In this paper we study the design of efficient trace-revoke schemes for content protection. In state-of-art, broadcast encryption and traitor tracing are viewed as two orthogonal problems. Good traceability and efficient revocation seem to demand different types of design. When combined into trace-revoke schemes, existing schemes only offer efficiency on one aspect but weak on the other. Moreover, there are two major styles of pirate attacks, namely the clone device attack and anonymous re-broadcasting attack. In current state-of-art, defending against these two attacks are viewed as two different problems that demand different trace-revoke schemes. In current state-of-practice, a content protection system has to deploy two trace-revoke schemes in order to provide complete protections against both attacks. As a result, the system incurs the complexity of having to manage two schemes, even worse the overall strength of the system is the weakest link in either scheme.

In this paper we present a unified trace-revoke system that can offer superior efficiency on both traceability and revocation capability as well as simultaneously defend against two attacks in a unified way. Our unified system offers everything that the original two schemes combined can provide, but our system is much simpler and more efficient. The design of our unified framework carries both scientific and real world practical significance. We reduce the tracing time from tens of years to hours. The much improved simplicity and efficiency of our unified system caused it to be adopted by the new version of AACS, Advanced Access Content System, the industry content protection standard for the new Blu-ray high-definition-video optical discs. Scientifically our design shows it is possible to design an efficient broadcast encryption scheme and traitor tracing scheme in a unified way. We also showed the equivalence of the two major types of attacks which are currently viewed as different attacks. This opens brand new directions for future research on broadcast encryption and traitor tracing.