1 Reliable and Private Communication

- **What is it?** Sender and a receiver do not share keys. They want to privately and reliably communicate over a network provided that the number of nodes (or edges) the adversary can control is limited and that the network has enough connectivity.
- **Potential applications:** Prevent Denial of Service, backup in case public key is broken, prevent the UK being the subject of a death-switch.
- **Results achieved on:**
  1. Ethernet like networks: solved a 13 year open problem (by Franklin-Wright)
  2. Point-to-point networks: generalised Kurosawa-Suzuki Eurocrypt 2008 result
  3. Almost Secure Message Transmission (slightly relaxed security): more efficient protocols
  4. The directed graph case: introduced the problem, found conditions for special case.
  5. Other results: showing others wrong, color adversary structures.
- **Illustrative examples:**

![Diagram of a network with nodes and edges]


2 Secret Sharing and Threshold cryptography

- **What is it?** Secret sharing allows backup of data in a reliable and private manner.
- **Potential applications:** Cloud storage, distributed security
- **Results achieved on:**
  1. Threshold cryptography: three new schemes, one based on pairings
  2. Secret sharing: linking bounds to combinatorics
- **Publications at:** FC 2006, ICITS 2008, ISC 2007

3 Voting

- **Plurality voting is not optimal:**

<table>
<thead>
<tr>
<th>Voter 1</th>
<th>Voter 2</th>
<th>Voter 3</th>
<th>Voter 4</th>
<th>Voter 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most preferred candidate:</td>
<td>A</td>
<td>A</td>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>Second preferred candidate:</td>
<td>B</td>
<td>B</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Least preferred candidate:</td>
<td>C</td>
<td>C</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>

- **Results achieved on:**
  1. Equilibria of plurality voting with abstentions, e.g., is sequential voting better?
  2. Hacking Helios 2.0, an Internet voting scheme using lots of cryptography

3. A new Internet voting scheme: submitted
4. Other results: (a) Keeping the tally private, (b) Klein bottle routing.

4 Secure multiparty computation

- **What is it?** Parties $P_1, P_2, \ldots, P_n$ knowing respectively $x_1, x_2, \ldots, x_n$ want to privately compute $f(x_1, x_2, \ldots, x_n)$, i.e., nothing leaks more than what follows from the output.
- **Potential applications:** Private cloud computing, privacy in general.
- **Results achieved on:**
  1. Using black-box groups to perform secure multi-party computation
  2. Reduce the use of VSS to make it more practical: submitted
  3. Asymmetric Trust and its applications in secure multi-party computation
- **Some details:**

![Diagram of a network with nodes and edges]

Sun-Yao-Tartary (2008) made a link with perturbation theory.
- **Publications at:** Asiacrypt 2007, Crypto 2007, Journal of Cryptology (accepted).

5 Critical infrastructures

- **Results achieved on, e.g.:**
  1. Robust Operations, i.e., how to make a robust variant of an operational research problem?
  2. Identifying critical infrastructures, e.g., using AND/OR graph models
  3. Analysing concrete vulnerabilities, e.g., potential weaknesses of Internet Banking
  4. Anti-jamming networks and constructing resilient data networks
- **Publications at:** COCOON 2005, ICITS 2011, IPL 2011, ISORA 2005

6 Other

- **Results achieved on:**
  1. Privacy in social networks, e.g., privacy in Facebook versus Google+
  2. Efficient and proven secure hybrid encryption
  3. Efficient key stream authentication using combinatorics
  4. Key distribution, e.g., for conferences using pairing based cryptography, or non-malleable while robust against active adversaries
  5. Cryptanalytic study, e.g., of E0, Luffa, Rabbit Shannon Cipher