QKD Notes

G-RIPS Sendai 2025
Summer 2025

Mitsubishi-B Team

Min-Cut KRP Bound

In a Key Relay Protocol we seek to establish a min-cut feasibility bound.

We have n user pairs (a_i, b_i) who want to each share a secure, random key k_i. We refer to the smallest cut $\delta(S)$ to which S contains all a_i and $G - S$ contains all b_i as the minimum cut. The size of this minimum cut is taken to be $|\delta(S)|= m$.

On each edge of this minimum cut, we number them e_j where $j = 1 \dots m$ and on each edge there lives a local key source realized by a QKD link, which shares the primitive local key l_j securely between one node in S and one node in $G - S$. Assume each key is of a unit bit length.

The public channel announcements are treated as a all-encompassing P. Define the multi-index vector variables $K = \{k_i\}_{i=1\dots n}$ and $L = \{l_j\}_{l=1\dots m}$

The reconstruction of the keys by b is performed with some bijective linear function $f_i(L, P)$ for all b_i. Evidently, the security of our protocol relies on three properties

1. $H(K|L, P) = 0$, that is given L and P, one can deterministically resolve the keys K. We call this the **correctness** condition.
2. $I(K; P) = 0$, that is, the public channel announcements do not admit information gain on the secret keys. We call the **privacy** condition.
3. $H(K) = n$, that is the secret keys are independent and uniformly generated. We call this the **independence** condition.

We appeal to the following information-theoretic inequality

$$\begin{aligned} H(K) &= \underbrace{\cancel{H(K|L,P)}}_{\text{via correctness}} + \underbrace{\cancel{I(K;P)}}_{\text{via privacy}} + I(K;L|P) \\ &= I(K;L|P) \\ &\leq H(L|P) \\ &= H(L) \\ &= m \end{aligned}$$

The first line can be intuitively thought to be that the deterministic information about the keys is entirely dependent on L, conditioned on prior knowledge of P. This gives, for **correctness** and **privacy** we require $H(K) = m$ whilst for **independence** of the keys we require $H(K) = n$. As such, the feasibility constraint is that given n user pairs and a min-cut set m, a necessary but not sufficient condition is that

$$n \leq m$$

We can further refine this to wiretap sets by considering the information on the wiretapped edges W. Consider the following relation with $L - W$ and $P + W$. The analagous relation holds, and $|L - W|$ can be thought of the wiretap-restricted feasibility constraint.

To see why this generalizes to any linear network code, note that under a bijective function f_b,

$$H(X) = H(f_b(X))$$

It also may generalize to unequal link capacities. Treat each link larger than unit capacity as multiple links in our described construction. Lastly, this may work for SNC as well, simply treat $P = \emptyset$.

Ideas: SNC with multiple SC uses - repeated edges? Nodes can send different information down different edges. Same time? KRP is possible on tree graphs with edge disjoint paths. likewise in general case.