* Bulletproofs+: Shorter Proofs for Privacy-Enhanced Distributed Ledger(06月) [[pdf]](https://eprint.iacr.org/2020/735.pdf)
* 作者：Heewon Chung ， Kyoohyung Han ，Chanyang Ju ，Myungsun Kim ，Jae Hong Seo
* 关键词： 零知识证明；范围证明；密码学协议
* 简介：这篇文章优化了bulletproofs，协议生成的proof是同类别中最短的，具体的来所，当证明一个已承诺的值范围是（0，264）时，在128比特安全参数下，证明大小为576字节，这是原协议(Bulletproofs, IEEE Security and Privacy 2018)的85%。