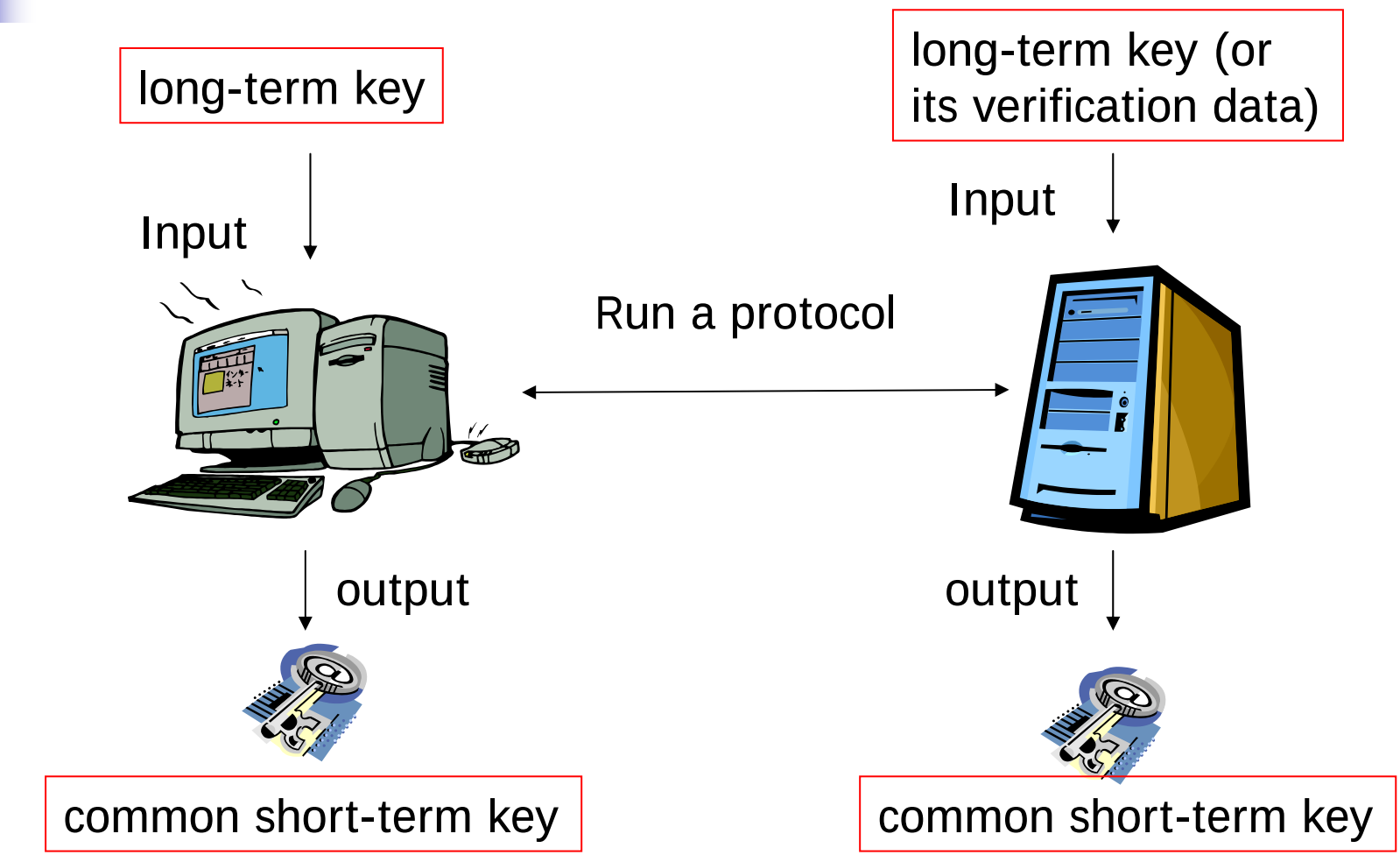
鍵共有の証明可能安全性

東京大学 生産技術研究所
古原 和邦

Authenticated Key Establishment (AKE)



Classification of AKE (1/2)

- # of entities (2 ≦ n)
  - n party + 1 on-line TTP
  - n party + 1 off-line TTP
  - n party + 0 TTP
- Authentication type
  - (Anonymous)
  - One-side
  - Mutual

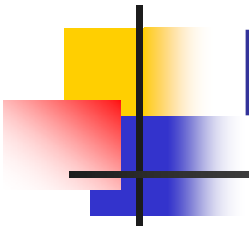
TTP: Trusted Third Party

Classification of AKE (2/2)

- Strength of long term secret
  - Strong secret
    - Signing key
    - Decryption key
    - Long common key
  - Weak secret
    - Human memorable short password

- Underlying problem
  - Discrete-log
    - Diffie-Hellman
  - Factoring
    - RSA
    - Rabin

What should be proven and how?



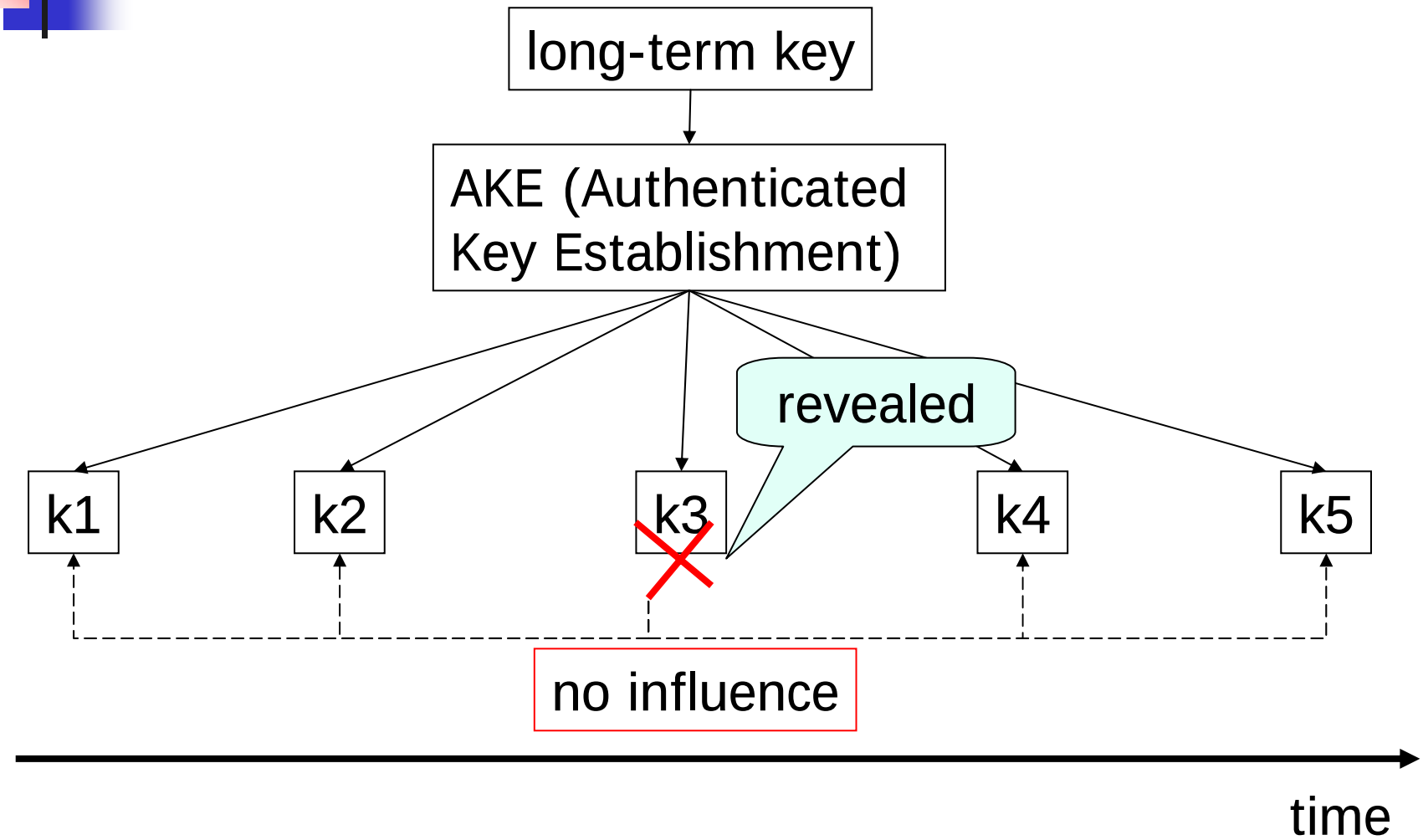
- Achievable goal
  - Usually, guessing any of fresh short term keys is hard
- Against which attacks
- Under some assumptions
  - E.g. DDH problem is hard etc.

- How

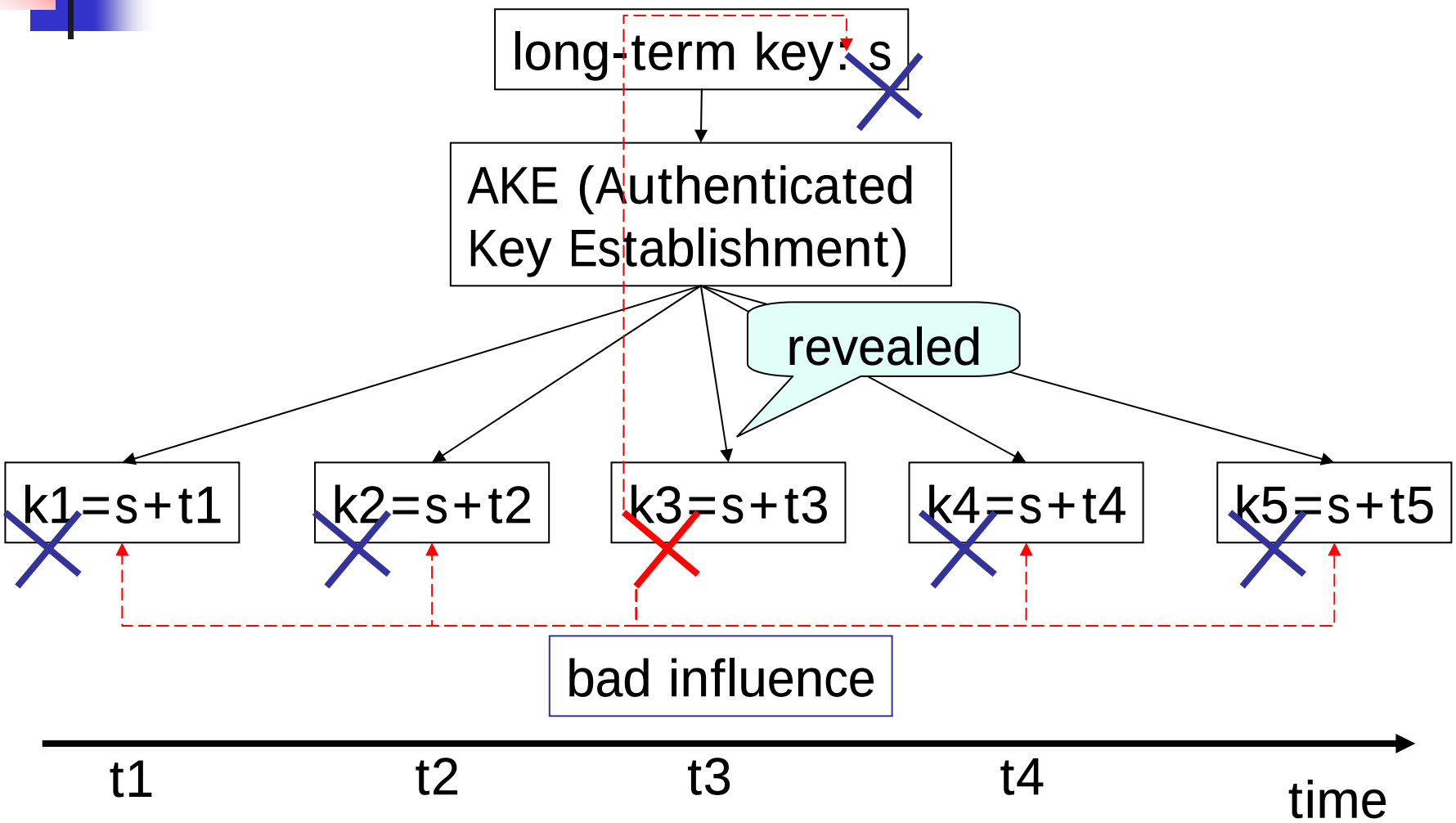
Attacks on AKE

- Eavesdropping
- Impersonation
  - Replay
  - Intruder-in-the-middle
- Short-term key (session key) revealment
- Long-term key corruption (forward secrecy)

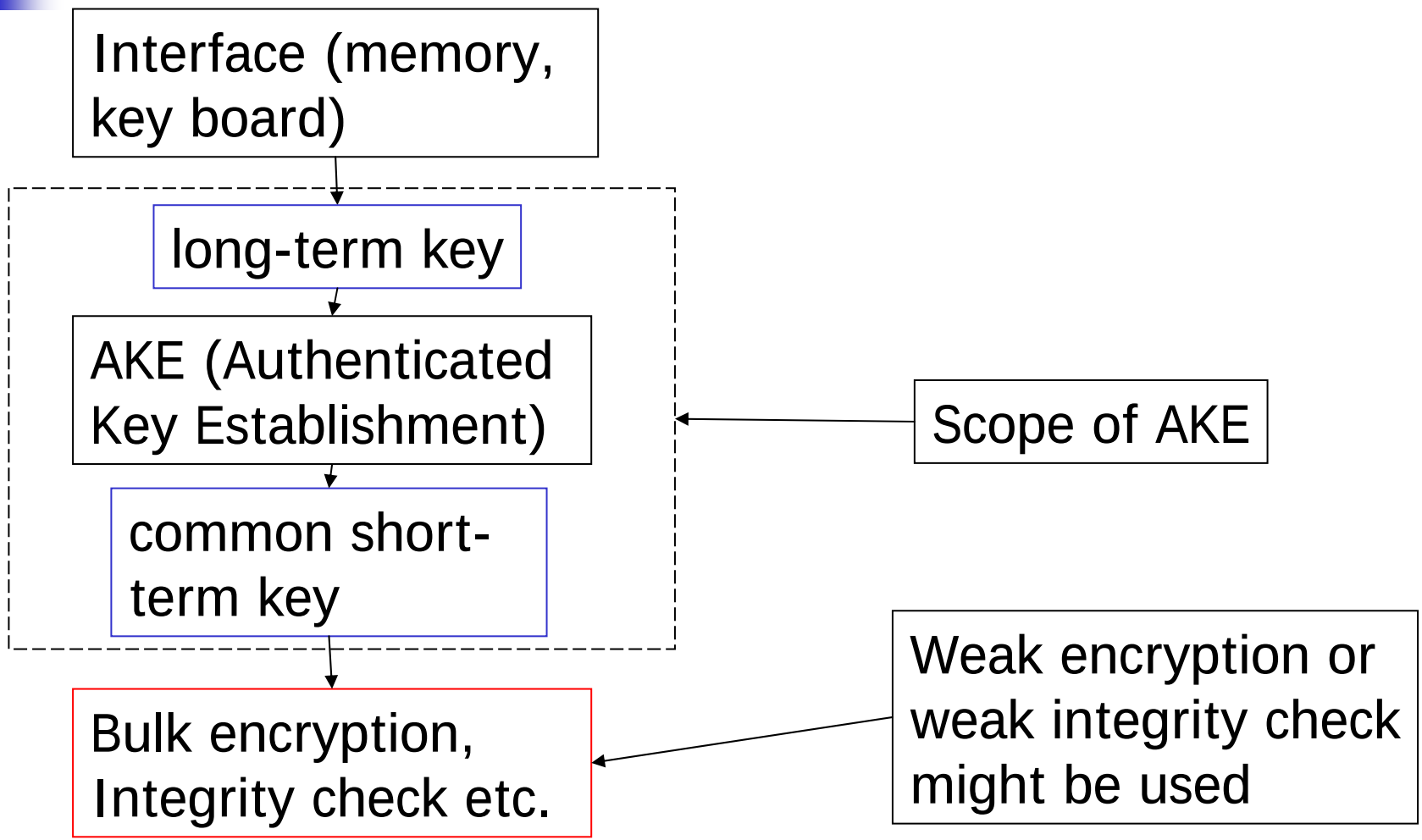
Ideal characteristics against revealment



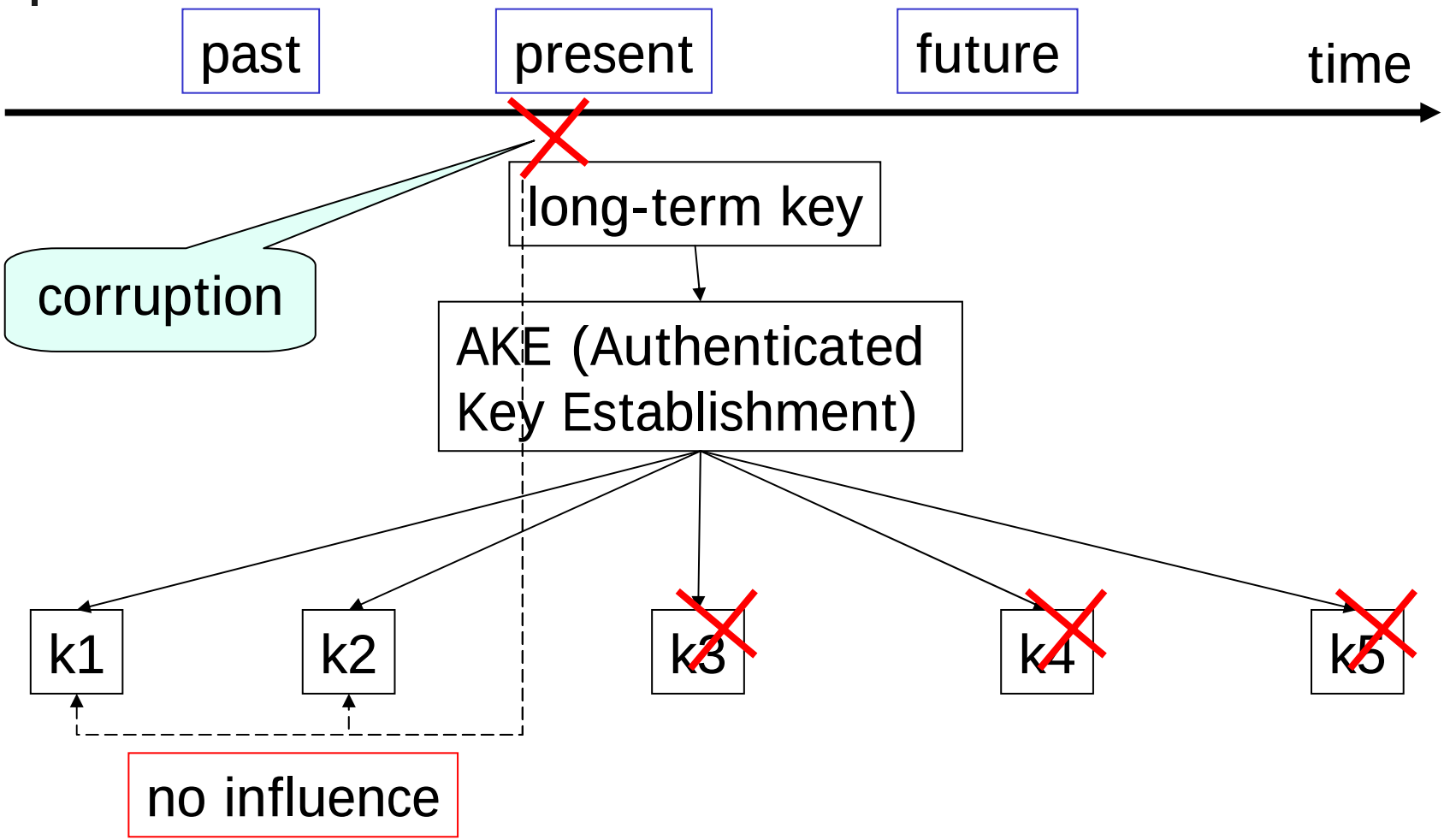
Toy Bad Example



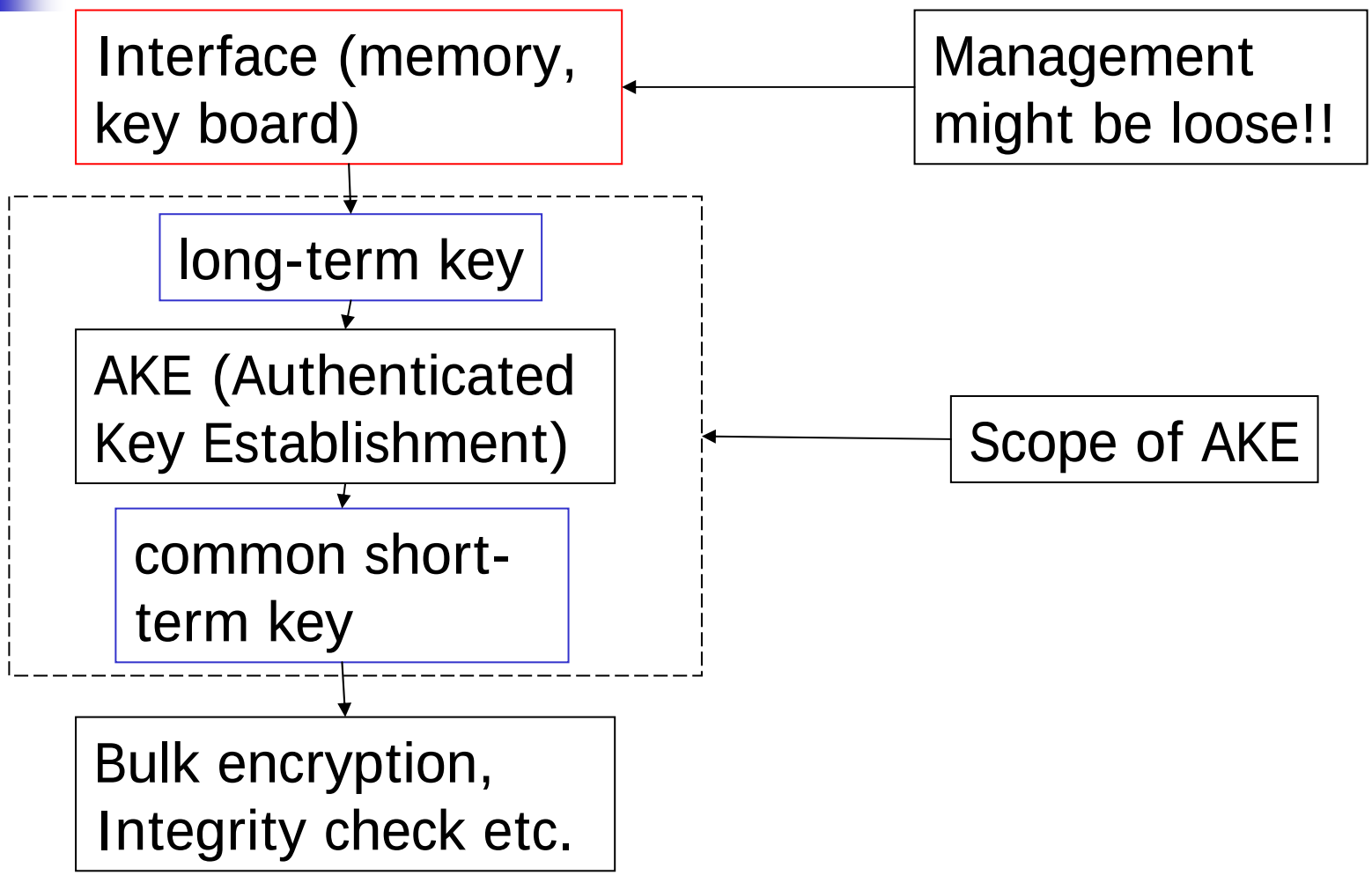
Why Revealment?



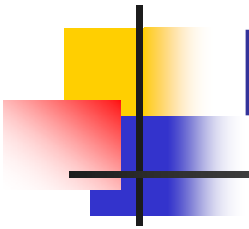
Ideal characteristics against corruption (Forward Secrecy)



Why Corruption?

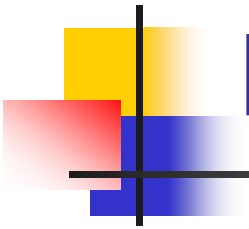


What should be proven and how?



- Achievable goal
  - Usually, guessing any of fresh short term keys is hard
- Against which attacks
- Under some assumptions
  - E.g. DDH problem is hard etc.

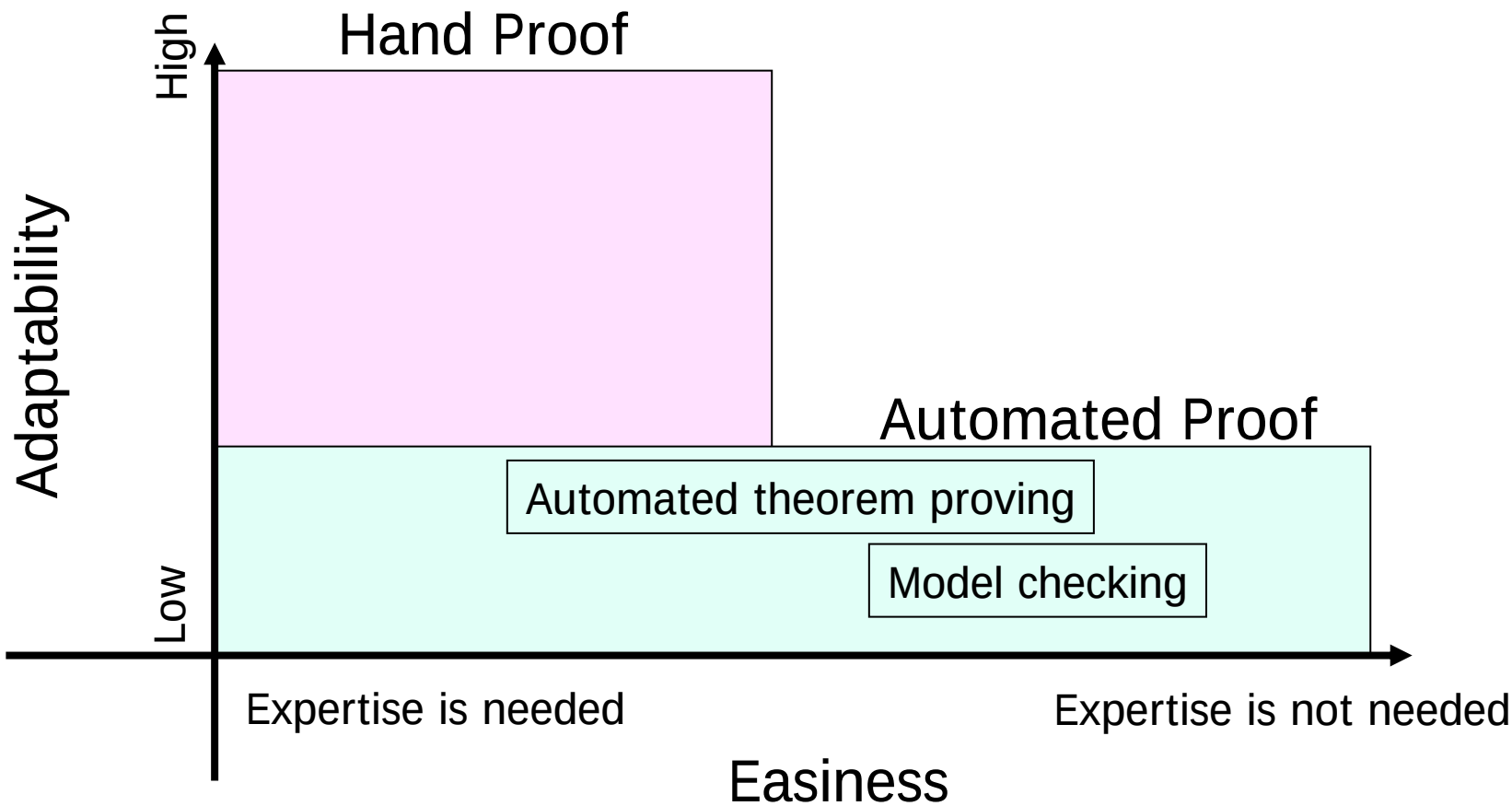
- How



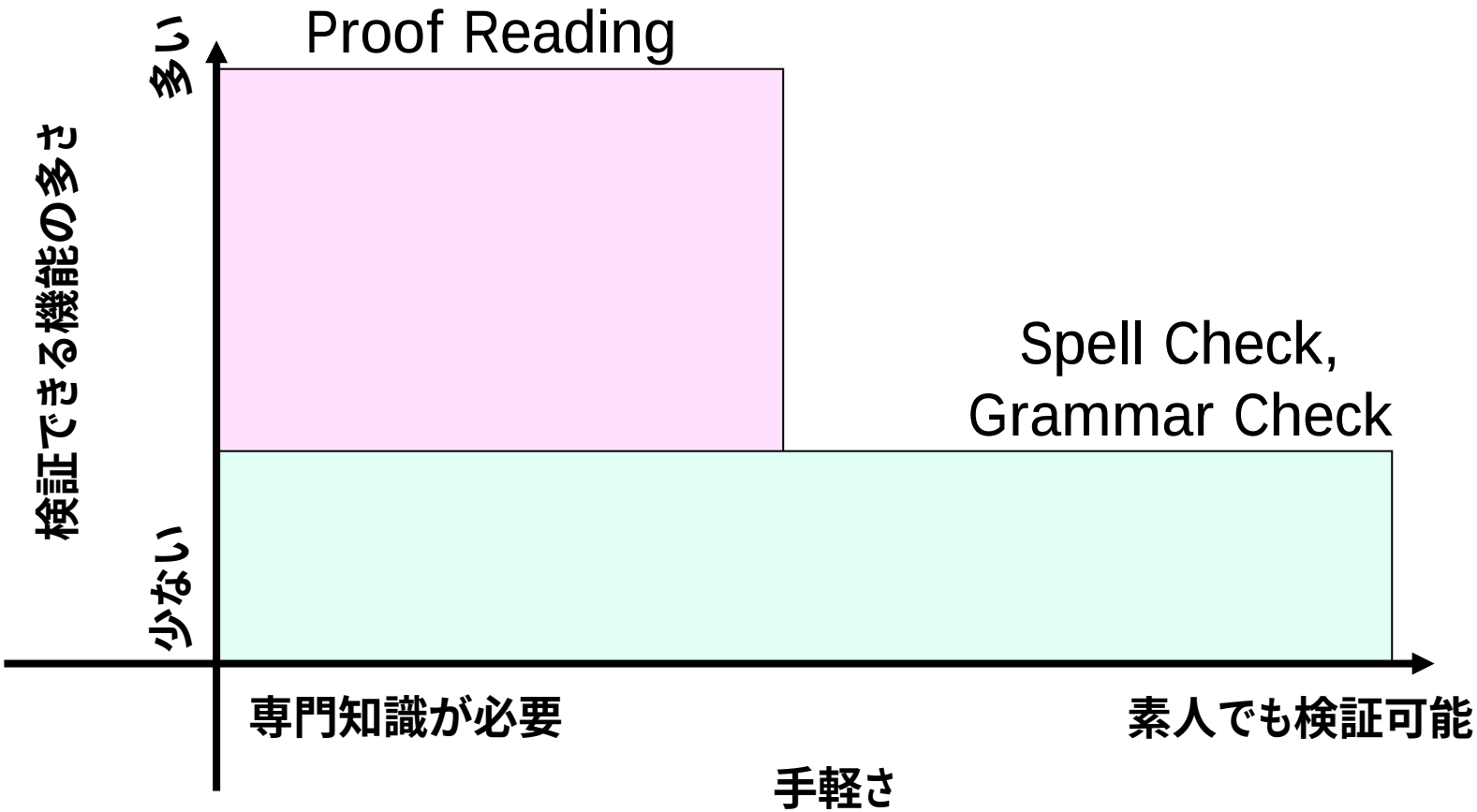
How to prove

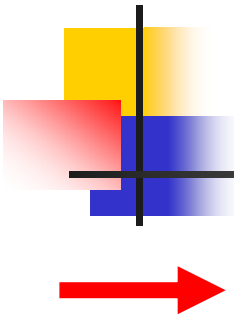
- Hand Proof
  - Reduction approach
  - Real-world-ideal-world approach
- Automated Proof (Formal Verification)
  - Model checking
    - Exhaustive search of all possible states
  - Automated theorem proving
    - Automation of usual proof techniques

Hand vs. Automated



英語の文章に例えると

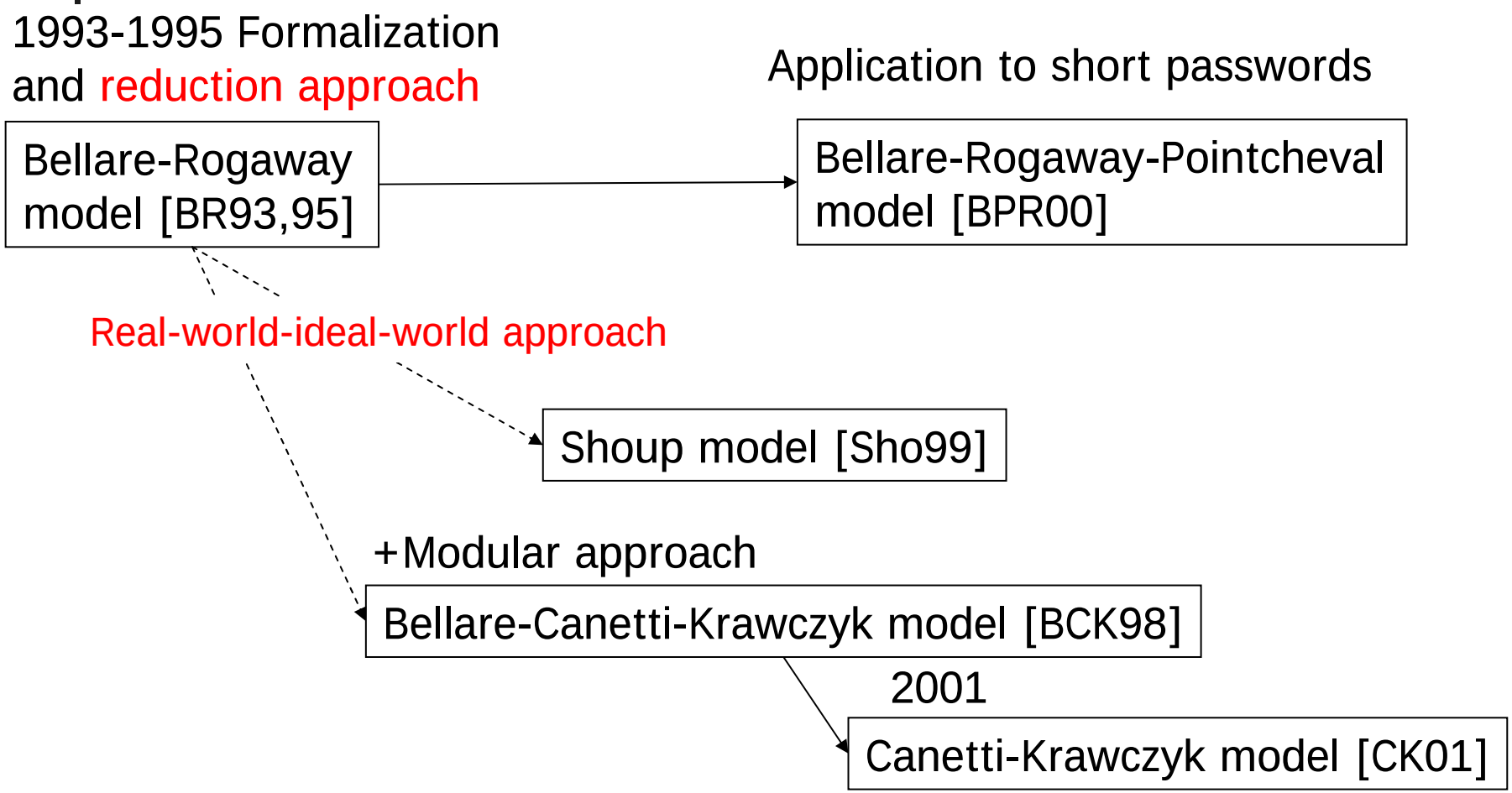

Proof Reading
Spell Check,
Grammar Check
多い
少ない
検証できる機能の多さ
専門知識が必要
素人でも検証可能
手軽さ



How to prove

- Hand Proof
  - Reduction approach
  - Real-world-ideal-world approach
- Automated Proof (Formal Verification)
  - Model checking
    - Exhaustive search of all possible states
  - Automated theorem proving
    - Automation of usual proof processes

History of Hand Proof

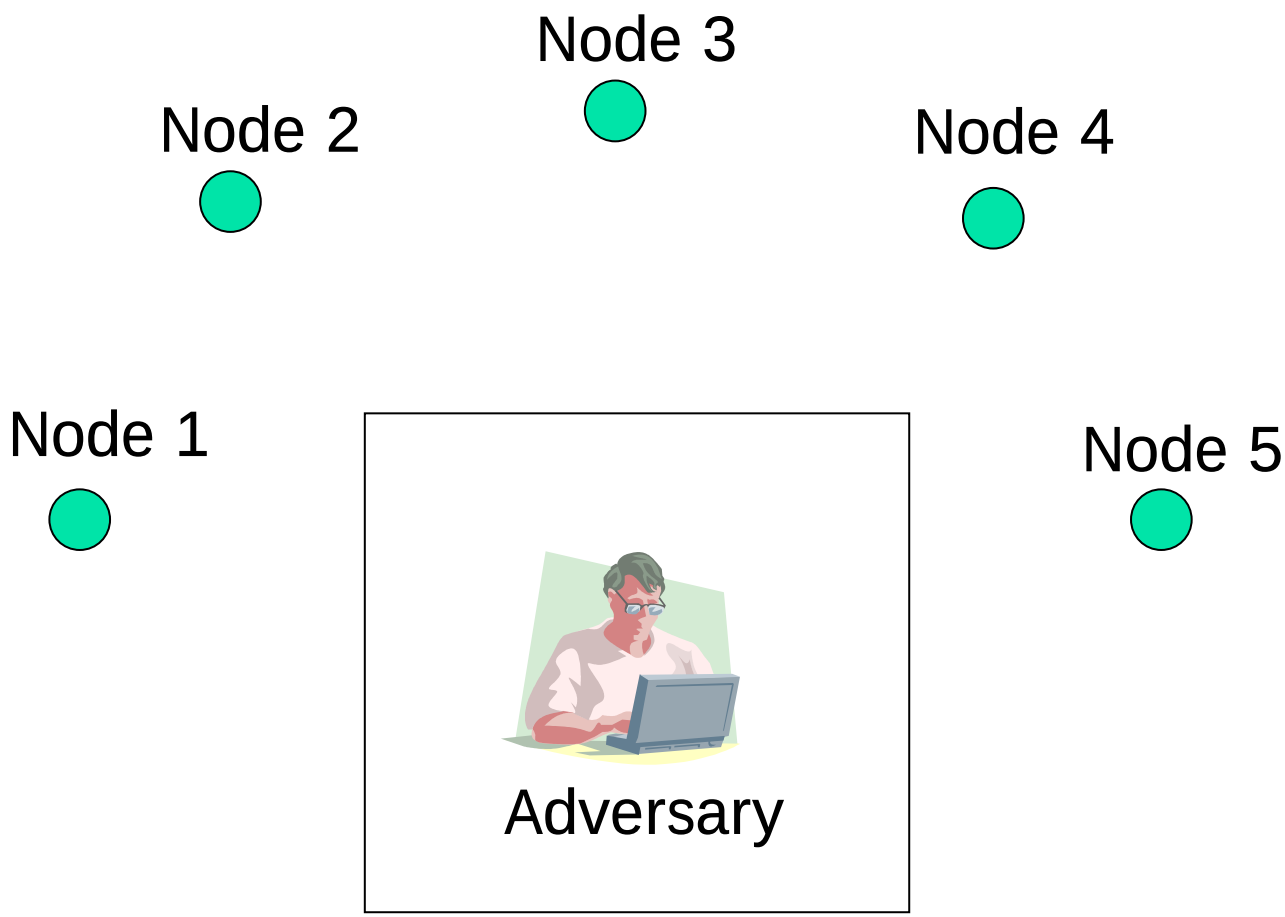


How to prove

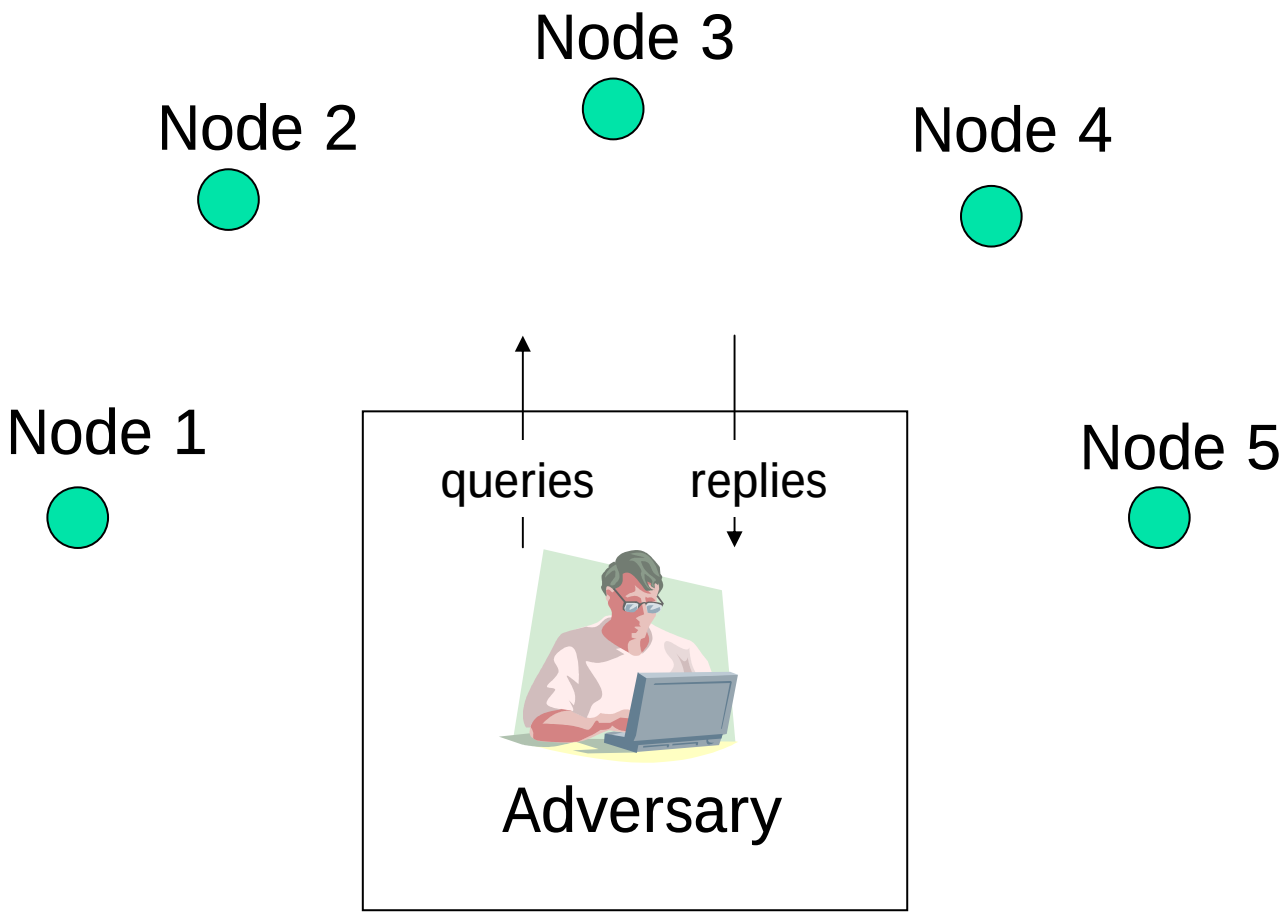
Common Procedures

- Hand Proof
  - Reduction approach
  - Real-world-ideal-world approach
- Automated Proof (Formal Verification)
  - Model checking
    - Exhaustive search of all possible states
  - Automated theorem proving
    - Automation of usual proof processes

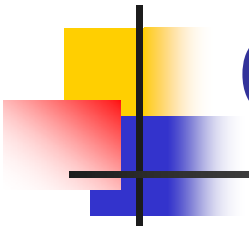
Adversary's View (1/2)



Adversary's View (2/2)

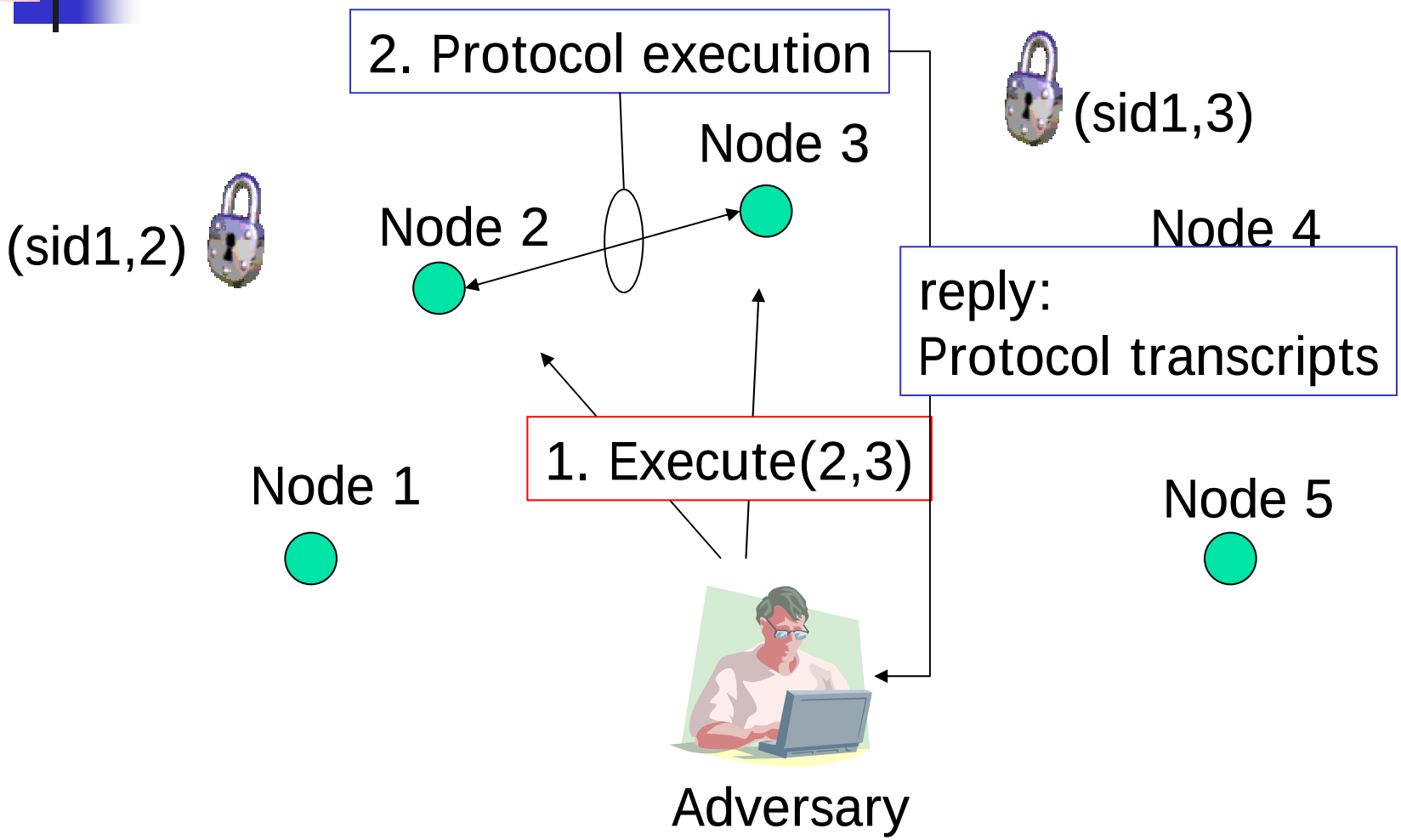


Oracles modeling the attacks

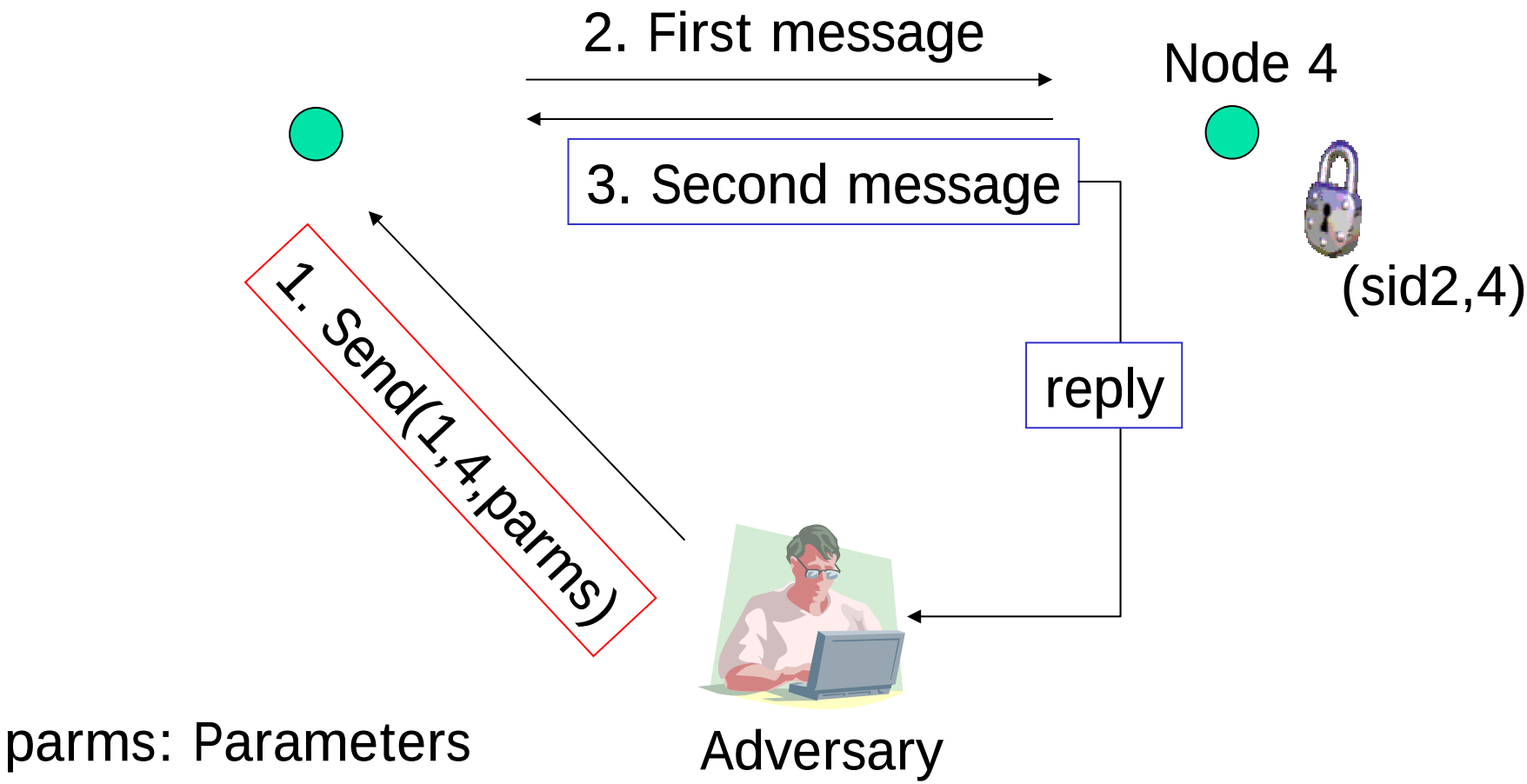


- Eavesdropping
  - -> Execute Oracle
- Impersonation
  - -> Send Oracle
- Short-term key revealment
  - -> Reveal Oracle
- Long-term key corruption
  - -> Corrupt Oracle

Execute Query

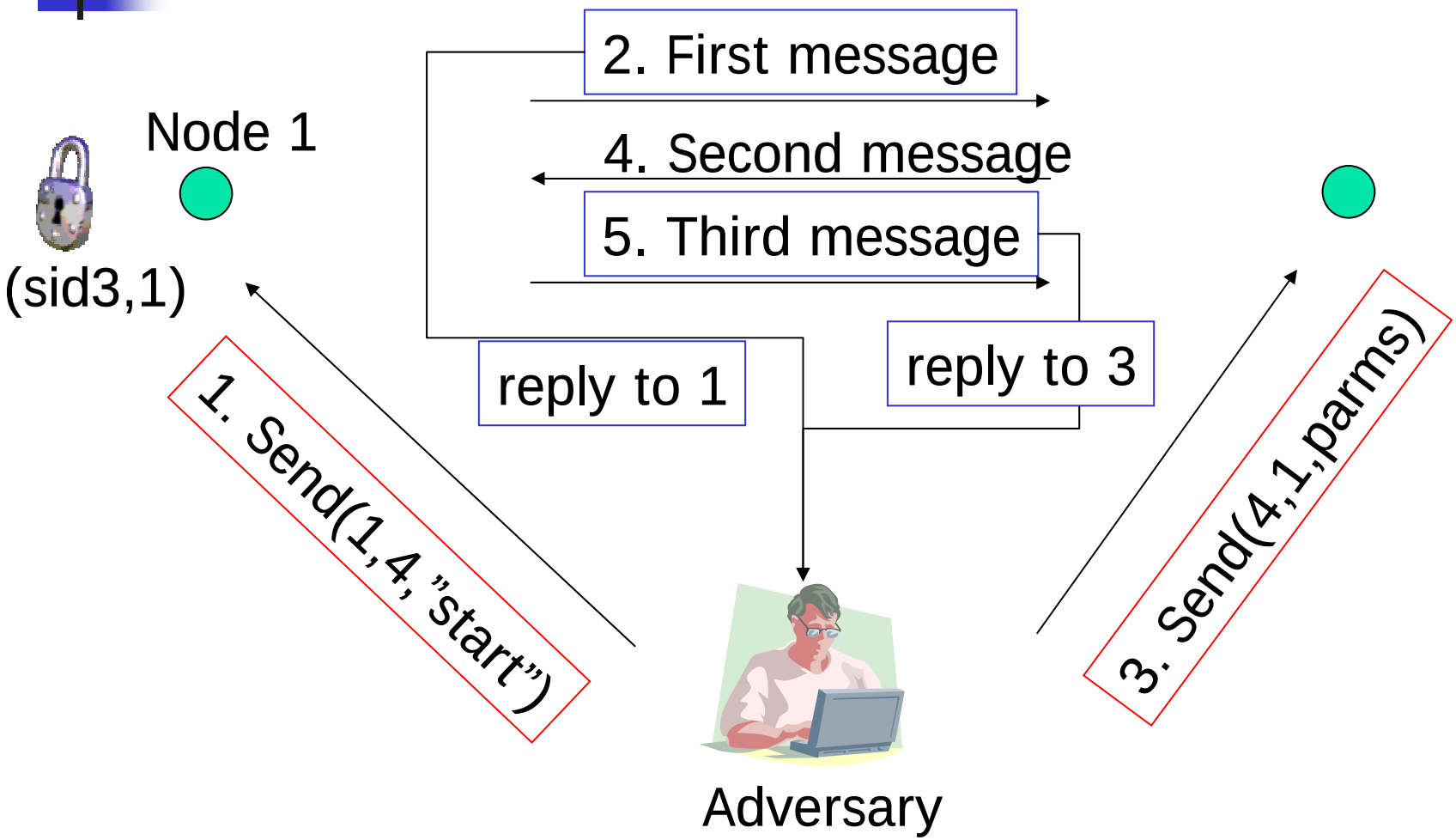


Send Query: Impersonation of Node 1

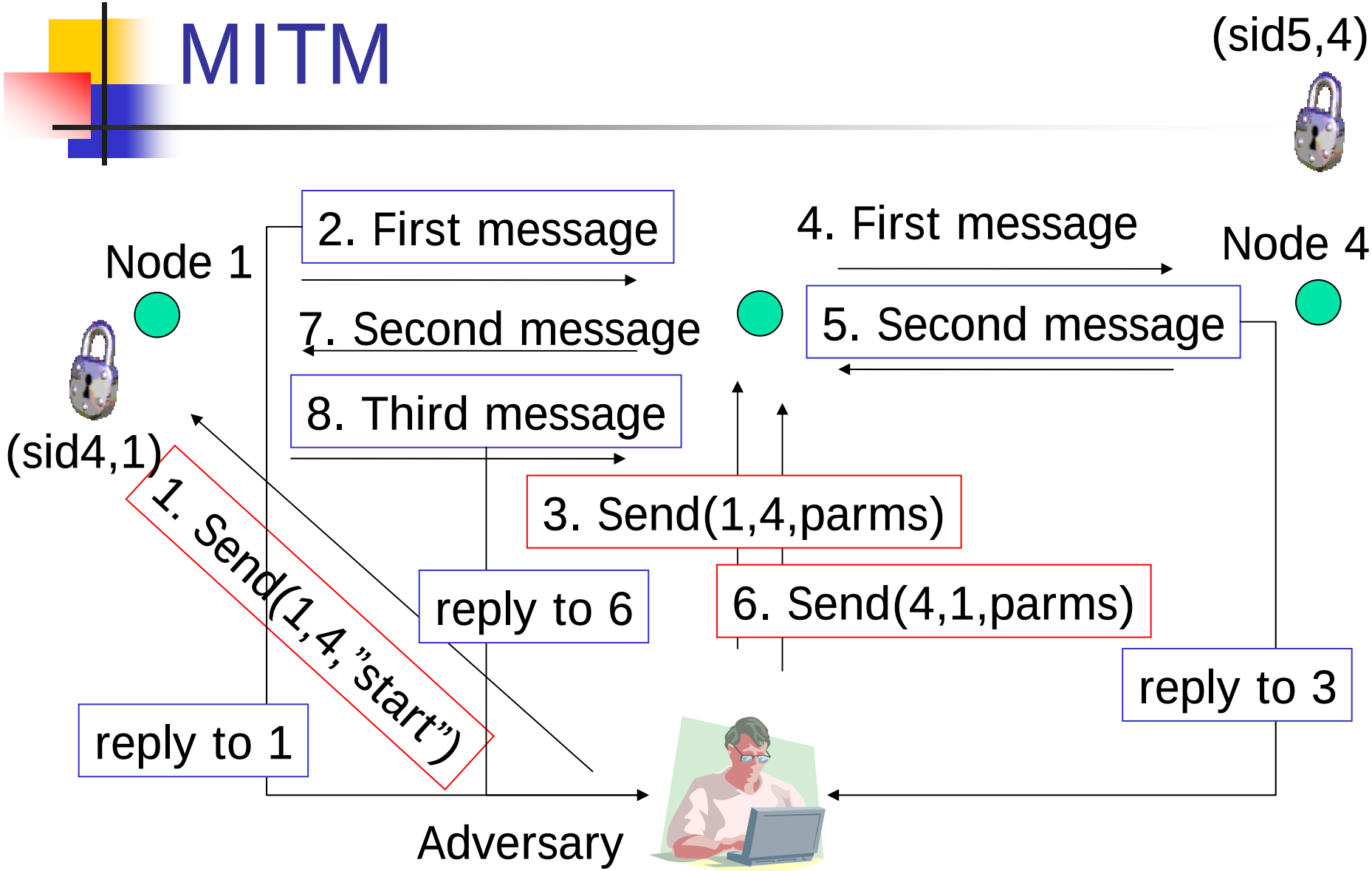


parms: Parameters

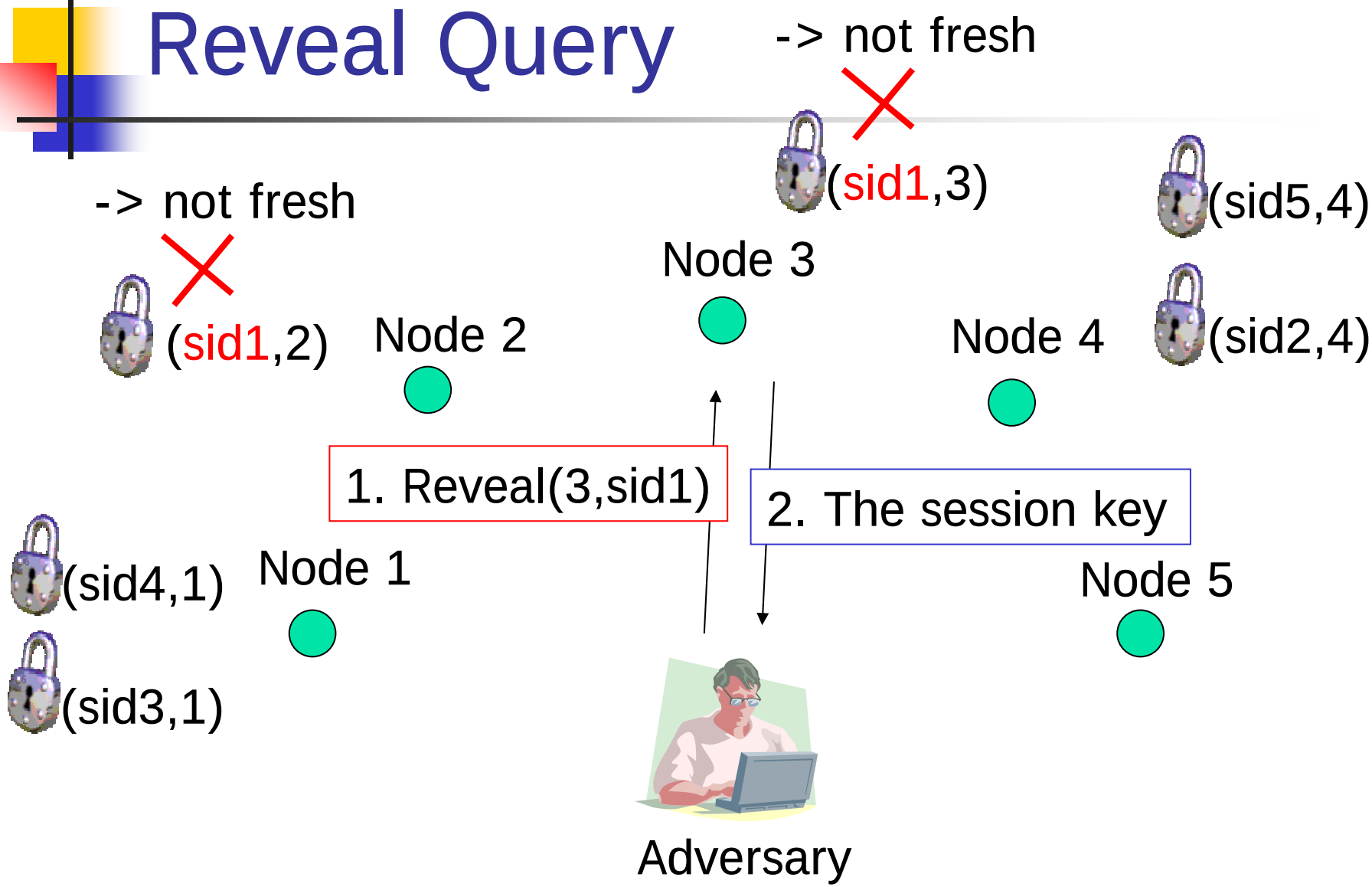
Send Query: Impersonation of Node 4



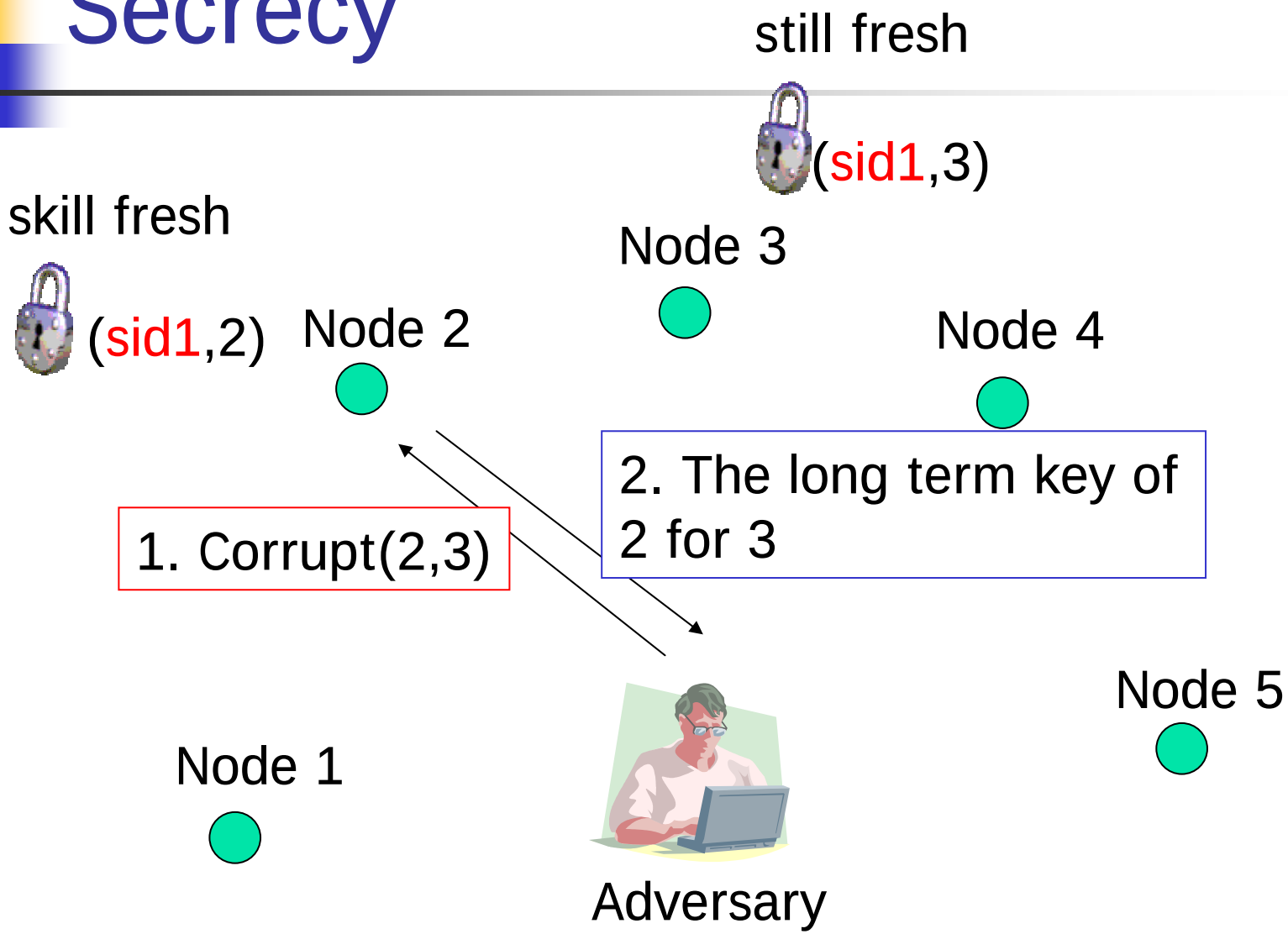
Send Query: MITM



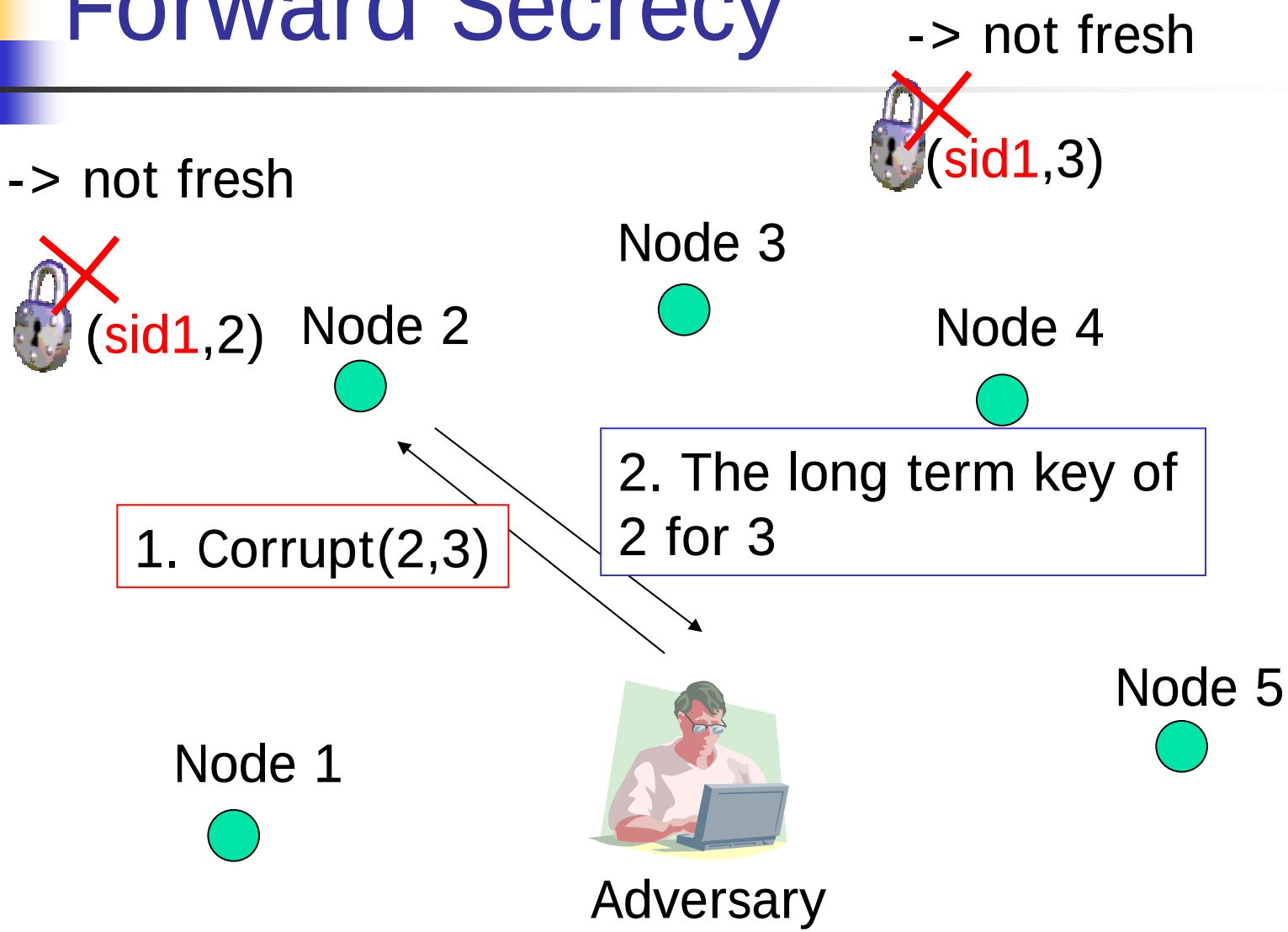
Reveal Query



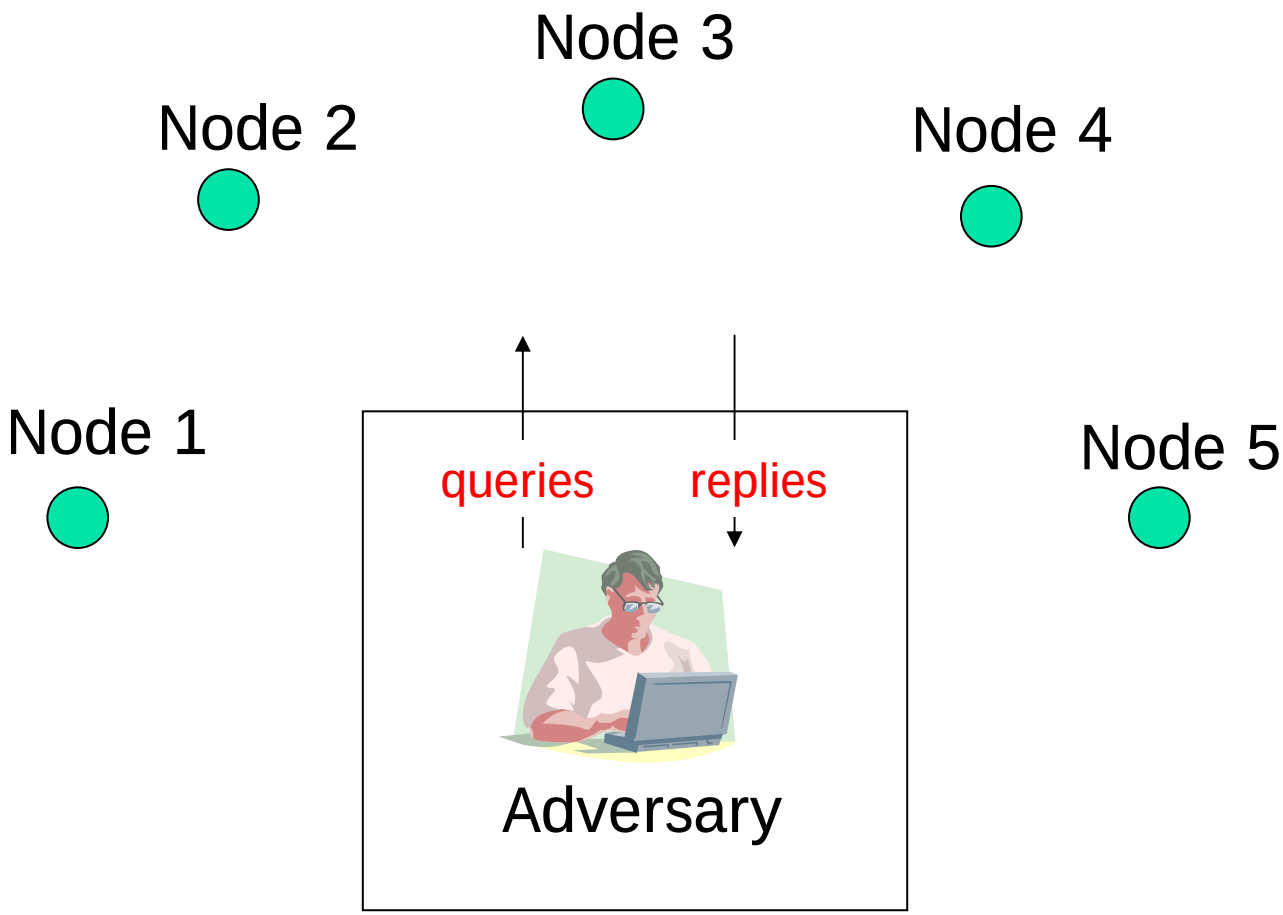
Corrupt Query for Forward Secrecy



Corrupt Query for Non Forward Secrecy



Adversary's View

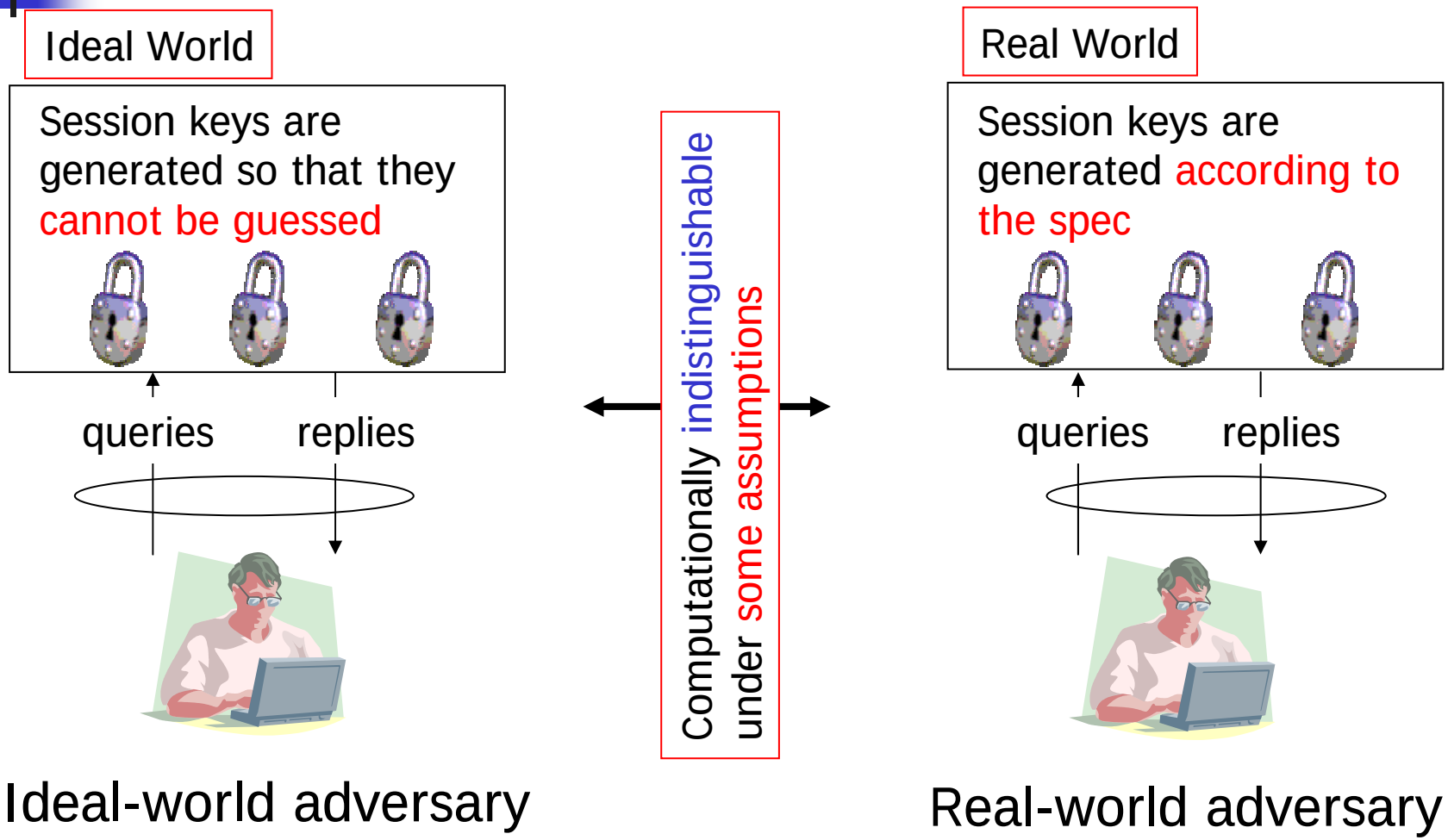


How to prove

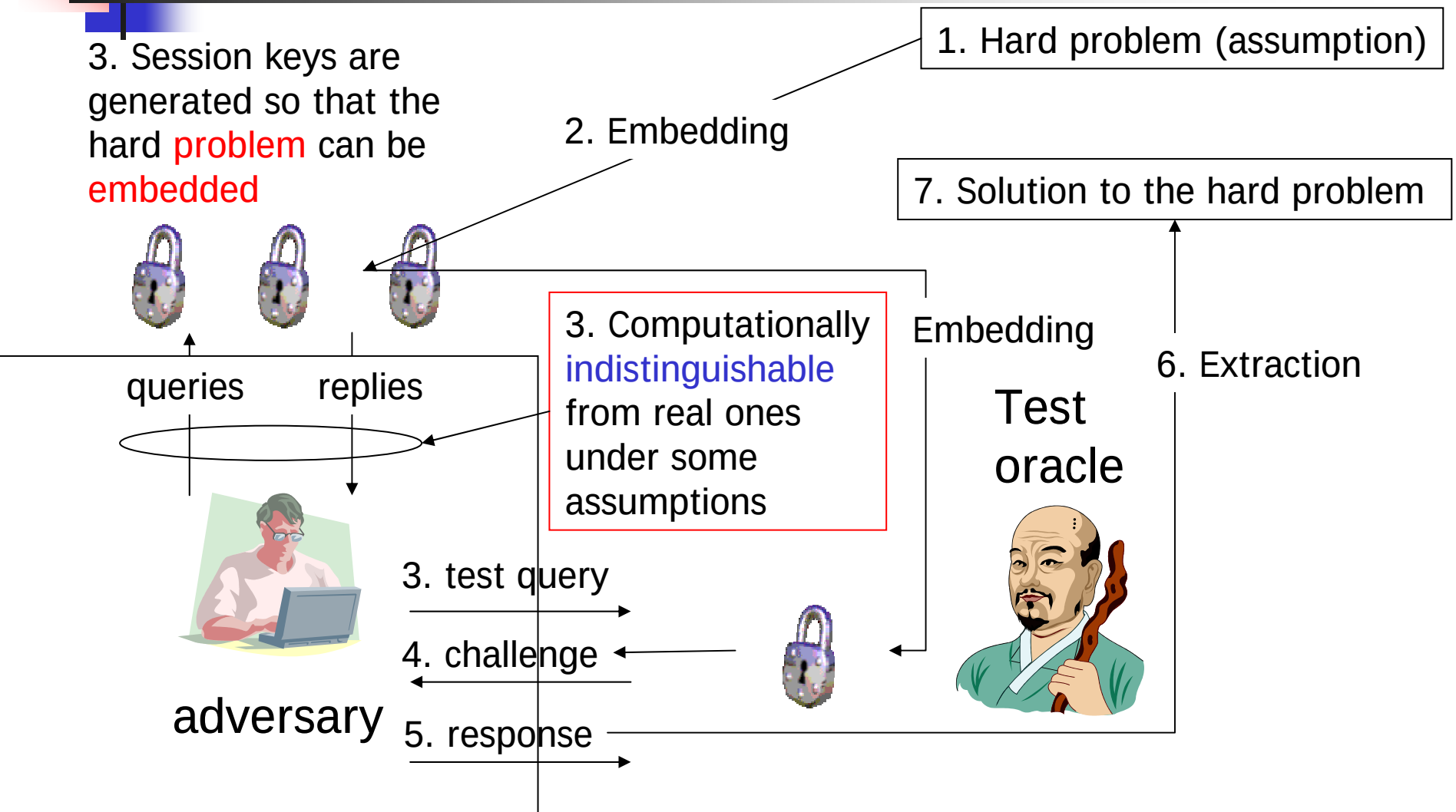
Differences

- Hand Proof
  - Reduction approach
  - Real-world-ideal-world approach
- Automated Proof (Formal Verification)
  - Model checking
    - Exhaustive search of all possible states
  - Automated theorem proving
    - Automation of usual proof processes

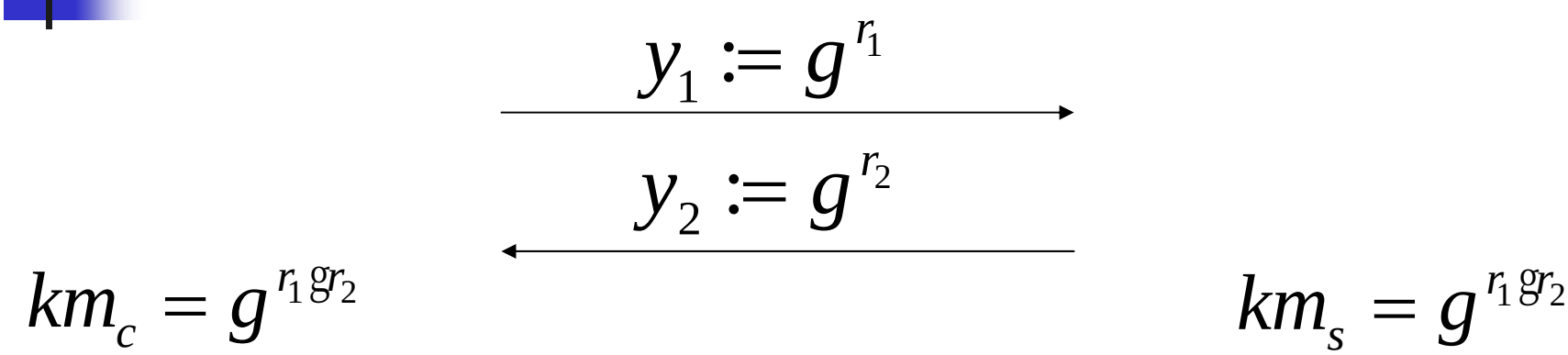
Real-World-Ideal-World Approach



Reduction Approach



Toy Example: Anonymous DH

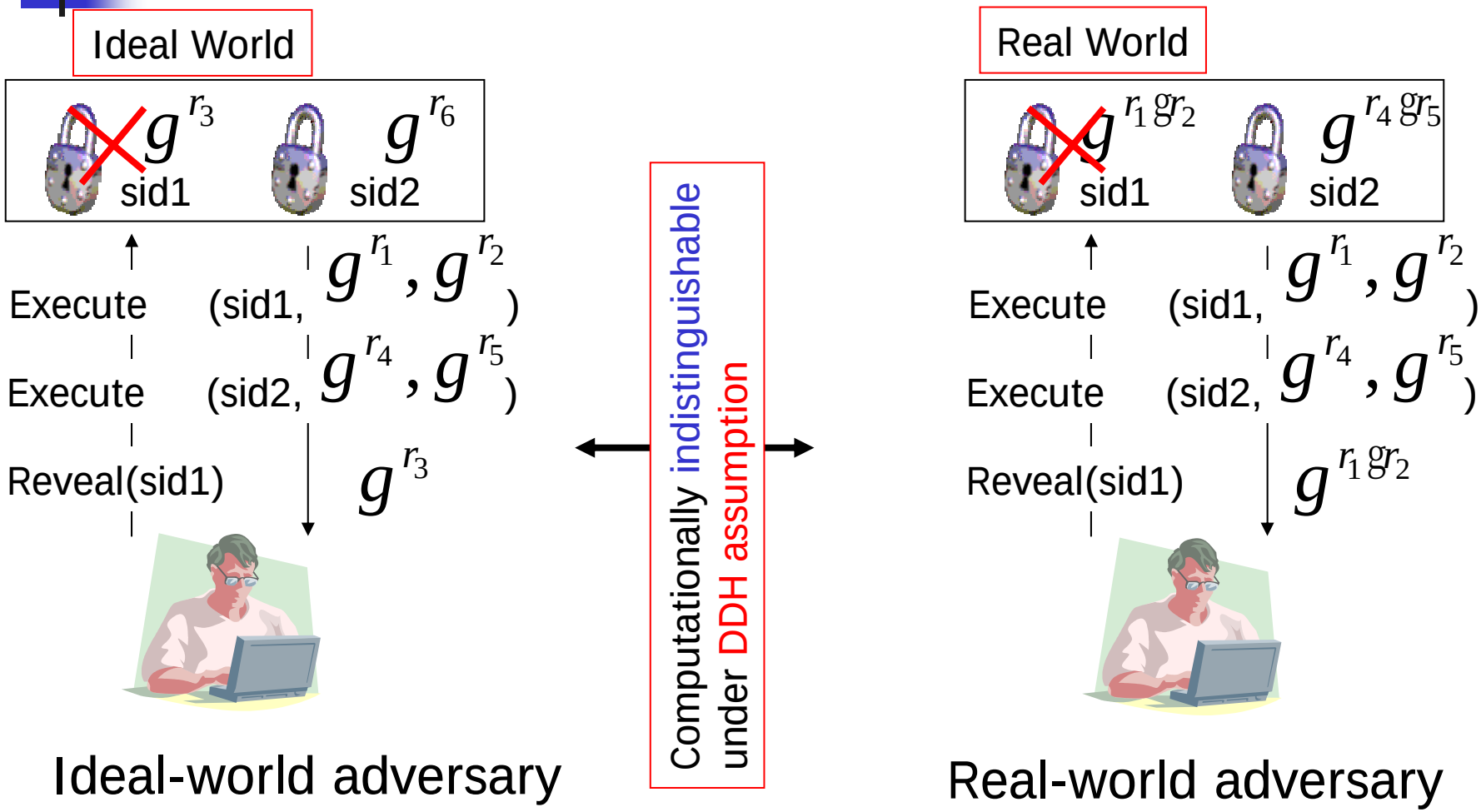


- Assumption:
  - DDH is hard, i.e. $(g^{r_1}, g^{r_2}, g^{r_1 r_2}) \approx (g^{r_1}, g^{r_2}, g^{r_3})$

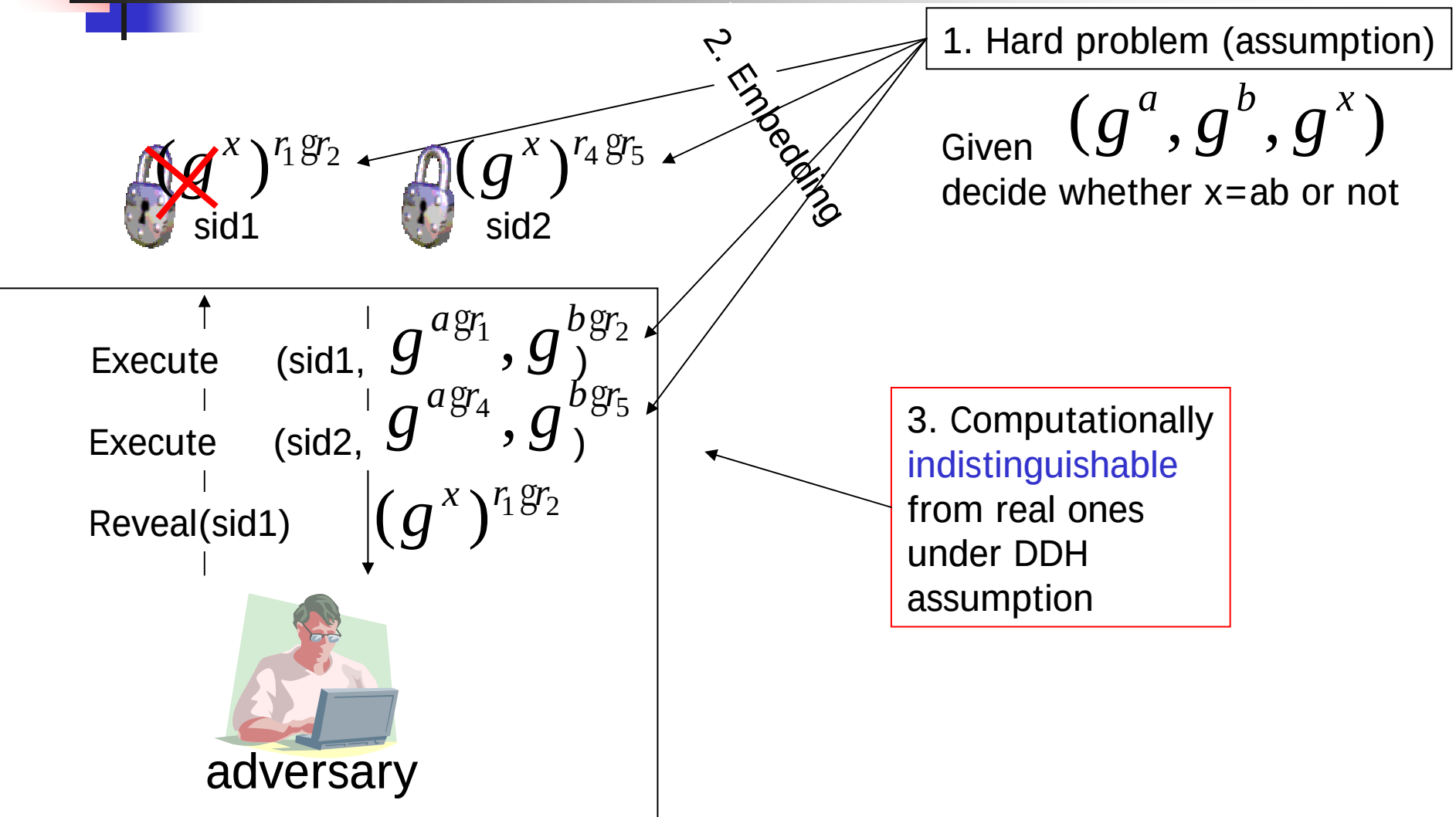
Computationally Indistinguishable

  - Only Execute and Reveal queries are allowed

Proof in Real-World-Ideal-World Approach



Proof in Reduction Approach (1/2)



Proof in Reduction Approach (2/2)

1. Hard problem (assumption)

Given (g^a, g^b, g^x)
decide whether x=ab or not

$(g^x)^{r_1} g^{r_2}$ sid1

$(g^x)^{r_4} g^{r_5}$ sid2

3. Test(sid2)

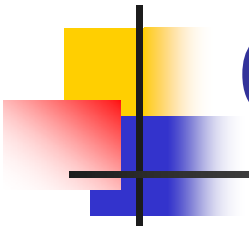
4. challenge:
Given
decide "real" or "random"


adversary

5. response

6. Extraction

If "real" x=ab.
Otherwise x≠ab.



Conclusion

- Explained the idea behind hand proofs

- Adversary's view
- Oracle queries
  - Execute, Send, Reveal and Corrupt
- Reduction approach
- Real-world-ideal-world approach