报告摘要

在信息存储与传输过程中往往会受到敌方恶意的代数篡改。2008年 Crammer 等人推广和总结了已有的方案,提出了代数操作可检码(AMD 码)的概念。最优的 AMD 码能以很高的概率检测到任何的代数篡改。到目前为止,已有的构造 AMD 码的方法并不多,大体可以分为两类:其中一类构造方法是基于代数的;另一类是基于组合的方法。如何构造出更多的最优的 AMD 码仍是信息安全领域研究的难点和重点。我们将围绕 AMD 码的结构讲述几种基于组合的方法构造最优的 AMD 码。