Cloud computing represents a paradigm shift in the way we use computing resources. Many availability, cost, and scalability constraints are removed by the possibility of outsourcing cheaply to ‘the cloud’. However, such activity introduces new security concerns—many of which can be addressed by cryptographic solutions towards data confidentiality, integrity and authenticity over networks. Cryptography is therefore an essential component of any cloud infrastructure.

The increasing emphasis on ‘the cloud’ has focused the attentions of the research community onto fully homomorphic encryption (FHE)—viewed by some as the “holy grail” of cryptography by virtue of the fact that it allows arbitrary computations to be carried out on encrypted data. Such versatility would allow sensitive information (e.g. patient medical records or financial data) to be processed securely in the cloud, with the resulting output accessible only to authorised parties (i.e. those in possession of appropriate decryption keys).

Though a practical scheme remains some way off, homomorphic encryption is a fast moving area of research—and one in which the crypto group at Bristol is heavily involved, with substantial and ongoing contributions encompassing mathematical aspects, security issues, and applications.

Motivation

Cloud computing represents a paradigm shift in the way we use computing resources. Many availability, cost, and scalability constraints are removed by the possibility of outsourcing cheaply to ‘the cloud’. However, such activity introduces new security concerns—many of which can be addressed by cryptographic solutions towards data confidentiality, integrity and authenticity over networks. Cryptography is therefore an essential component of any cloud infrastructure.

The increasing emphasis on ‘the cloud’ has focused the attentions of the research community onto fully homomorphic encryption (FHE)—viewed by some as the “holy grail” of cryptography by virtue of the fact that it allows arbitrary computations to be carried out on encrypted data. Such versatility would allow sensitive information (e.g. patient medical records or financial data) to be processed securely in the cloud, with the resulting output accessible only to authorised parties (i.e. those in possession of appropriate decryption keys).

Though a practical scheme remains some way off, homomorphic encryption is a fast moving area of research—and one in which the crypto group at Bristol is heavily involved, with substantial and ongoing contributions encompassing mathematical aspects, security issues, and applications.

Application to secure cloud computing

FHE schemes support arbitrary multiplications and additions of encrypted data. While schemes which support a single homomorphic operation have been known for a long time, the first full scheme was realised by Gentry in 2009.

The starting point for Gentry’s construction is a Somewhat Homomorphic (SH) scheme (that is, one which supports a limited number of additions and multiplication) which he modifies to make it bootstrappable (that is, able to support homomorphic evaluation of its own decryption circuit).

Finally, he shows that any bootstrappable SH encryption scheme can be converted into an FHE scheme. His approach has given rise to the description of several different FHE schemes, but none as yet can be considered close to practical (that is, latency of the schemes remains infeasibly high for them to be usefully implemented in real-world applications).

Security

Lattices are mathematical objects with both algebraic and geometric properties. Ajtai showed in 1996 that some of these properties are very useful in cryptography and lattices have since been used to construct cryptographic primitives. In fact, the first construction of a Fully Homomorphic Encryption scheme by Gentry in 2009 was based on lattices.

While several new schemes based on other structures have been proposed, the main line of research into FHE still focuses on lattices. Thus, understanding lattices holds the key to understanding the security of these FHE schemes.

Funding and Collaboration

- EPSRC via grant EP/I03126X/1.
- DARPA via the PROCEED project.
- European Commission via ECRYPT II.
- ERC via Advanced Grant CRIPTO.
- Industrial Collaborators: IBM T.J. Watson, Trend Micro.