

**Asiacrypt 2017 Best Paper**