Sharing confidential information with privacy

Luca Melis

March 8, 2014

1 Background and motivations

The word *privacy* commonly refers to the ability of a person or a group to make information about themselves private. The availability of sensitive information about an individual often results in having power over that person and thereby generating serious concerns on potential misuse by governments, corporations or even other individuals. Indeed, many countries have laws and constitutions that in some way limit privacy.

In today's world, data is generally shared in a digital format and gathered by third parties. Thus the disclosure of private information is becoming a critical concern raising legal, monetary or even emotional, privacy issues. The need for privacy-preserving sharing of confidential information happens in many realistic scenarios. A typical scenario may involve two parties: one that needs information from the other that is either motivated, or obliged, to share only the requested information. Consequently, there is a struggle between information sharing and privacy. Let's consider the following examples:

- **Law enforcement** Two national law enforcement bodies (e.g., USAs FBI and UKs MI5) want to compare their respective databases of terrorist suspects. National privacy laws prevent them from revealing bulk data, however, by treaty, they are allowed to share information on suspects of common interest.

- **Genomics** Genome Sequencing (WGS) is a revolutionary technology that determines the complete genetic blueprint of any organism. Risks of a genome disclosure motivate the need for secure storage and testing of human genomes. In particular, there is a need for genetic testing by physicians and/or laboratories without full access to individuals' genomes. In an idealized future setting, genetic tests should only disclose the required minimum amount of information. At the same time, genomics and biotechnology companies often treat test details as trade secrets, since they represent valuable intellectual property.

- **Face recognition** Automatic recognition of human faces is becoming increasingly popular in civilian and law enforcement applications that require reliable recognition of humans. A typical application scenario for privacy-preserving face recognition concerns

a client who privately searches for a specific face image in the face image database of a server.

- **Internet security** Internet service providers (ISP) usually maintain a *black-list* of potential attackers. Each ISP is motivated to know if others ISPs have some blacklist members in common without revealing the whole list.

The aforementioned examples motivate the need for privacy-preserving sharing of confidential information and pose two main technical challenges:

1. how to enable this type of sharing such that parties learn no information beyond what they are entitled to
2. how to do so efficiently, in real-world practical terms.

2 Cryptography Protocols and Open Problems

References

[1] Jonay I. González Hernández, Pilar Ruiz-Lapuente, Hugo M. Tabernero, David Montes, Ramon Canal, Javier Méndez and Luigi R. Bedin, No surviving evolved companions of the progenitor of SN1006, Nature, **489**, 533-536 (2012).