The channel coding theorem and the security of binary randomization

Poorvi Vora
Hewlett-Packard Co.

Context: Theory of variable privacy

- Theory of security allows binary choice for data revelation:
  - Bob is trusted/untrusted
  - If he is trusted, data is revealed to him using a perfect protocol
- Information leakage necessary for a number of interactions
  - Even the revelation of a sum using ZK protocols leaks information about the variables; this information is valuable to Bob and Alice
- Randomization can be used for personal privacy, in a "privacy market"

Randomization: binary-valued

HIV? $\xrightarrow[P(lie) = 1/3]{P(truth) = 2/3}$ Yes

stats. over many are accurate

After the protocol, the possibilities are skewed

the answer is most likely to be correct

Computationally and information-theoretically imperfect

Best measure so far [AA01]: change in entropy (mutual information)

Protocol as channel

Protocol Input: The truth value of "X has HIV"

Output: Perturbed value of the bit.
Probabilities: of truth: 2/3, of lie: 1/3

Put input bit through a communication channel with probability of error 1/3

Channel output indistinguishable from protocol output;
Tracker wishes efficient communication over channel
Capacity = maximum change in entropy

Attacks on randomization - repeating the question

- An attack: asking the same question many times
- Can be thwarted by
  - never answering the same question twice, or
  - always answering it the same.
- Query repetition:
  - corresponds to an error-correcting code word

    a a a a a a a
  - probability of error is monotonic decreasing with *n* for *n*-symbol code words
  - rate of code = 1/*n*

Error

Known that:

- tracker can reduce estimation error indefinitely
- by increasing the number of repeated queries indefinitely;

$$n \to \infty \Rightarrow \varepsilon_n \to 0$$

- and that this is the best he can do with repeated queries

$$\varepsilon_n \to 0 \Rightarrow \text{cost per data point} = n/1 \to \infty$$

Is the following an attack?

- Requested Bit 1: “location = North”;
- Requested Bit 2: “virus X test = positive”;
- Requested Bit 3: “gender = male” AND “muscular sclerosis = present”

If

(location = North) $\oplus$ (virus X test = positive)

$\Leftrightarrow$ (gender = male) AND (muscular sclerosis = present)

Then: A3 = A1$\oplus$A2; check-sum bit;

M = number of possible strings of interest; n = no. of queries

rate = $(\log_2 M)/n$ = 2/3 i.e., k/n

Deterministically-related query sequence (DRQS)

Theorem: *Channel codes are DRQS attacks and vice versa*

A code is

- a (binary) function from M message words to n code bits
- an estimation function *from* n bits *to* one of M message words

The only difference between codes and DRQS attacks is that the coding entity in the communication channel knows the bits

The tracker does not know the bits, but forces a pattern among them through the queries

What kind of information transfer do DRQS attacks provide?

Recall: repetition attack sacrificed rate (1/n) for accuracy

Does looking at more than one target bit at a time help the tracker?

Can he maintain the rate of a DRQS attack while decreasing estimation error?

i.e., Can he maintain k/n while $\varepsilon_n \rightarrow 0$

Shannon (1948) Channel Coding ("second") Theorem
Existence result; tight upper bound on transmission efficiency

(Really only weak law of large numbers)

Codes exist for reliable transmission at all rates below capacity

A channel cannot transmit reliably at rates above capacity.

Reliable transmission *defined as* decreasing error arbitrarily while maintaining rate

Existence of reliable DRQS attacks

- Shannon (1948): Codes exist for reliable transmission at all rates below capacity
- Forney (1966): Existence of polynomial-time encodable and decodable Shannon codes
- Spielman (1995): Construction of linear-time encodable and decodable codes approaching Shannon codes

$\Rightarrow$ Corollary: Construction methods for linear time DRQS attacks with k/n approaching $\mathcal{C}$ while $\varepsilon_n \rightarrow 0$

Types of attacks

- PRQS (Probabilistically-related Query Sequence) Attacks: Queries are probabilistically-related to required bits. *Most general*
- DRQS (Deterministically-related Query Sequence) Attacks: Queries are deterministically-related to required bits. *Among most efficient*
- Reliable attacks: maintain rate while increasing accuracy

Theorem: *The rate of a reliable PRQS attack is tightly bounded above by protocol capacity*

A channel cannot transmit reliably at rates above capacity

$\Rightarrow$ Corollary: The capacity of a protocol is the (tight) upper bound on the rate of a reliable DRQS attack.

$\Rightarrow$ While the protocol is not perfect, there is a cost to exploiting its non-perfectness

Bound also holds for: $\varepsilon_n \rightarrow 0$; adaptive, non-deterministic; also many other protocols

i.e. $\varepsilon_n \rightarrow 0 \Rightarrow \lim k/n \leq \mathcal{C}$

Theorem: *Lower bound on total queries for arbitrarily small error*

If requested bits are all independent, minimum queries when maximum rate:

Minimum no. of queries on average
= target entropy/maximum rate
= target entropy/channel capacity;

$$n \geq k/\mathcal{C} - \delta$$

Shown using the source-channel coding theorem which enables entropy to be addressed separately from the query pattern

We have shown that

The tracker can do better by
- increasing the number of points combined in a single query
- i.e. there exist attacks for which

$$n \rightarrow \infty \Rightarrow \varepsilon_n \rightarrow 0$$
$$\varepsilon_n \rightarrow 0 \not\Rightarrow n/k \rightarrow \infty$$

There is a tight lower bound on the limit of n/k such that

$$n \rightarrow \infty \Rightarrow \varepsilon_n \rightarrow 0$$

i.e, $(n \rightarrow \infty \Rightarrow \varepsilon_n \rightarrow 0) \Rightarrow \lim n/k > 1/\mathcal{C}$ Privacy measure
Recall: $\mathcal{C}$ is max. value of change in entropy

Why our approach is so powerful

- All other information-theoretic approaches stop with the notion of entropy, and do not approach the notion of a channel
- All they provide access to is Shannon's first (source coding) theorem

"entropy is the minimum number of bits required, on average, to represent a random variable"

- Communication channels provide access to other work on both information theory and coding
- Clearly just a beginning

This work was influenced by conversations with

Umesh Vazirani

Gadiel Seroussi

Cormac Herley