IT Security 2024/2025
Exercise Sheet 13
– Anonymization & Secure Multiparty Computation –

Markus Krämer

Publication: 16.01.2024
Deadline: 22.01.2024 10:00

Lightning Survey ⚡

Exercise 1 (Privacy Models, optional)**.** Look at the following table and write your answer into `anonymization.txt`.

Name	ID	Gender	Adress	City	Years	Position	Illness
Dieter	1	m	Main Street 1	53115 Bonn	20	CEO	Cancer
Flo	2	m	Beach Club 7	53121 Bonn	2	Worker	flu
Maren	3	f	Main Street 3	53115 Bonn	17	Secretary	flu
Martin	4	m	Avenue 27	53121 Bonn	1	Worker	flu
Doris	5	f	Boulevard 4	53115 Bonn	18	accounting	flu
Heinz	6	m	Avenue 77	53121 Bonn	12	management	flu
Lisa	7	f	Main Street 64	53332 Bornheim	8	Worker	Cancer
Laura	8	f	Avenue 34	53489 Sinzig	9	Worker	Cancer
Horst	9	m	Main Street 10	53115 Bonn	19	management	Cancer
Emil	10	m	Beach Club 3	53121 Bonn	4	Worker	flu
Carsten	11	m	Beach Club 13	53121 Bonn	14	management	flu
Yvonne	12	f	Main Street 3	53115 Bonn	16	accounting	Cancer

(1) Define the following terms: Direct identifier, quasi identifier, sensitive attribute

(2) Name the identifiers, quasi-identifiers and sensitive attributes of the employees table

(3) Turn it into a k-anonymous table

(4) Turn it into a l-diverse table

(5) Does your table support t-closeness?

Exercise 2 (Privacy beyond t-closeness, optional)**.** Define the following privacy models and write your answer into `privacy-models.txt`.

(1) k-map

(2) k^m-anonymity

(3) Average risk

(4) Population uniqueness

(5) δ-disclosure privacy

Exercise 3 (True/False Questions, 3 points)**.** Mark these statements as true or false in `smc.yml`.

(1) In the prosecutor model honest parties get a reward

(2) For reaching l-diversity, all l sensitive attributes of a data-set must occur in an equivalence class

(3) Unsorted matching attacks are possible because vulnerable anonymized data-sets had not been permuted

(4) In SMC, the number of participating parties is limited to two

(5) In OT_2^1 Bob gets to know only one message

(6) In GC, Bob shares his input labels with Alice

(7) Free-XOR is compatible with half-gates

(8) GC are secure under the Malicious Model

(9) In GRR_3 the number of gates is reduced from four to three

Exercise 4 (Garbled Circuits, optional)**.** Get familiar with libraries for garbled circuits. Write your answers into `gc-libraries.txt`.

(1) Make yourself familiar with the library Fairplay[1] How is the library working? Explain the parties and how a written program is turned into a working process. Explain the SHDL language.

(2) Which gate types are supported. Give examples for at least three gate types, written in SHDL.

(3) What is the Bristol Fashion Format[2]? Which types of gates can be handled? Give an example for each gate type

(4) Make yourself familiar with the library JIGG[3]. Which parties exist and how are they working together? Which optimizations are supported?

Exercise 5 (Garbled Circuits, 7 points)**.** Implement the boolean circuit in Figure 1.

(1) Implement the circuit in Fairplay and use the SHDL language. (4P) Submit both files `fairplay.Opt.fmt` and `fairplay.Opt.circuit`.

(2) Implement the circuit in JIGG. Submit it as `jigg.txt`. (3P)

(3) Construct a truth table and explain the output of the circuit. Write your answer into `truth.txt`.

[1] https://www.cs.huji.ac.il/project/Fairplay/Fairplay.html
[2] https://nigelsmart.github.io/MPC-Circuits/
[3] https://github.com/multiparty/jigg

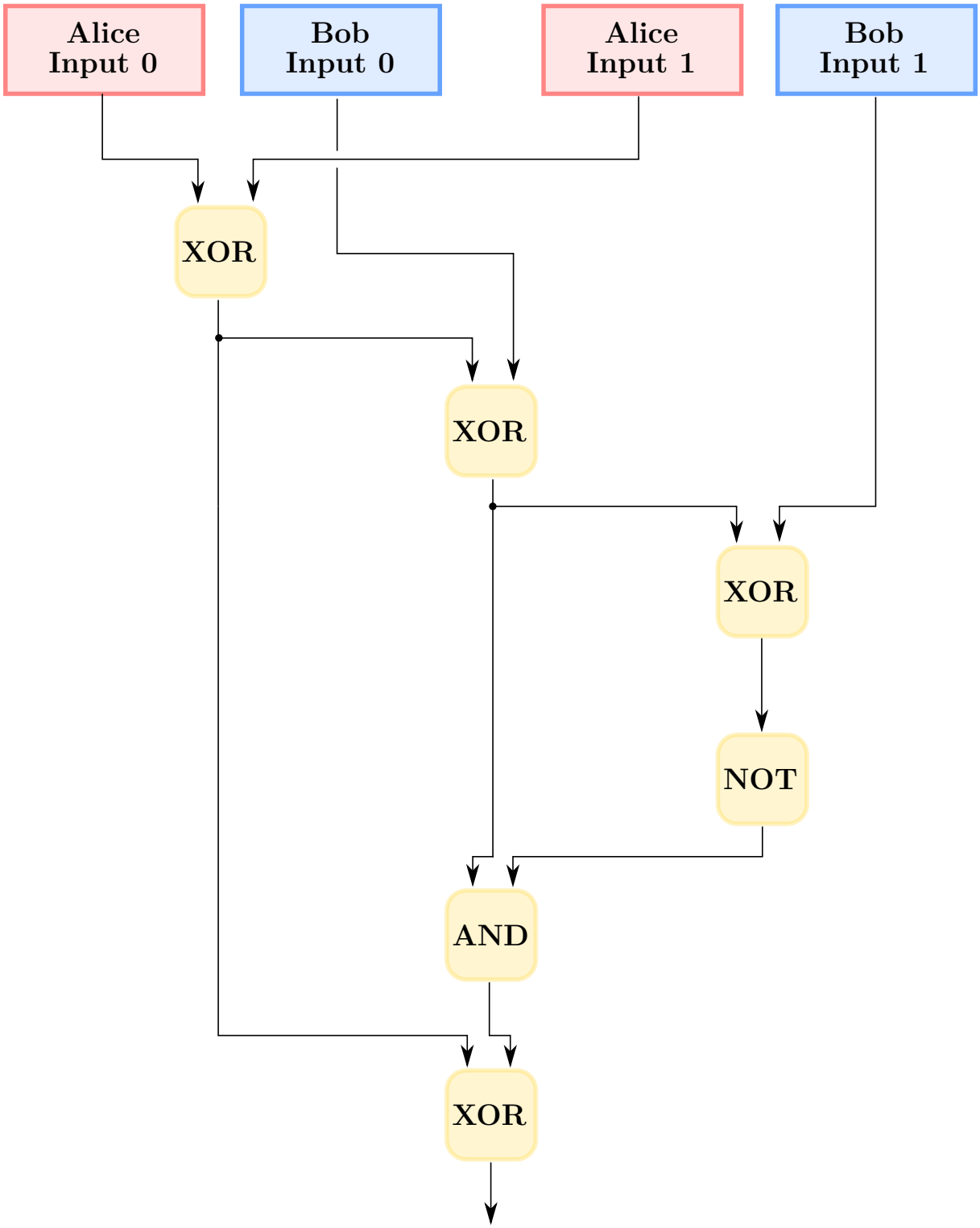

Figure 1: Boolean Circuit