1. **Title**
    1. Shadow p2p is anonymous network aiming to be more anonymous than all others
    2. Presentation focus on novel techniques created
2. **A need for anonymity**
    1. Anonymity is in demand, lots of situations it is useful / necessary
    2. Examples
        1. Spies don't want to reveal their identity in enemy territory
        2. Criticising some governments can get you arrested and imprisoned
        3. Apostasy, illegal in 14 countries, punishable by death in 9
3. **What is anonymity**
    1. Namelessness + unremarkability
    2. Namelessness: removing identifying features
    3. Unremarkability: being places amongst many other similar entities
    4. I created 4 new methods to achieve these effects
4. **Cross**
    1. The Shout
        1. Method for one-way message sending with neither sender or receiver being identified to the other
    2. Shout groups
        1. Protects the shout mechanism from attacks by an adversary
    3. Public key hiding
        1. Allows public keys to be scrambled to prevent recognition but such that they can still be used as public keys
    4. Uni-directional toroidal network
        1. Network structure more anonymous than mesh network
5. **Shouts**
    1. In this project, identity is IP address
    2. Shouts send messages from sender to receiver.
        1. Sender has shout list, only one address is the receiver
        2. A packet is sent to each address in the shout list
        3. Receiver anonymised amongst list of IP addresses
        4. The sender uses IP spoofing to remove their identity from the packets
    3. Cannot tell if an IP address is participating in the network or not
    4. Inefficient but anonymity is of primary concern
6. **Shout Groups**
    1. Shouts are flawed
        1. Sender can search shout list
    2. Shout groups hinder attacks by having multiple receivers
        1. Can detect search and do something about it
    3. Shout groups also need to be designed to prevent shout group members acting in a hostile manner
        1. This made shout groups the most difficult problem
        2. Requires a solution to a secure multiparty computation problem
        3. Still no complete solution
7. **Public Key Hiding**
    1. Works with ElGamal
    2. Technique essentially ephemeral key creation to hide public key
    3. Applied in Shadow P2P to hide public keys in messages
        1. Packets can now use “ephemeral onion routing”
            1. Onion routing
                1. packets have multiple layers of encryption
                2. layers are added / removed with each node traversed

        2. Intermediate nodes can add a layer of encryption to a packet
            1. Without pre-agreeing encryption keys
    4. Technique also applied to routing so that intermediate node only knows which direction to send packet in, not where it is going
8. **Uni-directional Toroidal Network**
    1. Designed to be more anonymous than meshnet
        1. Meshnet node placement may be affected by location
        2. Nodes may be rearranged for better performance
        3. This reveals information
            1. As the location of a node helps determine its position in the network...
            2. Its position in the network gives information about its real world location
        4. My network structure prevents this being an issue
            1. Peers connect to one another in a rigid structure
            2. Connections never rearranged for performance
            3. In many cases, it can be predicted where the new peer will appear in the structure before it joins
                1. Shows that all information regarding the peer's connection is ignored
    2. Designed to prevent traffic analysis where an adversary attempts to collect all packets of a given communication
        1. The network is uni-directional
            1. Packets going from A to B must take different routes from packets going from B to A
        2. The grid provides routing options
            1. Packets have multiple routes between any pair of nodes
            2. Spreading out traffic in an intelligent manner amongst the routes can disguise large data transfers
            3. Source routing is used to ensure traffic takes the selected route
9. **Is surprisingly flexible**
    1. I conceived a way to exploit the properties of the toroid to make more space in the grid
        1. Unroll to provide more space
        2. Roll up to reduce space
    2. Double space in each dimension
        1. Replicate the grid
        2. Existing nodes are placed in the same positions in each of the expansion directions
        3. No new physical connections need to be made
        4. New nodes replace existing nodes in the grid
10. **This concludes the techniques I have invented**
    1. From these techniques I have designed a fully functional network
    2. The description in my thesis covers
        1. Additional components required
        2. How all the components interact
    3. Network not intended to be practical
        1. Demonstration of how the techniques should be used
    4. Analysis of components shows that novel techniques work as expected
        1. Attacks on shout groups
            1. take a lot of effort
            2. take a long time
            3. adjustable level of protection
        2. Public key hiding is cryptographically secure
        3. Network structure
            1. made a proof of concept simulation
            2. shows that expansion, contraction, joining and leaving all perform as expected