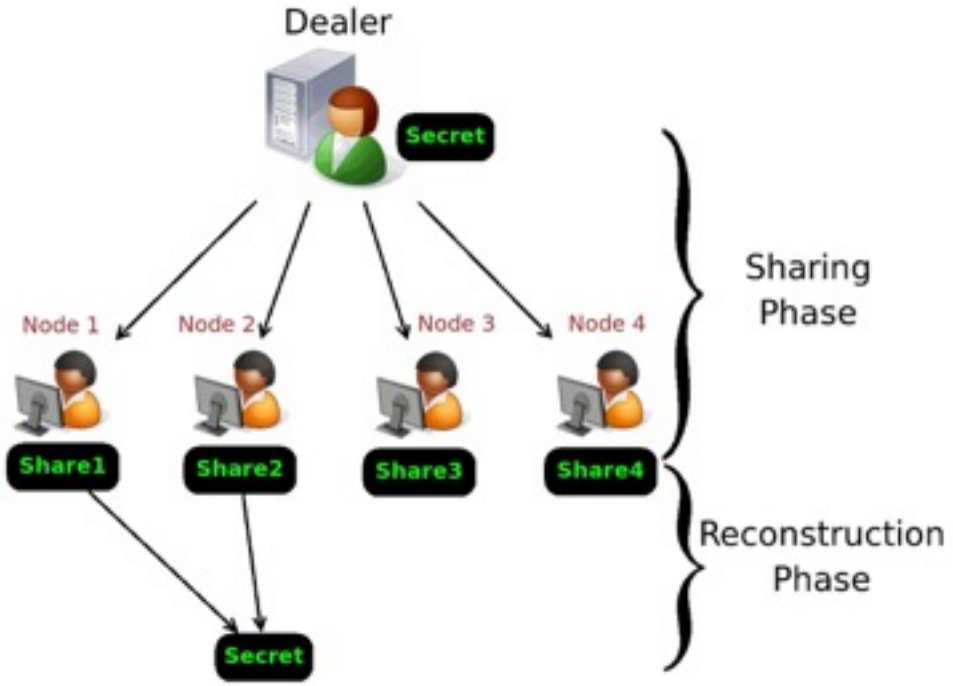


Secret Sharing

Dr. Aniket Kate
Purdue University

The cryptographic trust problem

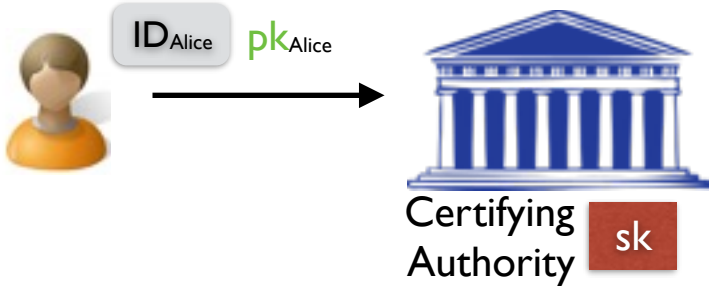
- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

The cryptographic trust problem

- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

The cryptographic trust problem

- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system



The cryptographic trust problem

- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

The cryptographic trust problem

- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

- How to realize such a trusted party?

The cryptographic trust problem

- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

- How to realize such a trusted party?
  - Find such an individual/group/organization, and justify their trustworthiness

The cryptographic trust problem

- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

- How to realize such a trusted party?
  - Find such an individual/group/organizatic and justify their trustworthiness

The cryptographic trust problem

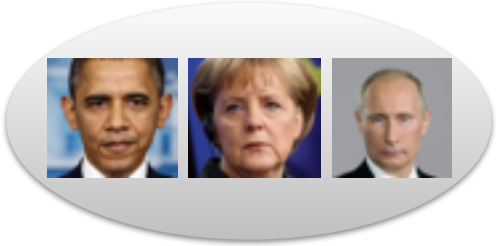
- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

- How to realize such a trusted party?
  - Find such an individual/group/organizatic and justify their trustworthiness
  - Use multi-party computation (MPC) or a distributed authority

The cryptographic trust problem

- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

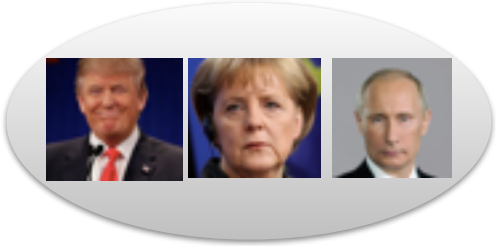
- How to realize such a trusted party?
  - Find such an individual/group/organizatic and justify their trustworthiness
  - Use multi-party computation (MPC) or a distributed authority



The cryptographic trust problem

- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

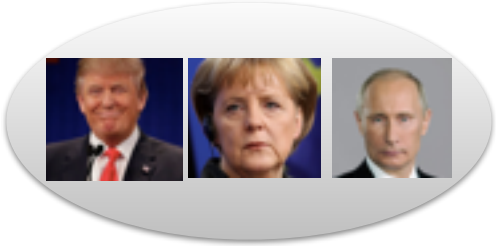
- How to realize such a trusted party?
  - Find such an individual/group/organizatic and justify their trustworthiness
  - Use multi-party computation (MPC) or a distributed authority



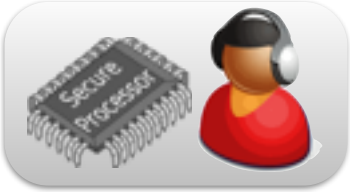
The cryptographic trust problem

- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

- How to realize such a trusted party?
  - Find such an individual/group/organizatic and justify their trustworthiness
  - Use multi-party computation (MPC) or a distributed authority



  - Employ a trusted hardware module that performs cryptographic operations



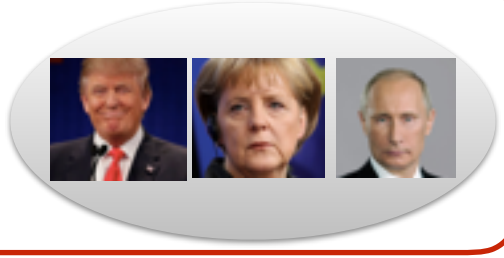
The cryptographic trust problem

- In secure systems, an authority is often required to
  - protect some secret, and
  - employ the secret in a manner defined by the system

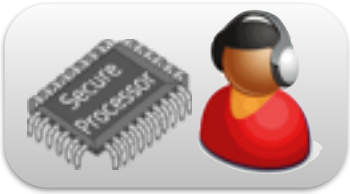
- How to realize such a trusted party?
  - Find such an individual/group/organizatic and justify their trustworthiness

CNNIC 中国互联网络信息中心 CHINA INTERNET NETWORK INFORMATION CENTER

  - Use multi-party computation (MPC) or a distributed authority



  - Employ a trusted hardware module that performs cryptographic operations



Secret Sharing

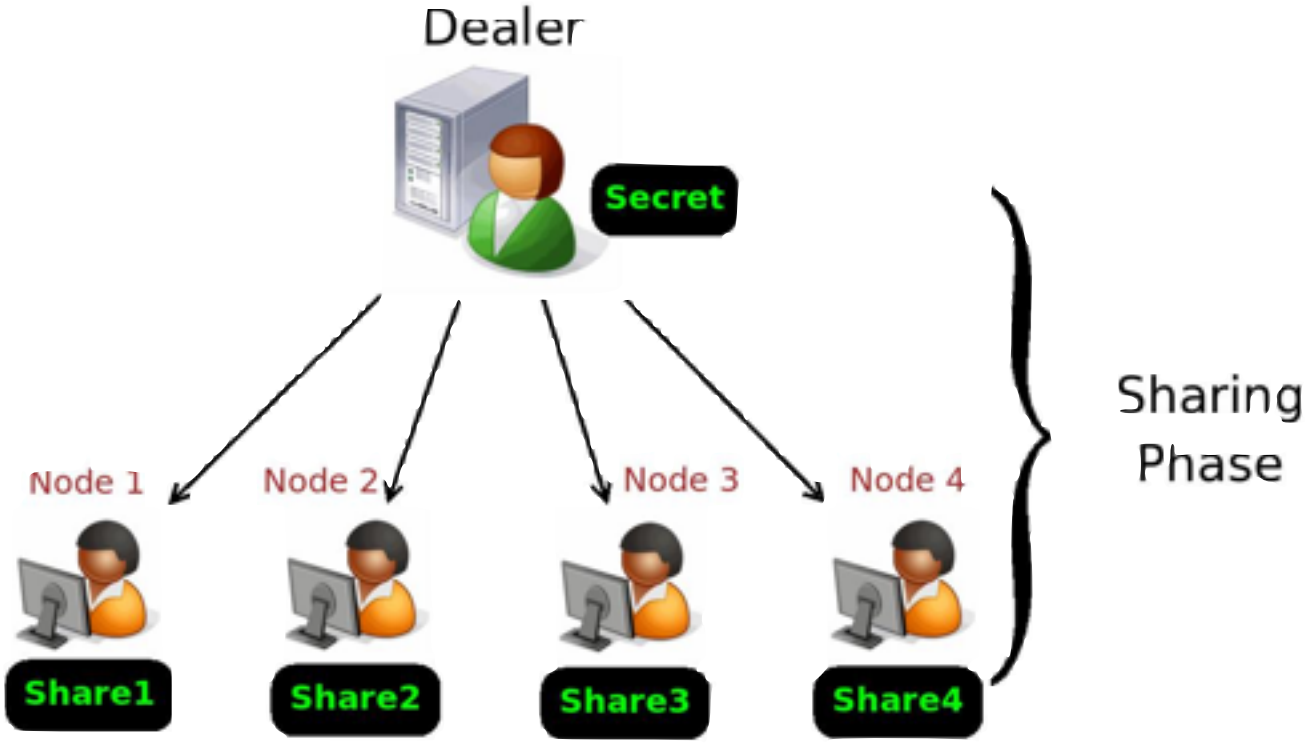
- The notion of secret sharing was introduced independently by Shamir and Blakley in 1979

- For integers n and t such that n > t >= 0, an (n,t)-secret sharing (SS) scheme is a method used by a dealer D
  - to share a secret s among a set of n parties (the sharing phase) in such a way that
  - in the reconstruction phase any subset of t+1 or more parties can compute s, but subsets of size t or fewer cannot

- What is the relation between n and t
  - against a passive adversary controlling any t parties?
  - against an active adversary controlling any t parties?

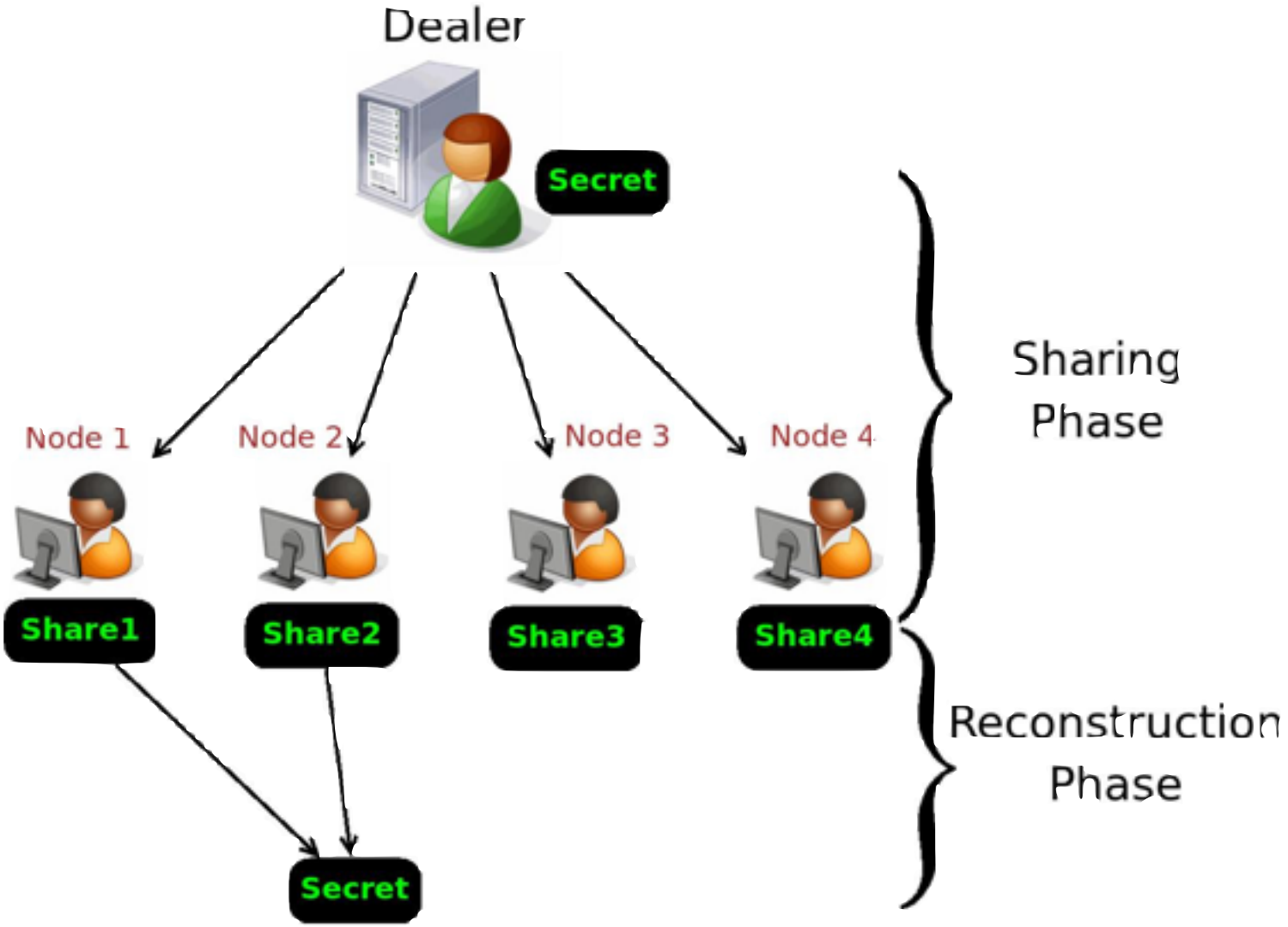
Secret Sharing Basics

- Sharing Phase



Secret Sharing Basics

- Reconstruction Phase



Shamir Secret Sharing

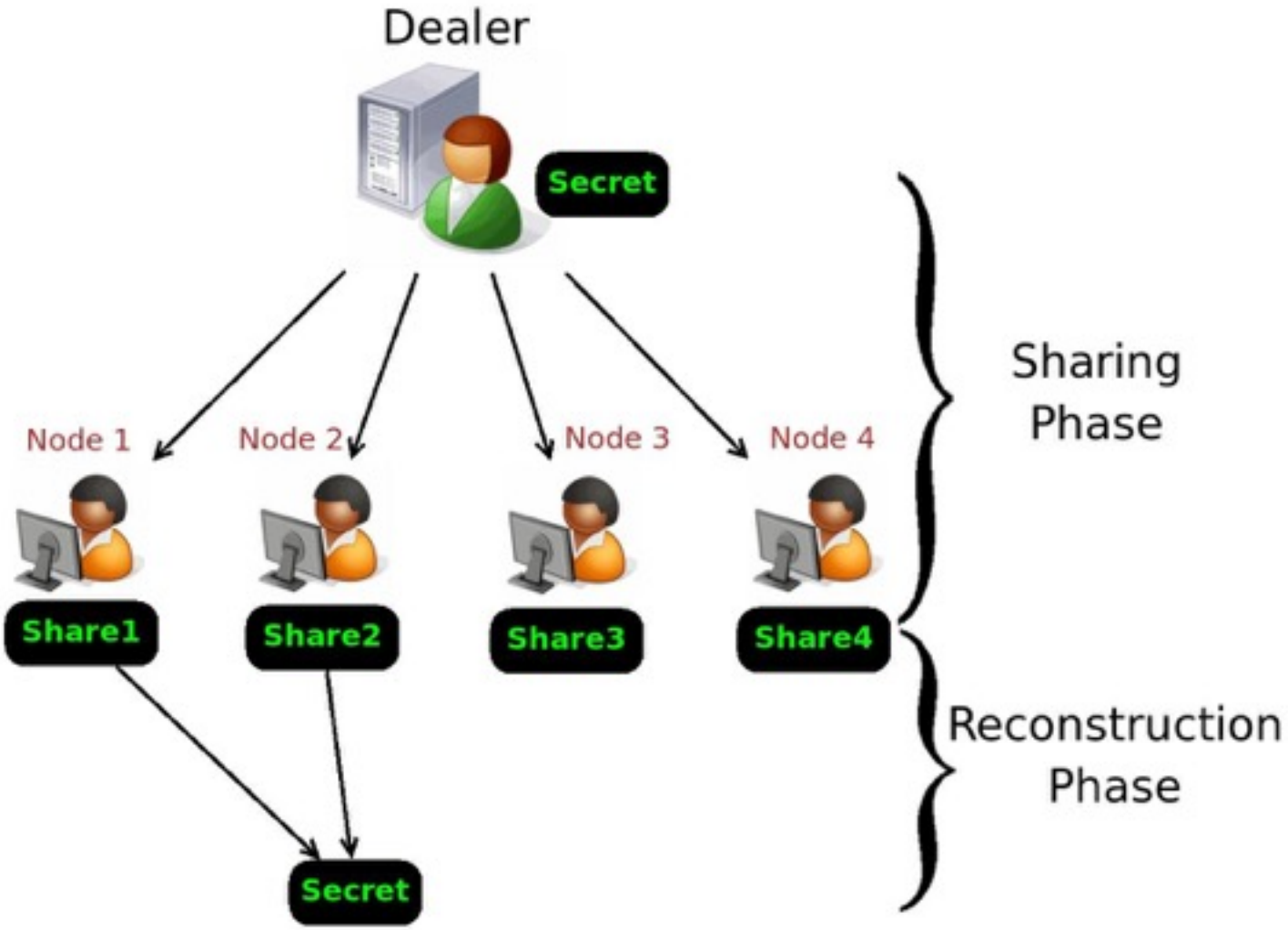
- Shamir's secret sharing based on polynomial evaluations and Lagrange interpolation is the standard SS scheme

- To share a secret $s \in F_p$ along $n < p$ players, the dealer D
  - chooses a degree-t polynomial $f_D(x) = s + r_1x + r_2x^2 + \ldots + r_tx^t$, for coefficients $r_i \in F_p$ chosen uniformly at random
  - computes and send $y_i = f(i)$ to i^{th} node/party; share $s_i = (i, y_i)$
  - We represent the output of sharing phase as [s]

- Any subset Q of t+1 or more players, can reconstruct the secret s as $s = \sum_{i \in Q} \lambda_i y_i$, where $\lambda_i = \prod_{j \in Q \setminus \{i\}} \frac{j}{j-i}$

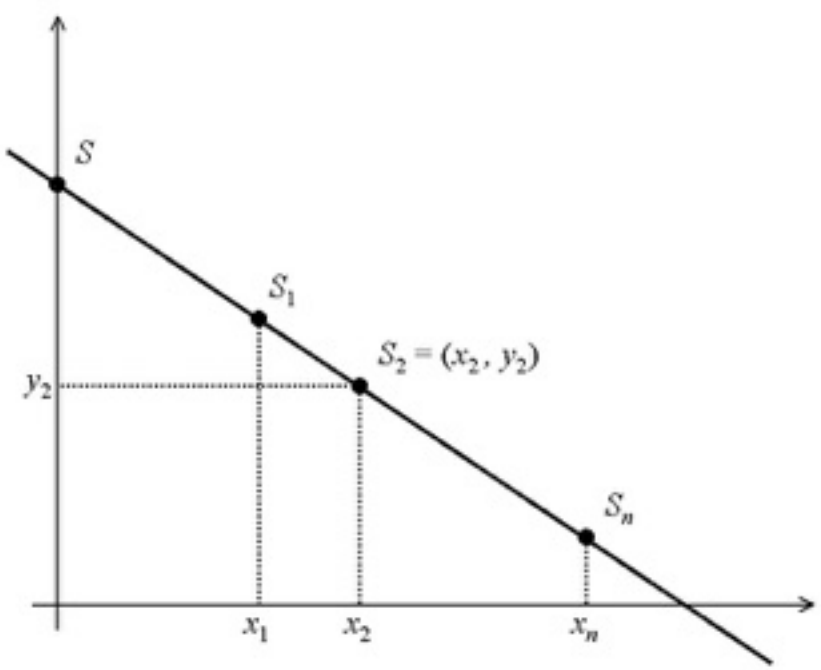
- This secret sharing is additive homomorphic

Example: (4,1)-Secret Sharing

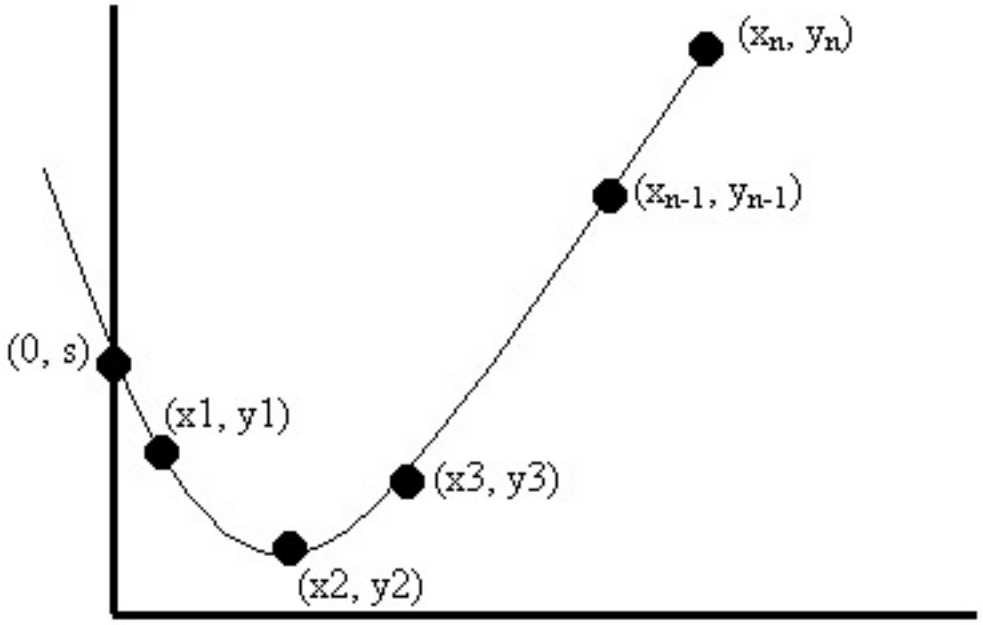


Shamir Secret Sharing Examples

- (n,1)-secret sharing

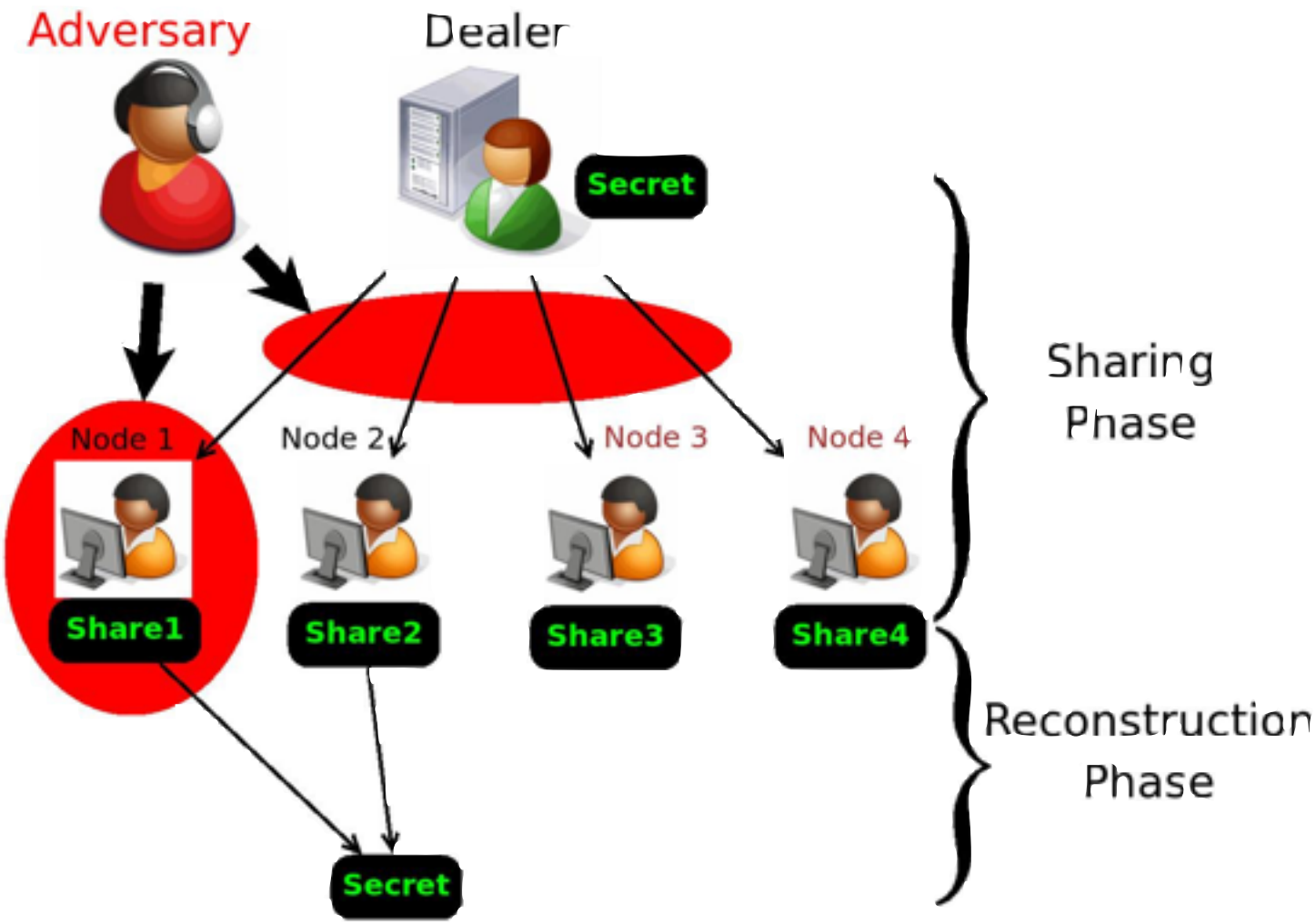


- (n,2)-secret sharing



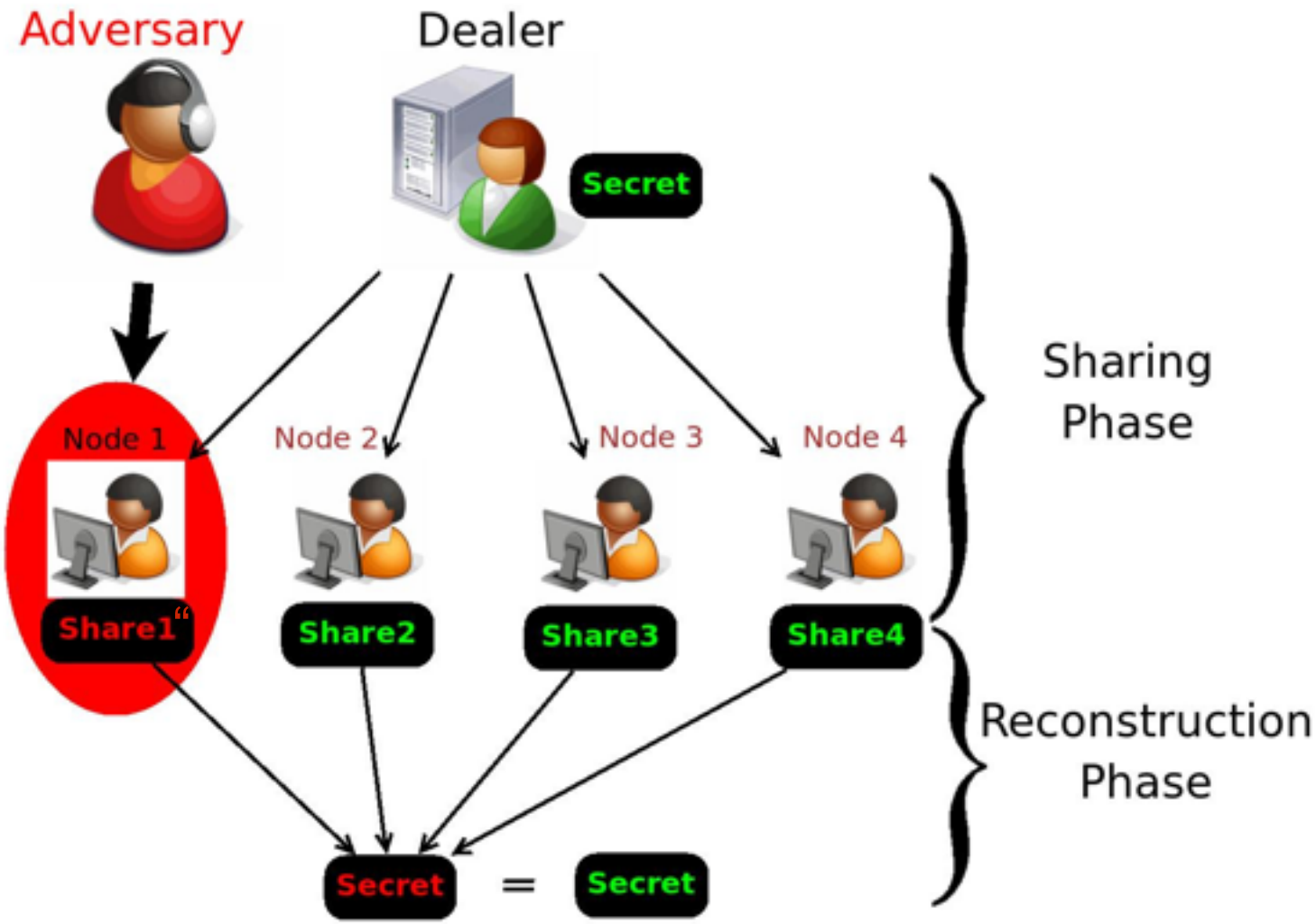
Attacks on Secret Sharing

- Attacking Secrecy/Privacy



Attacks on Secret Sharing

- Attacking Correctness



Bounding Adversary Behavior

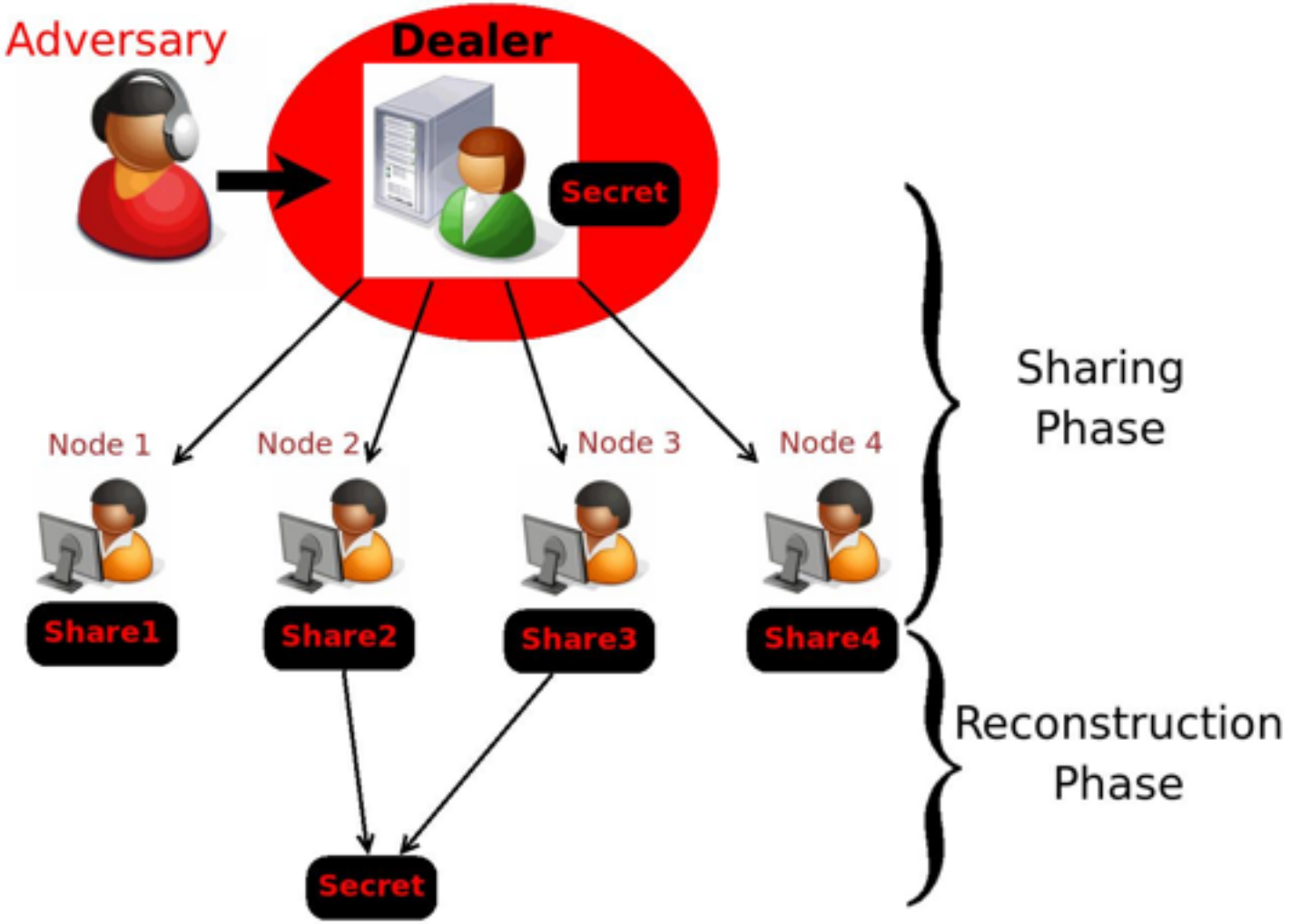
- What is the relation between n and t
  - against a passive adversary controlling any t parties?
  - against an active adversary controlling any t parties?

    (Discussion on the board)

- What if the dealer is malicious?
  - Example Scenarios: Multi-party Computations; Threshold Cryptography

Attacks on Secret Sharing

- Attacking Commitment



Verifiable Secret Sharing

- Secret sharing with three properties
  - Secrecy
  - Correctness
  - Commitment

(Discussion on the board)