Damgård, Nielsen, Orlandi: *Secure Distributed Systems*

Danny Nygård Hansen

10th September 2022

5 • Confidentiality

5.1. Confidentiality, Secret-Key Systems

One-time pad: We give a different (and complete!) proof of Theorem 5.1, which says that the ciphertext produced by a one-time pad is uniformly distributed.

Let $m_1 \cdots m_n$ be the message, and let $\mathsf{K}_1, \ldots, \mathsf{K}_n$ be i.i.d. Bernoulli random variables with parameter 1/2 denoting the bits of the key. The ciphertext then consists of bits $\mathsf{C}_i = m_i \oplus \mathsf{K}_i$, which themselves are random variables. The claim is then that given bits $c_1, \ldots, c_n$, we have

$$P(\mathsf{C}_1 = c_1, \ldots, \mathsf{C}_n = c_n) = 2^{-n}.$$

Notice now that $m_i \oplus \mathsf{K}_i = c_i$ if and only if $\mathsf{K}_i = m_i \oplus c_i$. Since the K_i are independent, it thus follows that

$$\begin{aligned} P(\mathsf{C}_1 = c_1, \ldots, \mathsf{C}_n = c_n) &= P(m_1 \oplus \mathsf{K}_1 = c_1, \ldots, m_n \oplus \mathsf{K}_n = c_n) \\ &= P(\mathsf{K}_1 = m_1 \oplus c_1, \ldots, \mathsf{K}_n = m_n \oplus c_n) \\ &= \prod_{i=1}^{n} P(\mathsf{K}_i = m_i \oplus c_i) \\ &= 2^{-n} \end{aligned}$$

as desired.