Q1. Can we use XTS without applying the second tweak?

만약 같은 contents를 가진 sector 2개가 있다면, 같은 key를 사용하여 암호화하였을 때 나오는 cipher text가 동일해지고, attacker가 같은 contents를 가진 sector 2개를 유추하기 쉽다.

따라서 각 sector 별로 다른 random IV를 사용해야 하는데, device에 각 random IVs를 저장할 공간이 없으므로 sector의 numbers를 사용하였고, 이 또한 유추하기 쉽기 때문에 2번의 tweak을 거치게 한 것이다.

따라서 모든 sector에 다른 content가 존재한다고 가정하면(empty인 sector도 2개 이상이면 안 된다.), 1번의 tweak만을 사용하여도 된다.

Q2. Is it necessary to encrypt tweak before using it?

tweak을 encrypt할 때 사용하는 이유는 보안을 한 층 더 강화하기 위해서이다. 사용하지 않아도 지장은 없지만 공격받을 위험이 높아지기 때문에 필수적은 아니어도 되도록 사용하는 것이 좋다.