STORK Position Paper

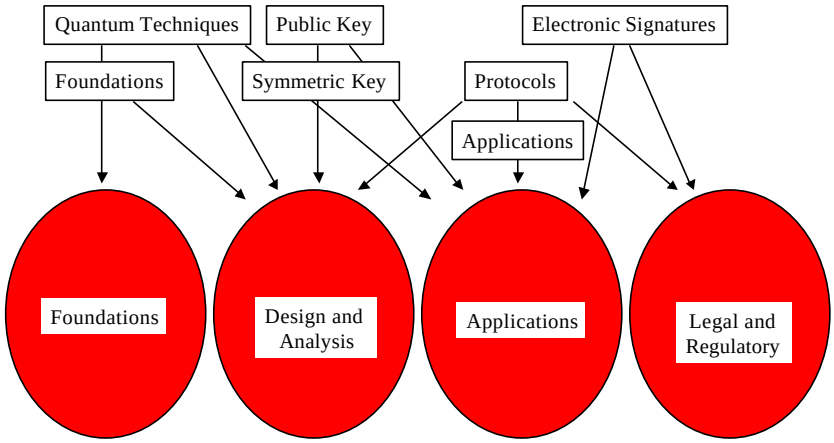
Sean Murphy and Matt Robshaw

Information Security Group
Royal Holloway, University of London
Egham, Surrey, TW20 0EX

The Position Paper

- "Towards a roadmap for future research"
  - current research efforts can be somewhat fragmented
    - within a research area and between research fields
  - for this position paper we solicited a range of opinions from colleagues
    - rather than focusing on any particular research area, we chose to reflect a diverse set of research interests
      - quantum computing, algorithm and protocol design and analysis, legal and regulatory aspects

STORK Workshop



Foundations

- Development of theoretical techniques
  - push towards provable security
  - improved techniques for the use of primitives
    - as well as providing answers this work poses new questions
      - different models of security
      - new models of security
      - practical relevance of security proofs
- Quantum techniques
  - ongoing development of quantum cryptography
  - ongoing development of quantum computing
    - typically independent of mainstream cryptographic research
      - potentially profound implications

Analysis and Design

- Analysis
  - the analysis of algorithms and protocols will always be a vital area of research
    - we need to have confidence in the basic building blocks we use

Analysis and Design

- Design
  - algorithm and protocol design is as strong as ever
    - pressures from foundational work
      - how to choose and use algorithms
    - pressures from within the field
      - new discoveries in cryptanalysis and design
      - having alternatives at hand is eminently sensible!
    - pressures from application development
      - highly restricted resources have important implications for the choice and the design of cryptographic algorithms

Applications

- There is (at least) one particular application area that is likely to drive considerable research
  - we frequently use the term *pervasive computing*
    - all but the simplest objects have some moderate level of computing power
  - there is an increasing trend towards *pervasive awareness*
    - all but the simplest objects interact with one another in a practically continuous way

Applications

- Convergence is likely to be driven at the application level
  - there is rarely a one-size-fits-all solution
  - different technology components already use their own established techniques
    - an installed based could make things difficult
    - it is likely to be a very considerable task to unravel the ensuing spaghetti of initiatives and proposals as convergence takes hold

Cryptographic Technology as a Component

- The picture is somewhat bigger than the core technology
  - helping Alice and Bob is complicated
    - establishing the technology (the algorithms and the protocols)
    - facilitating and enabling the supporting infrastructure
    - ensuring there is a match with business, legal and market requirements
- There can sometimes be unwelcome consequences
  - in a pervasively-aware world there are significant privacy issues
    - transactional or personal information

Legal and Regulatory Issues

- There are pressing (legal) problems to which fundamental research might make a contribution
  - privacy protection
  - digital rights management
  - ongoing efforts to extend and facilitate e-business
- Can fundamental research be helpful elsewhere?
  - understanding CA/RA liability issues
  - understanding the implications of new ID-based public key techniques

Conclusion

- "Towards a roadmap for future research"
  - very broad remit
  - within this position paper we highlight several aspects to this process
    - identifying open research problems
    - recognizing cryptographic technology as a component of the overall solution
    - balancing both reactive and proactive research efforts