PET-bootcamp example exam questions

January 2025

The following are example questions (and answers) for the PET-bootcamp exam. Do note these questions only cover a subset of the material of the course. The actual exam will cover more topics.

1 Differential Privacy

Recall that a mapping $M : \mathcal{X} \to \mathcal{Y}$ is ε-differentially private if for all output subsets $S \subseteq \mathcal{Y}$ and pairs of neighboring databases $D, D' \in \mathcal{X}$ where $d_H(D, D') = 1$ it holds that

$$Pr[M(D) \in S] \leq e^{\varepsilon} Pr[M(D') \in S] \ . \tag{1}$$

Suppose now that the output set $\mathcal{Y}$ is *finite*. Then, prove that the following alternative definition is equivalent to the standard ε-differential privacy definition given above: for all output *elements* $y \in \mathcal{Y}$ and pairs of neighboring databases $D, D' \in \mathcal{X}$ where $d_H(D, D') = 1$ it holds that

$$Pr[M(D) = y] \leq e^{\varepsilon} Pr[M(D') = y] \ . \tag{2}$$

To prove equivalence, you need to prove first that the standard definition implies the alternative one, and then that alternative definition implies the standard one.

Answer. Obviously, the standard definition implies the alternative one: if Inequality (1) holds for all subsets $S \subseteq \mathcal{Y}$, then it also holds for singleton subsets of the form $S = \{y\}$, for all $y \in \mathcal{Y}$.

For the opposite direction, suppose that Inequality (2) holds for all neighboring datasets $D, D' \in \mathcal{X}$. Since $\mathcal{Y}$ is finite, for all subsets $S \subseteq \mathcal{Y}$ it holds that:

$$Pr[M(D) \in S] = \sum_{s \in S} Pr[M(D) = s] \ . \tag{3}$$

By applying Inequality (2), from (3) it follows that:

$$Pr[M(D) \in S] = \sum_{s \in S} Pr[M(D) = s] \leq \sum_{s \in S} e^{\varepsilon} Pr[M(D') = s] \ . \tag{4}$$

But now, the right hand side of Inequality (4) can be rewritten as:

$$\sum_{s \in S} e^{\varepsilon} Pr[M(D') = s] = e^{\varepsilon} \sum_{s \in S} Pr[M(D') = s] = e^{\varepsilon} Pr[M(D') \in S] \ . \tag{5}$$

Therefore, putting together the left hand side of inequality (4) with the right hand side of equation (5) we obtain:

$$Pr[M(D) \in S] \leq e^{\varepsilon} Pr[M(D') \in S] \ , \tag{6}$$

which is exactly Inequality (1) arising for the standard definition of ε-differential privacy.

2 Secret sharing

Suppose we do Shamir secret sharing in $\mathbb{Z}_{13}$ with 3 players and threshold 2.

- The players secretly share secret A through polynomial $p_A(x) = 4 + 5x$.
- The players secretly share secret B through polynomial $p_A(x) = 7 + 3x$.

(a) What is the value of secrets A and B?

(b) What are the shares of the 3 players for secrets A and B?

(c) How can the players securely compute a secret sharing of $A + B$? In particular: what do they need to compute and/or communicatie, and what does the polynomial p_{A+B} look like?

Answer.

(a) The secret is the polynomial evaluated at $x = 0$, so $A = 4$ and $B = 7$.

(b) The share of player $i = 1, 2, 3$ is the polynomial evaluated at i, so the share of player 1 is $p_A(1) = 4+5 = 9$; the share of player 2 is $p_A(2) = 4+5*2 = 14 = 1 \bmod 13$; the share of player 3 is $p_A(3) = 4+5*3 = 19 = 6 \bmod 13$. The same for B: $p_B(1) = 7 + 3 = 10$; $p_B(2) = 7 + 3 * 2 = 13 = 0 \bmod 13$; $p_B(3) = 7 + 3 * 3 = 16 = 3 \bmod 13$.

(c) The players need to locally add their shares: $p_{A+B}(1) = p_A(1) + p_B(1) = 9+10 = 19 = 6 \bmod 13$; $p_{A+B}(2) = p_A(2)+p_B(2) = 1+0 = 1$; $p_{A+B}(3) = p_A(3) + p_B(3) = 6 + 3 = 9$.
There is no communication needed for addition. The new polynomial is $p_A(x) + p_B(x) = 11 + 8x$.

3 Homomorphic Encryption

The textbook RSA cryptosystem is partially homomorphic. Recall for textbook RSA the encryption algorithm described as follows:
Given the public key (n, e) a message $m \in \mathbb{Z}_n$ is encrypted as follows:

$$c = m^e \bmod n$$

(a) Explain what partially homomorphic encryption property is. You might use the RSA cryptosystem described above for your explanation. Highlight the difference between a fully homomorphic and a partially homomorphic encryption scheme.

(b) Consider two ciphertexts $c_1 = m_1^e \bmod n$ and $c_2 = m_2^e \bmod n$ with $m_1, m_2 \in \mathbb{Z}_n$. Show with these ciphertexts c_1 and c_2 that RSA is multiplicative homomorphic.

Answer.

(a) A partially homomorphic encryption scheme supports one type of operations over ciphertexts without intermediate decryption. In the case of RSA, we can multiply two ciphertexts, and the decryption of this multiplication result is the product of the two underlying plaintexts. A fully homomorphic encryption scheme does not only support one type of operation over ciphertexts (for example multiplication as for RSA) but at least two (for example addition as well), such that arbitrary circuits can be evaluated over ciphertexts without intermediate decryption.

(b) We can see from $c_1 \cdot c_2 \bmod n = m_1^e \cdot m_2^e \bmod n = (m_1 \cdot m_2)^e \bmod n$ that the product of the ciphertexts results in a ciphertext of the underlying plaintexts. Thus, RSA is multiplicative homomorphic as explained in part (a).

4 Zero-knowledge proofs

What properties does a of zero-knowledge proof have? Provide a brief explanation of each of the properties.

Answer. Properties

- *Completeness* If the statement is true, an honest prover will always be able to convince an honest verifier. This assures the validity of the proof when the statement is correct.
- *Soundness* This principle ensures that if the prover is trying to deceive the verifier with a false statement, they will fail to convince the verifier with high probability. It's a measure of the system's resistance to fraudulent proofs.

- *Zero-knowledge* The verifier learns nothing other than the fact that the statement is true. The proof does not reveal any other information, including any details about how the statement is true.