Cryptographic Randomised Response Techniques

Mrinal Nandi
West Bengal State University, Barasat, India
International Crypto-Webinar
Acknowledgement: Prof. Palash Sarkar, ISI, Kolkata

27th August, 2020

Some Sensitive Questions

- Are you a smoker?
- Did you take drug in past?
- Have you taken bribes in the past?
- Have you avoided paying income tax?
- Do you believe in the supremacy of upper castes?
- Do you drink alcohol?

Survey on Sensitive Questions

- All of these questions, have Boolean (yes/no) answers.
- Population is divided into yes/no groups.
- The purpose of a survey would be to estimate the yes/no proportions.
- For each question, one may not answer or answer incorrectly for different fear.

Estimate a variable

- If you ask a school students that, How much money you carry with you?
- The answer is a variable.
- The purpose of a survey would be to estimate the average of the money carrying by a group of people.
- One may declined to give the answer.

How to estimate?

- Estimate a variable.
- sum of two random numbers X and Y is a random number with $E(X+Y)=E(X)+E(Y)$
- So if we know $E(X+Y)$ and $E(X)$ we can find $E(Y)$ without knowing Y.
- How to estimate a boolean variable.

Randomized Response Technique: Warner (1965)

- Simple formulation: Toss a coin; answer 'yes' if it comes up tails; answer correctly if it comes up heads.
- Consider the 'no'-group among the respondents; about half of them will get tails and answer 'yes'; the other half will answer truthfully and say 'no'.
- So, if $x\%$ of the answers are 'no', then among the respondents about $2x\%$ are actually 'no'.
- The interviewer gets the desired estimate.
- Possible deniability: respondents answering 'yes' can claim that the coin came up tails.

Warner's Formulation

- A responder tells the truth with some fixed pre-determined probability $p > 1/2$ and lies with probability $(1 - p)$.
  For example, roll a die; lie if it comes up 1 or 2; otherwise tell the truth.
- Suppose among n respondents, x is the size of the 'yes'-group and R is the random variable counting the actual number of 'yes' responses.
- Then $E(R) = px + (1 - p)(n - x)$ and so $x = \frac{E(R) - n(1-p)}{2p-1}$.
  R is an estimate for $E(R)$; given R, we can estimate x.

Other Formulations

- **Innocuous(not related with the survey) question:** truthfully answer the question with probability p and with probability $(1 - p)$ answer an unrelated innocuous question such as
- 'flip a coin: did you get tails?'.
- Is your birth day falls between 1st January and 30th June?

Polychotomous RRT

- A respondent can belong to one of m mutually exclusive groups. Suppose π_i is the proportion of people who belong to group i.
- Choose probabilities $p_0, p_1, \ldots, p_m$, such that $p_0 + p_1 + \cdots + p_m = 1$; a respondent either reveals her true type with probability p_0 ; or answers i with probability p_i. Let q_i be the proportion of respondents who answer i; then $q_i = p_0\pi_i + p_i$ and so $\pi_i = \frac{q_i - p_i}{p_0}$.

Malicious Intentions

- Consider the following question:
  Do you believe in the supremacy of the upper castes?
- Those who do have such belief may wish to bias the outcome of the survey by always answering truthfully.
- Those who do not have such belief will follow the protocol honestly or may wish to bias the outcome of the survey by always answering truthfully..
- The outcome of the survey will be biased.
- Usual randomized response techniques will not work in this case.

(Cryptographic) RRT Protocol

- Two-party protocol: Interviewer and Responder.
- The responder has a private bit b.
- The parties exchange some information.
- At the end of the protocol, the interviewer gets to know a bit c which is equal to b with probability p and equal to $1 - c$ with probability $1 - p$.

Can be use for election

CRRT Protocol: Desired Properties

- **Deniability:** The responder should be able to claim with reasonable probability that the bit learned by the interviewer is not b.
- **Bounded Bias:** The probability that $c = b$ is at most p even if the responder maliciously deviates from the protocol.
  Ensures that the responder cannot bias the outcome of the protocol in any way other than changing its own secret bit.

Execution using TTP

- There is a trusted third party (TTP).
- The responder sends the secret bit b to TTP.
- The TTP generates a bit c such that $c = 0$ with probability $p (p > 1/2)$.
- The TTP provides the interviewer with the bit $b \oplus c$.
- If the responder is honest, then the interviewer gets b with probability p.

Security

Possible deniability: The responder can always claim that the secret bit was $1 \oplus b$.

Bounded bias:

- Suppose the responder sends a bit y to TTP which is equal to b with probability q.
- Then the TTP sends the bit $z = c \oplus y$ to the interviewer.
  $Pr[z = b] = qp + (1 - q)(1 - p)$; this probability is between $(1 - p)$ and p.

Real World

The goal of a real world protocol is to simulate the ideal world protocol without a TTP.
Behaviour of the parties.

- Honest-but-curious: follows the protocol honestly.
- Malicious: deviates from the protocol.

Real World CRRT Parties

Interviewer:

- Honest-but-curious: follows the protocol, but may perform computation to learn the secret bit of the responder.
- Malicious: can deviate from the protocol in an attempt to learn the secret bit of the responder.

Responder:

- Honest-but-curious: follows the protocol but is interested in learning the outcome of the survey.
- Malicious: can deviate from the protocol in an attempt to bias the outcome of the survey.

CRRT Schemes and Related Work

- H. Kikuchi, J. Akiyama, G. Nakamura and H. Gobioff. Stochastic Voting Protocol to Protect Voters Privacy. In 1999 IEEE Workshop on Internet Applications.
- A. Ambainis, M. Jakobsson and H. Lipmaa. Cryptographic Randomized Response Techniques. In Public Key Cryptography, 2004.
- T. Moran and M. Naor. Polling With Physical Envelopes: A Rigorous Analysis of a Human-Centric Protocol. In Eurocrypt 2006.
- P. Golle, F. McSherry and I. Mironov. Data Collection With Self-Enforcing Privacy. ACM Transactions on Information Systems and Security, 2008.
- M. Z. Ashrafi and S. K. Ng. Collusion-Resistant Anonymous Data Collection Method. ACM Conference on Knowledge Discovery and Data Mining, 2009.

Moran-Naor Physical CRRT Protocol-1

Requires physical envelop or scratch-off cards

Interviewer prepares card:

- A card has four scratch-able bubbles arranged in two rows of two bubbles each.
- In each row, the bubbles hide the words ‘yes’ and ‘no’.

Responder is given a card:

- Scratches a random bubble in each row.
- If opposing answers are revealed, then the responder scratches out the remaining bubble in the unfavoured row.
- If same answers are revealed, then the respondent picks a row at random and scratches out the remaining bubble in that row.

Interviewer gets back the scratched-off card:

- One row of the card is eliminated.
- Counts the result shown in the other row.

Moran-Naor Physical CRRT Protocol-1: Security Intuition

- In exactly 3/4 of the cases, the counted result will match the responder's intended result.
- Without invalidating the entire card, the responder cannot succeed with higher probability.

Possible Deniability: Responder can always claim that both rows were 'bad' and the result did not reflect the actual intention.

- Since the interviewer does not know which were the two bubbles that were scratched first, the responder's deniability cannot be refuted.
- Deniability is preserved even if the interviewer cheats. The only way to cheat without being unavoidable caught is to place the same answer under both bubbles in one of the rows. Considering the distribution of responses in all four cases (cheating/honest, yes/no) shows that this does not help the interviewer.

Moran-Naor Physical CRRT Protocol-1: Security Intuition

Bounded Bias: The responder learns the result before the interviewer and can decide to quit.

- Since the interviewer does not know the respondent's outcome, this has the effect of biasing the result of the poll.
- By counting the number of prematurely halted protocol executions, the interviewer can accurately estimate the number of cheating responders.

Moran-Naor Physical CRRT Protocol-2

Requires 'tamper-evident distinguishable' envelopes.
Respondent prepares envelopes:

- Takes three envelopes labeled '1', '2' and '3';
- Chooses one envelope at random and places the unfavoured answer in it;
- Places the favoured answer in the other two envelopes.

Moran-Naor Physical CRRT Protocol-2

Interviewer opens envelopes:

- Chooses a random envelope and opens it and reveals the card to the responder.
- Asks the responder to declare which of the other two envelopes contain a card with the opposite answer. Opens the indicated envelope.
  - If this envelope indeed has the opposite answer, then the interviewer records the answer on the first card and returns the third (unopened) envelope to the responder.
  - If both opened envelopes contain the same answer the interviewer opens the third envelope as well.
  - If the third envelope contains the opposite answer, the interviewer records the answer on the first card as the response to the poll.
  - If all three envelopes contain the same answer, with probability $2/3$, the interviewer records the answer appearing in the envelopes and with probability $1/3$ records the opposite answer.

Moran-Naor Physical CRRT Protocol-2: Security Intuition

Bounded Bias: Responder gets her wish with probability $2/3$ no matter what she does.

- Envelopes correctly filled up: the interviewer chooses the non-favourable envelope with probability $1/3$.
- All envelopes have the same answer: the interviewer chooses the opposite answer with probability $1/3$.

Moran-Naor Physical CRRT Protocol-2: Security Intuition

Possible Deniability:

- The interviewer can open all three envelopes. But, then the responder can see that the seal on the returned envelope has been broken and know that the interviewer was cheating.
- The interviewer can open two envelopes before telling the responder which of the two was opened first. The interviewer hopes that the responder will not ask him to return the opened envelope.

Summary

- Motivation for RRT and the issue of maliciously behaving parties.
- Informal idea of security of CRRT.
- Brief descriptions of the Moran-Naor protocols for CRRT using physical devices.

Future work:

- CRRT is a meeting point of statistics and cryptography and few works have been done so far.
- How to capture cryptographic aspects of more complicated RRT scenarios, such as polychotomous RRT?
- Actual implementation and deployment of any CRRT protocol.

Any question?

Thank you . . .