ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

Algorithms for Radio Networks

Public Key Cryptography and Byzantine Generals Problems

University of Freiburg
Technical Faculty
Computer Networks and Telematics
Prof. Christian Schindelhauer

CoNe Freiburg

IIF
INSTITUT FÜR
INFORMATIK
FREIBURG

Asymmetric Encryption

- **E.g. RSA, Ronald Rivest, Adi Shamir, Lenard Adleman, 1977**
  - Diffie-Hellman, PGP
- **Secret key: sk**
  - Only the receivers of the message know the secret key
- **Public key: pk**
  - All participants know this key
- **Generated by**
  - keygen(sk) = pk
- **Encryption function f and decryption function g**
  - Known to everybody
- **Encryption**
  - f(pk,text) = code
  - everybody can generate code
- **Decryption**
  - g(sk,code) = code
  - only possibly by receiver

Example: RSA

- **R. Rivest, A. Shamir, L. Adleman**
  - On Digital Signatures and Public Key Cryptosystems, Communication of the ACM
- **Algorithm is based on the computational complexity of integer factorization**
- **1st example**
  - 15 =   ? * ?
  - 15 = 3 * 5
- **2nd example**
  - 386581864584112731912956727734835955 744479041028993358648355204744 3 = 123456789012345678901234567890020 9 * 313131313131313131313131313130022 7

- **To this day no efficient integer factorization algorithm is known**
  - Yet, multiplication can be done efficiently
  - Prime numbers can be found efficiently
    - Since prime numbers occur frequently
    - Efficient randomized prime number tests are available

RSA

- **Generation of keys**
  - Choose two random prime numbers p, q with k bits ($k \geq 500$).
  - $n = p \cdot q$
  - e is a number relatively prime to $(p - 1) \cdot (q - 1)$.
  - $d = e^{-1} \bmod (p - 1)(q - 1)$
    - i.e. $d \cdot e \equiv 1 \bmod (p - 1)(q - 1)$
- **Public key pk = (e, n)**
- **Secret key sk = (d, n)**
- **Encoding**
  - Partition message in block sizes of 2k bits
  - Interprete block M as number $0 \leq M < 2^{2k}$
  - Code: $P(M) = M^e \bmod n$
- **Decoding**
  - $S(C) = C^d \bmod n$
- **Correctness follow from the little theorem of Fermat**

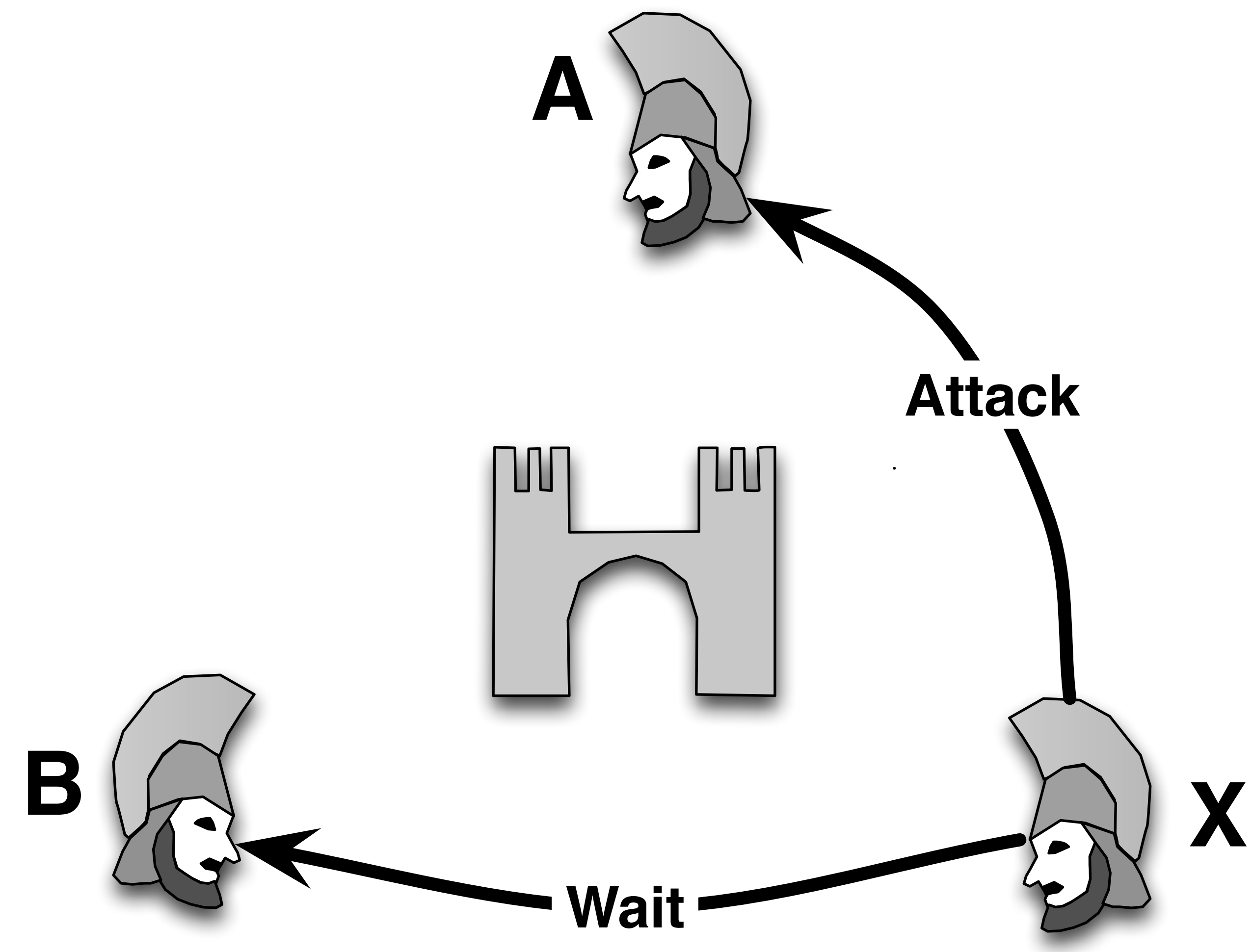
Digital Signatures

- **Digital Signatures**
  - signer has a secret key **sk**
  - document will be signed with the secret key
  - and can be verified with a public key **pk**
  - public key is known to all

- **Example of a signature scheme**
  - m: message
  - Signer
    - computes **h(text)** with cryptographic hash function **h**
    - and publishes m and **signature = g (sk, h (text))**, **g** is the decryption function
  - Checker
    - computes h(text)
    - and verifies **f (pk, signature) = h (text)** for the asymmetric encryption function **f**

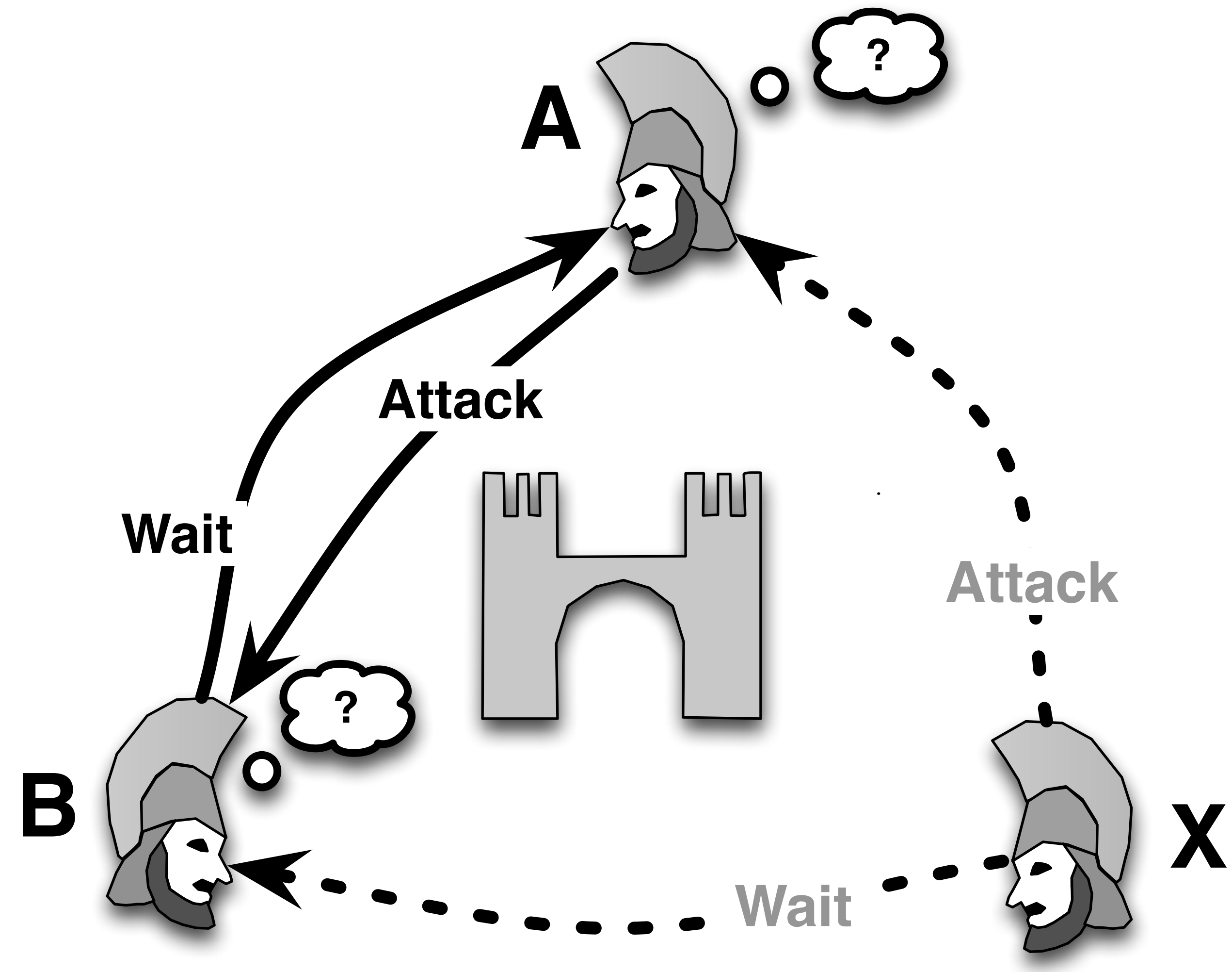
Problem of Byzantine Generals

- **After the hijacking of a node in a network it can cause malicious actions on the network**
  - This problem is known as the Byzantine Generals problem
- **3 armies are ready to conquer the enemy castle**
  - These are separated and communicate via messengers
  - If only army attacks then all will loose
  - If two armies atteck, they will win
  - If no army attacks, they will win
    - (because the defenders will starve out)
- **But one general is an evil traitor**
  - you do not know who ...



Problem of Byzantine Generals

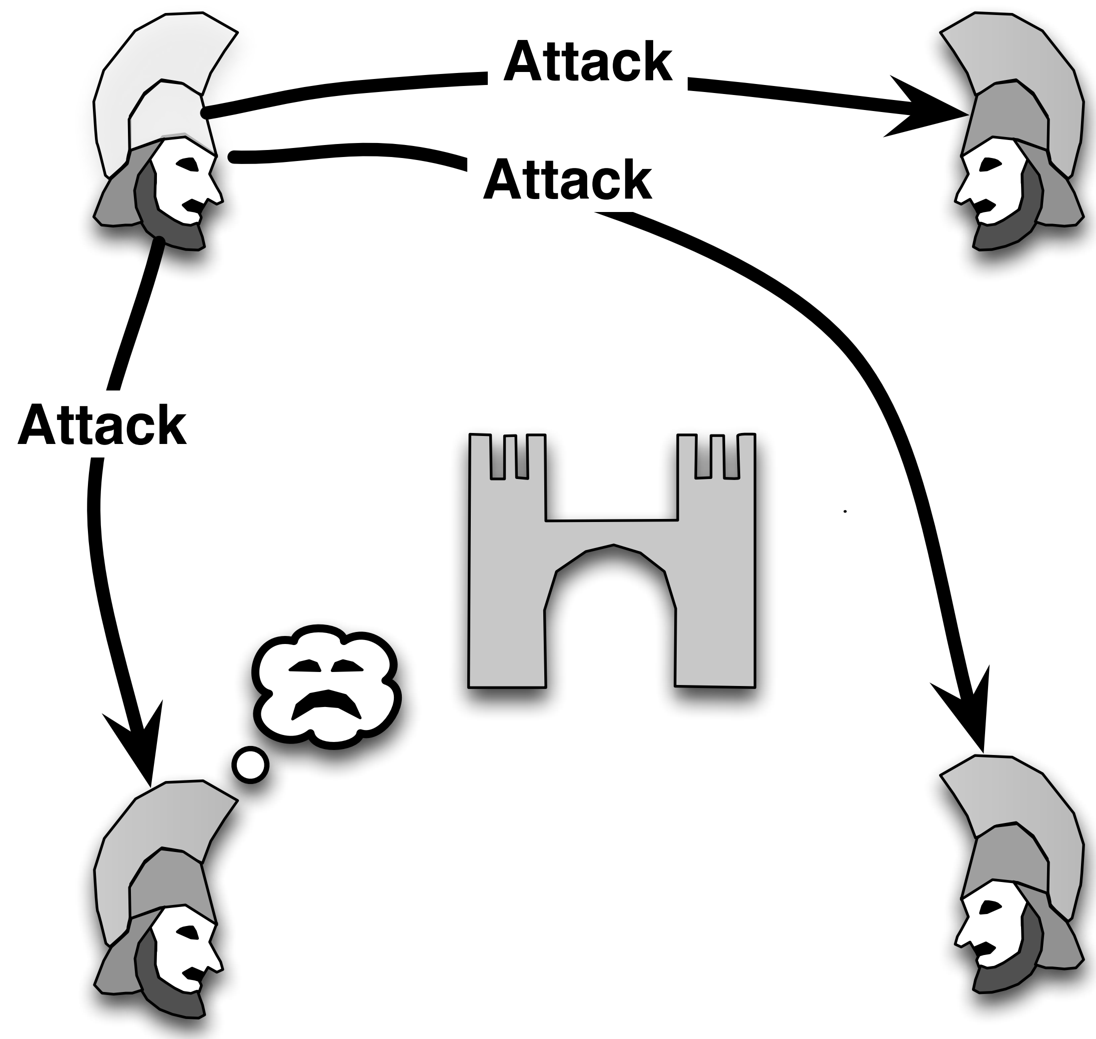
- **The traitorous general X tries to**
  - persuade A to attack
  - persuade Be to wait
- **A tells B about the command**
- **B tells A about the command**
  - Something is wrong
  - But nobody can tell who is cheating
    - Even after further communication



Byzantine Agreement

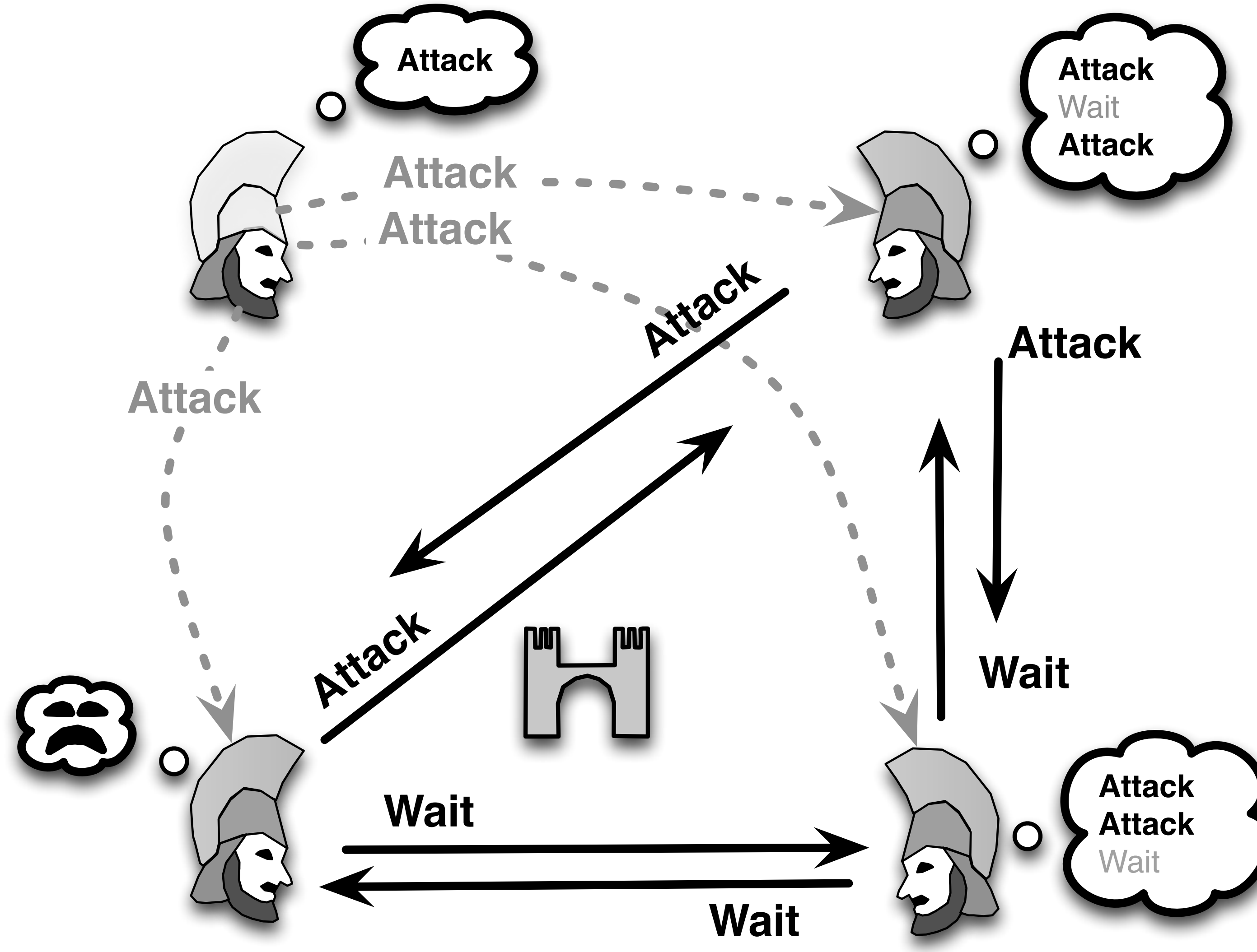
- **Theorem**
  - The problem of the three Byzantine generals cannot be solved*
- **For four generals, the problem is solvable**

* if all participants have no computing limitations



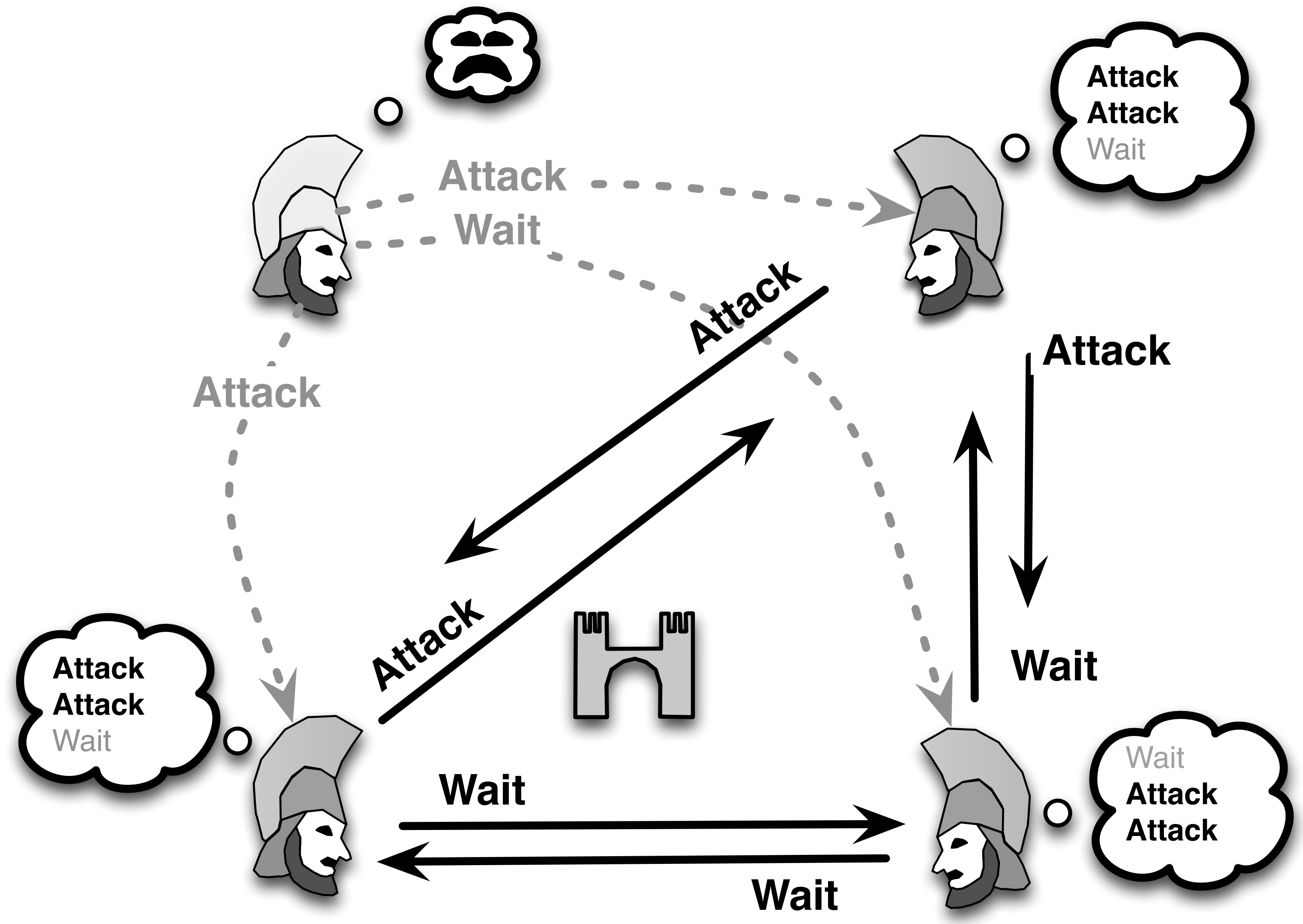
Byzantine Agreement

- **For four generals, the problem is solvable:**
  - 1 general, 3 officers problem
  - consider a (loyal) general and three officers.
  - Disseminate information to all officers of the loyal generals
- **Algorithm**
  - General A sends his command to all others
    - A follows his own command
  - Any other office sends that its received order to all others
  - Each officer calculates the majority decision of the orders of B, .., D



Byzantine Agreement
What if General A is a Traitor

- **For four generals, the problem is solvable:**
  - 1 general, 3 officers problem
  - consider a (loyal) general and three officers.
  - Disseminate information to all officers of the loyal generals
- **Algorithm**
  - General A sends his command to all others
    - A follows his own command
  - Any other office sends that its received order to all others
  - Each officer calculates the majority decision of the orders of B, .., D



Solution of the Byzantine General Problem

- **Theorem**
  - If m generals are traitors, then at least 2m +1 generals must be honest such that the problem of the Byzantine Generals is solvable.
- **This barrier is tight if we do not allow cryptography**
  - i.e. if you have powerful computers which can break into every encryption
- **Theorem**
  - If a digital signature scheme is available, then any number of false generals can be dealt with
- **Solution:**
  - Every general signs his commands
  - In each round every general forwards all commands and signatures to all others
  - Each inconsistent command or false forwarding can be immediately detected and proved
  - False silence or changed commands can be detected

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithms for Radio Networks

Public Key Cryptography and Byzantine Generals Problems

University of Freiburg
Technical Faculty
Computer Networks and Telematics
Prof. Christian Schindelhauer

CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG