Exercise Sheet 14

Cryptography and Security 2022

Exercise 1 TCHO Encryption

The goal of the exercise is to study the TCHO public-key cryptosystem.

- We consider the usual $+$ and $\times$ operations in $\mathbf{Z}_2$.
- The plaintext space is $\{0,1\}$ (we encrypt a single bit) and the ciphertext space is $\{0,1\}^\ell$ (the ciphertexts are ℓ-bit long).
- The public key is an irreducible polynomial of degree d with coefficients in $\mathbf{Z}_2$ denoted $P(z) = P_0 + P_1 z + \cdots + P_d z^d$.
- The secret key is a polynomial of degree d_K with coefficients in $\mathbf{Z}_2$ denoted $K(z) = K_0 + K_1 z + \cdots + K_{d_K} z^{d_K}$.
- These two polynomials are such that:
  - $P(z)$ divides $K(z)$ in $\mathbf{Z}_2[z]$;
  - $K(z)$ has a total number w of nonzero coefficients which is low. We assume that w is odd.
- We define four elementary operations.
  - **Repetition:** Given a plaintext x, we define the ℓ-bit vector $C(x) = (x, \ldots, x)$ (all components of $C(x)$ are equal to x).
  - **LFSR:** Given a d-bit vector $r = (r_0, r_1, \ldots, r_{d-1})$, we define its expansion to an ℓ-bit vector $(\ell > d)$ by using the relation

    $$r_{i+d} = \sum_{j=0}^{d-1} r_{i+j} P_j$$

    for $i = 0, \ldots, \ell - 1 - d$ in $\mathbf{Z}_2$.
    Note that this relation is linear. We let $\mathcal{L}_P(r) = (r_0, r_1, \ldots, r_{\ell-1})$.
  - **Biased sequence:** Given a random seed r' we define $\mathcal{S}_\gamma(r')$ as a random ℓ-bit string such that the probability that each bit is 0 is given by $\frac{1+\gamma}{2}$ (its probability of being 1 is thus $\frac{1-\gamma}{2}$).
  - **Cancellation:** Given $y \in \mathbf{Z}_2^\ell$, we define $K \otimes y \in \mathbf{Z}_2^{\ell - d_K}$ by

    $$(K \otimes y)_i = \sum_{j=0}^{d_K} y_{i+j} K_j$$

    for $i = 0, \ldots, \ell - 1 - d_K$ in $\mathbf{Z}_2$.
- **Encryption:** To encrypt the bit x with randomness r and r', compute:

  $$\mathsf{Enc}_P(x; r, r') = C(x) + \mathcal{L}_P(r) + \mathcal{S}_\gamma(r')$$

  with component-wise addition over $\mathbf{Z}_2$.

1. Show that given $C(x) + \mathcal{S}_\gamma(r')$, the plaintext x can be recovered if γ is not too small. What is the complexity of the attack in terms of ℓ?

2. Show that given $C(x) + \mathcal{L}_P(r)$, the plaintext x can be recovered. What is the complexity of the attack in terms of d?

3. Show that for any $x \in \mathbf{Z}_2$ we have $K \otimes C(x) = (x, x, \ldots, x)$.

4. Show that for any $r \in \mathbf{Z}_2^d$ we have $K \otimes \mathcal{L}_P(r) = 0$.

5. Show that for a random r' all bits of $K \otimes \mathcal{S}_\gamma(r')$ have the same distribution and a probability of being 0 of $\frac{1}{2}(1 + \gamma^w)$.
   Hint: For any i, $(K \otimes \mathcal{S}_\gamma(r'))_i$ is the XOR of exactly w independent bits of bias γ.

6. Given $\mathsf{Enc}_P(x; r, r')$ and $K(z)$, give an algorithm to recover x. What is its complexity in terms of the parameters d_K and ℓ?

7. To study the security, give an algorithm to recover $K(z)$ given $P(z)$, d_K and w. What is its complexity?
   Hint: if $K(z) = 1 + \sum_{j=1}^{w-1} z^{i_j}$, it satisfies a condition which can be written

$$1 + \sum_{j=1}^{\frac{w-1}{2}} z^{i_j} = \sum_{j=\frac{w-1}{2}+1}^{w-1} z^{i_j} \pmod{P(z)}$$