Design and Implementation of a Practical Security-Conscious Electronic Polling System

Lorrie Faith Cranor

Outline

- Desirable properties for voting systems
- Traditional voting systems
- Cryptographic voting protocols
- The Sensus polling protocol
- The Sensus implementation
- Evaluation
- Conclusions

How Does an Election Work?

Registration

Validation

Collection

Tallying

Desirable Properties

- Accuracy
- Democracy
- Privacy
- Verifiability
- Convenience
- Flexibility
- Mobility

Traditional Election Systems

- No standards for US elections
- Reliance on trusted parties for security and privacy
- Absentee ballots and vote-by-mail add mobility, sacrifice privacy
- No mechanisms for individual verification

Cryptography

- **Useful for**
  - hiding secret messages
  - creating unalterable, authenticated messages
  - digital signatures
- **Types**
  - secret key
  - public key

RSA Public Key Cryptography

- Uses public/private key pairs
- Public keys are distributed, private keys are kept secret
- A message sealed with a public key must be opened with the matching private key and visa versa
- Based on the idea that factoring large numbers takes a long time

How RSA Works

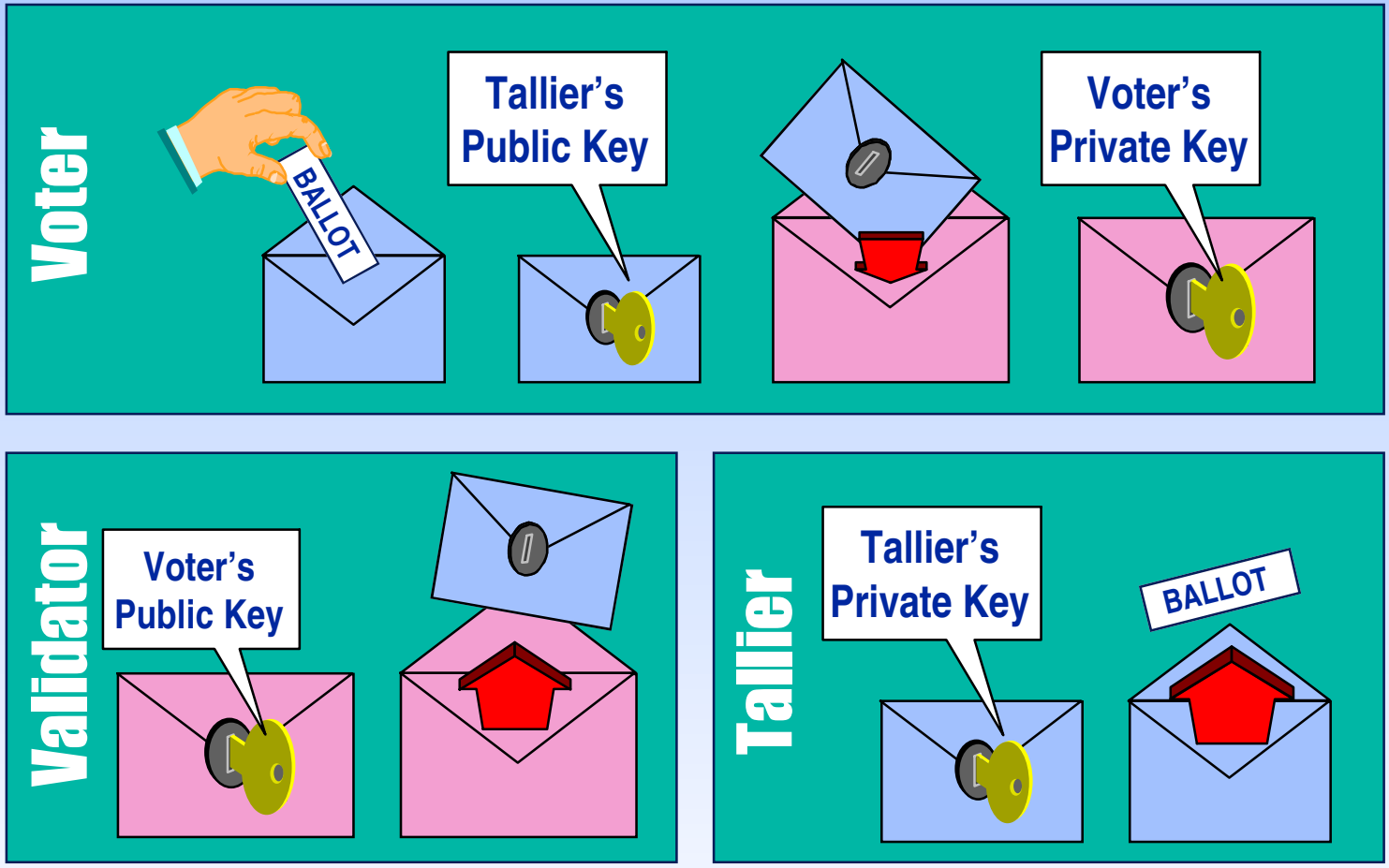
- **Key generation:**
  - pick two really big primes, p and q
  - calculate $n = pq$ and $x = (p-1)(q-1)$
  - pick an e that is relatively prime to x
  - calculate d such that $ed \bmod x = 1$
  - tell everyone your public key: n and e
- **Encryption of *m* :**
  - calculate $c = m^e \bmod n$
- **Decryption of *c* :**
  - calculate $m = c^d \bmod n$

from Matt Blaze's cryptography introduction tutorial

RSA

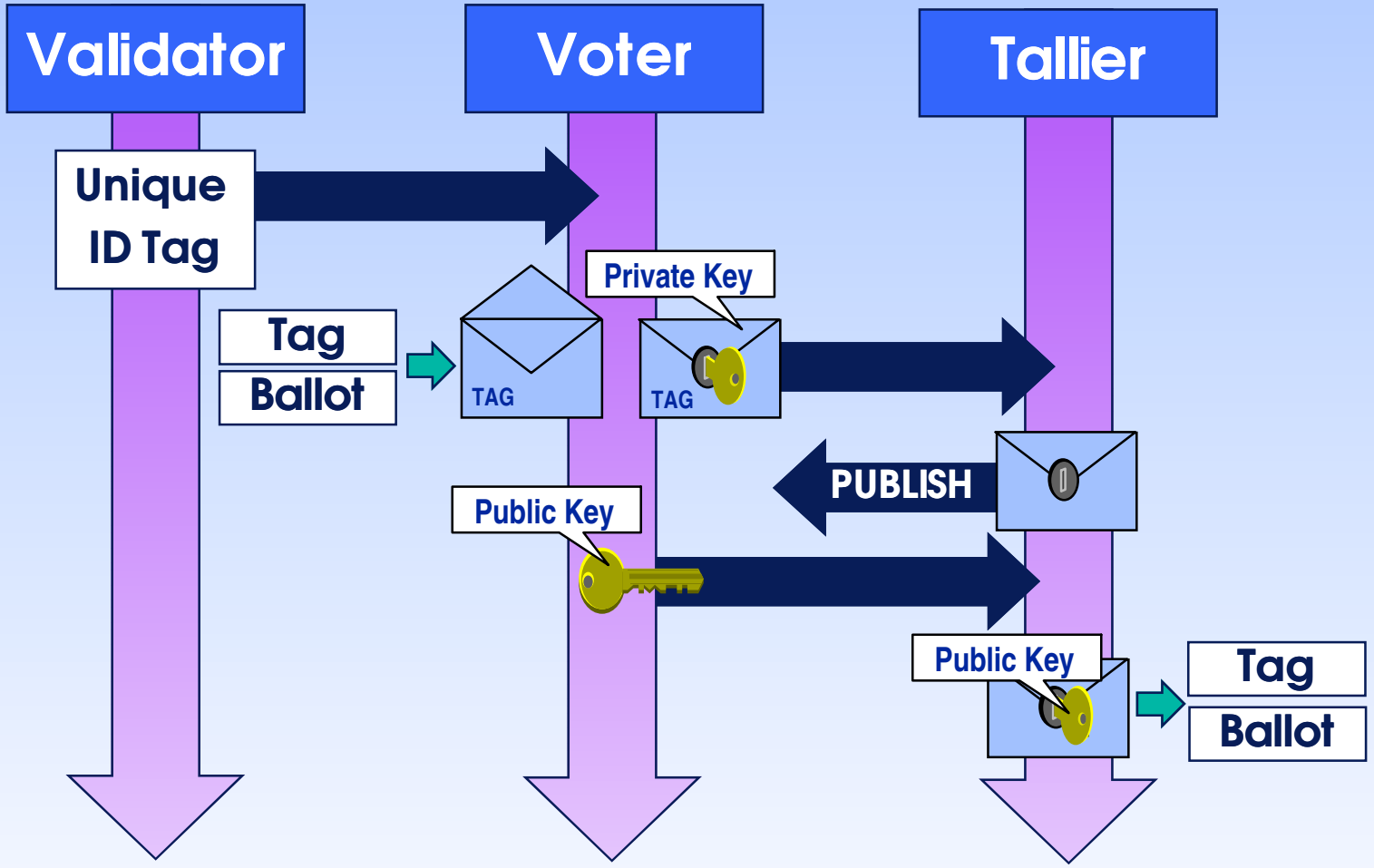
- Messages must be encoded as numbers between 0 and *n*
- Long messages must be broken down into parts
- Because RSA is slow, it is often used with faster secret key systems
- RSA is used to encrypt secret key or message digest

A Simplistic Voting Protocol



- *Tallier and validator can collude to violate privacy*

The Two Agency Protocol

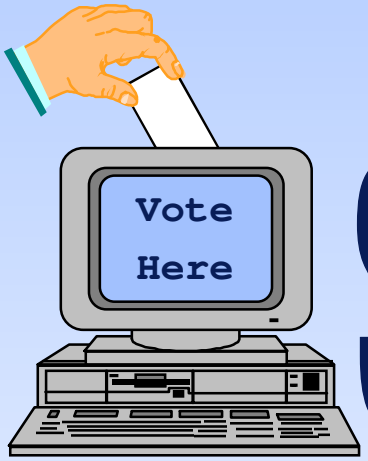


- *Tallier and validator can collude to violate privacy*

The One Agency Protocol

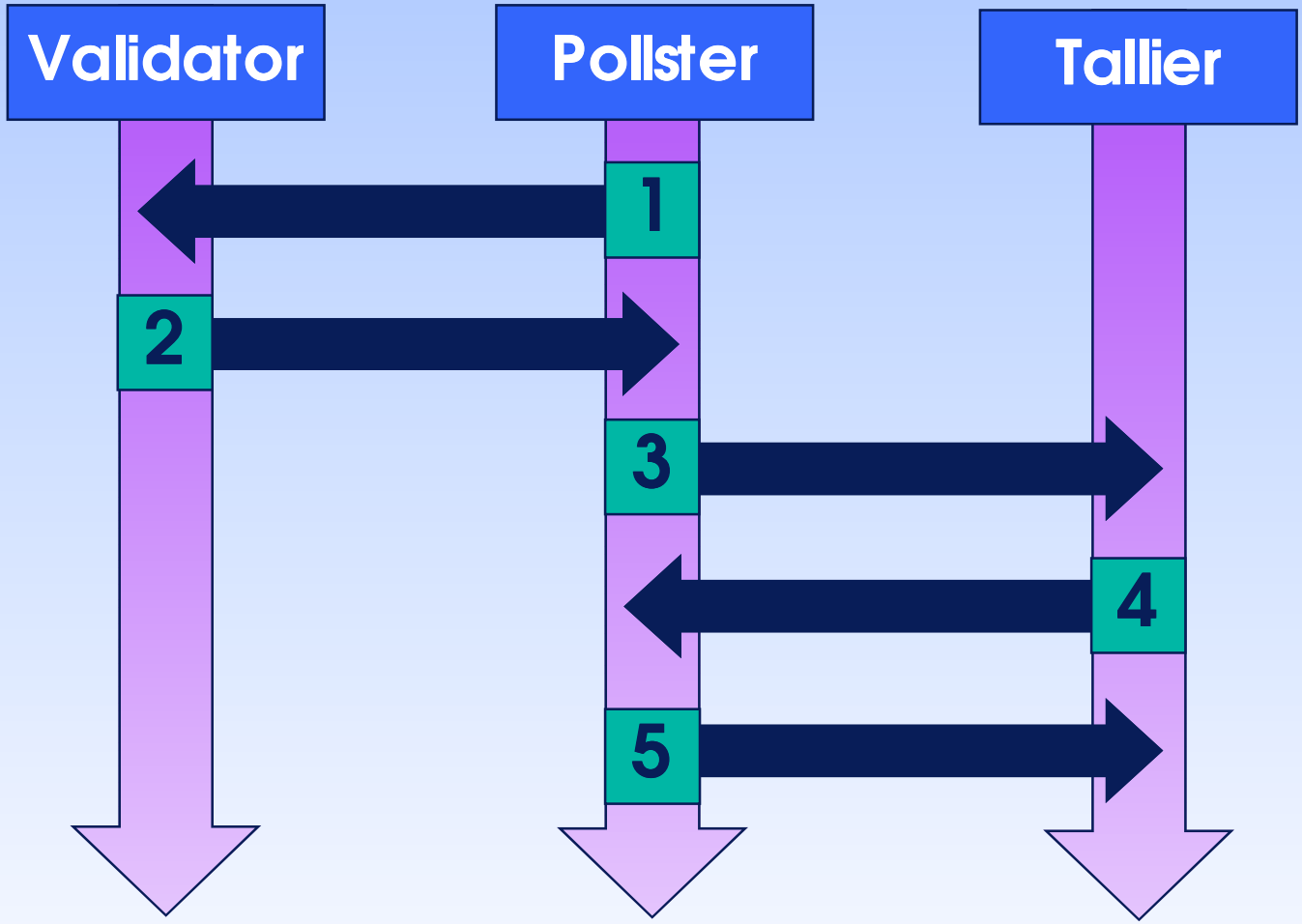
- Same as Two Agency Protocol except for tag distribution scheme
- ANDOS (all-or-nothing disclosure of secrets) protocol used
- ANDOS is very complex and does not scale well
- Not a *practical* solution to the collusion problem

Introducing . . .



Sensus

The Sensus Polling Protocol



Implementation

- Implemented in C and Perl on a UNIX system
- Uses RSAREF and Webget
- Includes Registrar, Pollster, Tallier, and Validator modules
- 5000 lines of C code, 375 lines of Perl code

Implementation: User Interface

- Text interface
- Shields voter from details of cryptographic functions and transactions with validator and tallier

Blind Signatures

- **Blinding (performed by voter):**
  - choose a random blinding factor r
  - compute and present for signing: $m \times r^e \pmod{pq}$ where m is the message
- **Signing (performed by validator):**
  - compute $(m \times r^e)^d$
  - this is equal to $r \times m^d \pmod{n}$
- **Unblinding (performed by voter):**
  - compute $r \times m^d / r = m^d \pmod{n}$

Assumptions

- Communication occurs over an anonymous channel
- Clear text messages cannot be intercepted
- Messages will not arrive at validator and tallier in the same order
- Strong encryption

Evaluation

- Accuracy
- Democracy
- Privacy
- Verifiability
- Convenience
- Flexibility
- Mobility

Extensions

- **User interface**
  - allow WWW browser to be used as interface to Sensus
- **Efficiency**
  - more space efficient file formats
  - faster cryptographic functions

Conclusions

- Sensus is a practical electronic polling system that satisfies the seven desirable properties of polling systems well