ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithms for Radio Network

Security for GSM, UMTS, WEP, WPA and TinySec

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

CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG

Security Requirements Mobile Phones

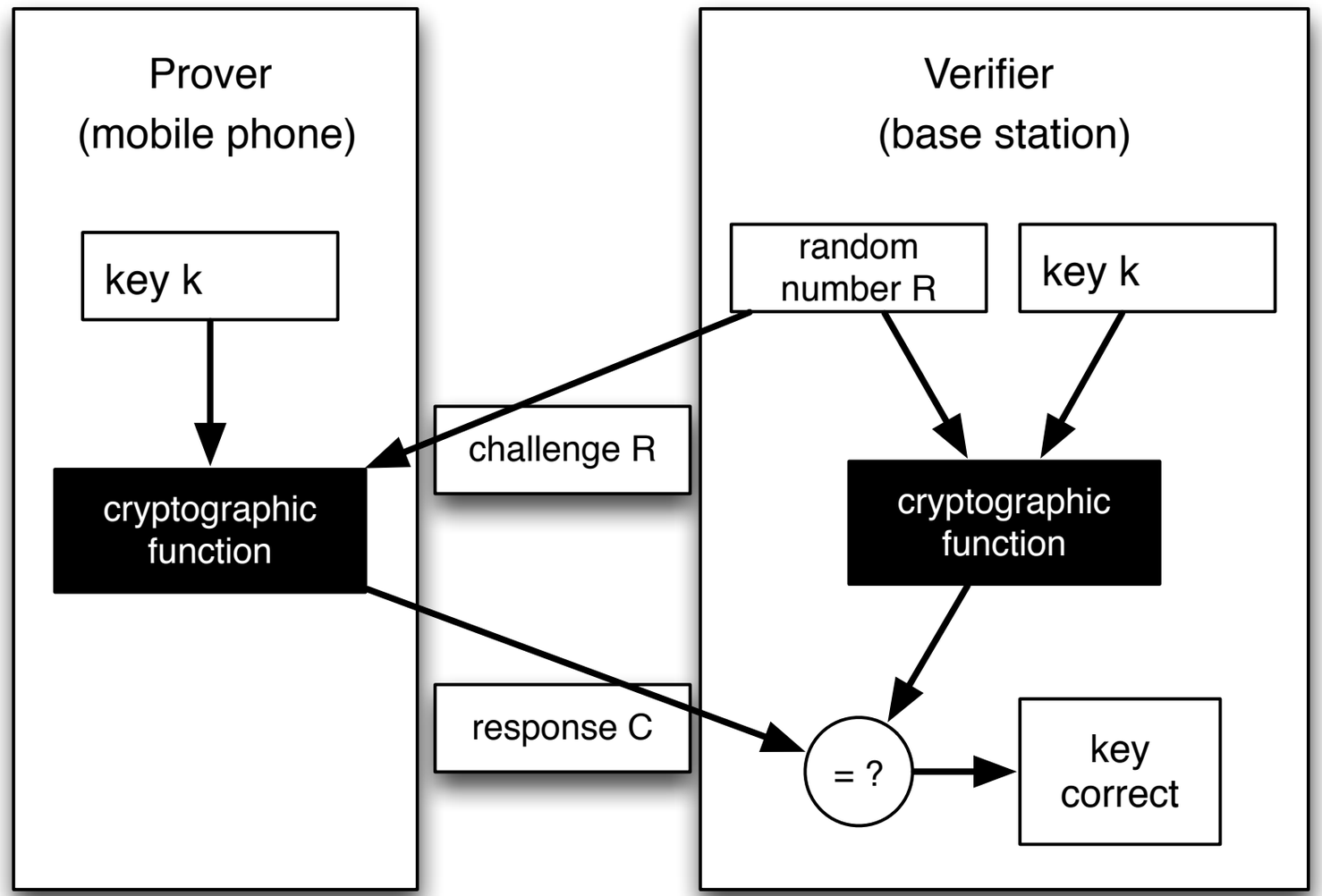
- **Network Providers**
  - Authentication of the user
  - Correct billing, no abuse
  - Efficiency (low overhead)
- **User's perspective**
  - confidentiality
  - no user profiles
  - Connection with the specified base station
  - correct billing

Security Algorithms
GSM

- **SIM card (smart card)**
  - 128-bit key
  - User: PIN and PUK
- **Smart card-based authentication**
  - with non-standard algorithm A3
- **Anonymity**
  - Use of temporary identification
- **Encryption to the base station**
  - A5/3 (Kasami) algorithm
  - replacing unsecure predecessor A5/1, A5/2

Challenge-Response-Authentication

- **Challenge-Response**
  - base station sends random number R (Challenge)
  - mobile phone
    - Calculates C = A3(K,R)
      - for card key K
    - sends C to the base station (Response)
  - base station checks result
- **Motivation**
  - no secret key is transmitted
  - no replay attacks possible



Improvements in UMTS

- **Encryption no longer stops at the base station**
- **Temporary communication key**
  - regular renewal
    - as a function of time and data volume
  - Symmetric 128-bit key
- **Network authenticates to the user**
- **UMTS uses improved, public, symmetric encryption**

Security Requirements in WLAN

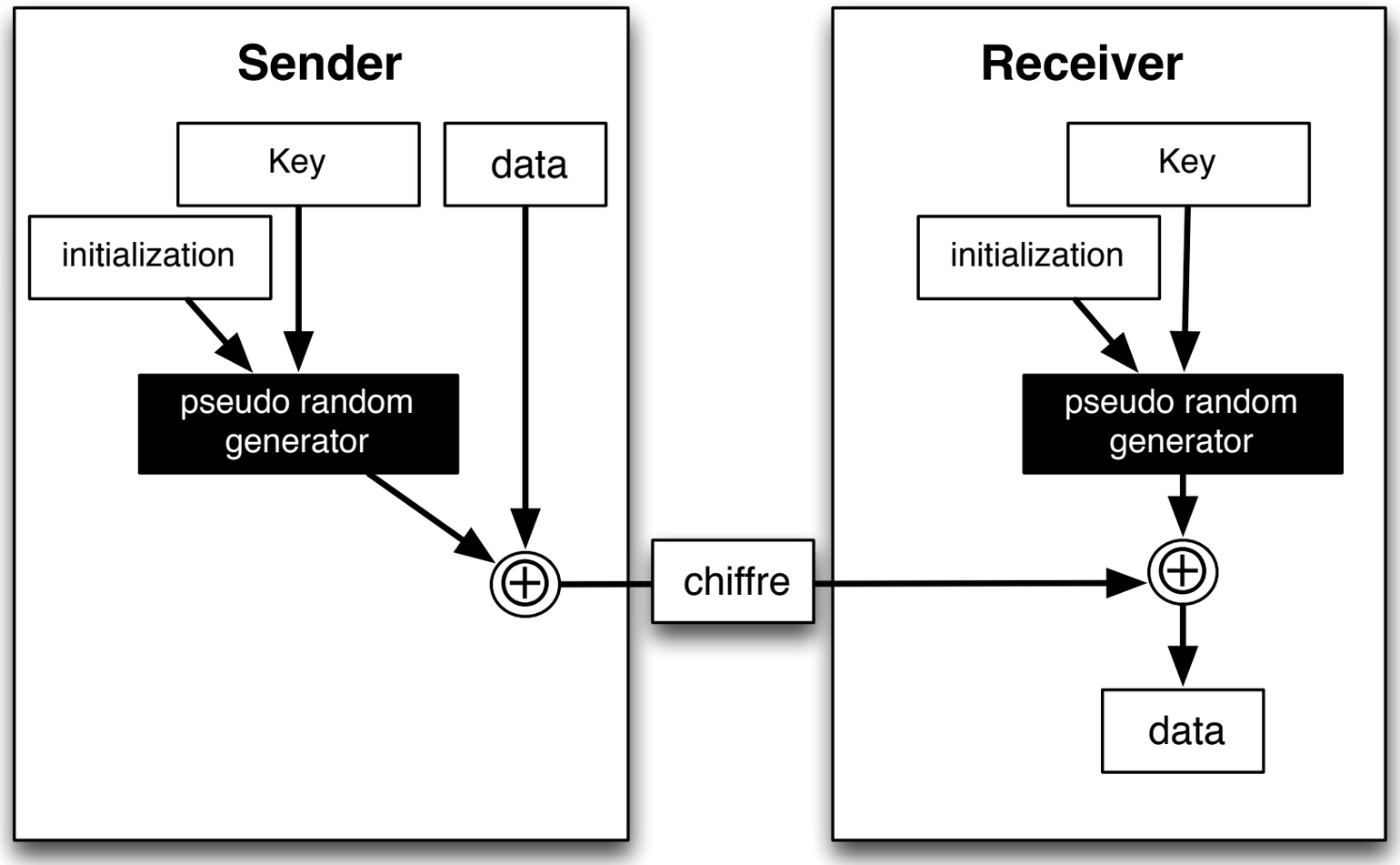
- **Authentication of**
  - the user or
  - the device
- **Protection of data transmitted**
  - against eavesdropping
  - and manipulation
- **Problems**
  - Hacker software available
  - Devices are spread widely and freely programmable

Wired Equivalent Privacy

- **Security mechanism for 802.11 WLAN**
  - Against overhearing of messages
  - known since 2001, significant weaknesses
- **64-bit WEP uses 40-bit key**
  - uses RC4 symmetric stream encoding
  - Alternatively, 128-bit WEP (104 bit key)
  - each with 24 bits for initialization
- **Weakness**
  - No message may be repeated
  - Also unsecure for large key size
  - No key management

Stream Ciphers

- **Encryption algorithm**
  - input as a byte stream (sequence of bytes)
  - bitwise Xor with pseudo-random sequence
- **Decryption**
  - bitwise Xor with same pseudo-random sequence
- **Important:**
  - exchange of the initialization of the random seed
  - Synchronous coding/ encoding
- **Example:**
  - Rivest code 4 (RC 4)



WPA

- **WPA: Wi-Fi Protected Access**
  - secure improvement over WEP
  - uses authentication server
    - Authenticiation Extensible Authentication Protocol (EAP)
  - or pre-shared key mode (PSK) for small networks
- **Uses RC4 with 128 bit keys stream ciphers**
  - dynamic key exchange using Temporal Key Integrity Protocol (TKIP)
- **Instead of CRC better data integrity through message integrity code (MIC)**
- **Frame counter prevents replay attacks**

Further Action in 802.11

- **Shield the insecure WLAN from the wired LAN intranet**
- **Additional layers of security at higher layers**
  - IPSec or SSL or SSH
- **Additional authentication**
  - e.g. VPN (Virtual Private Network)
- **Approval only of registered MAC addresses**
- **Suppression of network names**
- **In the future:**
  - Use AES instead of RC4

Security Risks in Wireless Sensor Networks

- **Overhearing of messages**
  - Breach of confidentiality
- **Falsification and inserting of false packets**
  - access control
  - integrity
- **Disruption of communication**
  - Replay of old messages (replay attack)
  - Denial of service

TinySec

- **Karlof, Sastr, Wagner**
  - TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, SenSys 2004
- **Security layer for wireless sensor networks**
- **Objectives**
  - access control
  - integrity of messages
  - confidentiality
  - Transparent to applications and programmers

TinySec-Design

- **A shared global symmetric cryptographic key**
- **Encryption in data link layer**
  - encryption and integrity protection
  - transparent for applications
- **Use of symmetric block-encryption**
  - either DES, AES, Skipjack, RC5
  - Also generates digital signatruers of messages
  - Message Authentication Code (MAC)

Discussion TinySec

- **TinySec provides**
  - access control
  - integrity of messages
  - confidentiality
- **TinySec does not prevent**
  - disruption
  - compromising of a node or a key node
  - replay attack
  - denial of service

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithms for Radio Network

Security for GSM, UMTS, WEP, WPA and TinySec

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

CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG