Identification Systems

Exercises 3

Piotr Syga

April 12, 2021

1. For the coupling from Lecture 5, show how to obtain the bound for τ for $n = 4$. You may use direct enumeration.

2. For the coupling from Lecture 5, give stricter bounds for $n = 6$ and $n = 8$.

3. Note that for the original process, the logarithmic part is followed by a constant $(3.6 \log n + 2)$, yet for the modification we have $\Theta\left(\sqrt{\log n}\right)$, explain the cause of this.

4. For the modified process, where $\frac{1}{8}$ of the ID is updated, find stricter bounds for $n = 4$ and $n = 6$.

5. Let us consider a system with $N = 64$ tags with IDs of length $8n = 32$ bits and a lifetime of $T = 10$ rounds find

   - the probability that there is at least 1 ambiguity
   - the probability that there is at least 1 ambiguity each round
   - the expected number of ambiguities

6. Recall the properties of Rapid Bit Exchange and Distance bounding protocols. You may refer to Brands and Chaum, Kim et al., Hancke and Bosk et al..