doi:10.1631/FITEE.1800576

题目：CAESAR 竞赛认证加密算法设计分析与安全性评估进展

概要：CAESAR 竞赛是 2013 年由美国国家标准与技术研究院（NIST）资助的认证加密算法征集竞赛，旨在征集综合性能和安全性优于 AES-GCM 的认证加密算法，能够同时实现完整性和机密性。最后入围的算法可能被推荐至工业界并标准化。竞赛分 3 个轮次，第 3 轮在 2018 年结束。本文首先介绍 CAESAR 竞赛候选算法的设计要求和筛选进展，然后从设计结构和加密模式两方面对最后一轮候选算法进行归类，之后综述了候选算法的综合性能与安全性分析进展，最后探讨了认证加密算法的设计和分析研究趋势。

关键词：CAESAR 竞赛；认证加密算法；分组密码；序列密码；哈希函数；安全性评估