Indian Institute of Technology, Kanpur
Computer Science and Engineering
Assignment 1
CS670: Cryptographic Techniques for Privacy Preservation

Instructor: Adithya Vadapalli

06/10/2025

This assignment is long! Please start early. Doing this assignment correctly is very important, as every other assignment will be built on this.

Deadline: October 17th, 2025, EOD on Hello IITK. No Extension will be given.

In assn 3 will have to update items : $v_0[j] = v_1[j] + \dots$

↳ some dot product dp.

In assn 2 the person downloading the item will be creating a dpf., → they will make it so that jth value is dp.

$V_0[j] \leftarrow V_0 + \text{Evalfull}(k_0)$ (same for v_1)

↳ but the user should not know dp ∴ this is not it?

→ Make sure assn 2 code is well modularized so that assgn 3 doesn't take time. → In assgn 2 do this for random m, make sure this can be done

In assn 3 : 1.) Create a DPF s.t. $m = 0$ { If you evaluate this dpf you should get no updates takes place }

2.) Let the final c.w. of the above dpf be fcw.

↳ client knows

3.) Secret share fcw among 2 servers : S_0 : FCW_0 , S_1 : FCW_1

↳ can get every layer except last layer.

$$\begin{tikzcd}[column sep=huge]
\begin{matrix} S_0 \\ FCW_0 \\ DP_0 \end{matrix} \arrow[r, shift right, "DP_0 + FCW_0"'] \arrow[d] & \begin{matrix} S_1 \\ FCW_1 \\ DP_1 \end{matrix} \arrow[l, shift right, "DP_1 + FCW_1"'] \arrow[d] \\
DP+FCW & DP+FCW
\end{tikzcd}$$

Now they will use this DP+ FCW ~~to~~ as final correction word, to get a dpf with DP as value.

* generate shares of dpf the same way as assign 1.

$$\frac{DP+FCW}{2} + \frac{DP+FCW}{2}$$

$$2DP +$$

Academic Integrity You have to do the assignment individually. You are encouraged to ask the instructor for help. Sign up on Piazza to ask for help: `https://piazza.com/iitk.ac.in/firstsemester2025/cs670`. Students can should come to the Instructor's office hours for help in coding. However, copying code from others or using AI tools without understanding the solution is not allowed and will result in 0 marks for the assignment. Students may be asked to explain their code and solution during evaluation.

Objective Write a C++ program named `gen_queries.cpp` that generates Distributed Point Function (DPF) queries and verifies their correctness.

Specifications:

1. **Program Name:** `gen_queries.cpp`
2. **Command-Line Arguments:**

   ```
   ./gen_queries <DPF_size> <num_DPFs>
   ```

   - `<DPF_size>`: Size of each DPF (domain size).
   - `<num_DPFs>`: Number of DPF instances to generate.
3. **Functionality:**
   - For each DPF:
     - Randomly choose an **index (location)** within the DPF's domain.
     - Randomly choose a **target value** for that index (this will be determined by the final correction word).
     - Call your `generateDPF()` function to generate the DPF keys.
   - Save or print the generated DPF queries as appropriate.
4. **Correctness Testing (`EvalFull` function):**
   - Implement a function named `EvalFull()` that:
     - Evaluates the DPF across all domain points for both keys.
     - Combines the outputs and checks if they reconstruct the correct target value at the chosen index, and zero elsewhere.
     - Prints `"Test Passed"` if the evaluation is correct and `"Test Failed"` otherwise.
5. **Implementation Notes:**
   - Use a cryptographically secure random generator (e.g., `std::random_device` and `std::mt19937_64`)
   - Keep the DPF interface modular:
     - `generateDPF(location, value)`
     - `evalDPF(key, index)`

    - `EvalFull(key, size)`

6. **Example Usage:**

   ```
   ./gen_queries 1024 10
   ```

   This should generate 10 DPFs, each of size 1024, test their correctness using `EvalFull`, and print the results.

Grading

- Correctness and Security: 80%
- Code clarity and documentation: 20%