The Privacy of Tracing Traitors

Moni Naor*
Weizmann Institute of Science

In this talk I will explore a connection between **traitor tracing** schemes and the problem of **sanitizing** data to remove personal information while allowing statistically meaningful information to be released. It is based on joint work with Cynthia Dwork, Omer Reingold, Guy N. Rothblum and Salil Vadhan [5]

Traitor tracing schemes are method of content distribution which enable a publisher to trace a pirate decryption box to a secret key (of a treacherous user) that was used to create the box. For example, consider a content provider who wishes to broadcast his content to a group of subscribers. To do this, he gives each of the subscribers a decryption box that uses a secret key. Unfortunately, a subscriber might now build and distribute a pirate decoder. Traitor tracing schemes ensure that if such a pirate decoding box is found, the content distributer can run a *tracing* algorithm to recover at least one private key used to create the box, and perhaps try to take legal action against this subscriber. Tracing schemes were first formally introduced by Chor, Fiat and Naor [4] and there are many constructions with various choices of the parameters (see [2] for recent references).

Consider **private data analysis** in the setting in which a trusted and trustworthy curator, having obtained a large data set containing private information, releases to the public a "sanitization" of the data set that simultaneously protects the privacy of the individual contributors of data and offers utility to the data analyst. The sanitization may be in the form of an arbitrary data structure, accompanied by a computational procedure for determining approximate answers to queries on the original data set. Alternatively it may be in the form of a "synthetic data set" consisting of data items drawn from the same universe as items in the original data set; queries are carried out as if the synthetic data set were the actual input.

The "gold standard" of privacy that has emerged in recent years is that of *differential privacy*: for any two neighboring data sets, one containing information about an individual and the other one not containing it, for any possible string released by the curator it should be difficult distinguish which of the two possible data sets yielded that response.

Recently there have been several powerful results showing that it is possible to sanitize data sets while allowing relatively accurate answers to queries. For instance, Blum, Ligett and Roth (STOC '08) showed the following: Let X be a universe of data items and $\mathcal{C}$ be a "concept" class consisting of efficiently computable functions $f : X \to \{0, 1\}$. Given a database $x \in X^n$, it is possible to obtain a *synthetic database* that remarkably maintains approximately correct fractional counts for *all* concepts in $\mathcal{C}$, while ensuring a strong privacy guarantee in the above sense.

The downside is that resulting mechanism is *not*, in general, computationally efficient and the natural question is whether it possible to obtain efficient solutions. It turns out that this question has deep connections to cryptography. When either $|\mathcal{C}|$ or $|X|$ are superpolynomial and assuming the existence of one-way functions there exist distributions on data sets and a choice of $\mathcal{C}$ for which there is no efficient private construction of a *synthetic* data set maintaining approximately correct counts.

Turning to the potentially easier problem of privately generating a data structure from which it is possible to approximate counts, there is a tight connection between hardness of sanitization and the existence of *traitor tracing* schemes. Using the scheme of Boneh, Sahai and Waters [3], and under the appropriate complexity assumptions, it is possible to obtain a distribution on databases and a concept class permitting *inefficient* sanitization, but for which *no efficient sanitization is possible*.

DRM'10, Oct 4, 2010, Chicago, Illinois, USA.

1. REFERENCES

[1] A. Blum, K. Ligett, and A. Roth. A learning theory approach to non-interactive database privacy. In *STOC*, pages 609–618, 2008.

[2] D. Boneh and M. Naor. Traitor tracing with constant size ciphertext. In *ACM Conference on Computer and Communications Security*, pages 501–510, 2008.

[3] D. Boneh, A. Sahai, and B. Waters. Fully collusion resistant traitor tracing with short ciphertexts and private keys. In *EUROCRYPT*, pages 573–592, 2006.

[4] B. Chor, A. Fiat, and M. Naor. Tracing traitors. In *CRYPTO*, pages 257–270, 1994.

[5] C. Dwork, O.Reingold, G. N. Rothblum and S. Vadhan, On the Complexity of Differentially Private Data Release In *STOC*, pages 381–390, 2009.