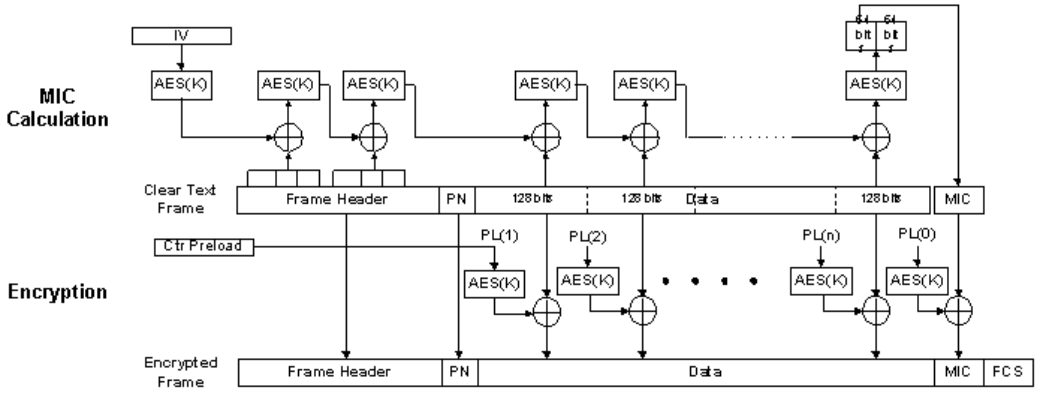
1. Bitlocker 加密概述

Bitlocker 是自 Windows Vista 引进的磁盘卷加密方案，也被称为 BDE（Bitlockeer Driver Encryption）。从加密对象上分，BDE 有两种模式：本地磁盘加密模式，以及 Bitlocker-to-go 模式。本地磁盘加密模式仅适用于加密 NTFS 格式的本地磁盘。Bitlocker-to-go 则用于加密可移动磁盘，格式包括 FAT，exFAT，FAT32，以及 NTFS。其差别在于加密磁盘数据结构的不同。

在加密方式以及加密算法的实现上，每个 Windows 版本的 BDE 都略有不同。在 Windows 8 之前，Bitlocker 加解密算法使用的是 AES-CBC，加可选的 Elephant Diffuser。Windows 8 之后，Elephant Diffuser 因为优化问题被移除了。而在 Windows 10 中新采用了一种 AES-XTS 算法，作为另一个可选的加解密算法。所有 FVEK 的加密都使用的是 AES-CCM 算法。VMK/FVEK 的密钥会和其哈希值一起保存，用来验证解密是否成功。

2. 密钥加解密算法

Bitlocker 使用标准 AES-CCM 算法对 VMK 和 FVEK 数据结构进行加解密，其中包含一个 CBC-MAC 效验码验证解密是否正确。

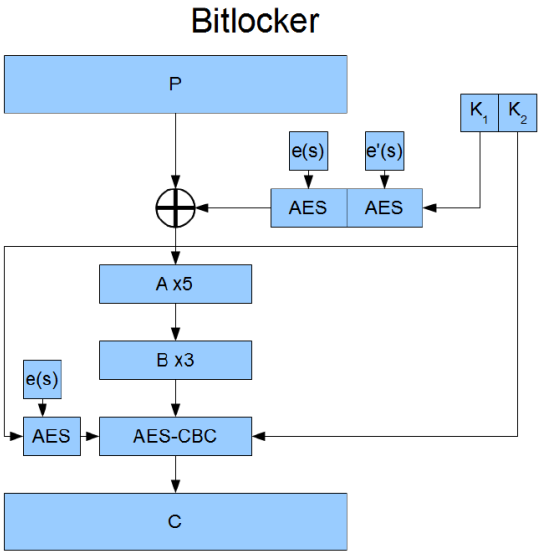


3. 数据加解密算法流程

3.1. Windows 8 前（AES-CBC + Elephant Diffuser）：

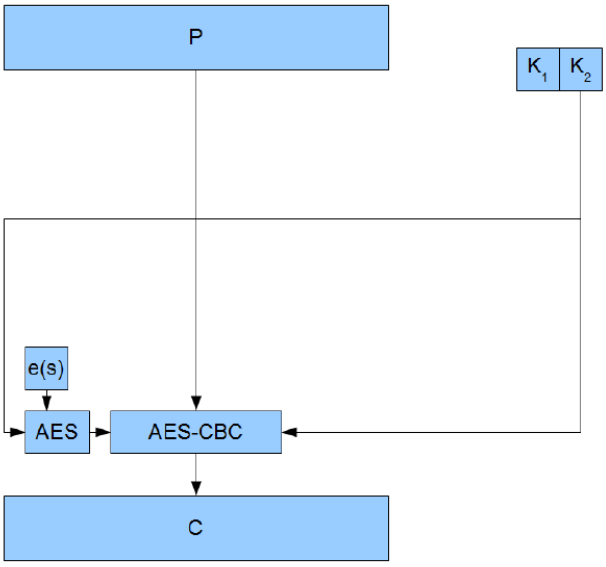
Windows 8 之前在进行 AES-CBC 数据加密前先使用 Elephant Diffuser 对明文

数据进行混淆。具体可参照 Niels Ferguson 在 06 年的论文（AES-CBC + Elephant diffuser A Disk Encryption Algorithm for Windows Vista）。



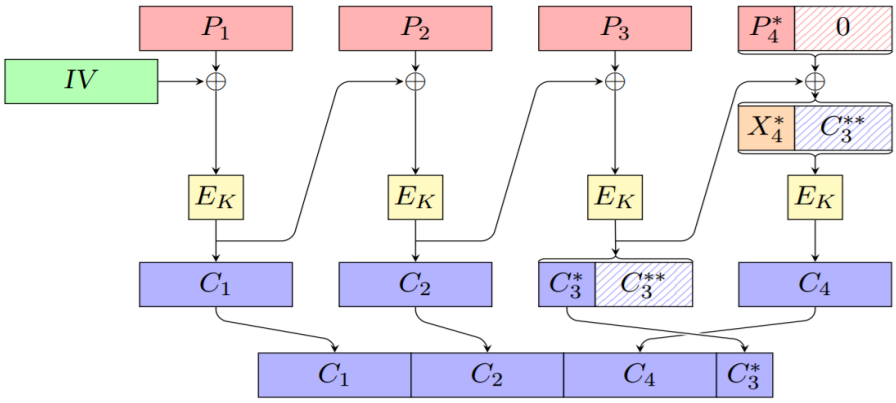
3.2. Windows 8 之后（AES-CBC）算法流程：

Windows 8 开始，微软从 Bitlocker 中移除了 Elephant Diffuser。



3.3. Windows 10 AES-XTS 算法流程：

Windows 10 中，微软增加了 AES-XTS 加密算法的加解密模式。基本的加密算法依旧是 AES-CBC。



4. Bitlocker 加解密流程

4.1. Bitlocker 加密

1）Bitlocker 会随机生成 VMK 密钥和 FVEK 密钥
2）VMK 密钥会被加密并存储在磁盘上多个地方，
3）VMK 密钥用于加密存储在磁盘上的 FVEK 密钥，AES-CCM
4）FVEK 密钥分为两部分：Sector Key 和 AES Key
5）Sector Key 类似于一个初始化向量，在加密前对明文进行异或操作
6）然后数据会通过两个扩散器，来增强加密的安全性
7）最后数据会使用 FVEK 中的 AES Key 进行 AES 加密，并存储在磁盘上。

4.2. Bitlocker 解密流程

1) 使用用户密钥，或者 TPM 模块中存储的密钥，或者 Bitlocker 恢复密钥解密出 VMK；
2) 使用 VMK 解密出 FVEK；
3) 使用 FVEK 中的 AES Key 解密出 Bitlocker 加密数据；
4) 通过两个扩散器还原数据
5) 使用 FVEK 中的 Sector Key 还原出明文数据