[学术][安全计算]Improved Primitives for MPC over Mixed Arithmetic-Binary Circuits [[pdf]](https://eprint.iacr.org/2020/338.pdf) （美密会）

作者：Daniel Escudero ;Satrajit Ghosh ;Marcel Keller ;Rahul Rachuri ;Peter Scholl

关键词：cryptographic protocols ;multi-party computation

摘要：设计了名为extended doubly-authenticated bits (edaBits)方法，该方法改进了安全多方计算中算术电路中共享数据与二进制数据类型之间的转换，可以提高一些非线性运算的效率，例如截断，比较，位分解。