加密芯片

1 芯片特性

1.1 用户区为 EEPROM

- 有 4 个用户分区
- 多种写入模式：单个 Byte、多个 Byte 和 Page 写入模式
- 每个分区都设有访问权限

1.2 配置区 2K-bit

- 客户可以定义 8-Byte 唯一 ID
- 可以定义访问权限、认证密钥种子、用户区读写密码

1.3 高安全性

- 有 64-bit 动态相互认证种子
- 有 8 组 24-bit 读写密码
- 认证和加密都有 4 组密钥种子
- 滚动加密

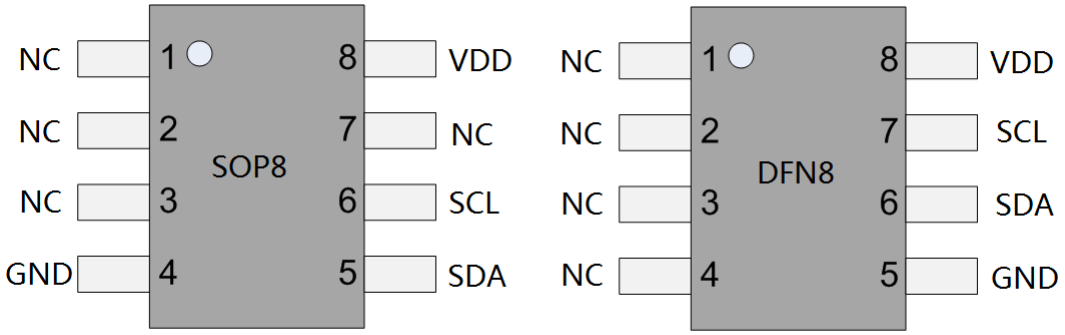
1.4 应用特征

- 电压范围：2.7V-5.5V
- 采用 2 线非标准 I2C 接口
- 通信频率最高可达 1.0 MHz
- 标准的 SOP8 封装

1.5 高可靠性

- 写操作可达 10 万次
- 数据保持可达 10 年

2 芯片封装和管脚定义



管脚定义如下所示：

Pad	Description
VCC	Supply Voltage
GND	Ground
SCL	Serial Clock Input
SDA	Serial Data Input/Output

3 配置区介绍

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	Reserved								Fabrication
$08	Fab Code		MTZ		ID Code A				
$10	ID Code B								
$18	DCR	Reserved							Access Control
$20	AR0	PR0	AR1	PR1	AR2	PR2	AR3	PR3	
$28	Reserved								
$30									
$38									
$40									
$48									
$50	AAC0	Ci0							Crypto
$58	SK0								
$60	AAC1	Ci1							
$68	SK1								
$70	AAC2	Ci2							
$78	SK2								
$80	AAC3	Ci3							
$88	SK3								
$90	Secret Seed G0								Secret
$98	Secret Seed G1								
$A0	Secret Seed G2								
$A8	Secret Seed G3								
$B0	PAC	Write0			PAC	Read0			Passwords
$B8	PAC	Write1			PAC	Read1			
$C0	PAC	Write2			PAC	Read2			
$C8	PAC	Write3			PAC	Read3			
$D0	PAC	Write4			PAC	Read4			
$D8	PAC	Write5			PAC	Read5			
$E0	PAC	Write6			PAC	Read6			
$E8	PAC	Write7			PAC	Read7			

$F0 $F8	Reserved	System

3.1 Fab Code

16-bit 寄存器，出厂值为：“10 10”，客户不能修改。

3.2 MTZ

存储器测试区共有 16-bit，是为了测试通信而定义的，任何时候都有权限读写 MTZ。

3.3 ID Code

可以定义 8-Byte 唯一 ID，出厂后只能读，不能修改。

3.4 **DCR**

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
		UAT	ETA	CS3	CS2	CS1	CS0

UAT：如果使能（UAT=“0”），允许无数次错误认证，AAC 无效。

ETA：如果使能（EAT=“0”），有 8 次错误认证或者校验的机会。如果 EAT=“1”，AAC 和 PAC 都只有 4 次错误机会。

CS0-CS3：芯片都能响应默认片选地址$B（1011），也能相应 CS0-CS3 对应的地址值。

3.5 **访问寄存器 AR**

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
PM1	PM0	AM1	AM0	ER			

PM(1:0)-密码模式

PM1	PM0	权限
1	1	不需要密码校验
1	0	需要写密码校验
0	1	读写密码都需要校验
0	0	

当 PM=“11”时，访问用户区不需要密码校验

当 PM=“10”时，写用户区需要校验写密码，读用户区不需要校验读密码

当 PM=“01”或者“00”时，读和写用户区需要校验写密码，只读用户区需要校验读密码。

AM(1:0)-密码模式

AM1	AM0	权限
1	1	不需要认证
1	0	写需要认证
1	0	读写都需要认证
0	1	

当 AM=“11”时，访问用户区不需要认证

当 AM=“10”时，写用户区需要认证，读用户区不需要认证

当 AM=“01”时，读和写用户区都需要认证

ER-encryption required

当 ER=“0”，如果要正确地读写用户区，主机需要启动加密模式。

当 ER=“1”，主机可以启动加密模式，如果不启动，也可以访问用户区，但通信

是不加密的。

3.6 密码寄存器 PR

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
AK1	AK0				PW2	PW1	PW0

AK(1:0)-认证 Key，这 2 位定义 4 组加密种子 G0-G3 的一组，这个加密种子在认证加密过程被使用。
PW(2:0)-密码设定，这 3 位定义 8 组密码中的一组作为用户区的密码。

3.7 安全密码（secure code）

安全密码对应的是 write7 密码，只有正确校验了安全密码，才能修改配置区

3.8 Ci 和 SK

加密认证时，存储对应的 Cix 和 SKx，不必理会。

3.9 G0-G3

加密认证种子，要和软件的认证种子一致。

3.10 Passwords

密码可以用来保护用户区的读和写，这里有 8 组密码，可以通过 PR 寄存器选择一组来保护相应的用户区。如果校验了写密码，那么读和写都可以，如果只校验读密码，那么只可以读。

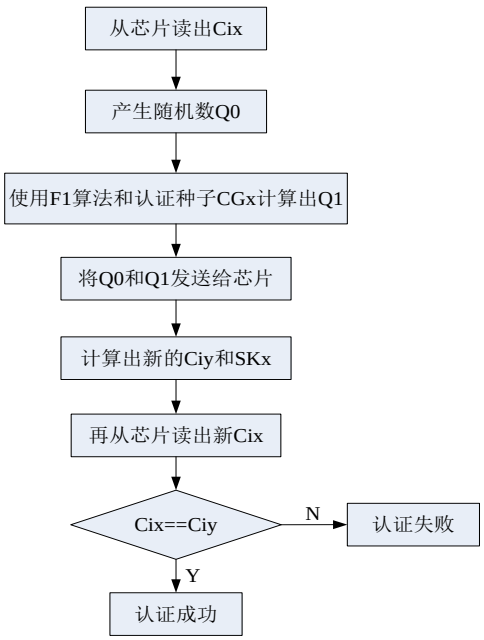
4 通信模式

4.1 标准模式

芯片默认就是标准模式，任何类型的数据都没有加密，通信的数据是明文。

4.2 认证模式

通过访问寄存器 AR/PR 来设定。在这种模式，配置区的密码是加密的，如果发送命令验证读写密码，那么都是以密文形式进行。对于用户区，芯片必须成功认证之后，才能访问用户区，通信是明文。认证过程如下所示：



4.3 加密模式

通过访问寄存器 AR 来设定，在这种模式下，配置区的密码和用户区的通信都是加密的，以密文形式进行。加密模式启动过程是在认证模式启动的基础上，把 CGx 改成计算出的 SKx 再认证一次，如果认证成功，加密模式就启动了。

5 保险丝

该加密芯片共有 4 个保险丝，“fuse byte”给出了保险丝的状态，“0”表示已熔断。Bits 4 到 7 是预留位

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
				SEC	PER	CMA	FAB

为了锁住 ID Code B，SEC 出厂时已被熔断，默认的 ID Code B 全为“FF”。要熔断 fuses，必须要按照下面的次序：

FAB – 锁住 Fab Code

CMA – 锁住 ID Code A

PER – 锁住剩余的配置区

如果不按照这个次序熔断 fuses，那肯定是错误的。

Fuse 访问权限表如下所示：

Zone	OP	Fuse			
		SEC=0	FAB=0	CMA=0	PER=0
Fab Code	R	Free	Free	Free	Free
	W	Secure Code	Forbidden	Forbidden	Forbidden
MTZ	R	Free	Free	Free	Free
	W				
ID Code A	R	Free	Free	Free	Free
	W	Secure Code	Secure Code	Forbidden	Forbidden
ID Code B	R	Free	Free	Free	Free
	W	Forbidden	Forbidden	Forbidden	Forbidden
Access Control	R	Free	Free	Free	Free
	W	Secure Code	Secure Code	Secure Code	Secure Code
AACx Cix	R	Free	Free	Free	Free
	W	Secure Code	Secure Code	Secure Code	Forbidden
SKx	R	Secure Code	Secure Code	Secure Code	Forbidden
	W				
Secret	R	Secure Code	Secure Code	Secure Code	Forbidden
	W				
PW	R	Secure Code	Secure Code	Secure Code	Write PW
	W				
PAC	R	Free	Free	Free	Free
	W	Secure Code	Secure Code	Secure Code	Write PW
User	R	AR	AR	AR	AR

Zones	W				

说明：芯片默认是 SEC=0 对应的权限，如果 FAB 熔断，那么 FAB=0 对应的权限起效，如果 CMA 熔断，那么 CMA=0 对应的权限起效，如果 PER 熔断，那么 PER=0 对应的权限起效。

6 该芯片采用 2 线非标准 I2C 通信协议，操作命令如下所示：

Item	INS	P1	P2	P3	Data(N)
Write user zone	$B0	$00	Addr	N<$10	N bytes
Read user zone	$B2	$00	Addr	N	
Write conf zone	$B4	$00	Addr	N<$10	N bytes
Write fuses	$B4	$01	FusesID	$00	
Send checksum	$B4	$02	$00	$02	2 bytes
Set user zone	$B4	$03	Zone	$00	
Read conf zone	$B6	$00	Addr	N	
Read fuses	$B6	$01	$00	$01	
Read checksum	$B6	$02	$00	$02	
verify auth	$B8	$0X	$00	$10	Q0+Q1(16bytes)
verify Encry	$B8	$1X	$00	$10	Q0+Q1(16bytes)
Verify W-PW	$BA	$0X	$00	$03	3 bytes pw
Verify R-PW	$BA	$1X	$00	$03	3 bytes pw

说明：1、写操作之后要延时 10ms，verfiy auth 和 verify Encry 要延时 20ms。
2、Q0 为 8 个 byte 的随机数，Q1 是 F1 算法计算出来的 8 个 byte 数据。
3、W-PW 表示写密码，R-PW 表示读密码。