

STORK: Position Paper

Crypto Group, Bristol University, UK

1. BACKGROUND

The following represents the cryptographic interests of the following groups at the University of Bristol:

- Cryptography and Information Security Group
- Centre for Information Technology and Law
- Quantum Computing Group

Currently we have projects running in areas as diverse as **elliptic curve cryptography**, **provable security**, **lattice reduction**, **identity based encryption**, **quantum computing**, **implementation techniques** and **legal issues**. Further details can be found on the following web page

<http://www.cs.bris.ac.uk/Research/CryptographySecurity/>

2. FOUNDATIONS

Public key cryptography relies on the hardness of certain mathematical problems. A prominent role is played by the discrete logarithm problem in cyclic groups of large prime order. Classes of such groups are essentially given by the multiplicative groups of finite fields and the point groups of **elliptic curves** over finite fields.

Elliptic curves over finite fields are of particular importance since the best known algorithm for solving the elliptic curve discrete logarithm requires exponential time, whereas for multiplicative groups of finite fields there are subexponential attacks known.

We expect research into the hardness of the elliptic curve discrete logarithm problem to continue at a pace greater than that of research into factoring and discrete logarithms. We also expect research to continue into hard mathematical problems such as **lattice reduction**. This is important for two reasons, firstly currently such problems are immune to the advent of quantum computers, and secondly some deployed schemes, such as NTRU, are based on such mathematical problems. This is despite very little being known about the practical security of systems such as NTRU.

If any small advance in factoring algorithms occurs then 1024 bit RSA moduli could conceivably become weak, leaving most fielded RSA systems as potentially weak. However, a significant advance in ECDLP algorithms would be needed to render 160 bit ECC as weak. In addition a technological lead in ECC will be crucial to the European technological infrastructure since the suitability of ECC for mobile phones, PDAs and other small devices, will only increase the future importance of this technology

However, we believe the overall importance of foundational research into the hard mathematical problems on which cryptography is based will start to diminish as the subject becomes more mature. As systems become more widely deployed the research focus will be more towards applications of cryptographic technology and the design and analysis of more complicated protocols.

3. DESIGN AND ANALYSIS

Design and analysis of practical protocols has been heavily influenced in recent years by the subject of **provable security**. This has mainly concentrated on defining the attack models and security goals of particular schemes. One problem with this area is that its definitions work at a level of abstraction which real world adversaries do not.

However, recent work by Manger and Whyte et. al., shows that whilst the attack models used in provable security are important conceptual tools they do not fully model real world adversaries. This is

particularly highlighted when one considers attacks such as side channel analysis, an area of particular concern to the computer architecture community.

We see that there is a major role for experts in provable security and experts in **implementation techniques** (both software and hardware) to come together to look at implementations which are “provably secure” in some sense, thereby removing some of the abstraction currently used. There are some early results in this vein, but to become fully useful such an idea will need extensive work as one needs to extend the definitional work in provable security down into the implementation layer.

4. APPLICATIONS

The applications of cryptography will extend. Of particular interest, both to our group and our colleagues in local industry, are the recent advances in **identity based encryption** (IBE) following the publication of the paper of Boneh and Franklin. Central to this primitive is the existence of a group where the Computational Diffie-Hellman problem is hard, but the Decision Diffie-Hellman problem is easy due to the existence of a bilinear pairing. Currently, the only instances of such groups are supersingular abelian varieties and the Tate pairing.

Other examples of pairing based cryptography include identity based signatures and key agreement, a one-round protocol for tripartite Diffie-Hellman and short signatures. We have been conducting research into applications of IBE in various e-commerce applications.

We have seen considerable interest from local companies in using IBE as a means to solve some of the security issues which traditional cryptographic techniques (both symmetric and public key) find hard to solve. These include better scaleability compared with traditional PKI solutions; natural methods for providing cryptographic separation between communities of interest; the use of split authorities to avoid a single point of compromise or failure; and flexible key semantics, empowering the sender of a message to determine what conditions a recipient must meet in order to read a message.

Other applications of cryptography to managing and controlling the content produced by the digital media industry we also see of growing importance. However, at this stage it is unclear whether a technical solution, a legal solution or a change in the business model will provide the long term solution.

5. LEGAL AND REGULATORY ASPECTS

We believe that a wide range of legal and regulatory issues associated with cryptology R&D, both in terms of broad policy analysis, and the development of legal and regulatory frameworks relating to specific areas of cryptology utilisation, have yet to be adequately explored. At the policy analysis level, the desire by national governments to take advantage of positive aspects of cryptographic technologies, whilst attempting to prevent uses perceived as harmful, has resulted in an uncertain and incoherent legal and regulatory environment. Technical research into uses of IBE, as opposed to symmetric or public key techniques, in conjunction with legal analysis by the CITL may provide some solutions to these issues.

With regard to developing legal and regulatory frameworks we feel that the following are important issues which we are perfectly placed to explore, due to the synergies between law and computer science found in the CITL itself, and in its relationship with its of Advisory Group of international businesses and legal experts.

- The provision and regulation of “cryptographic support services”, including Certification Authorities or Private Key Generators, to provide a suitable environment for widening use of encryption technologies
- The role of cryptography in Digital Rights Management. DRM has significant legal implications. There are issues relating to the chilling effect of such legislation upon research into cryptanalysis techniques. There are also wider issues relating to preservation of digital media materials by libraries and archives where these materials are wrapped in DRM technologies.