Question 1: Anonymous communications

Mario and Luigi are taking an online exam for which they are sitting in the same room. As in any exam, they are not allowed to communicate. The professor has informed the students that the WiFi LAN in the room, which students are obliged to be connected to, is being monitored for the use of messaging activities. To circumvent this prohibition, Mario and Luigi have installed P2PM, a peer-to-peer messaging application that allows them to send messages to each other without an intermediary server. To ensure that the monitoring for messaging applications does not detect their messages sent using P2PM, Mario and Luigi configure the app to send messages over the Tor network. Then, they use the app throughout the exam to help each other with the questions.

Part A – After the exam Mario and Luigi receive a note from the professor saying "*We told you not to communicate during the exam. You now get a 0 in the course*". Explain how the professor knows they communicated, indicating which capabilities let the professor make this inference.

Part B – After receiving the note from the professor, Mario tells Luigi "*I knew this was a bad idea! We should have configured P2PM to use Crowds! We would not have been caught*". Agree or disagree with Mario's statement and justify why.

Part C – Would Mixnets or DC networks enable Mario and Luigi to discuss questions during the exam without the professor (with capabilities you highlighted in part A) noticing? Justify your answer, explaining under which circumstances each mechanism would be suitable or why it wouldn't work.

Question 2: Location privacy

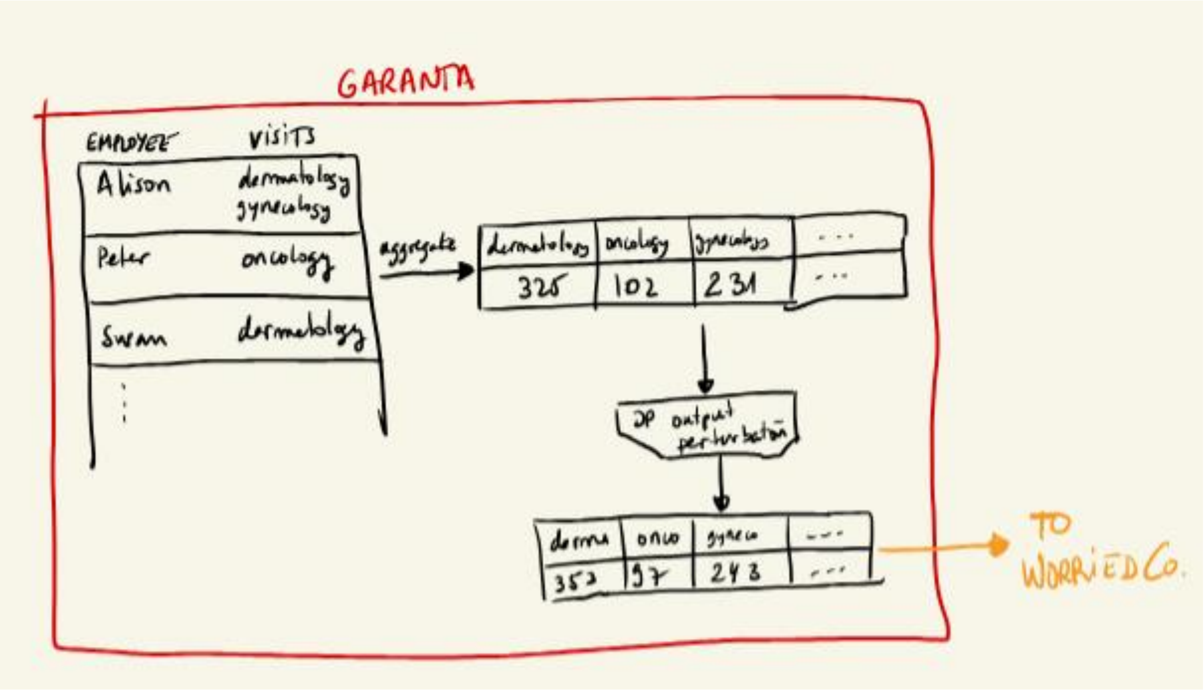
Cigros is a credit-card-only supermarket chain, i.e., clients can only pay with their credit cards. To optimize their product placement inside their stores, Cigros decides to track customers while they shop. To alleviate privacy concerns, Cigros places infrared cameras to cover 100% of the shop. These cameras do not allow Cigros to recognize faces, but Cigros can still see how people move across aisles and which products they take. Cigros claims that customers stay anonymous, and Cigros cannot know where specific customers were inside the supermarket.

Part A – Describe an attack that, given the information available to Cigros mentioned in the question, enables Cigros to profile customers based on all their interests, for example to send them targeted advertisements of products that they examined but did not buy. Your description must include the capabilities that enable Cigros to carry out such an attack.

Part B – Would your attack work even if Cigros changes to have only payments by cash? What privacy properties could customers retain?

Question 3: Private reports

Worried Co. is worried about the health of their employees. They partner with Garanta, the insurance company that insures all Worried Co. employees, to obtain statistics about doctor visits. Every month, Garanta aggregates the records of all employees to compute the total number of doctor visits per medical specialization (e.g., dermatology, gynecology, ...) and reports them to Worried Co.



Part A – To ensure privacy towards employees of Worried Co., Garanta only returns aggregated statistics per specialization and uses differentially-private output perturbation before publishing the statistics. Does output perturbation protect the privacy of the employees in this scenario? If yes, explain how Garanta would configure a differentially-private mechanism to release the aggregated statistics per specialization. Your explanation should include how each parameter is chosen and why. If not, explain why differentially-private output perturbation is not a desirable choice in terms of privacy protection and how private information could leak.

Part B – Worried Co. proposes to Garanta an alternative mechanism to obtain fine-grained statistics about doctor visits. Under this mechanism, each employee uses Tor to hide network-layer information and send to Garanta a vector of visits per specialization. Once they receive data from all employees, Garanta then sends a list with all the anonymized vectors to Worried Co.

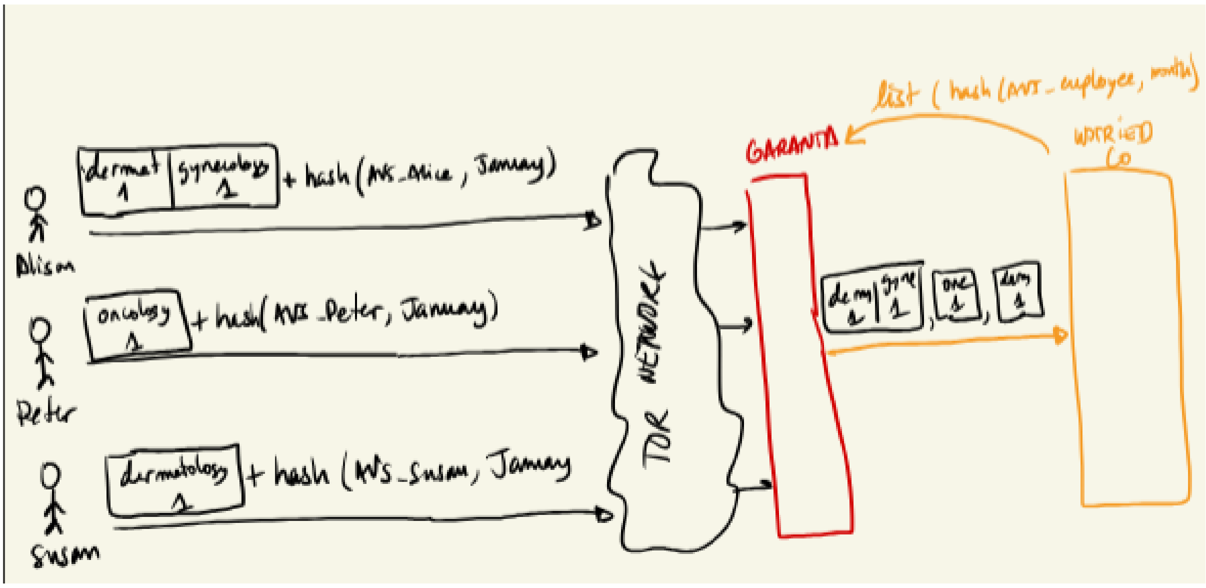
To avoid fake reports, Worried Co. wants to decide between two authorization mechanisms:

1) The company gives each employee 12 codes, one for each month of the year. The employees send the code along with the vector of visits each month. The codes are computed as follows:
`Code_of_the_month = Hash(AVS_employee||enrolment_date||month);` where, *AVS_employee* denotes the AVS number of the employee,

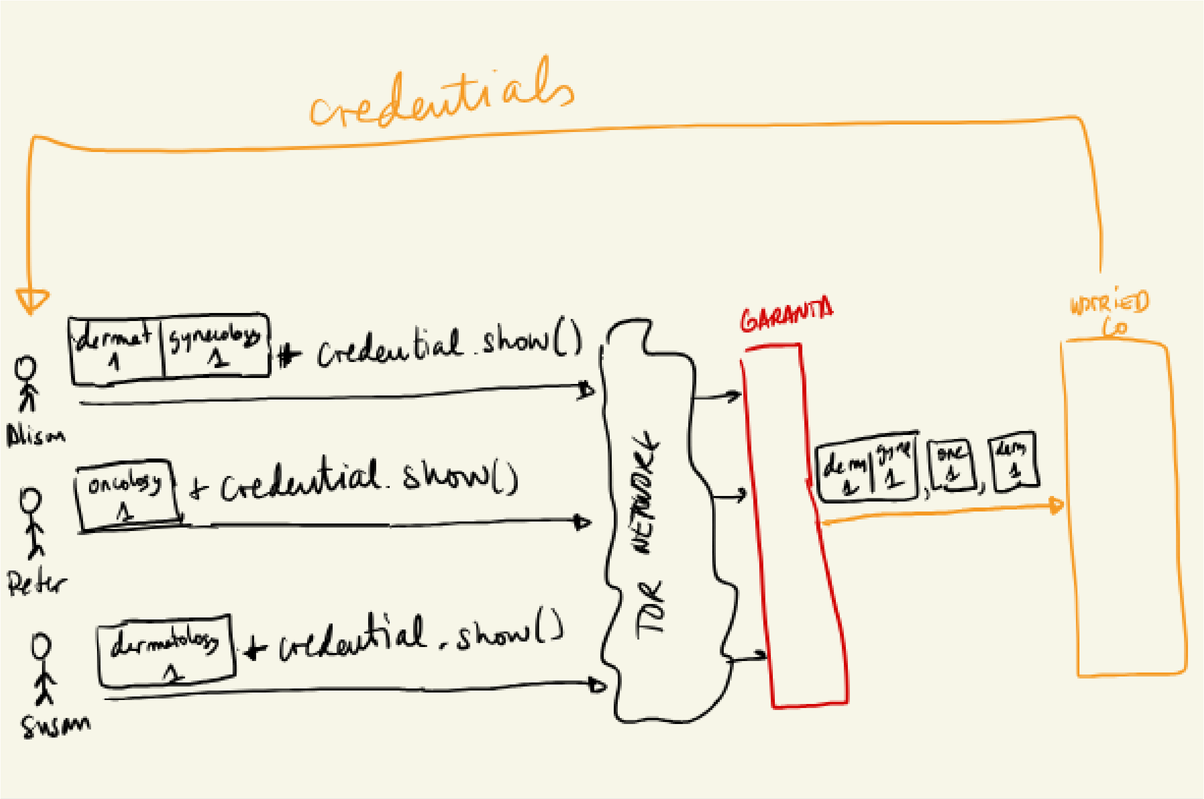
enrolment_date denotes the day the employee started working at Worried Co., *month* denotes the month during which the code is valid.

Worried Co. gives Garanta the list of all valid codes. Garanta uses this list to check that employees are authorized to send the report via the code sent with it.

THE IMAGE NEEDS TO BE REDONE WITH DATE_ENROLMENT



2) Worried Co. issues each employee an anonymous credential per month. Employees use these credentials to show to Garanta they are authorized to submit a vector for the current month.



Assuming the anonymous credentials are correctly implemented and the hash function is cryptographically secure, compare these two mechanisms in terms of: unforgeability, issuer unlinkability and verifier unlinkability. Your explanation must explicitly state who is the issuer and who is the verifier in your context, and what assumptions you have on their capabilities.

Note: The AVS number is the Swiss social security number, which is known to the employers and insurers of any person in addition to the person itself.