Boot

从 flash 0x0地址读取第一次boot时保存的secure digest和随机数IV

ROM bootloader发现efuse中ABS\_DONE\_0为1，secure boot被使能

硬件利用efuse中的secure boot key,随机数IV和加密的bootloader image计算新的secure digest

Flash中的secure digest与新的digest是否相同

Boot到软件bootloader，软件bootloader读取公钥，验证partition table和app images的签名

签名是否验证通过

停止Boot

Boot到app image，解密flash中的程序执行

否

否

是

是

Boot

软件bootloader发现efuse中ABS\_DONE\_0为0，secure bootloader没有使能

软件bootloader利用硬件产生的随机数作为secure boot key，将key保存在efuse中，对于软件读写保护

使用key、额外的硬件随机数IV和软件bootloader image计算出secure digest

将secure digest和随机数IV打包保存在flash的0x0地址

烧写efuse中的ABS\_DONE\_0永久使能secure boot

软件bootloader读取到FLASH\_CRYPT\_CNT为0，利用硬件产生加密key，保存在efuse中，对于软件读写保护

Bootloader用key对所有需要加密的数据在flash中原处加密

Bootloader将FLASH\_CRYPT\_CNT烧写为0x01，flash加/解密被使能

软件bootloader将自己重启，从加密的flash执行软件bootloader

软件bootloader再次检查ABS\_DONE\_0，这次已被置1

软件bootloader利用公钥验证partition table和app image签名

签名是否验证通过

停止Boot

Boot到app image，解密flash中的程序执行

软件bootloader检查FLASH\_CRYPT\_CNT，此时已被设置为0x01，flash加/解密已被使能

否

是