

# Solution Sheet 14

*Cryptography and Security 2025*

## Solution 1 TCHO Encryption

1. The  $C(x)$  is a repetition of  $x$  and  $\mathcal{S}_\gamma$  generates bits which are biased towards 0. We can just look at the majority of  $C(x) + \mathcal{S}_\gamma(r')$  which is most likely to be equal to  $x$ . The complexity is  $\mathcal{O}(\ell)$ . There is however a probability of giving an incorrect result which is bounded by

$$p = \sum_{i=\frac{\ell}{2}}^{\ell} \binom{\ell}{i} \left(\frac{1}{2}(1+\gamma)\right)^i \left(\frac{1}{2}(1-\gamma)\right)^{\ell-i}$$

2. Since  $K(1) = w \bmod 2 = 1$  and is a multiple of  $P(1)$  we must have an odd number of nonzero terms in  $P(z)$ . It is easy to check if  $C(x) + \mathcal{L}_P(r)$  satisfies the linear relation defined by  $P(z)$  or its opposite by just looking at the first  $d$  terms. The complexity is  $\mathcal{O}(d)$ .
3. From the definition of  $K \otimes y$  we can see that  $(K \otimes C(x))_i = K(x) \bmod 2$  for all  $i$ . Since  $w$  is odd, we have  $K(x) \bmod 2 = x$  so  $K \otimes C(x) = (x, x, \dots, x)$ .
4. Let  $y = \mathcal{L}_P(r)$ . Since  $K(z)$  is a multiple of  $p(z)$ , let us write  $K(z) = P(z)Q(z)$ . We have  $K_s = \sum_{i+j=s} P_i Q_j$  so

$$(K \otimes y)_t = \sum_{i,j} y_{t+i+j} P_i Q_j = \sum_j \sum_{i=0}^d y_{t+i+j} P_i$$

Clearly, we have  $\sum_{i=0}^d y_{t+i+j} P_i = 0$  for all  $j$  and  $t$ . So,  $K \otimes \mathcal{L}_P(r) = 0$ .

5. For any  $i$ ,  $(K \otimes \mathcal{S}_\gamma(r'))_i$  is the XOR of exactly  $w$  independent bits of bias  $\gamma$  so it has a bias of  $\gamma^w$ . Indeed, if  $b$  is a random bit of bias  $\gamma$ , it means that the probability of being 0 is  $\frac{1}{2}(1+\gamma)$  so  $\gamma = E((-1)^b)$ . If  $b_1, \dots, b_w$  are independent of bias  $\gamma$  we have

$$E((-1)^{b_1 \oplus \dots \oplus b_w}) = E((-1)^{b_1 + \dots + b_w}) = E((-1)^{b_1}) \times \dots \times E((-1)^{b_w})$$

Due to the independence, this is  $E((-1)^{b_1}) \dots E((-1)^{b_w}) = \gamma^w$ .

6. We compute  $K \otimes \text{Enc}_P(x; r, r')$  in time  $\mathcal{O}(d_K \ell)$ . Due to the previous questions, this must be equal to  $(x, x, \dots, x) + K \otimes \mathcal{S}_\gamma(r')$ . Assuming that  $\gamma^w$  is not too small and that  $\ell - d_K$  is large enough, we can recover  $x$  by computing the majority. The complexity is  $\mathcal{O}(d_K \ell)$ .
7. We compute a list of many  $1 + \sum_{j=1}^{\frac{w-1}{2}} z^{ij} \bmod P(z)$  and another list of many  $\sum_{j=\frac{w-1}{2}+1}^{w-1} z^{ij} \bmod P(z)$  and look for matching. This works with complexity  $\mathcal{O}(2^{\frac{w-1}{2}})$  which is not polynomial.