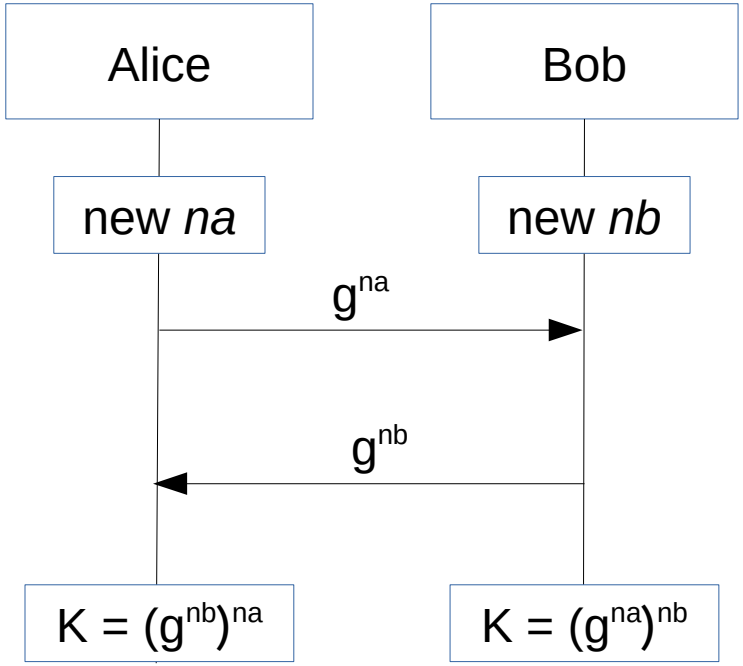
Man-in-the-Middle attacks revisited

Hugo Jonker, Rolando Trujillo, Sjouke Mauw

Open Universiteit
www.ou.nl

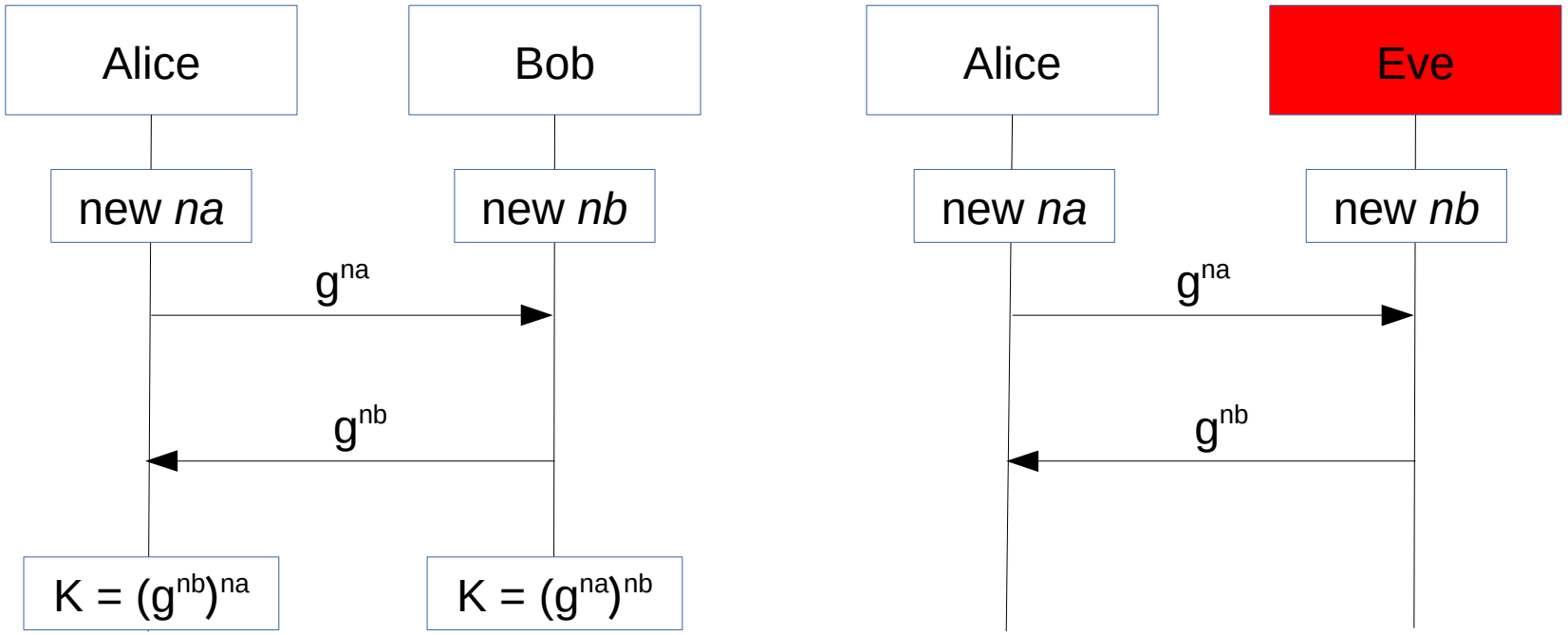
Man-in-the-middle attack

Diffie-Hellman



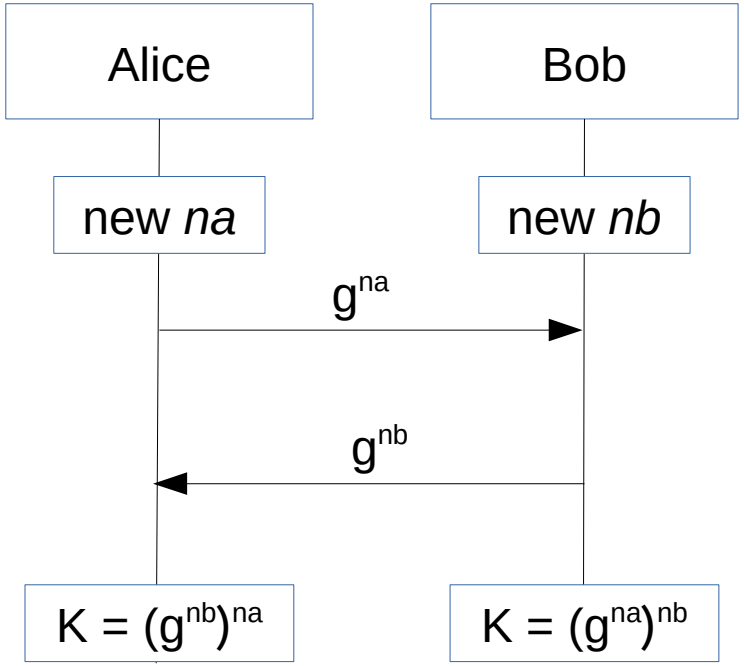
Man-in-the-middle attack

Diffie-Hellman

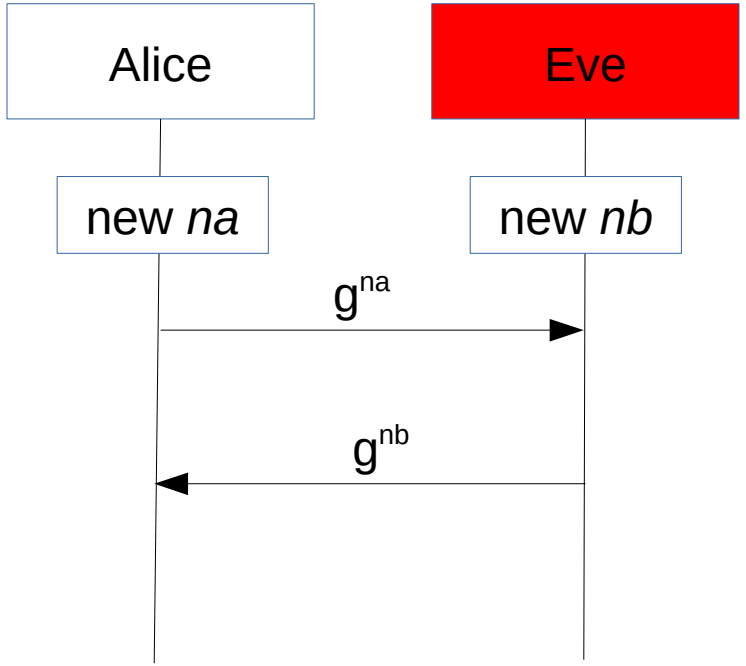


Man-in-the-middle attack

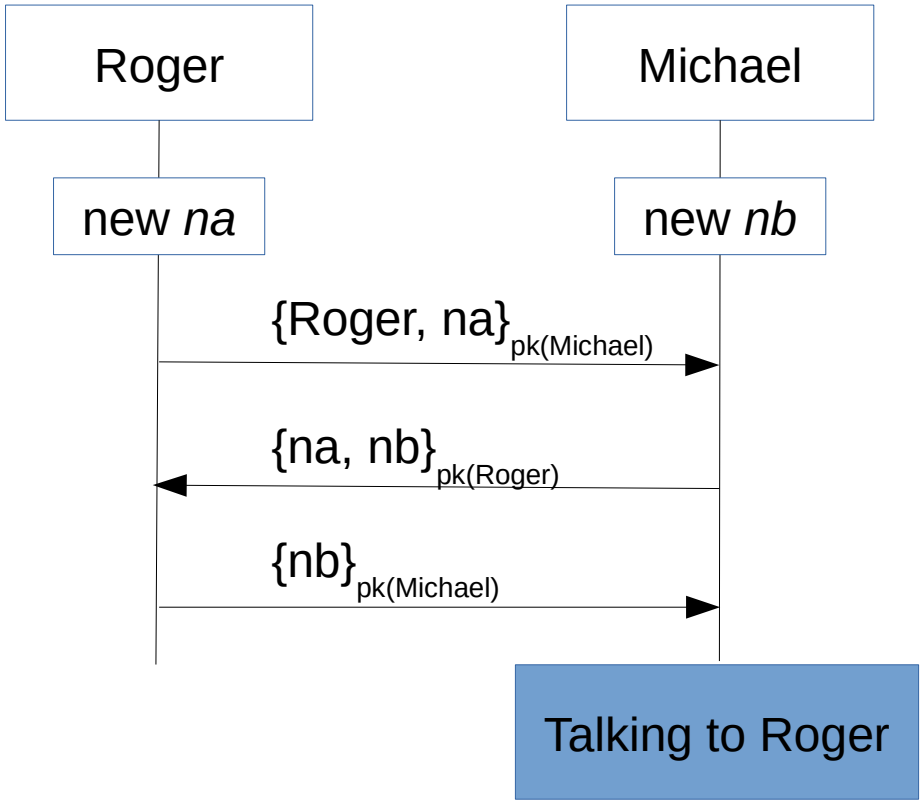
Diffie-Hellman



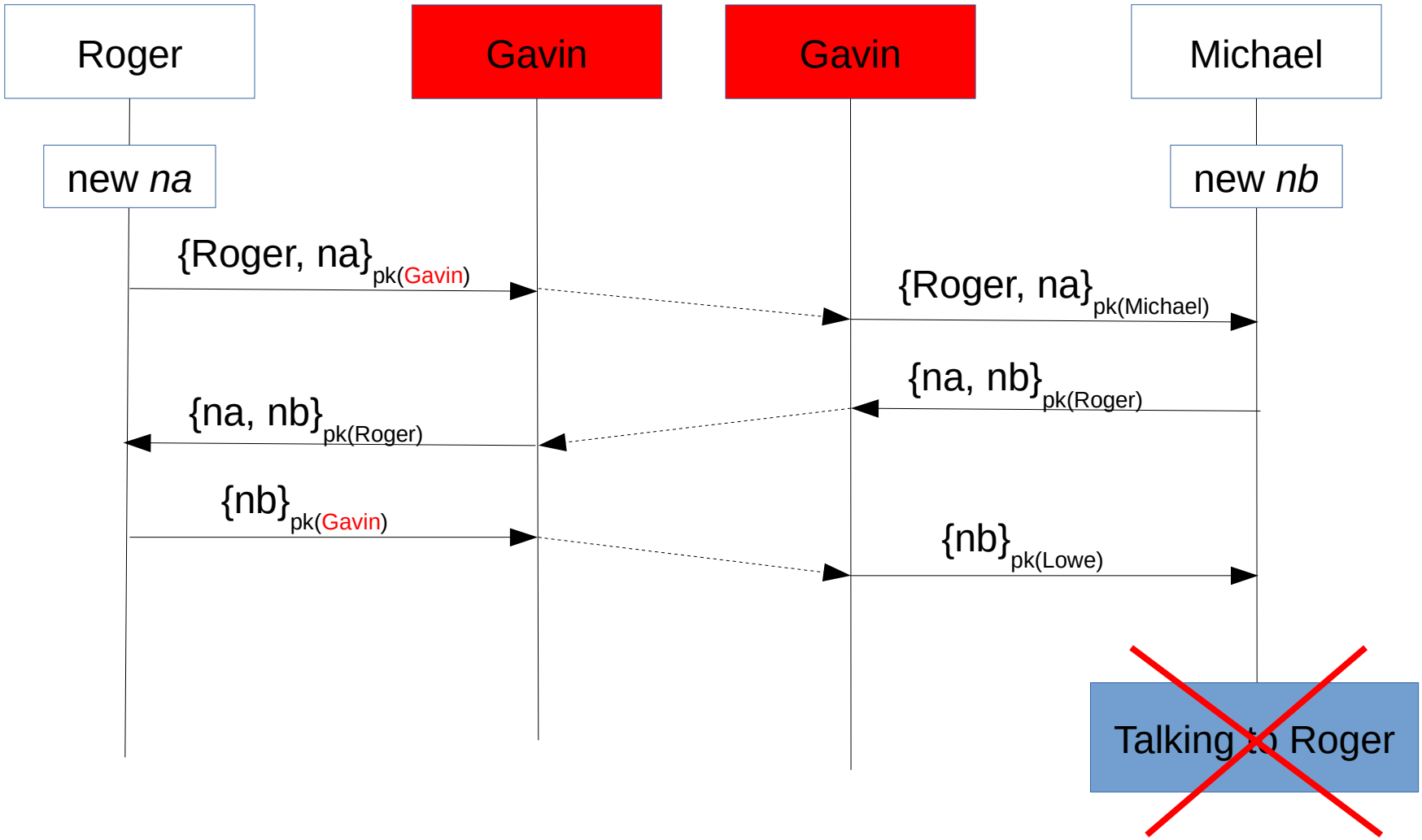
Diffie-Hell, man!



Needham-Schroeder



Needham, Schroeder & Lowe '95



Just a few of many examples

- Academic:
  - Diffie-Hellman: 1976?
  - Lowe on Needham-Schroeder: 1995
- Practice:
  - Moxie Marlinspike:
    - SSLsniff: 2002 attacks IE5.5
    - SSLstrip: 2009 (Black Hat 2009)

Conclusion: we're abundantly aware.

Stopping the MitM?

- Theory:
  - Modelchecking (~ 1995)
  - Tagging (~ 2003)
  - Tool support (mCRL, Scyther, Tamarin,...)
- Practice:
  - Certificate Authorities
  - DNSSec
  - Certificate Pinning
  - ...

Stopping the MitM?

- Theory:
  - Modelchecking (~ 1995)
  - Tagging (~ 2003)
  - Tool support (mCRL, Scyther, Tamarin,...)
- Practice:
  - Certificate Authorities
  - DNSSec
  - Certificate Pinning
  - ...

Conclusion: we've got this.

Meanwhile...

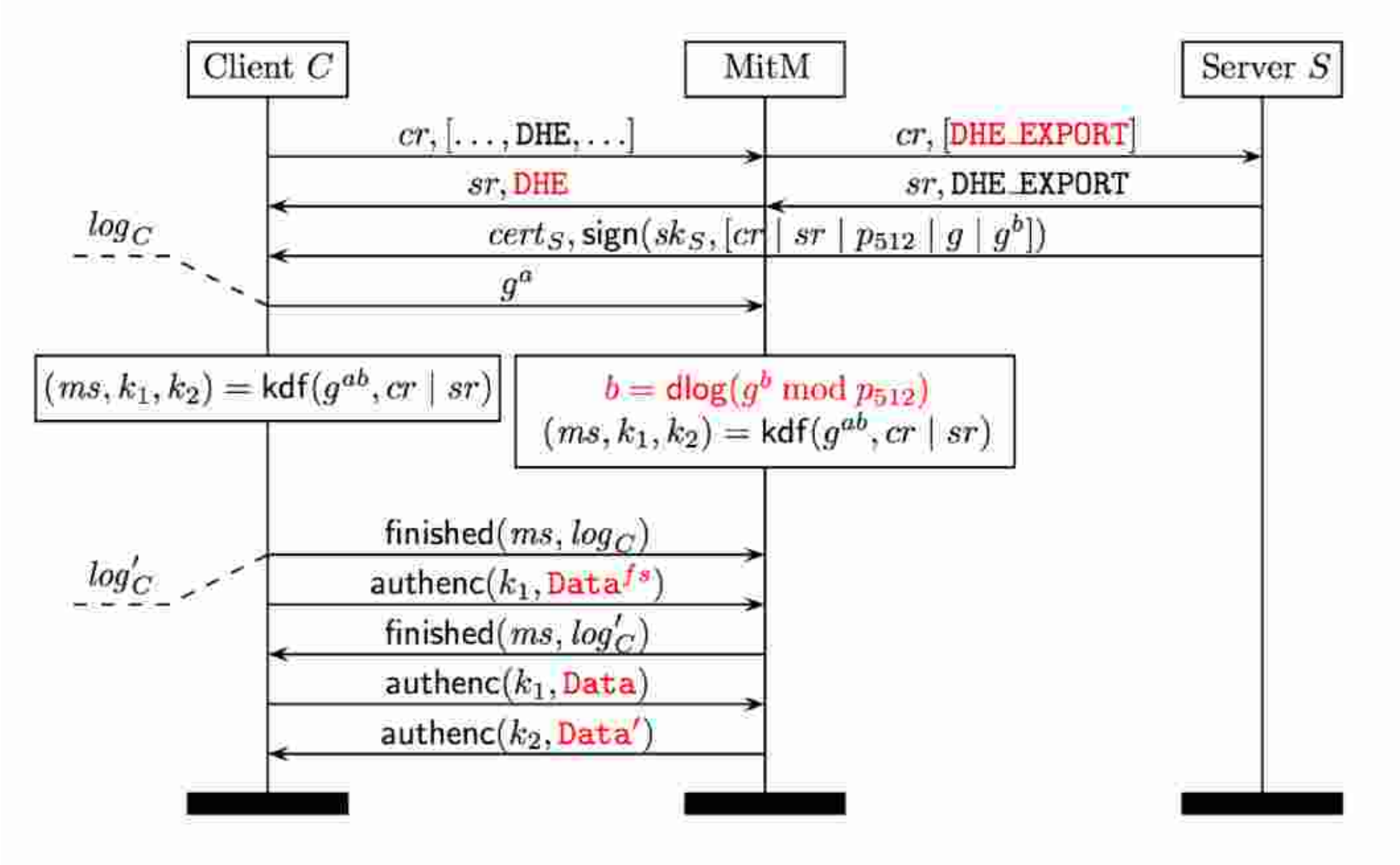
POODLE attack [MDK14]

- Force downgrade of TLS
- Attack SSLv3.0
  - RC4 is biased

FREAK attack [S&P15]

- US export restrictions mandated weak crypto (RSA < 512 bits)
- Still supported in some TLS implementations
- MitM changes cipher spec to “weak crypto”

LOGJAM attack [CCS15]



DROWN attack [ASS+16]

- Take client's encrypted TLS messages
- Use SSLv2.0 server as decryption oracle

DROWN attack [ASS+16]

- Take client's encrypted TLS messages
- Use SSLv2.0 server as decryption oracle

In general, the attacker must passively capture about 1,000 TLS sessions using RSA key exchange, make 40,000 SSLv2 connections to the victim server and perform 2^{50} symmetric encryption operations.

That's all theoretical, right?

MitM devices for cellphones:

- Stingray: $68,000
- Gossamer: $19,000
- Triggerfish: $90,000
- Hailstorm: $170,000

Conclusion:
We definitely do not “have” this.

Exploited flaws

- POODLE, Logjam, FREAK, DROWN: initialisation

- Cellphone MitM devices: new properties

Both cases: not accounted for by protocol.

Categorising attacks

- Protocol context
  - Initialisation
- User context
  - location

Solution directions

Embed context into formal security proofs

- With a trusted partner:
  context agreement

- Without a trusted partner:
  context verification

Context agreement

Definition 2 (Context agreement). *A party A achieves* context agreement *with another party B on B's context C_B if, whenever A completes a run of the protocol (apparently with B) then B has been previously running the protocol (apparently with A) and the observation of A on B's context is the same as B's observation of his context in that run, that is: $obs_A(C_B) = obs_B(C_B)$.*

Note: agreement on observed context, not on actual context.

Context verification

Definition 1 (Context verification). *A party A achieves* context verification *of her observation $obs_A(C_B)$ of the context C_B of party B if, whenever A completes a run of the protocol (apparently with B) then $obs_A(C_B)$ is correct with respect to C_B.*

Example application: GSM

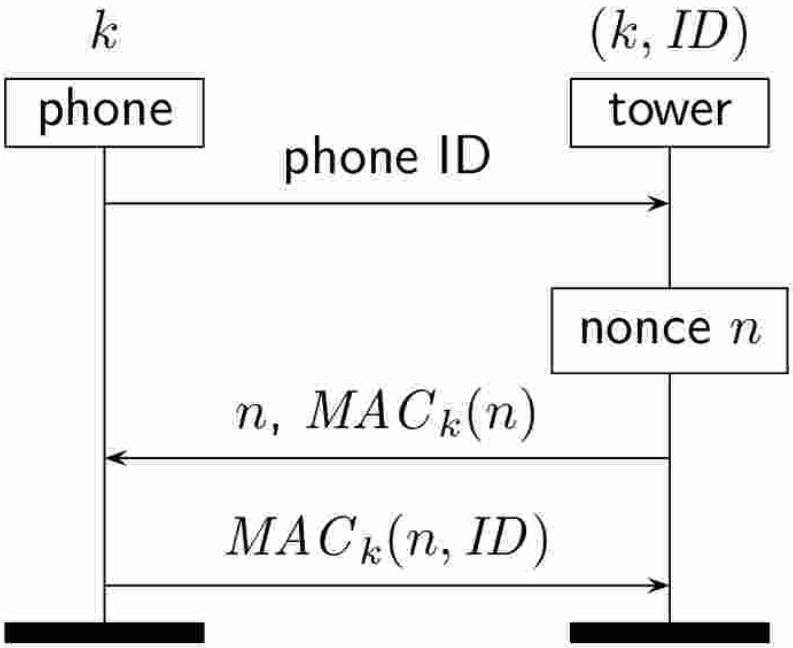


Fig. 1. Simplified UMTS protocol.

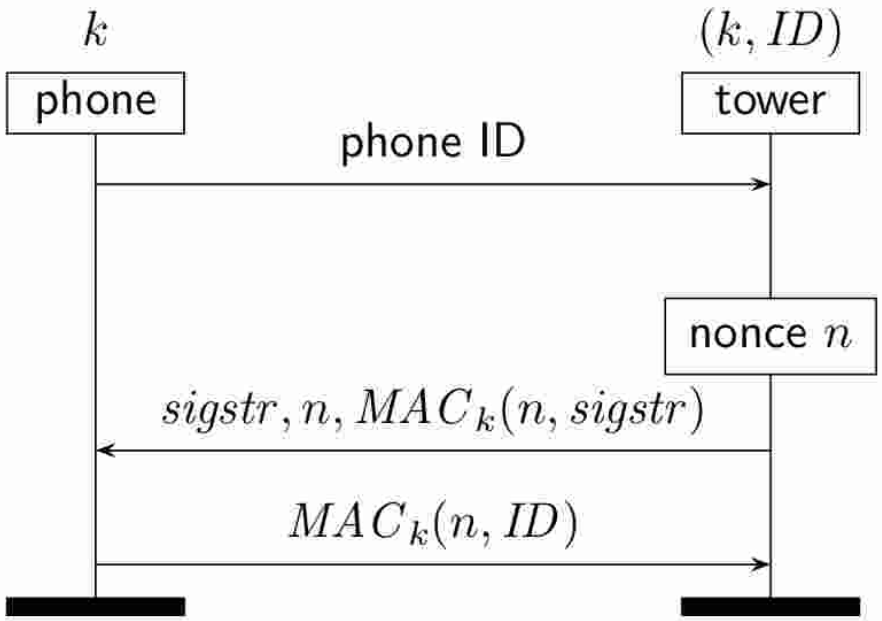


Fig. 2. Inclusion of context.

Conclusion

- Man-in-the-middle attacks still exist
- They are preventable
- Prevention:
  - Account for context
    - Protocol context (initialisation)
    - User context (location)
  - With or without trusted partner

Thank you for your attention!