# The road to 5G security

Prof. Steve Babbage

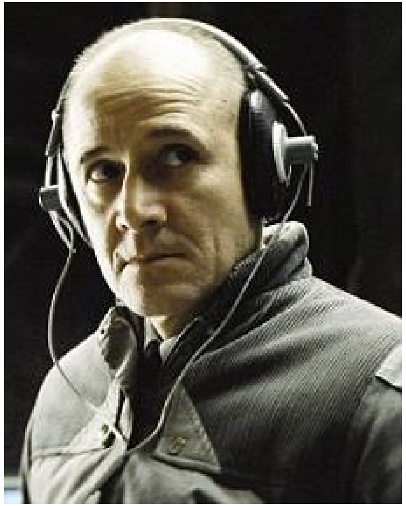
Vodafone Distinguished Engineer

# Contents of my talk

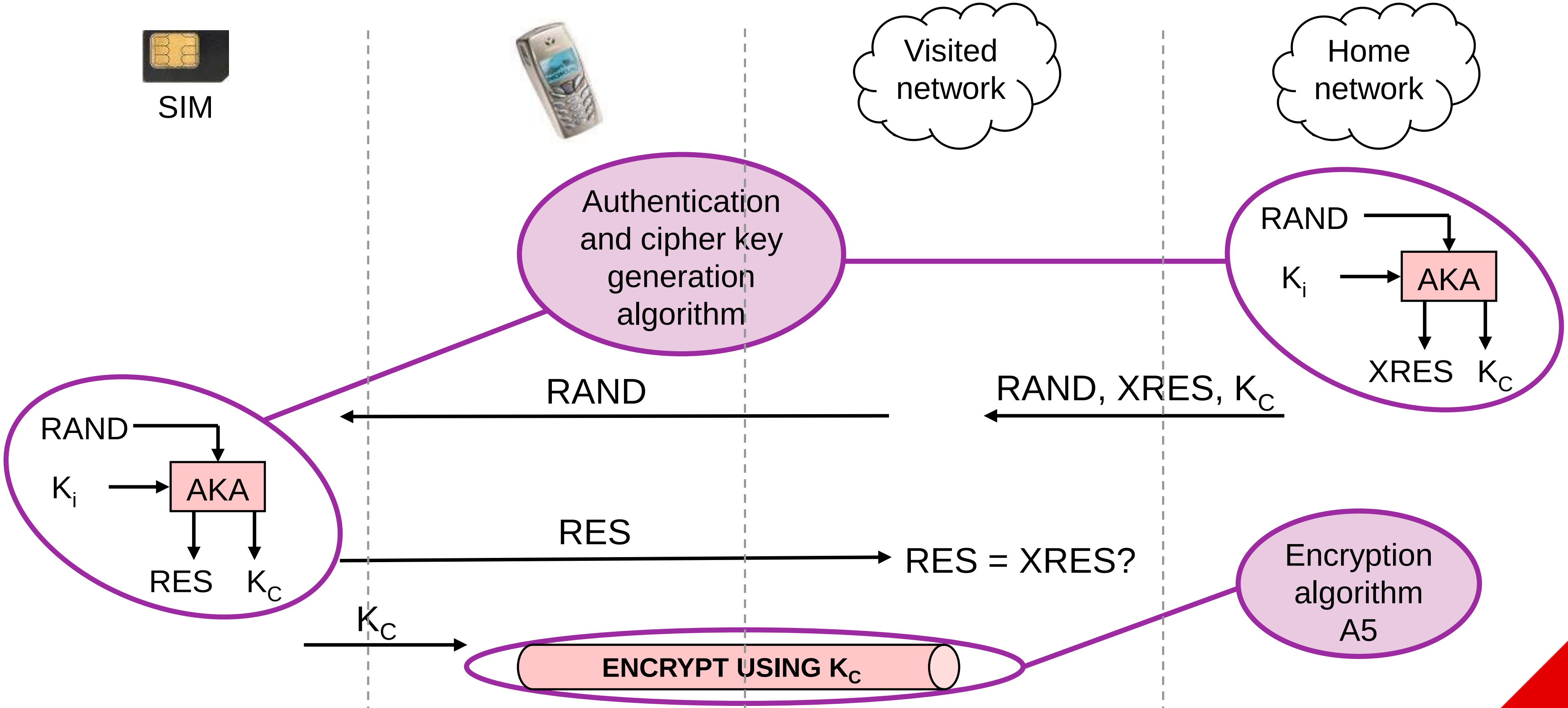
- The evolution of mobile security: 1G, 2G, 3G, 4G
- What is 5G anyway?
- New security improvements in 5G
- New areas of risk
- Work in progress

# Cryptography in mobile phone networks

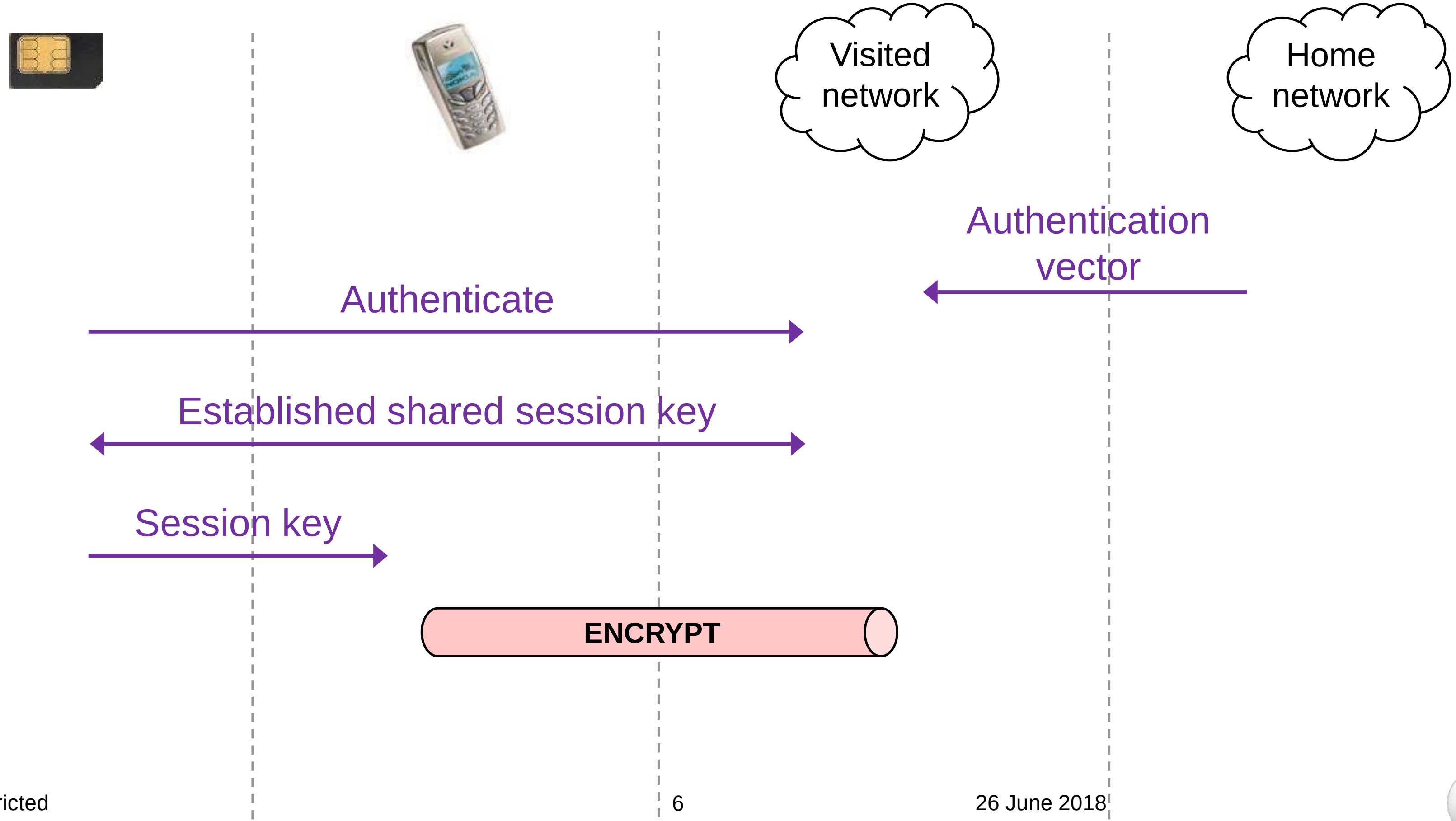
# First generation analog phones



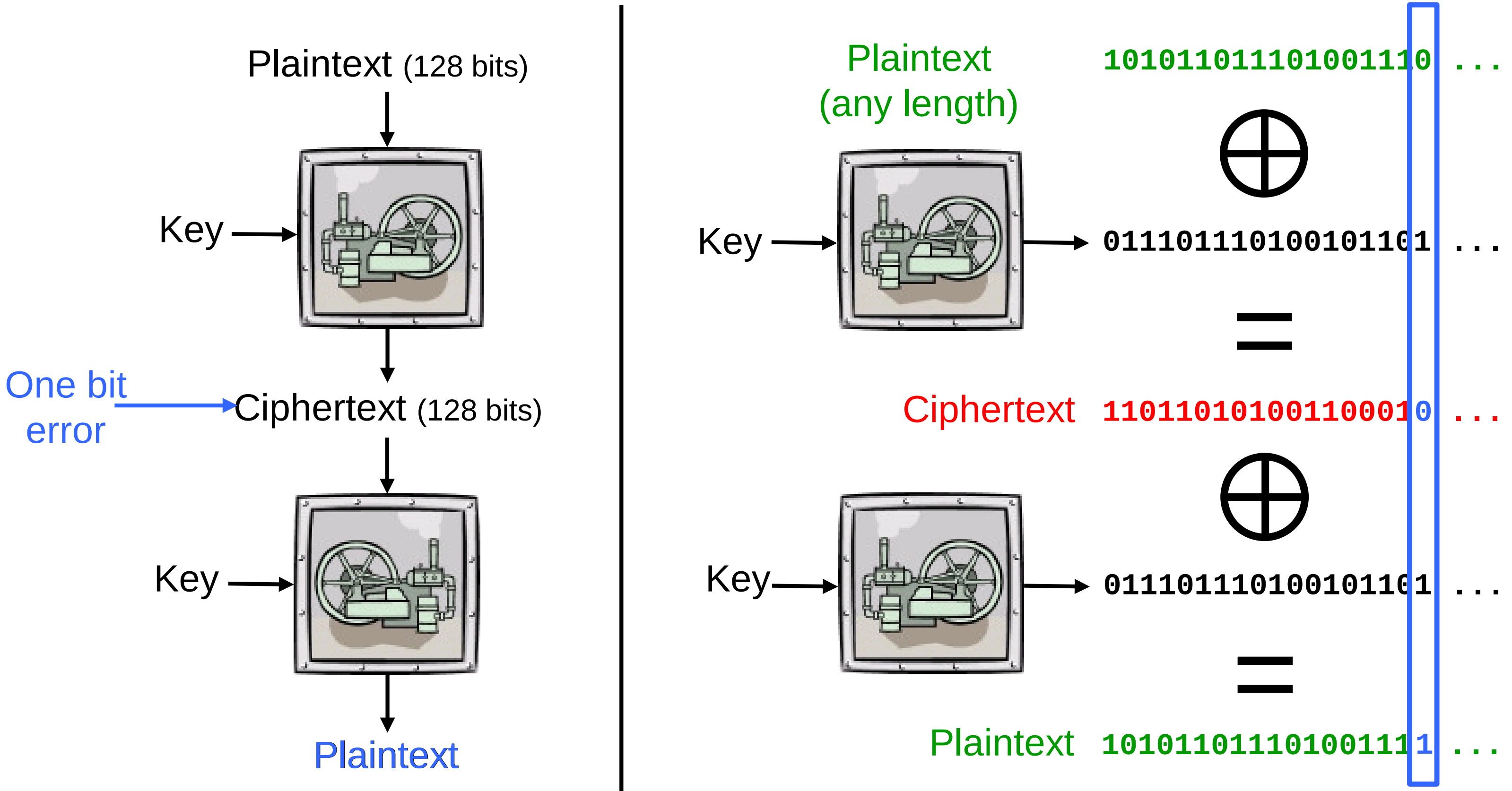
# GSM security architecture



# GSM security architecture



# Block ciphers and stream ciphers



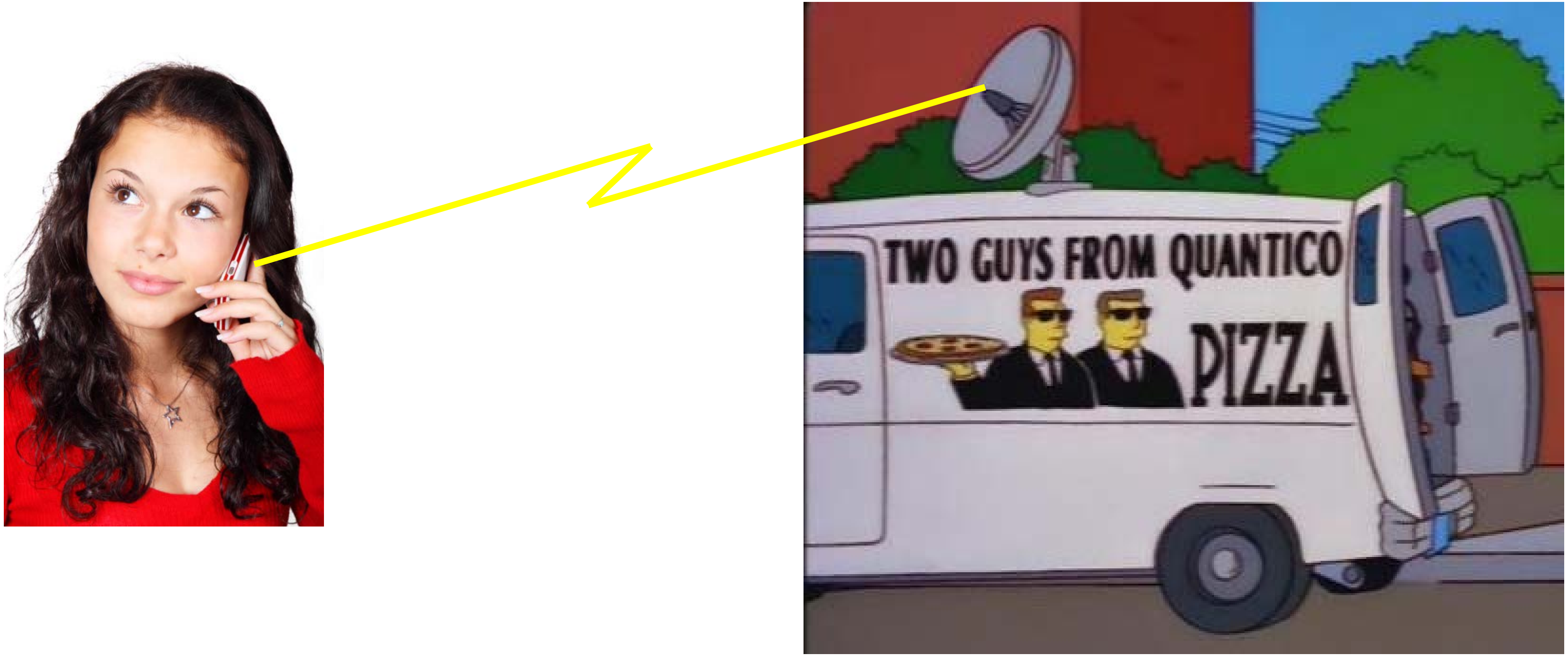
# The SIM

- A miniature “hardware security module”
- **Well made** SIMs, with **strong algorithms**, remain highly resistant to attack

# Some limitations of GSM security

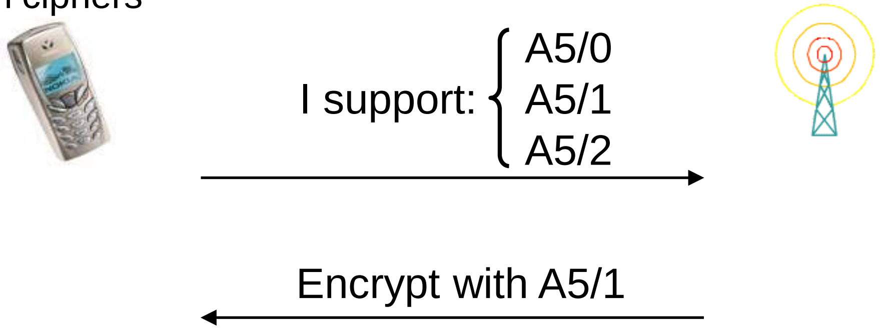
- The goals of GSM security
- Key length
- One-way authentication
- Weak (“export”) crypto algorithms, initially

# One-way authentication



# GSM algorithms

- Encryption algorithm must be standardised — operators can’t do their own thing
- Various algorithms: A5/0 (no encryption), A5/1, A5/2, A5/3, …
  - Always stream ciphers




- Authentication and key agreement algorithm need not be standardised
  - More on this later

# A5/1 attacks

- Several academic attacks from 1994 onwards
  - Guess-and-determine attacks
  - Statistical attacks
  - Algebraic attacks
- Time-memory-data trade-off attacks from 1995 onwards

- There’s also A5/2
  - For when A5/1 is too strong(!)

# A protocol problem

# The Barkan-Biham-Keller attack — eavesdropping

**Network** | **Victim mobile** | **Attacker**

RAND (Network → Victim mobile)

RES (Victim mobile → Network)

$K_C$

Start ciphering with **A5/3** (Network → Victim mobile)

Phone call (Network ↔ Victim mobile)

Same RAND (Attacker → Victim mobile)

RES (Victim mobile → Attacker)

$K_C$

Start ciphering with **A5/1** (Attacker → Victim mobile)

"OK", encrypted with **A5/1** (Victim mobile → Attacker)

*repeated several times*

"OK", encrypted with **A5/1** (Victim mobile → Attacker)

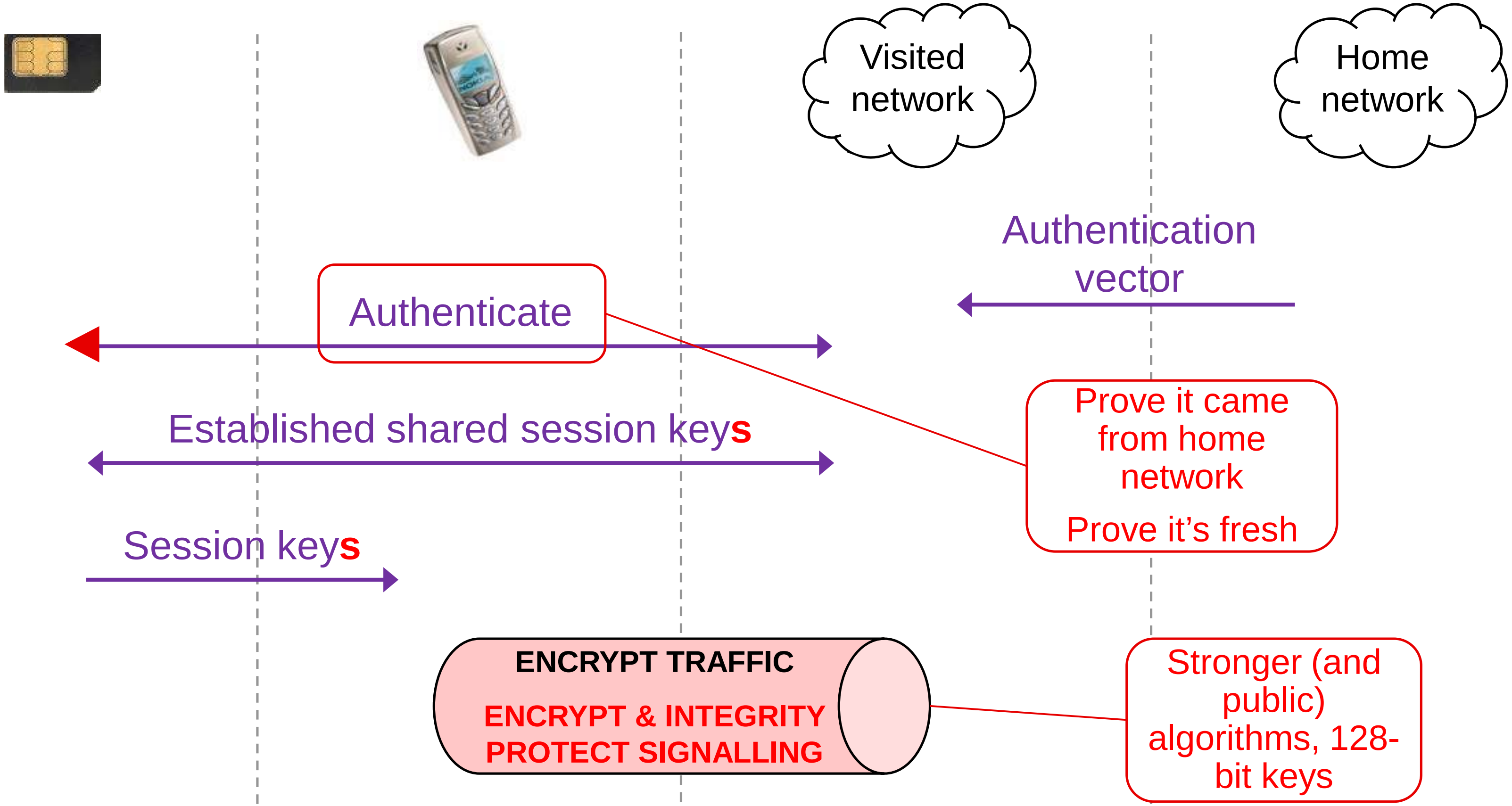
*Enough to break A5/1 and recover cipher key; now attacker has cipher key and can decrypt recorded call*

# The Barkan-Biham-Keller attack

- Exploits weak encryption algorithms
- Exploits ability to manipulate signalling …
  - So let's add that to our list of GSM security limitations

# 3G, 4G

# 3G security architecture



# Barkan-Biham-Keller and 3G

**Network** | **Victim mobile** | **Attacker**

RAND

RES

$K_C$

Start ciphering with **A5/3**

Phone call

Same RAND

RES

$K_C$

Start ciphering with **A5/1**

"OK", encrypted with **A5/1**

*repeated several times*

"OK", encrypted with **A5/1**

*Enough to break A5/1 and recover cipher key; now attacker has cipher key and can decrypt recorded call*

# Defining – and deploying – new GSM algorithms

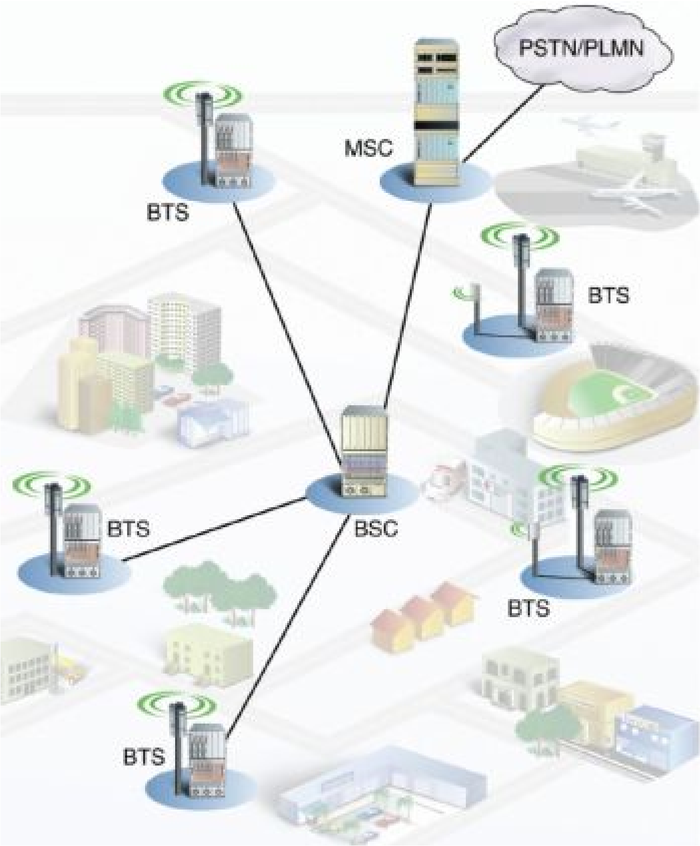
# New, strong, public GSM algorithm

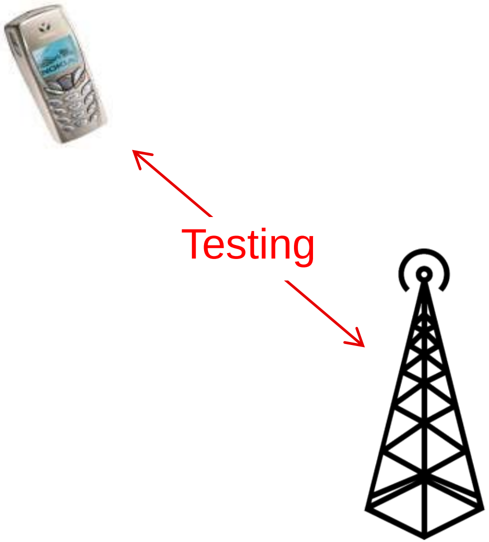
**3G encryption algorithm UEA1**

↓

**GSM encryption algorithm A5/3**

# So now we can replace A5/1 with A5/3 …



# GSM encryption algorithm status

| Algorithm | Status |
|---|---|
| A5/2 | Abandoned |
| A5/1 | Common<br>- sometimes with countermeasures |
| A5/3 | Growing<br>- now in all Vodafone markets |
| A5/4 | Testing |

# Radio interface algorithms in 3G

**3G**

- UEA1, UIA1 (already mentioned)
- UEA2, UIA2
  - Based on a stream cipher called SNOW 3G,
    developed from SNOW 2.0

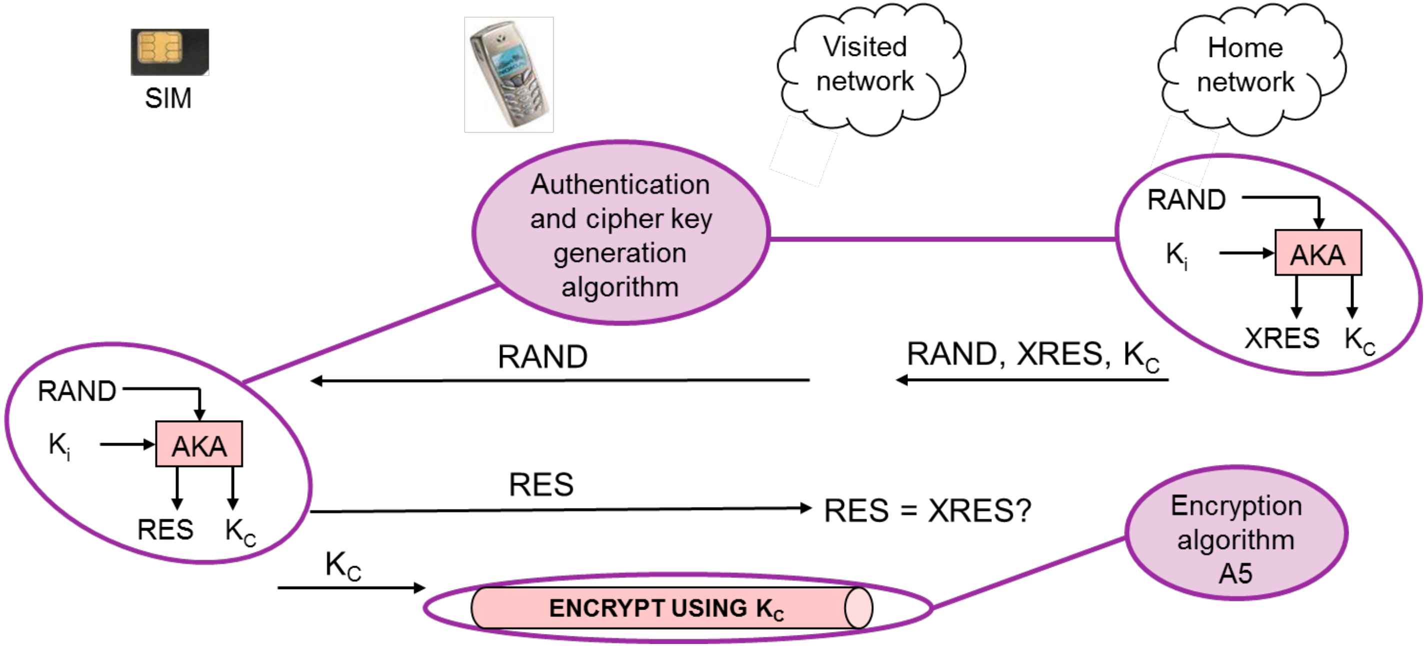
Both mandatory from day one

# Authentication and key agreement algorithms

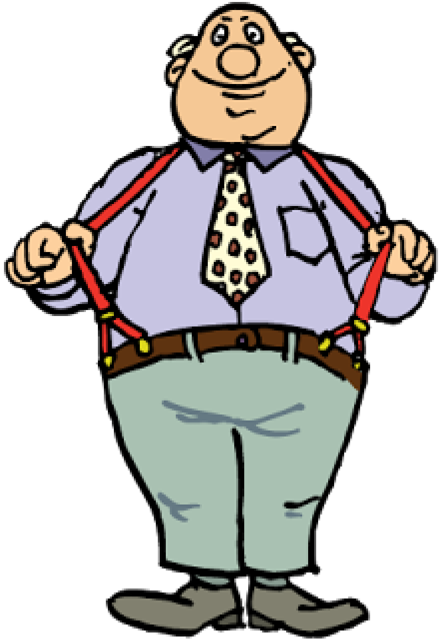
# Authentication and key agreement algorithms

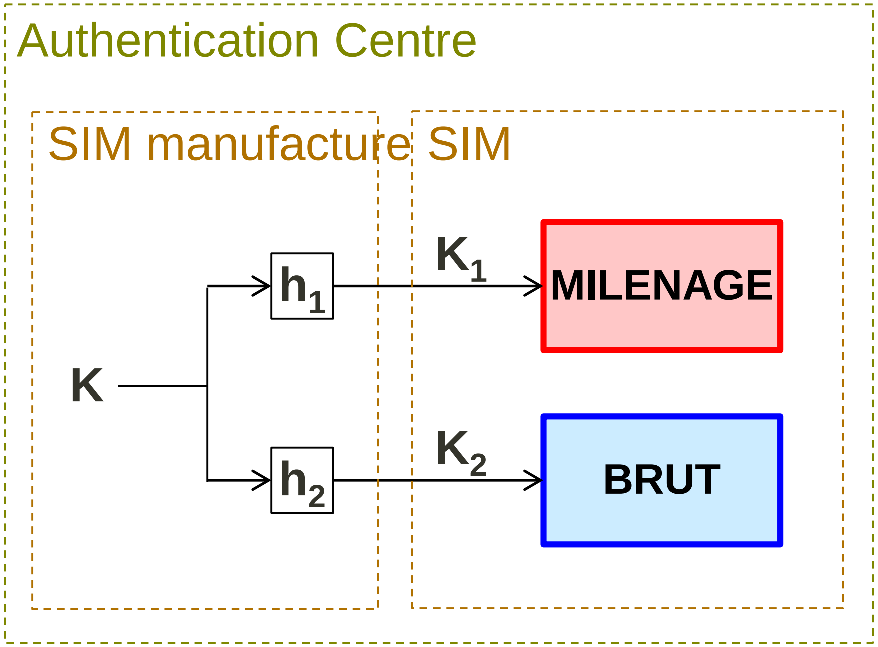
Operators can choose their own … but:

- COMP128
- COMP128-2, COMP128-3
- MILENAGE



# Vodafone dual algorithm





# 4G

# Evolution of security

| 2G | 3G | 4G |
| --- | --- | --- |
| Key length | Increased to 128 bits | |
| One-way authentication | Mutual authentication, tamper-proof signalling | Proves *which* network |
| Authentication and key agreement algorithms | Much better example algorithm | |
| Encryption algorithms | Full strength public algorithms | |
| Same cipher key, whatever the algorithm | | Different cipher key depending on choice of algorithm |

# Radio interface algorithms in 3G / 4G

**3G**

- UEA1, UIA1 (already mentioned)
- UEA2, UIA2
  - Based on a stream cipher called SNOW 3G,
    developed from SNOW 2.0

Both mandatory from day one

**4G**

- EEA1, EIA1
  - Identical to UEA2 and UIA2
- EEA2, EIA2
  - Standard constructions based on AES
- EEA3, EIA3
  - China specials!

Both mandatory from day one

# SIM evolution

# Embedded SIM

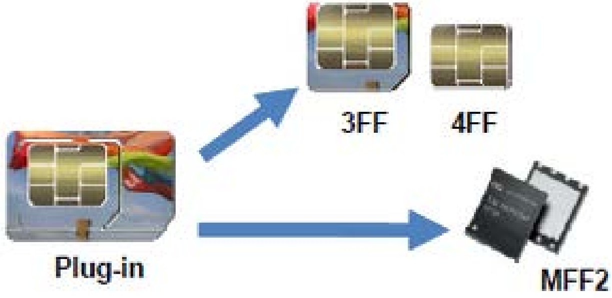
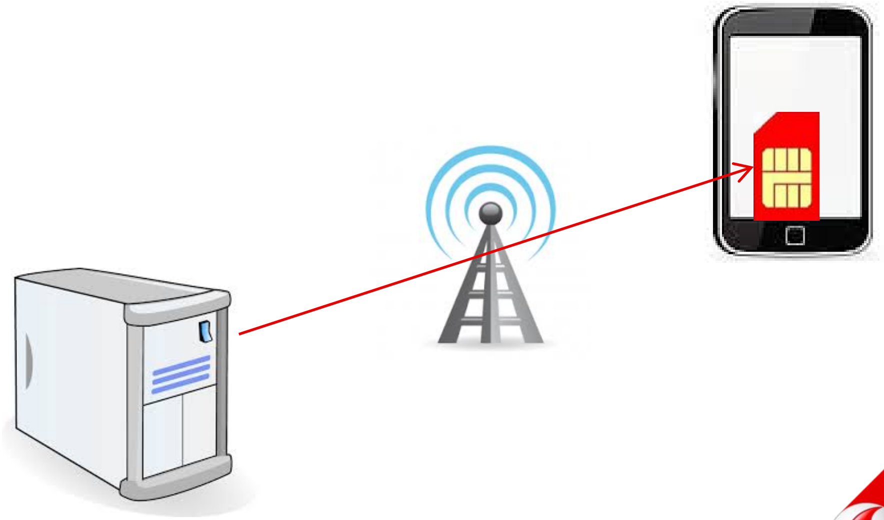
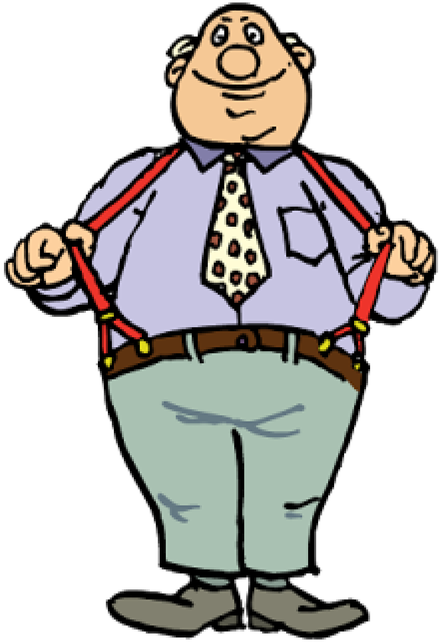



Image from ETSI slides by Dr Klaus Vedder, G&D

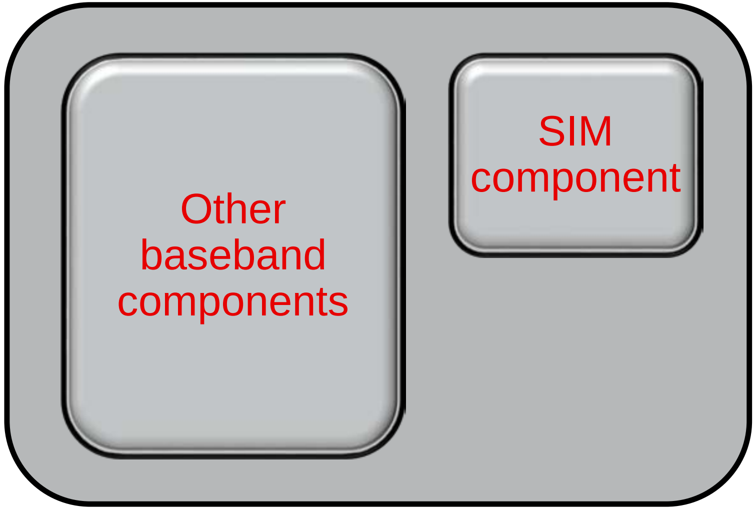


# Authentication and key agreement algorithms (reprise)

- COMP128
- COMP128-2, COMP128-3
- MILENAGE
- TUAK



# Integrated SIM




Physically separate silicon within chip

(not “Soft SIM”)

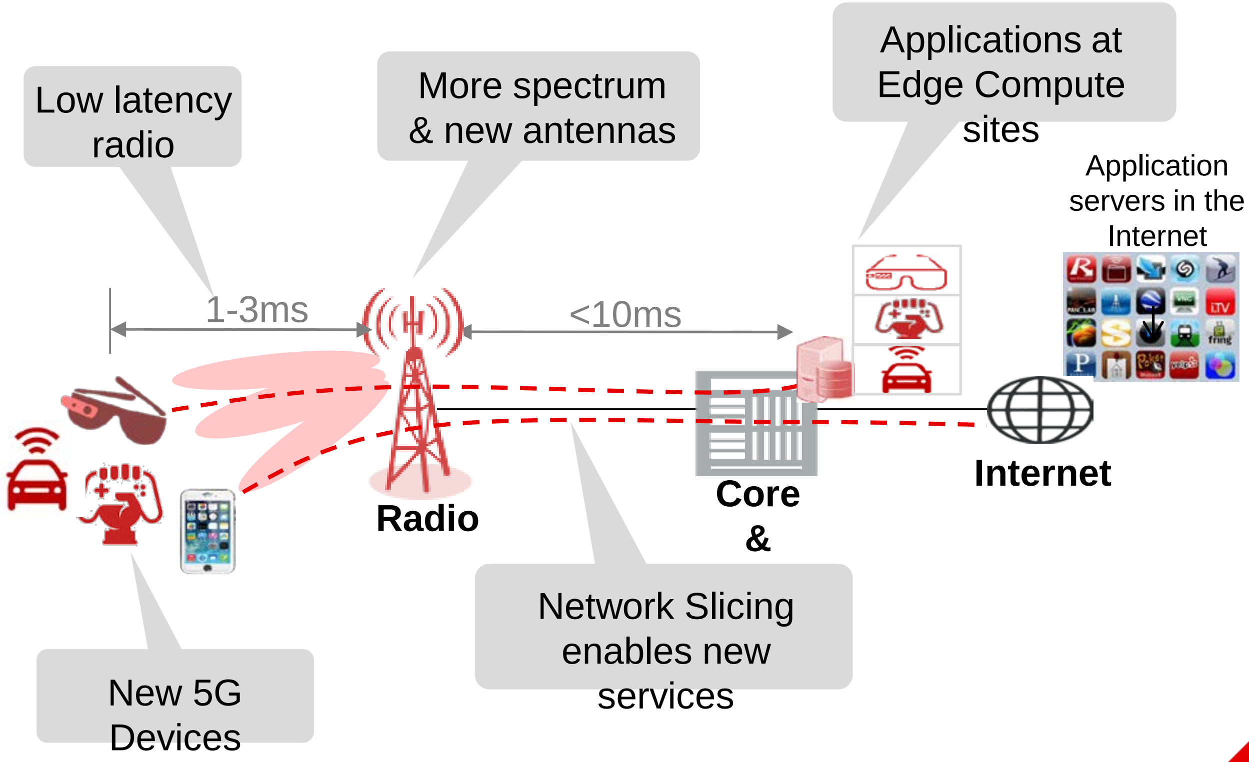
What is 5G anyway?

# 5G is a family of technologies …

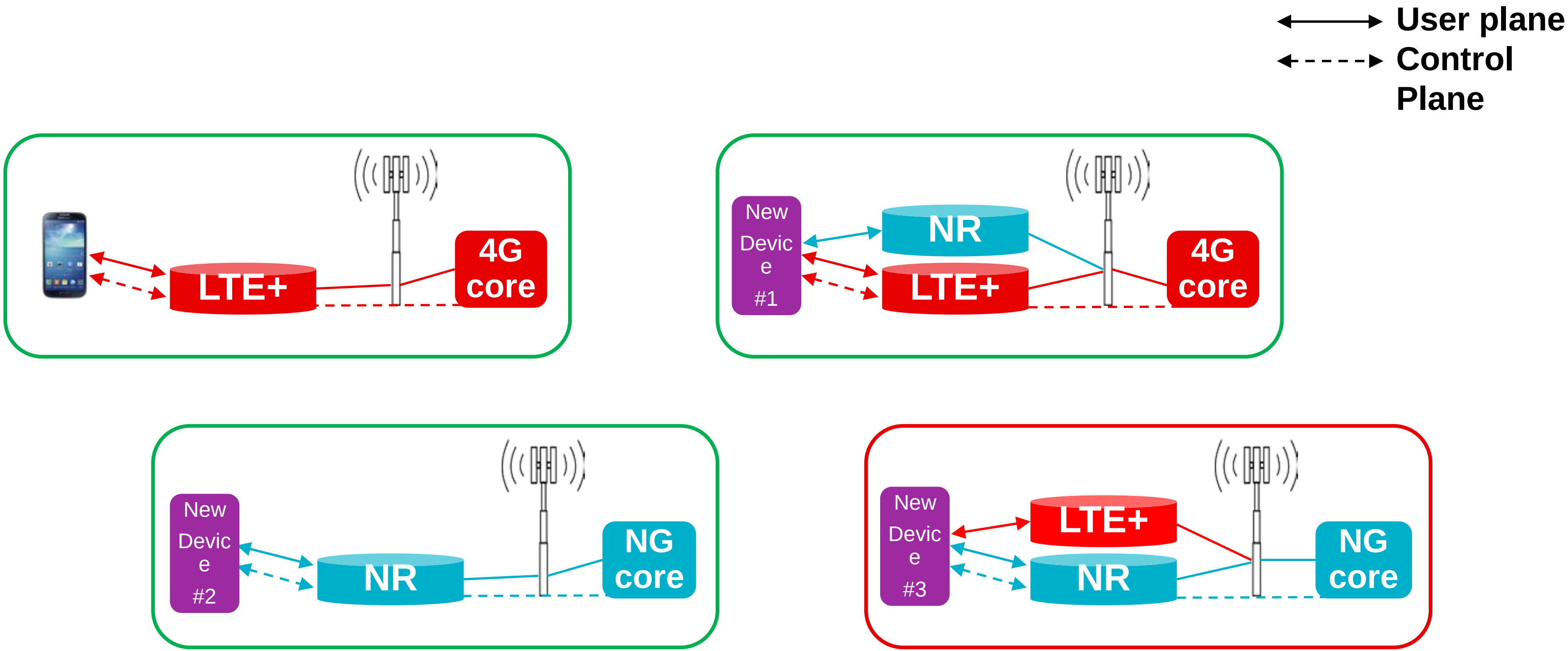
| 4G Evolution | 5G New Radio |
| --- | --- |
| • Gigabit Speeds<br>• Low latency radio<br>• Massive IoT | • New spectrum<br>• Very high bandwidths<br>• Even lower latency radio<br>• Ultra reliable |

**Architectural Evolution**

- Network Virtualisation
- Mobile Edge Computing
- Network Slicing



# … and a family of architectures



# Low Power, Wide Area IoT service


**10+ Years Battery Life** | **Deep Penetration** | **Mass Deployment** | **Low Bandwidth** | **Device Cost**

NB-IoT

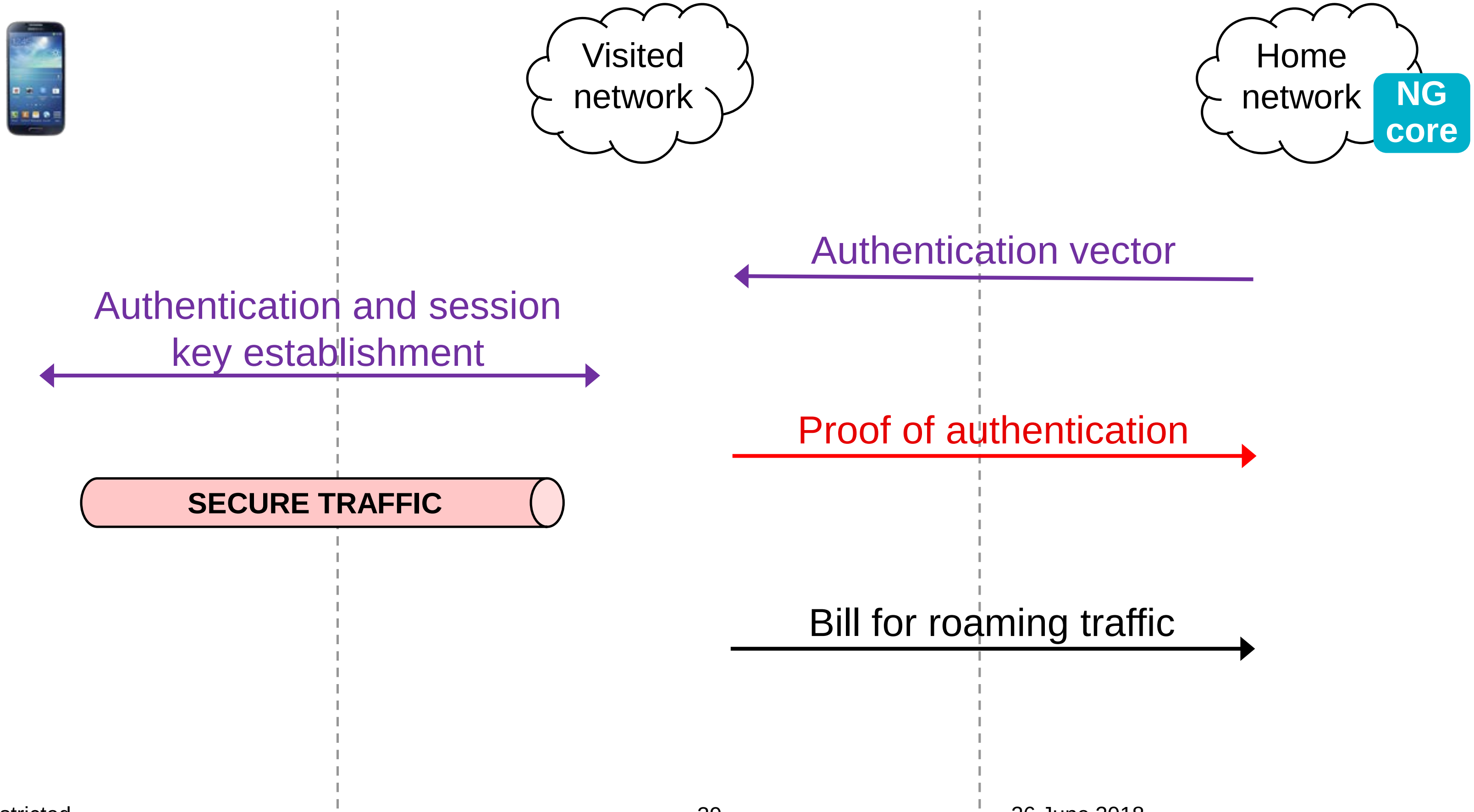
LTE+

NB-IoT

NR

# 5G – roaming fraud protection

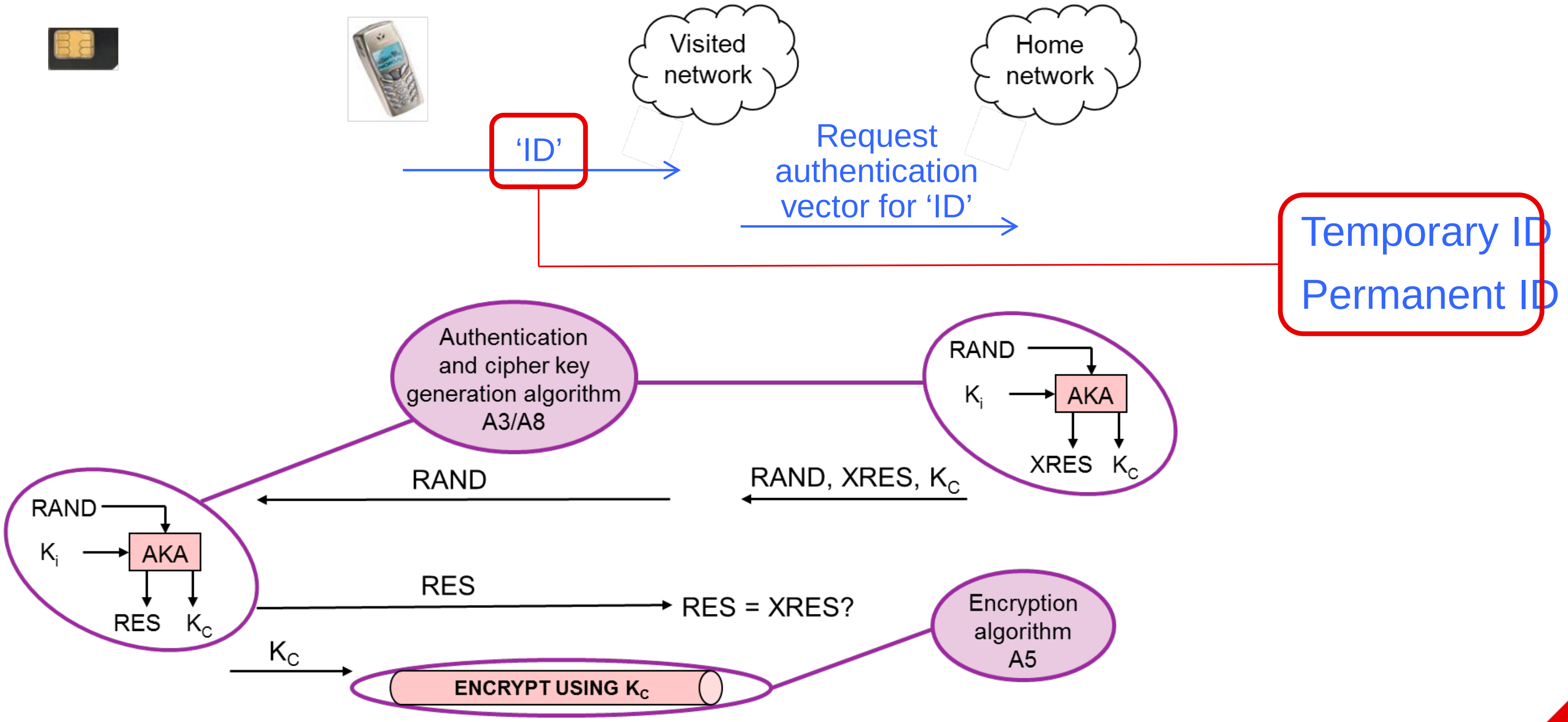
# Roaming fraud protection



# 5G

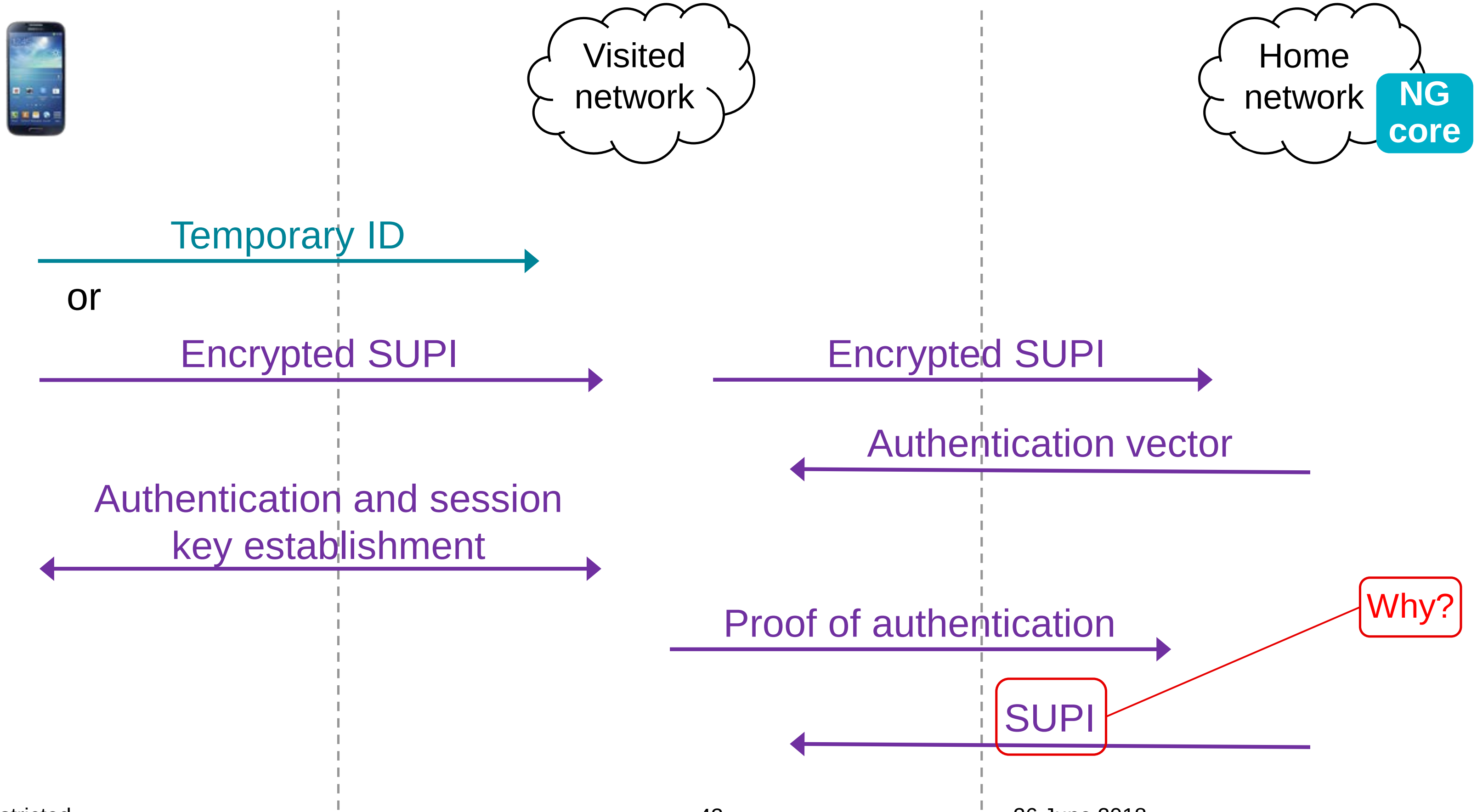
# – privacy enhancement

# Improved privacy



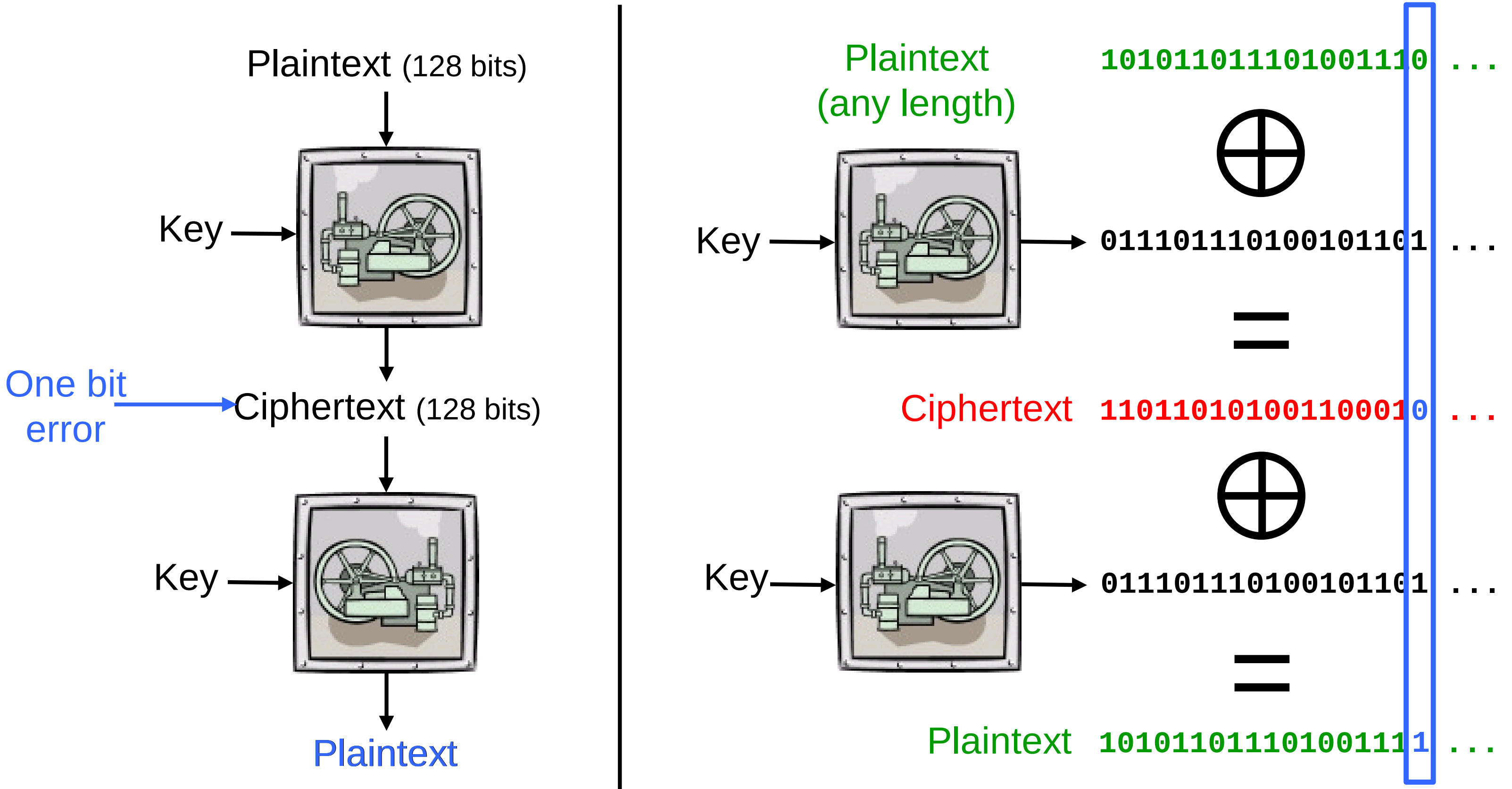
# IMSI catcher / Stingray
# IMSI sniffer

# ~~IMSI~~ SUPI privacy

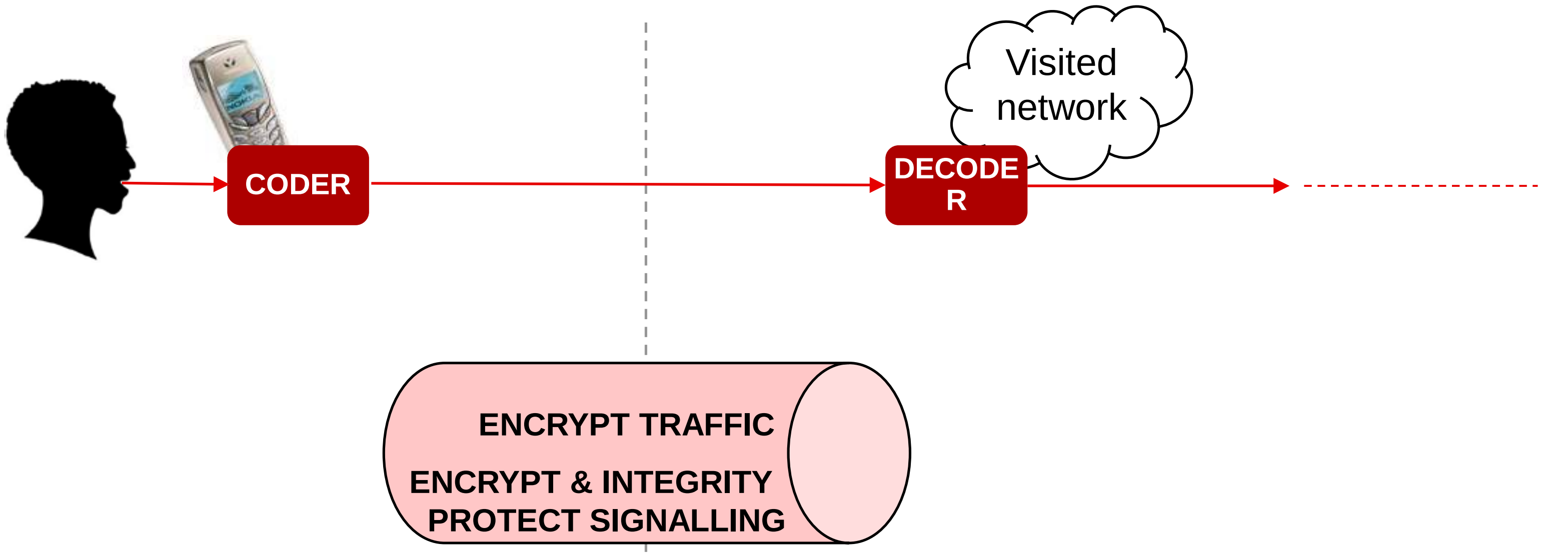


# 5G
# – user plane integrity

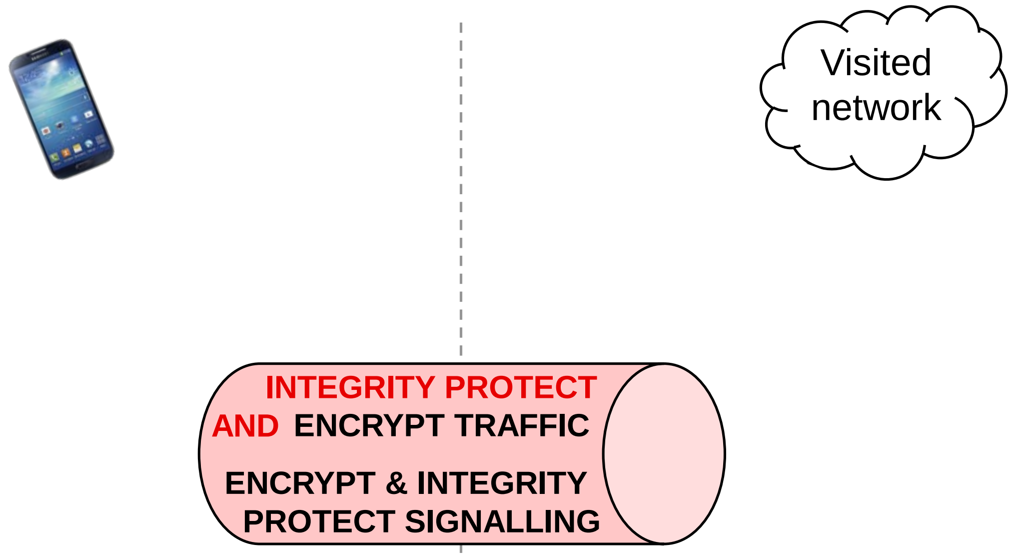
# Block ciphers and stream ciphers



# Traffic = mobile voice

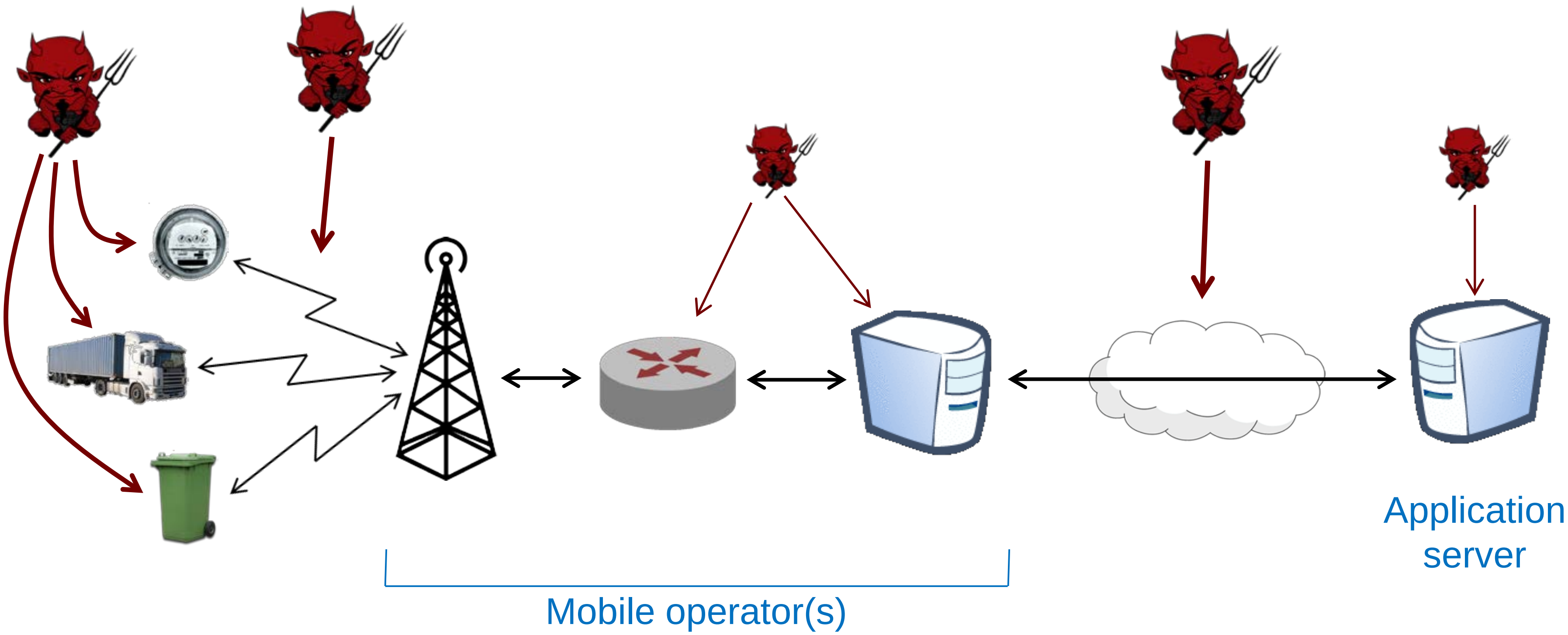


# User plane integrity protection

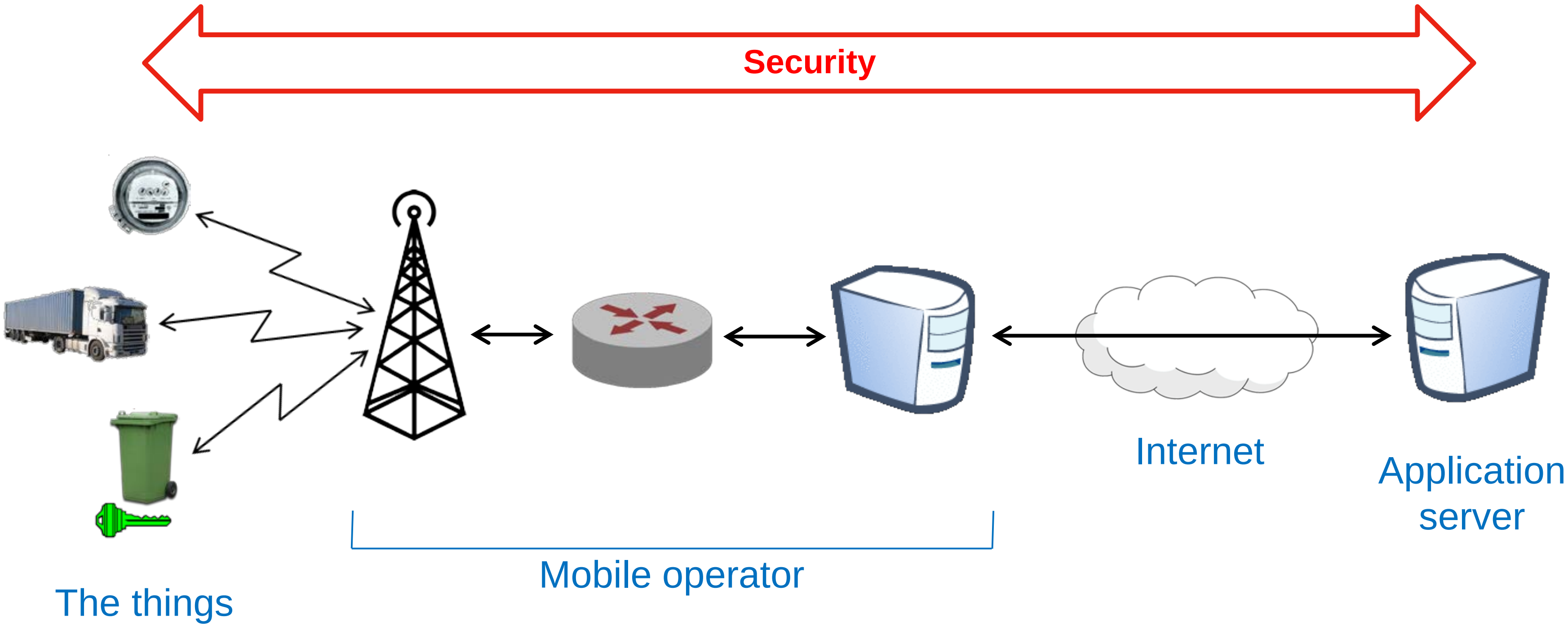


# IoT communication security

# The attack surface

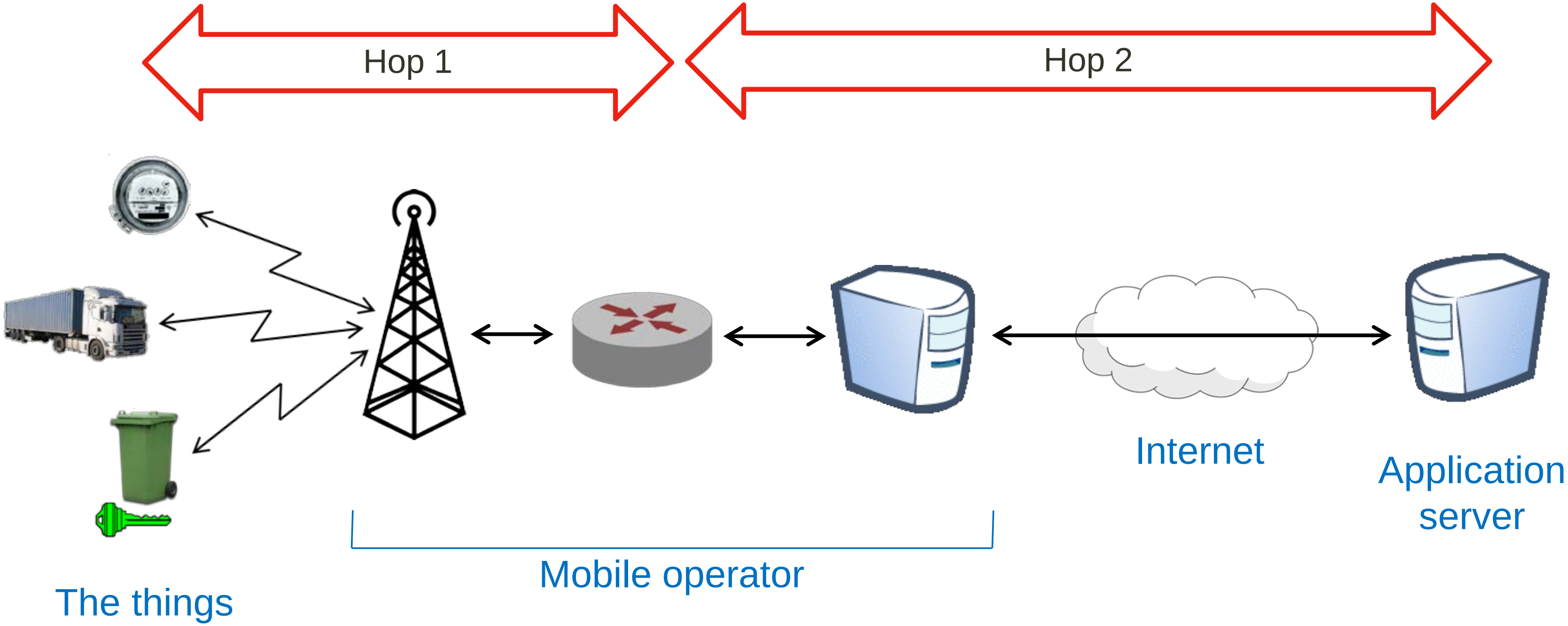


# End to end security

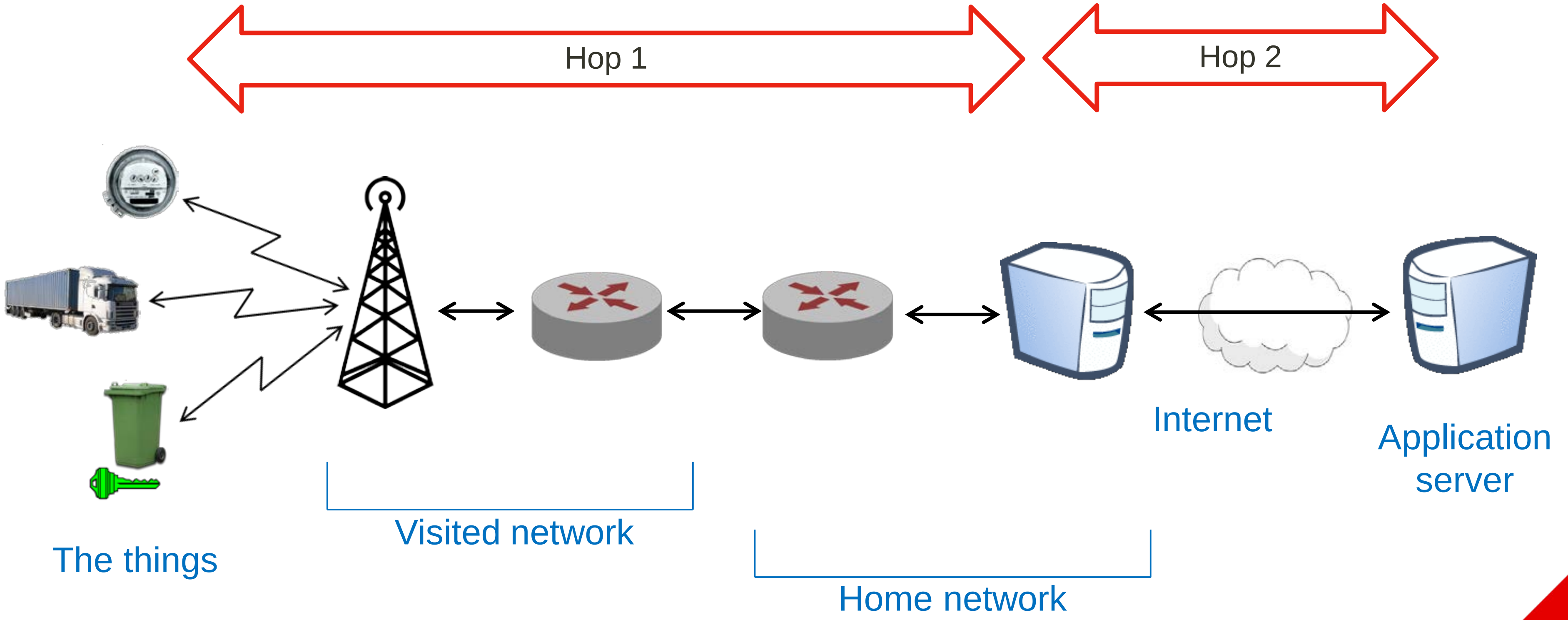



**… if your battery can handle it**

# BEST: battery efficient security for very low throughput Machine Type Communication devices



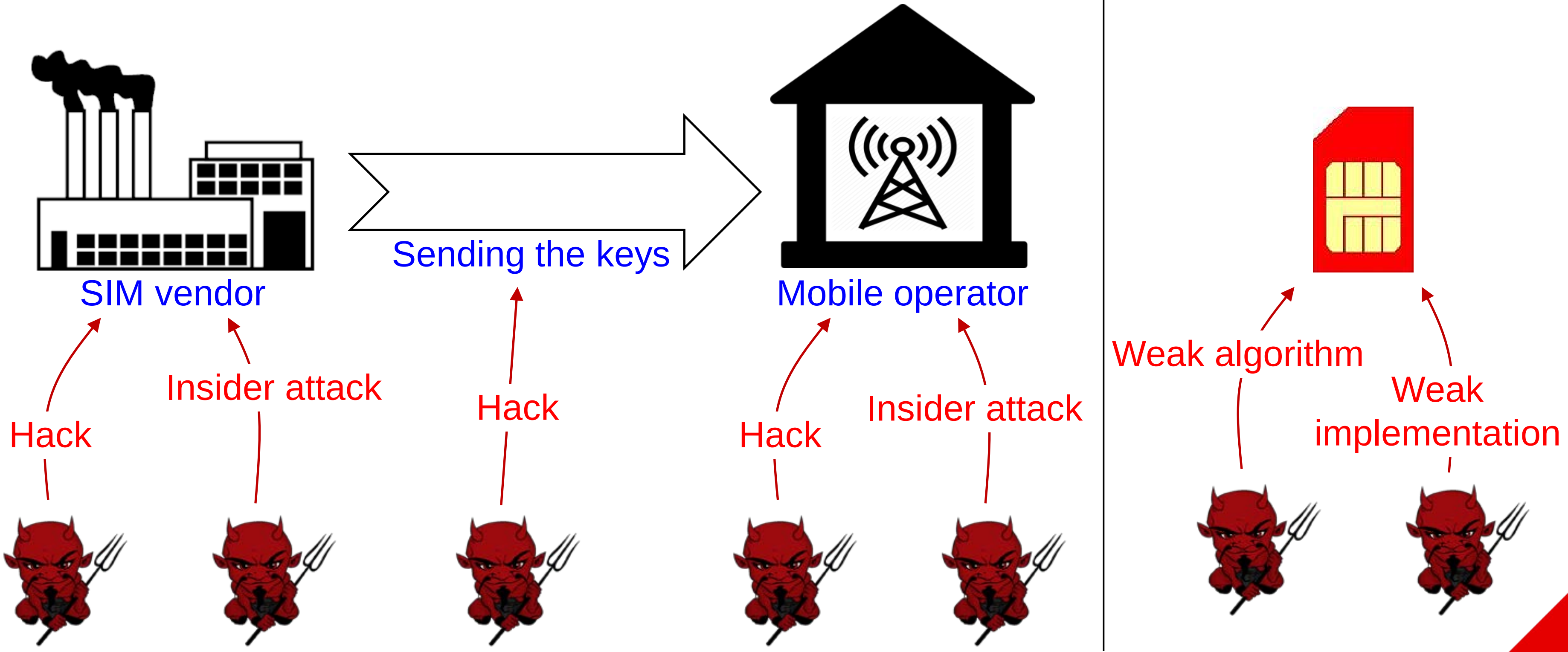
# BEST: battery efficient security for very low throughput Machine Type Communication devices



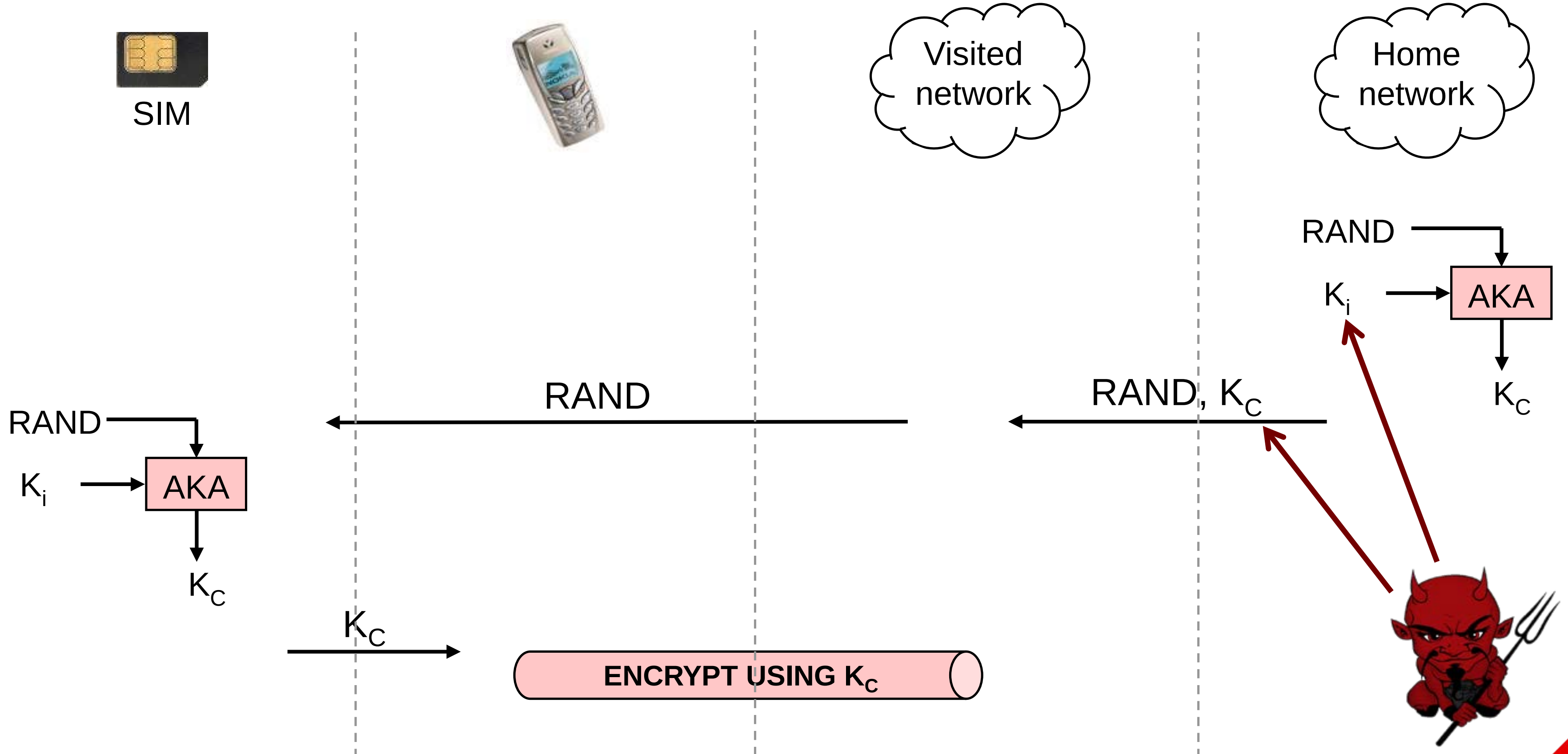
# Work in progress

# So 4G security is very good …
# … but what if the secret isn't secret?

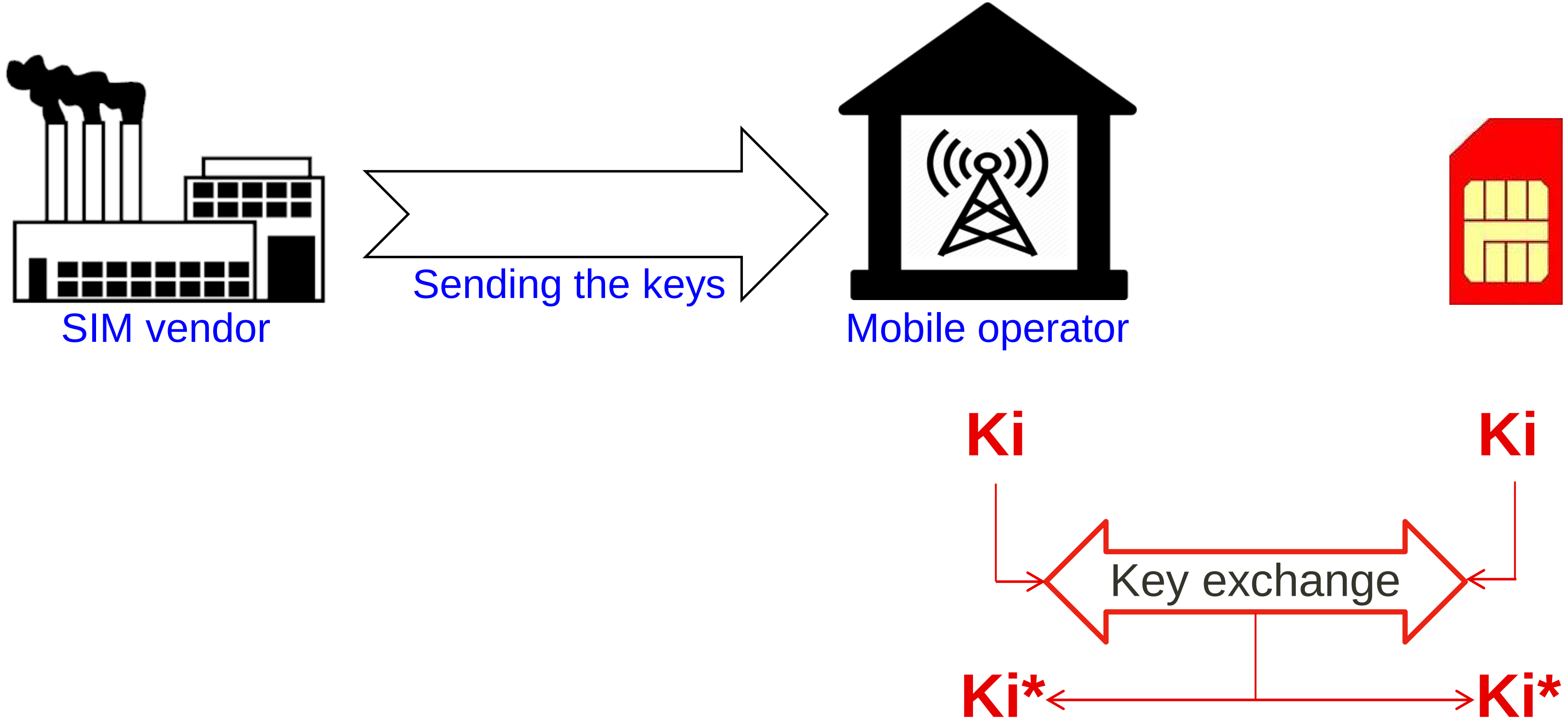
# How can the long term secret key leak?



# Creating shared session keys



# LTKUP: Long Term Key Update



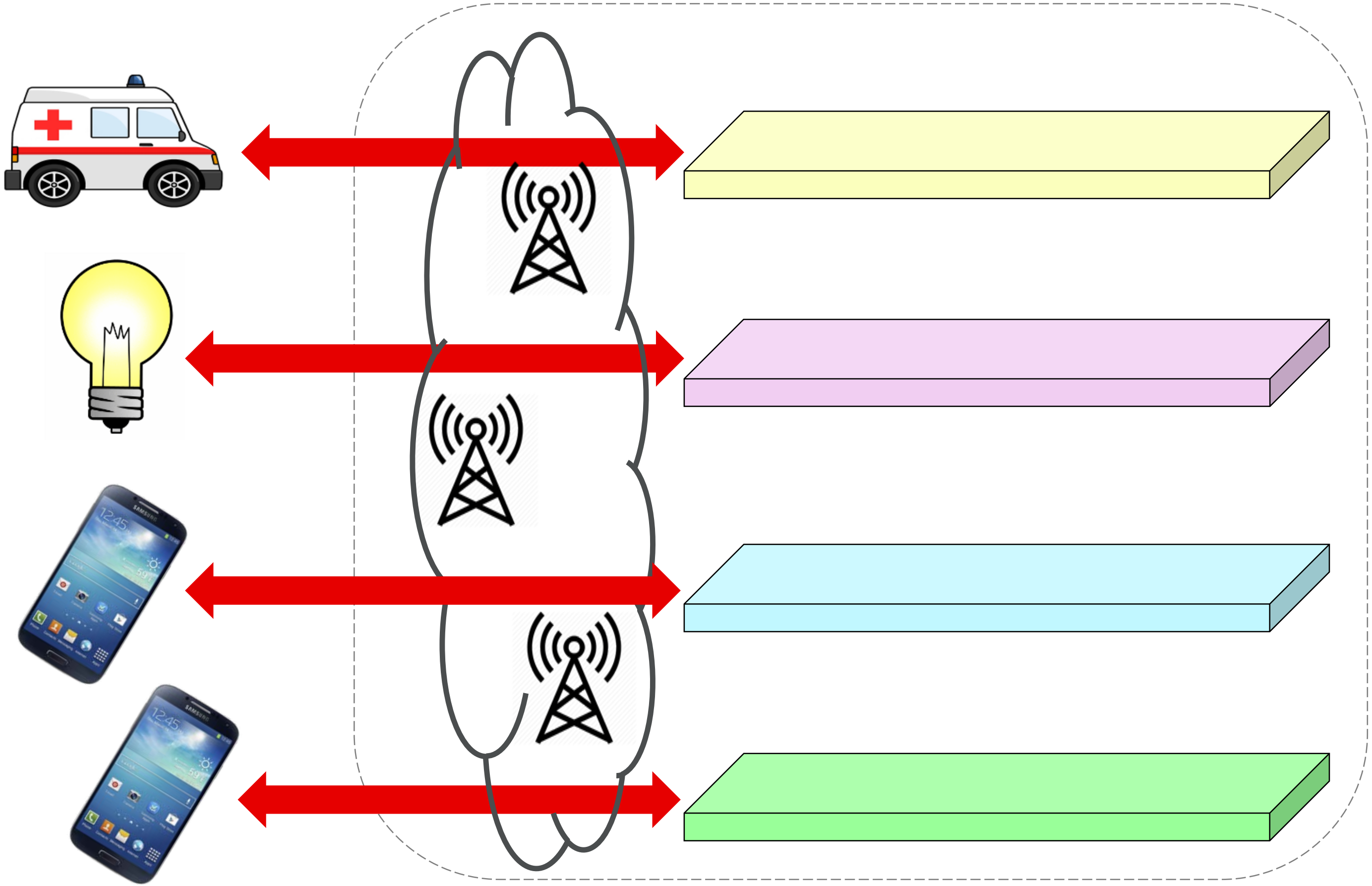
# Quantum


HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.
Dilbert.com DilbertCartoonist@gmail.com
4-17-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick

# Performance constraints on security

- Call set-up time matters to customers
  - Establishing a new key at the start of each call would take noticeably longer
  - So does that mean we can’t do it?
- Fast handover between cells is important for some services
  - So pass session key from old cell to new cell, rather than establishing a new one?
- Some devices need to run on batteries for years
  - So do we need to keep security protocol transmissions to a minimum?
- Some services need very high availability
  - So we mustn’t risk false positives when policing network access?

# Network slices



Optimise for integrity and availability

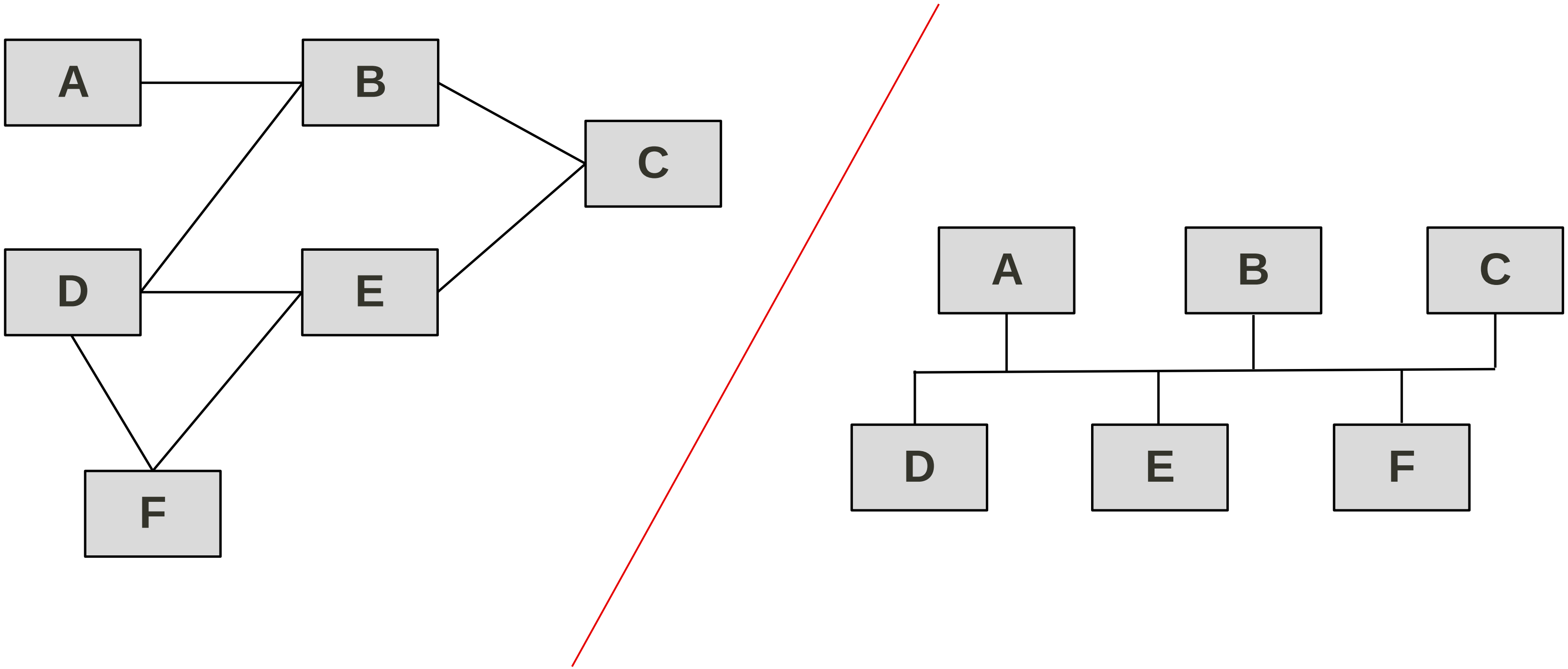
Optimise for battery life

Optimise for speed

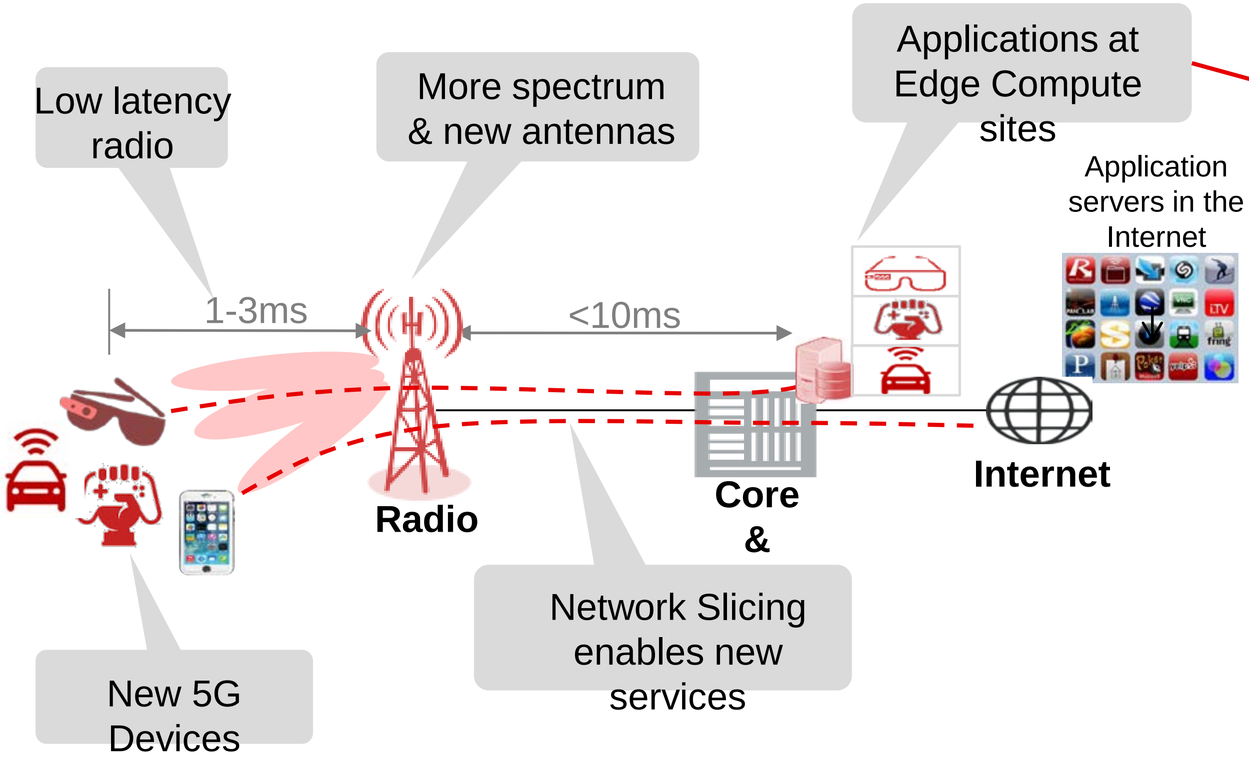
Optimise for security and privacy

# Handle with care

# Service based architecture



# Edge Computing

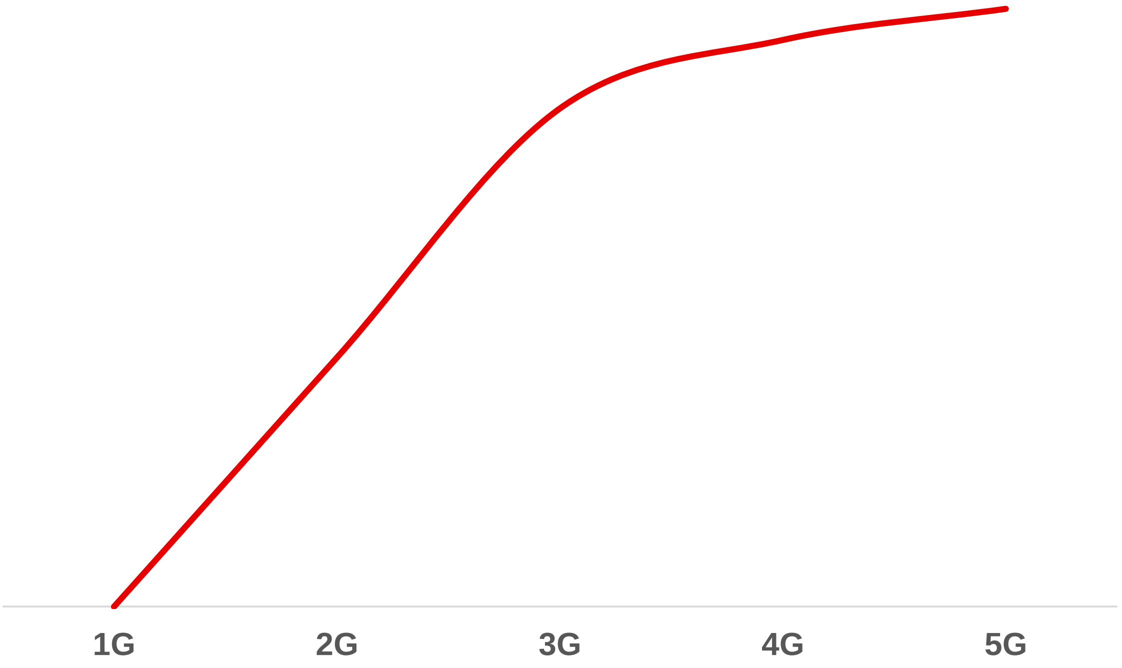



Application servers in more exposed sites

Network info or capabilities exposed to applications

# Final remarks

# Security evolution



# Thank you