IRSWKG 笔记

Effron Lu
SEU

版本：1.00
更新：2021 年 2 月 7 日

1 信息协调（Inforamtion Reconciliation）

信息协调实现方法分为两种：

* 基于 Cascade 信息协调协。Cascade 协议需要 Alice 和 Bob 有一个交互的过程, 在交互中纠错。
* 基于纠错码 (Error Correcting Code, ECC)，基于纠错码的信息协调只需要一方发送信息即可纠错，但相比较于 Cascade 协议而言泄露的信息量会大一点，计算开销也更加大。

基于纠错编码的信息协调实现流程如下：

1. Alice 随机选择一个比特串 r, 然后通过纠错编码的方式对 r 进行编码，记作 $Enc(r)$, $Enc(r)$ 的长度和量化后的比特串 q_A 的长度一样。
2. Alice 计算 $SS = q_A \otimes Enc(r)$。
3. Alice 把 SS 发送给 Bob。
4. Bob 收到 SS 后和自己量化得到的比特 q_B 进行异或
5. 使用纠错算法得到 $\tilde{r}$, 如果 q_B 和 q_A 不一样的比特数在纠错算法的纠错能力范围之内，那么 $\tilde{r}$ 和 r 一样。
6. 最后 Bob 使用纠错码的编码算法对 $\tilde{r}$ 进行编码后和 SS 进行一个异或，就可以得到比特串 q_A 了
7. 上述过程归纳为：$q'_B = SS \otimes Enc(Dec(SS \otimes q_B)) = SS \otimes Enc(\tilde{r})$

主流的纠错编码算法:BCH 编码、Turbo 编码、卷积编码、LDPC 编码、RS 编码.

2 隐私放大（Privacy Amplification）

隐私放大的实现方法可以分为：

1. 模糊提取器 (Fuzzy Extractor)
2. 全域哈希函数来 (Universal Hashing Functions)

3. **密码学哈希函数实现** (Cryptographic Hash Function)

密码学哈希函数实现流程：量化出来的这些比特，每 256 比特为一个分组，隐私增强后输出的最终密钥　度减短为 128 比特。