行相关性计算,从而判定私钥是否的确由器件本身产生.

3.3 SM2密钥生成和验证实验

我们对Trail1.1计算SM3散列值得到32字节的SM2密钥:CA 40 82 4D FB 3E 12 08 75 32 0C 37 1A 88 C0 56 CA 2D BE 2C 2A E2 AC 52 CF 29 3E F4 8E 18 CE 91,并在Nand Flash控制器STM32F103上使用软件编程实现了SM2算法,采用GM/T 0009—2012《SM2密码算法使用规范》所推荐的曲线参数.经使用测试用例对签名和验签操作进行验证,其中间结果和最终结果均正确.

4 总结

本文利用Nand Flash的物理特性,对Nand Flash芯片的1页进行重复编程操作,观察并记录其物理相邻页发生位翻转时的重复编程数,将此随机数作为Nand Flash的数字指纹信息,并以指纹信息为基础生成SM2私钥.经过实验计算测得,对同一块和页提取的两组数字指纹信息有很大的相关性,对不同的块和页提取的指纹信息几乎没有相关性,这表明使用此方法产生的SM2私钥与Nand Flash芯片本身是紧耦合的,且这种紧耦合性可以通过实验验证.

参考文献

[1] Bucci M, Germani L, Luzzi R, et al. A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC[J]. Computers, IEEE Transactions on, 2003, 52(4): 403-409.

[2] Lee B, Son K, Won D, et al. Secure data deletion for USB flash memory[J]. J Inf Sci Eng, 2011, 27(3): 933-952.

[3] Reardon J, Capkun S, Basin D A. Data node encrypted file system: Efficient secure deletion for flash memory[C]// USENIX Security Symposium. 2012: 333-348.

[4] Wang Y, Yu W, Xu S Q, et al. Hiding information in flash memory[C]// Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013: 271-285.

[5] Prabhu P, Akel A, Grupp L M, et al. Extracting device fingerprints from flash memory by exploiting physical variations[C]// Trust and Trustworthy Computing. Springer Berlin Heidelberg, 2011: 188-201.

[6] Wang Y, Yu W, Wu S, et al. Flash memory for ubiquitous hardware security functions: true random number generation and device fingerprints[C]// Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012: 33-47.

[7] Gal E, Toledo S. Algorithms and data structures for flash memories[J]. ACM Computing Surveys (CSUR), 2005, 37(2): 138-163.

[8] Suh G E, Devadas S. Physical unclonable functions for device authentication and secret key generation[C]// Proceedings of the 44th annual Design Automation Conference. ACM, 2007: 9-14.

[9] Lee J W, Lim D, Gassend B, et al. A technique to build a secret key in integrated circuits for identification and authentication applications[C]// VLSI Circuits, 2004. Digest of Technical Papers, 2004 Symposium on. IEEE, 2004: 176-179.