# Shadow P2P

Luke Murray

# A Need for Anonymity

Increase online privacy

Corporations monitoring activity

Oppressive governments

Secret agents

Circumvent censorship

Journalism

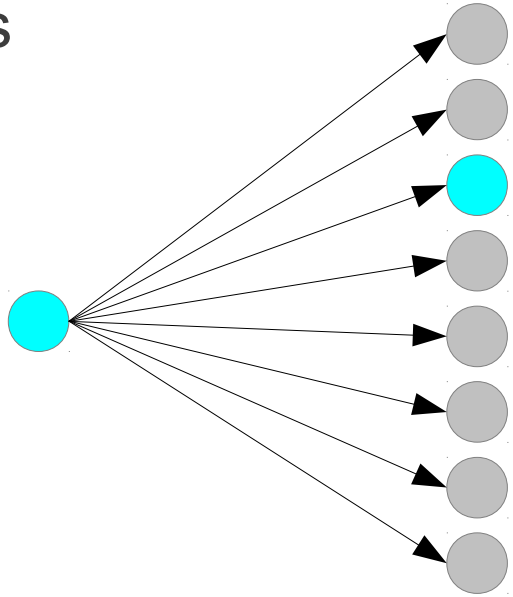
Anonymous tips

Whistle blowing

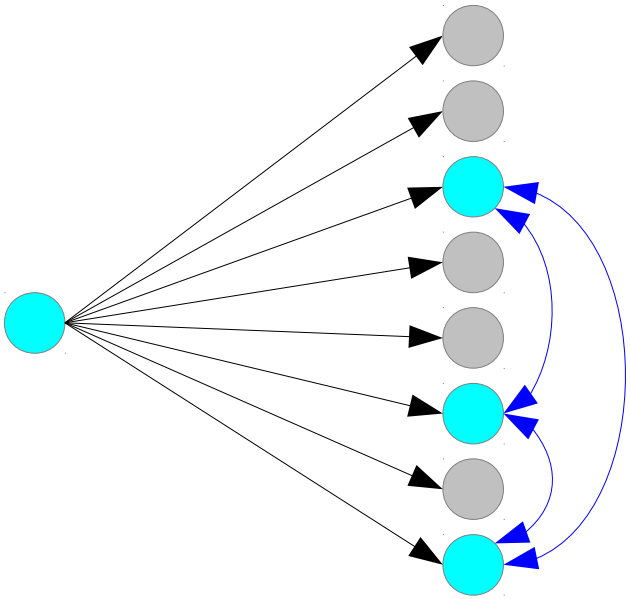
# What is Anonymity?

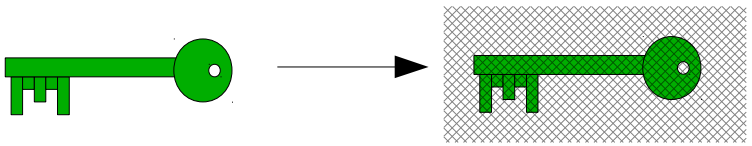
Namelessness + Unremarkablility

## Shouts

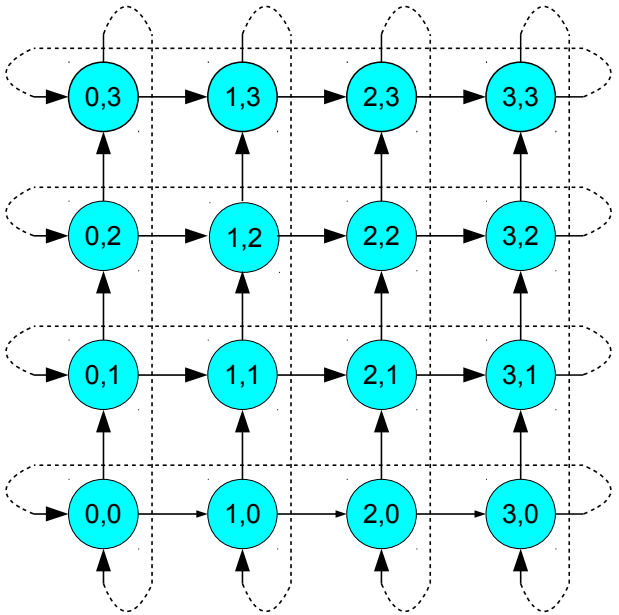


## Shout Groups





## Public Key Hiding

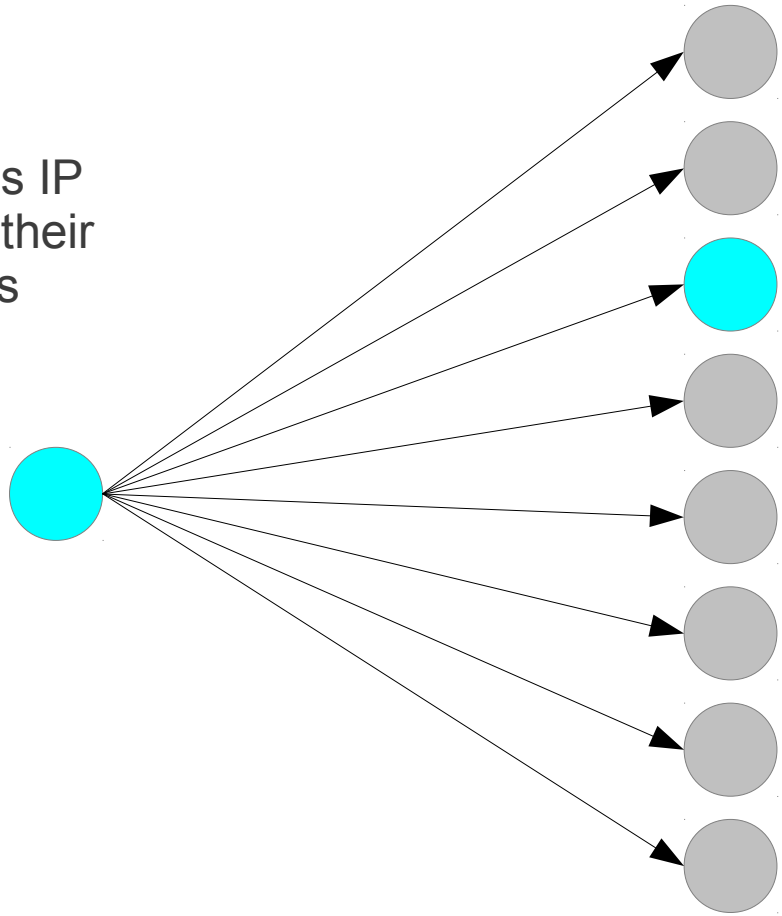



## Network Structure

# Shouts

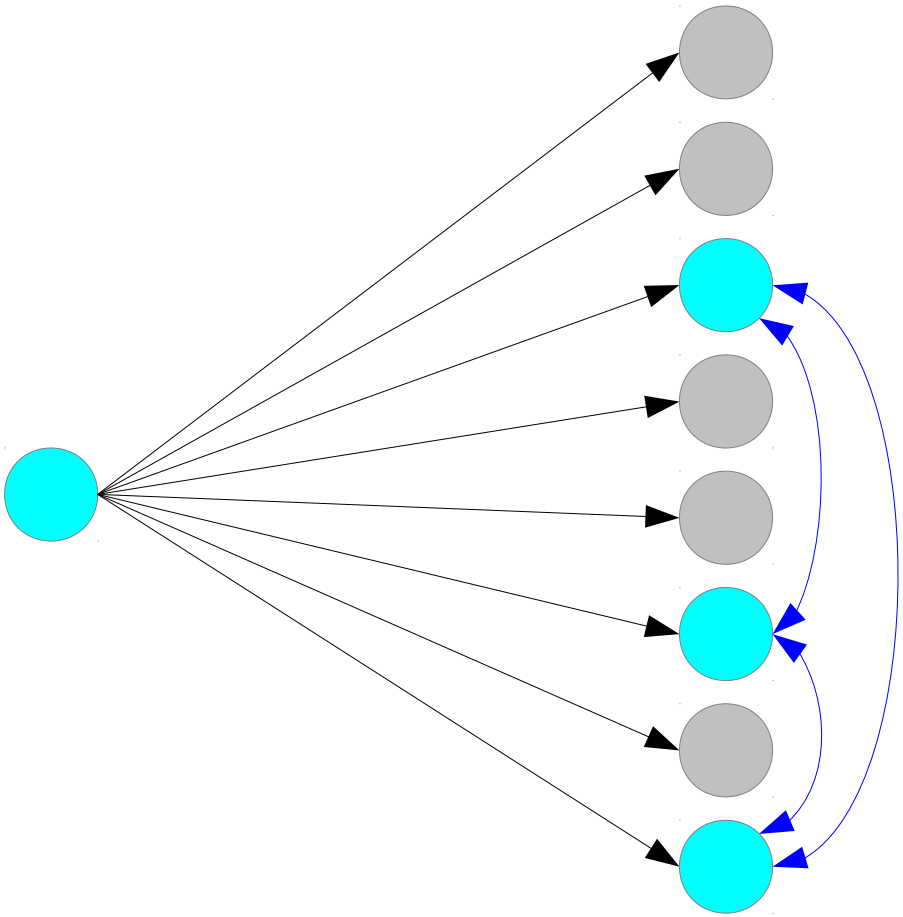
IP Spoofing + Multicast

The sender performs IP spoofing to remove their identity from packets



The shout list obscures the receiver's IP address amongst many others

# Shout Groups



Multiple receivers put their IP addresses into a shout list

The shout group members inform each other about the messages they receive

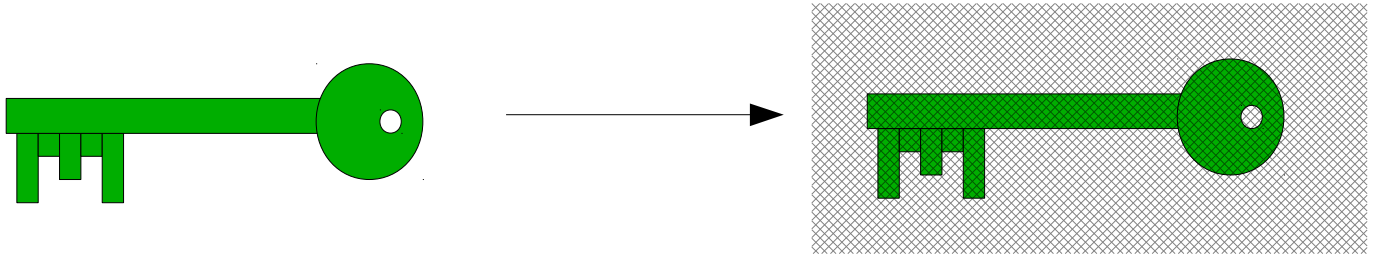
By doing this they can detect attacks on the shout list by a hostile sender

The hostile sender can then be hindered in their attack to an extent where the attack becomes infeasible

# Public Key Hiding

Public keys are tied to the identity of their owner

By applying the hiding technique to the public key, the receiver can remain anonymous



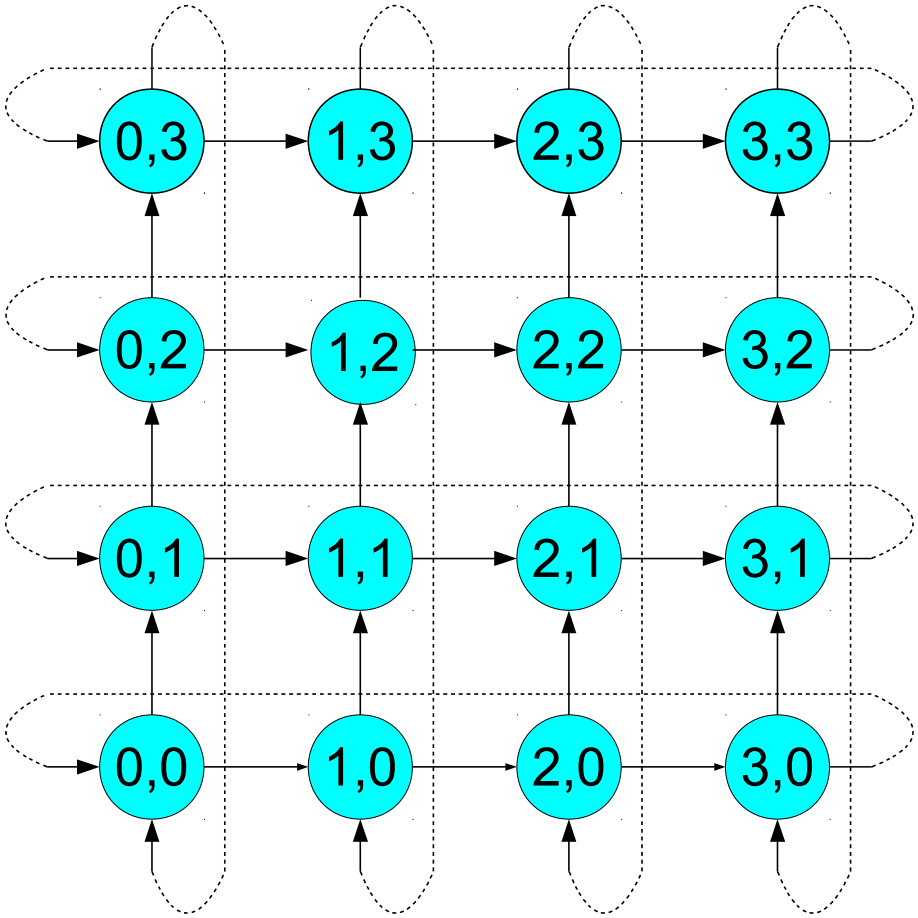
Messages with containing the public key that was used for encryption will give away the identity of the receiver

This technique only works with specific cryptosystems

# Uni-directional Toroidal Network Structure

Most other anonymous networks use a “meshnet” structure

Meshnets can reveal information about the location of a peer

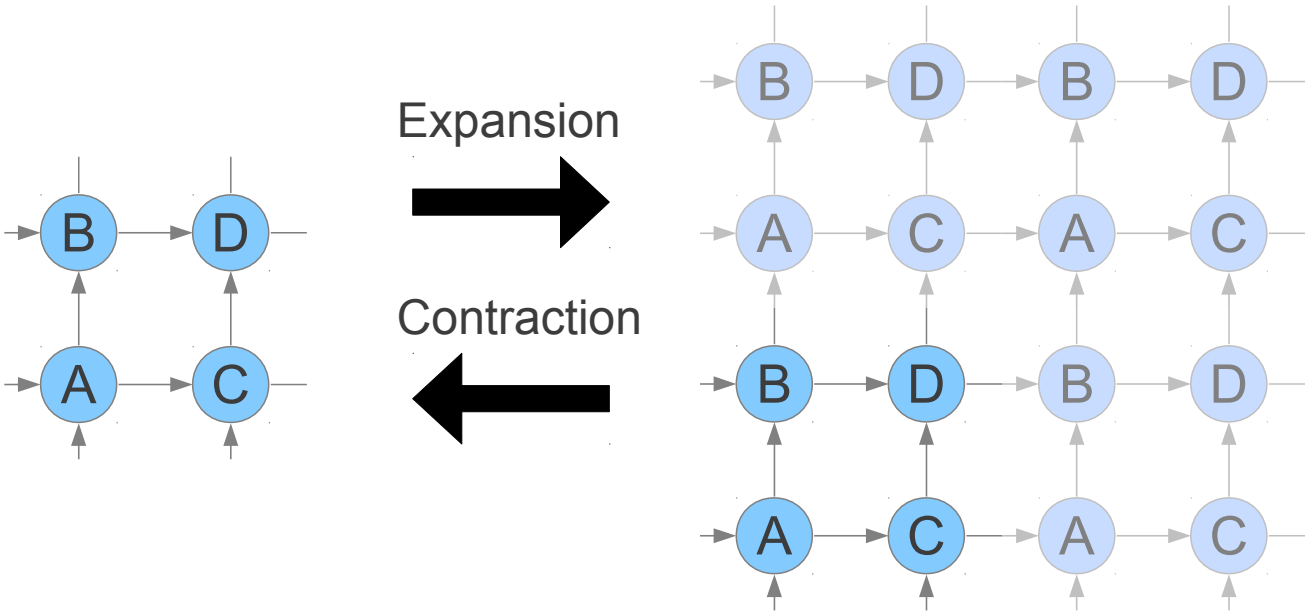



By arranging the nodes in this way, all location information is removed

Messages have multiple routes from each sender to each destination

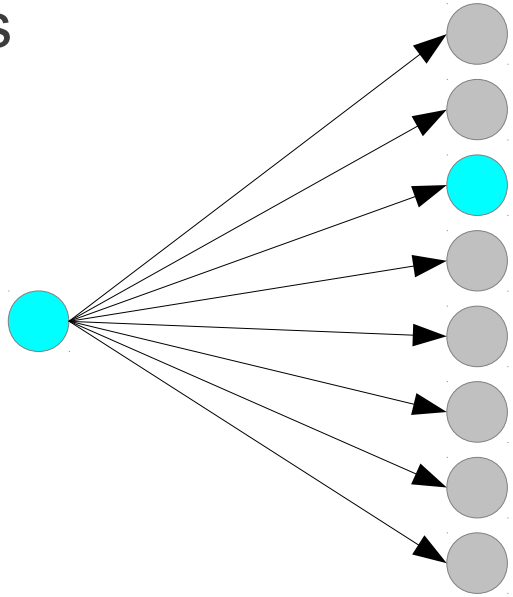
Responses must take a different path to return to the sender

# Network Resizing

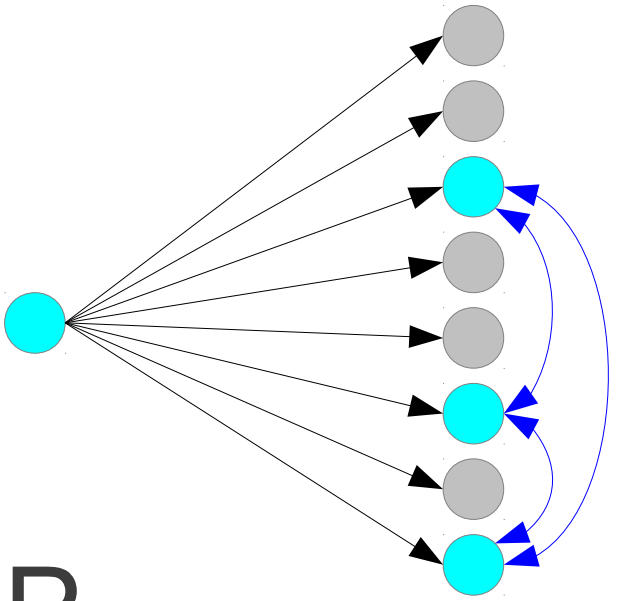


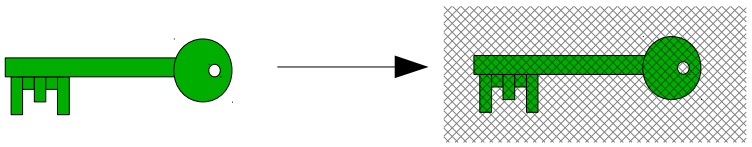
# Shadow P2P

## Shouts

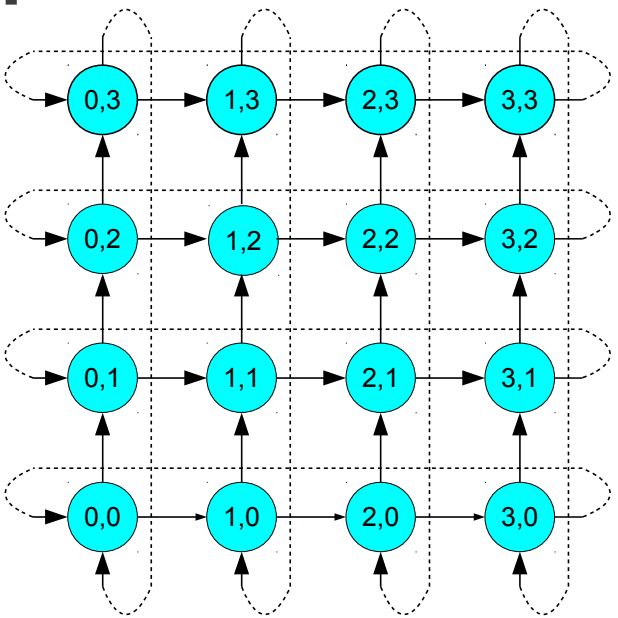


## Shout Groups





## Public Key Hiding




## Network Structure