(More) cryptographic protocols

Myrto Arapinis
School of Informatics
University of Edinburgh

October 19, 2017

Authentication and key agreement protocols

Authentication and key agreement

- Long-term keys should be used as little as possible to to reduce "attack-srufarce"
- The use of a key should be restricted to a specific purpose
  e.g. you shouldn't use the same RSA key both for encryption and signing
- Public key algorithms tend to be computationally more expensive than symmetric key algorithms

$\rightsquigarrow$ Long-term keys are used to establish short-term session keys
e.g. TLS over HTTP, AKA for 3G, BAC for epassports, *etc.*

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

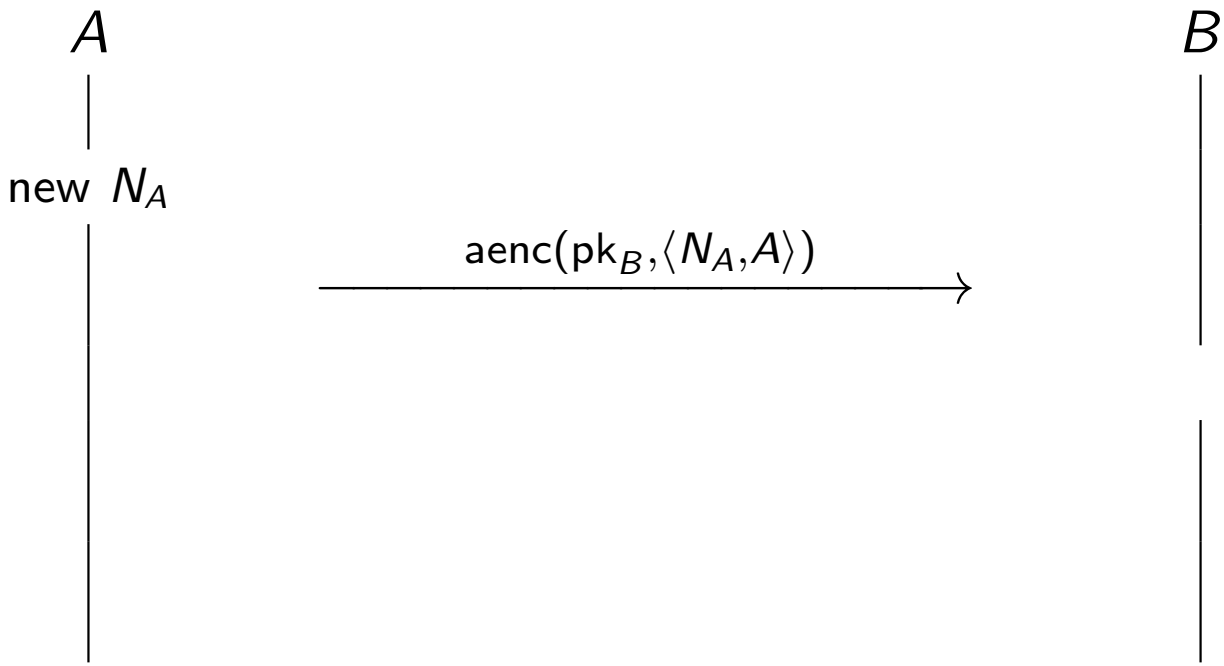
Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol

[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

Needham-Schroeder Public Key (NSPK)

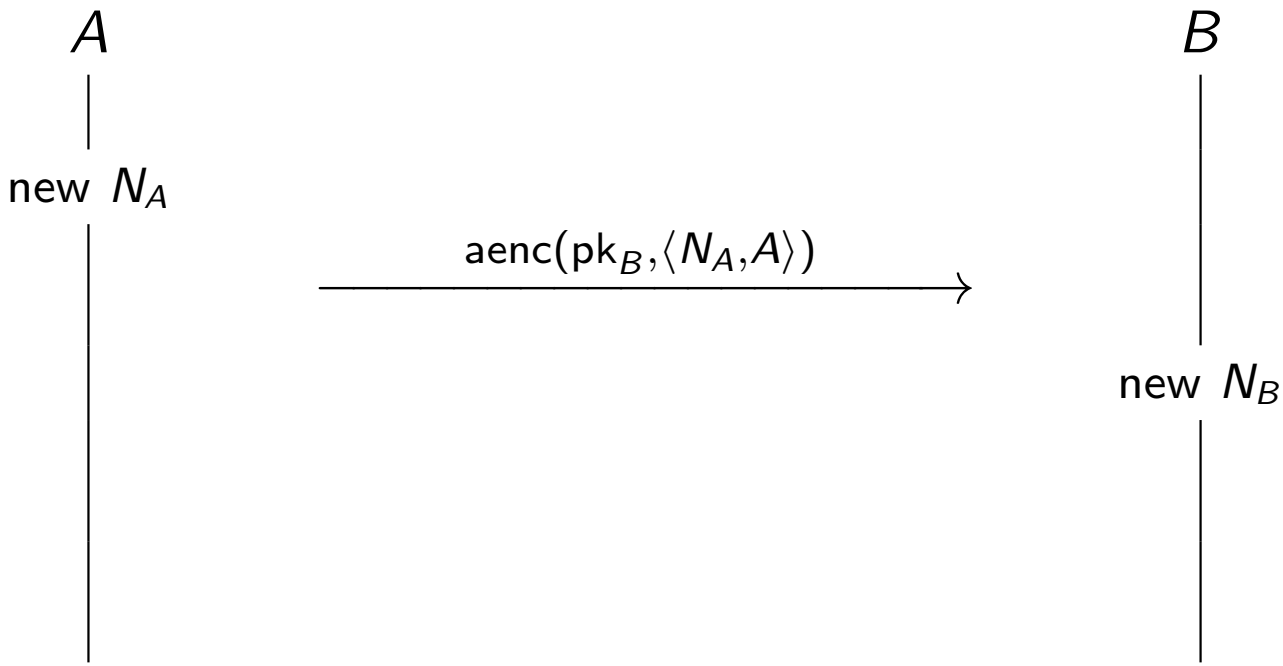
NSPK: authentication and key agreement protocol



[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

Needham-Schroeder Public Key (NSPK)

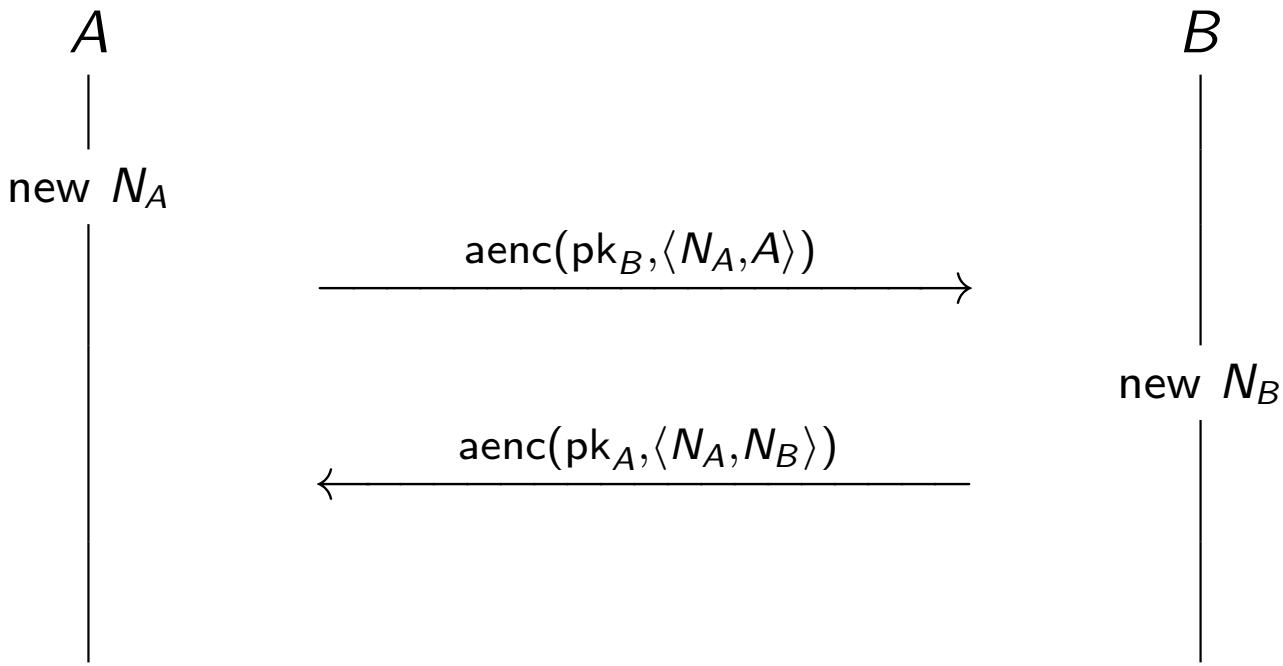
NSPK: authentication and key agreement protocol



[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

Needham-Schroeder Public Key (NSPK)

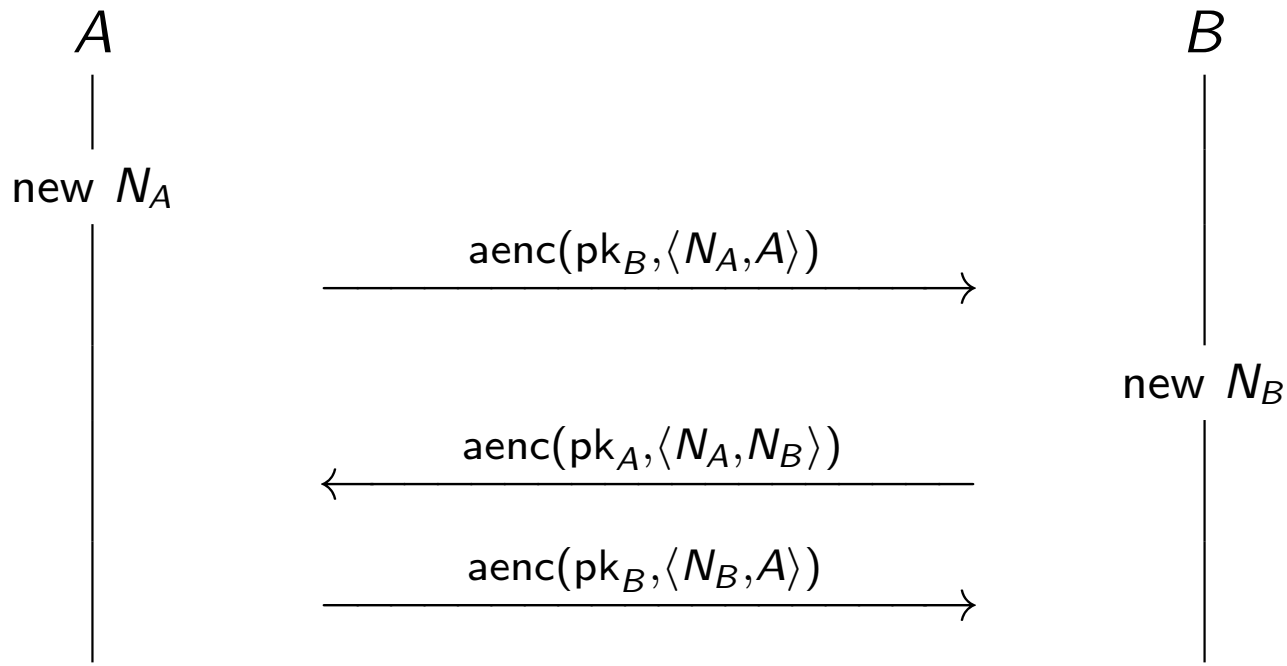
NSPK: authentication and key agreement protocol



[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

Needham-Schroeder Public Key (NSPK)

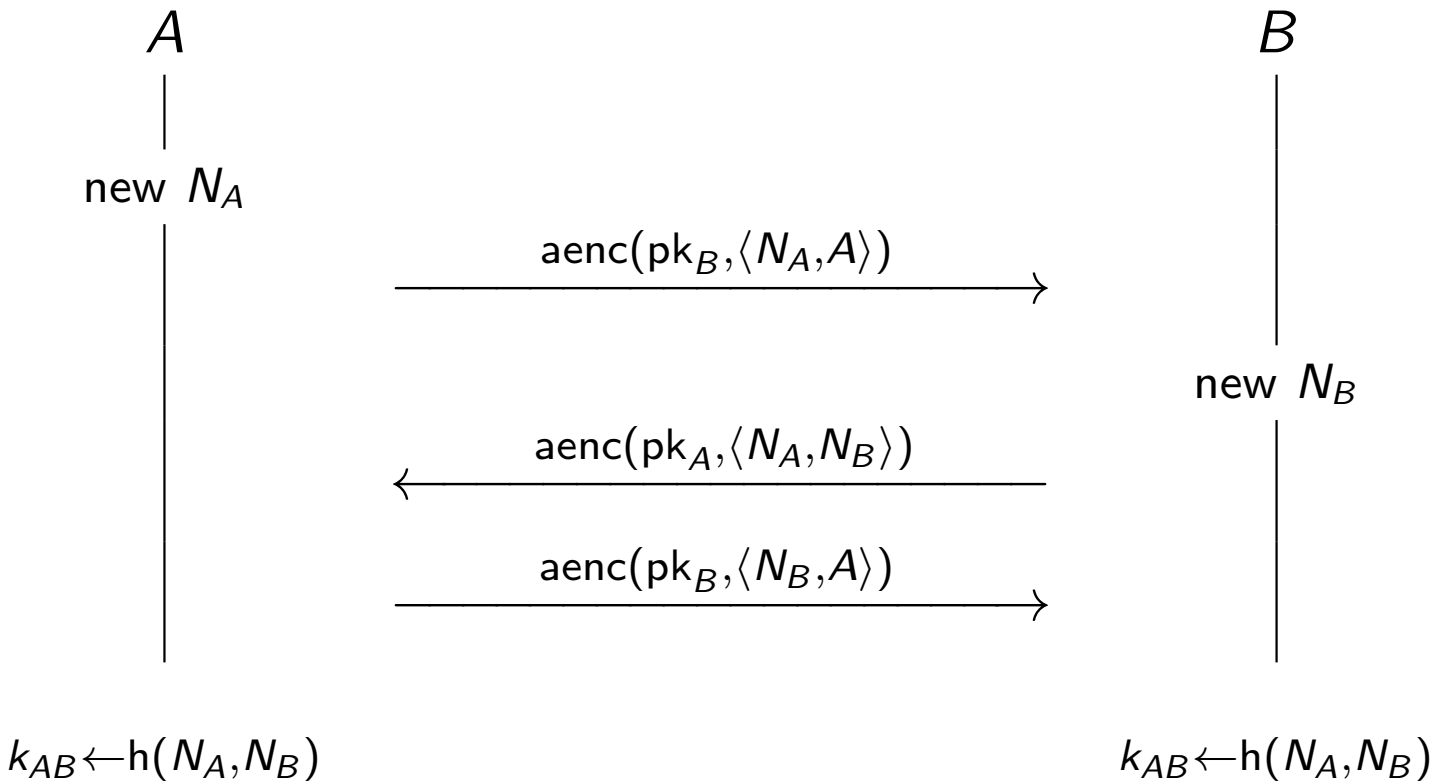
NSPK: authentication and key agreement protocol



[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

Needham-Schroeder Public Key (NSPK)

NSPK: authentication and key agreement protocol



[N. Roger, M. Schroeder, Michael. "Using encryption for authentication in large networks of computers". Communications of the ACM (December 1978)]

NSPK: security requirements

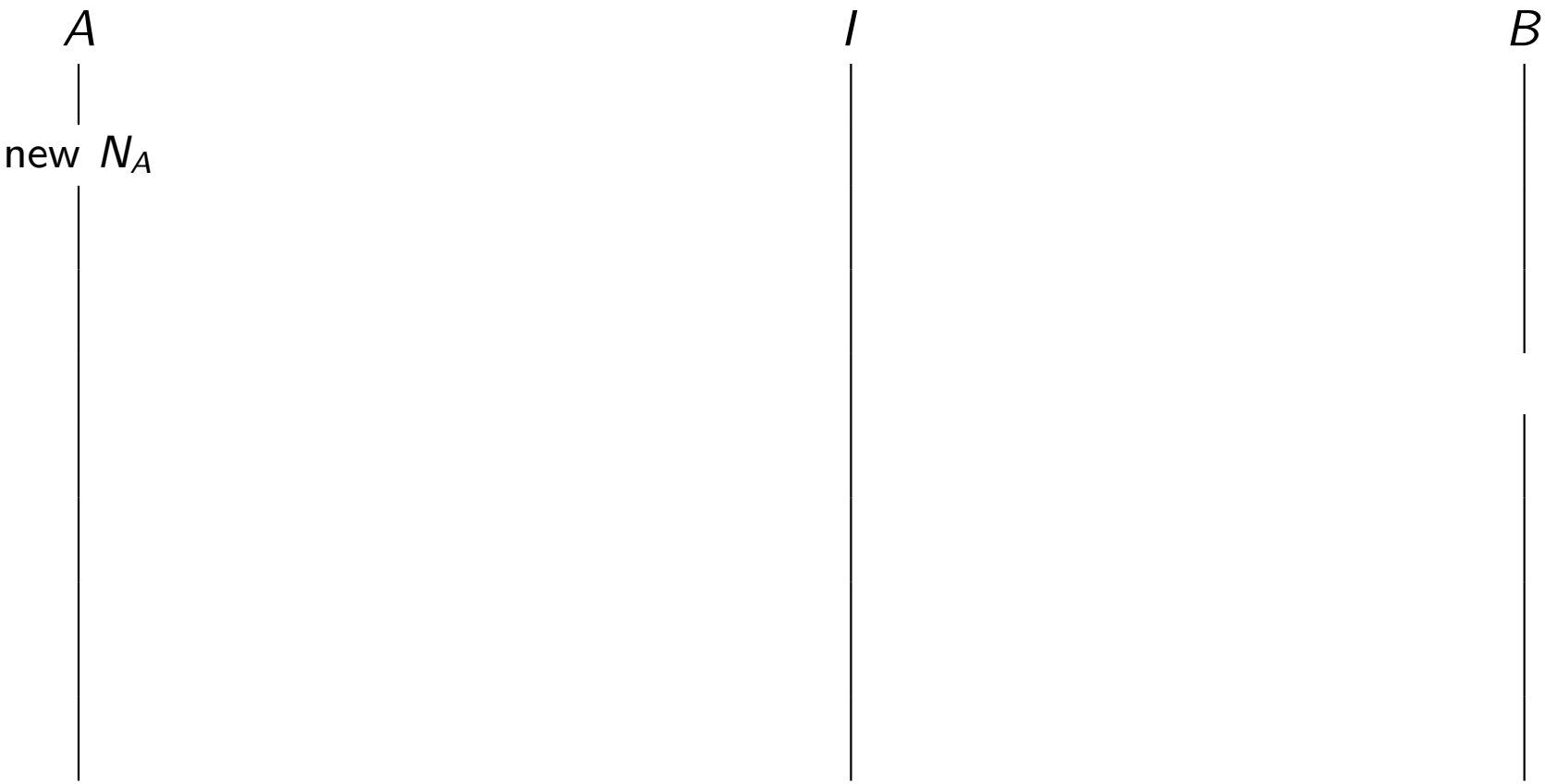
- Authentication: if Alice has completed the protocol, apparently with Bob, then Bob must also have completed the protocol with Alice.
- Authentication: If Bob has completed the protocol, apparently with Alice, then Alice must have completed the protocol with Bob.
- Confidentiality: Messages sent encrypted with the agreed key ($k \leftarrow \mathrm{h}(N_A, NB)$) remain secret.

NSPK: Lowe's attack on authentication

Attack found 17 years after the publication of the NS protocol!!

NSPK: Lowe's attack on authentication

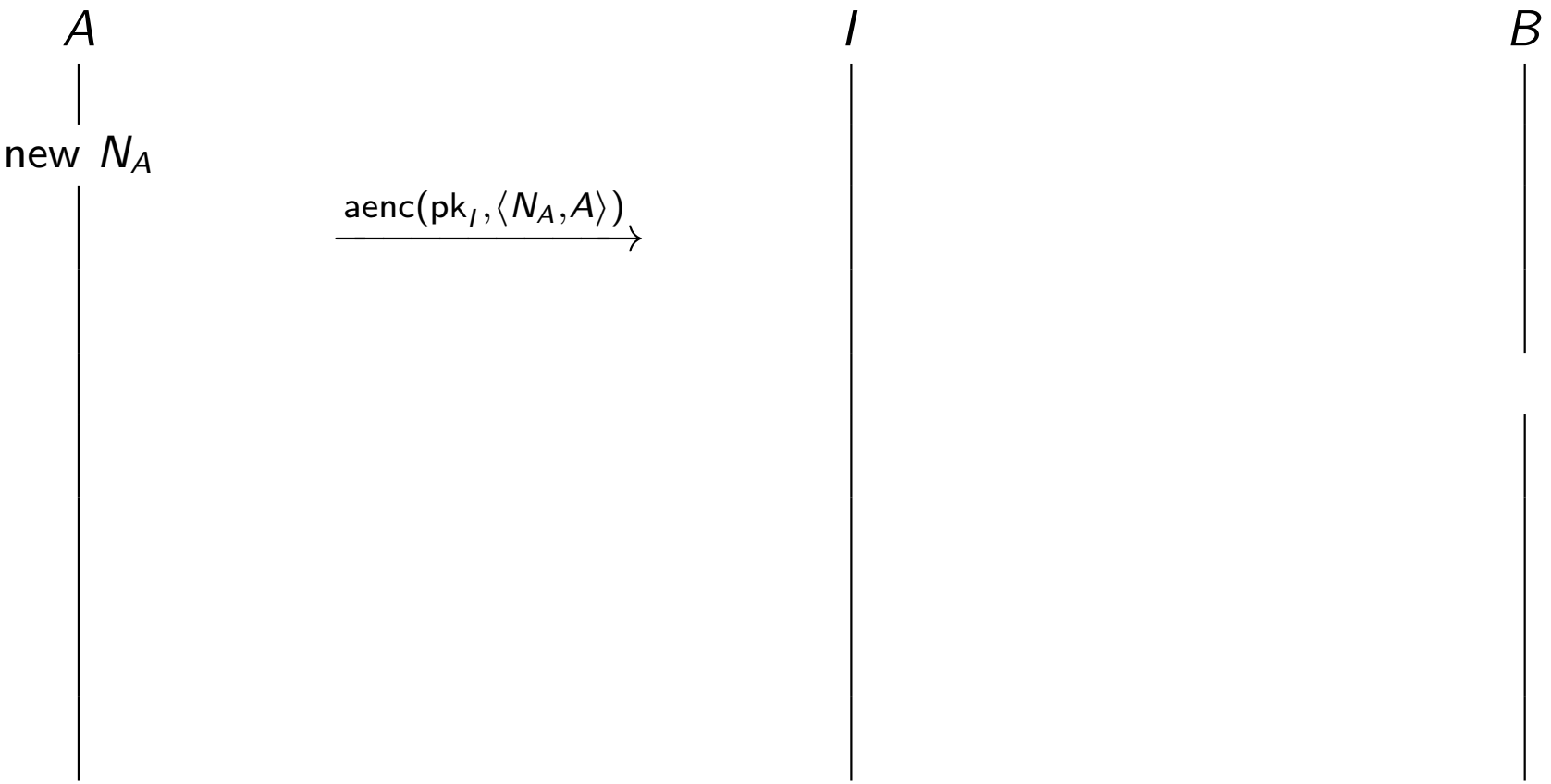
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

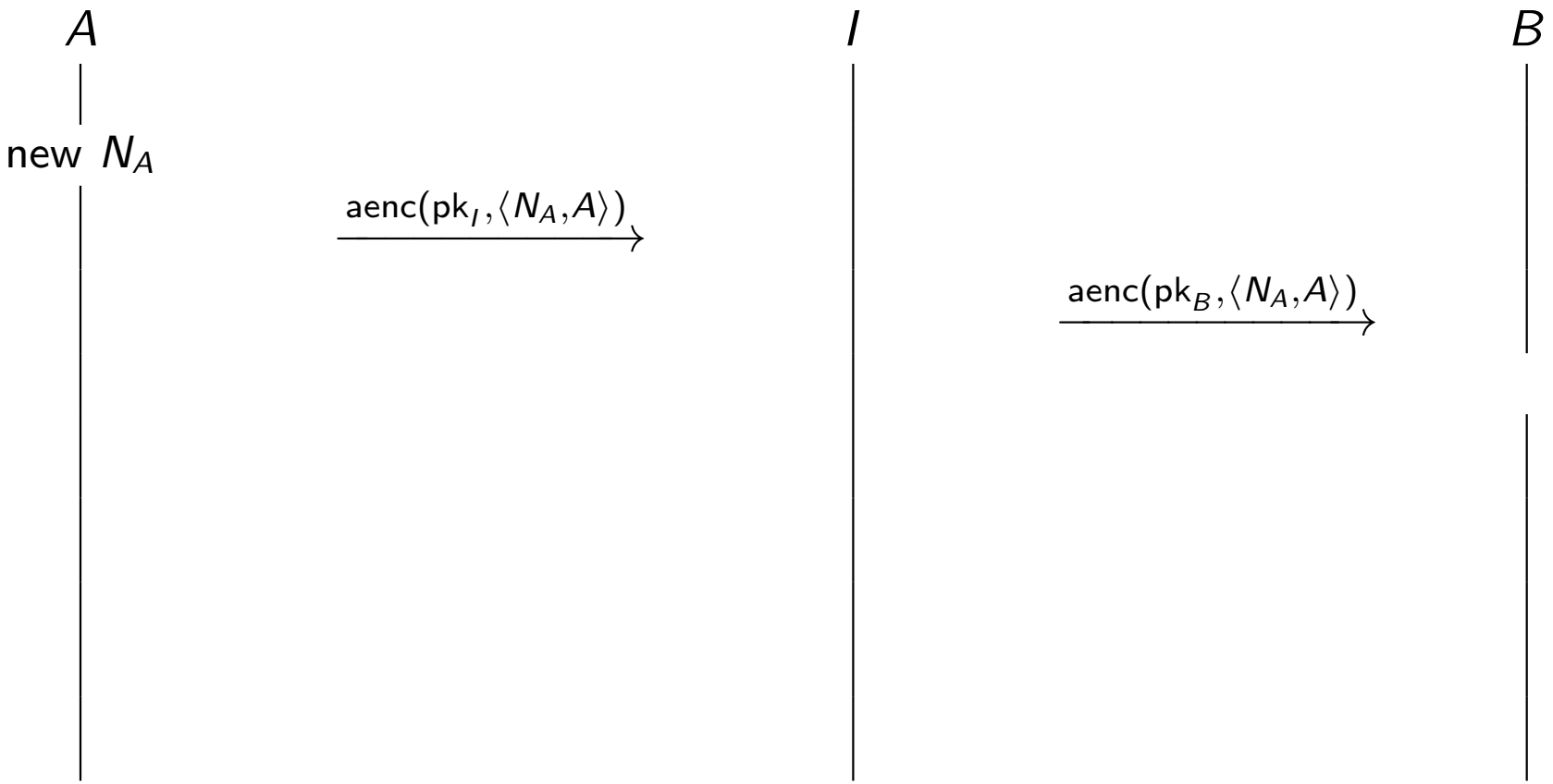
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

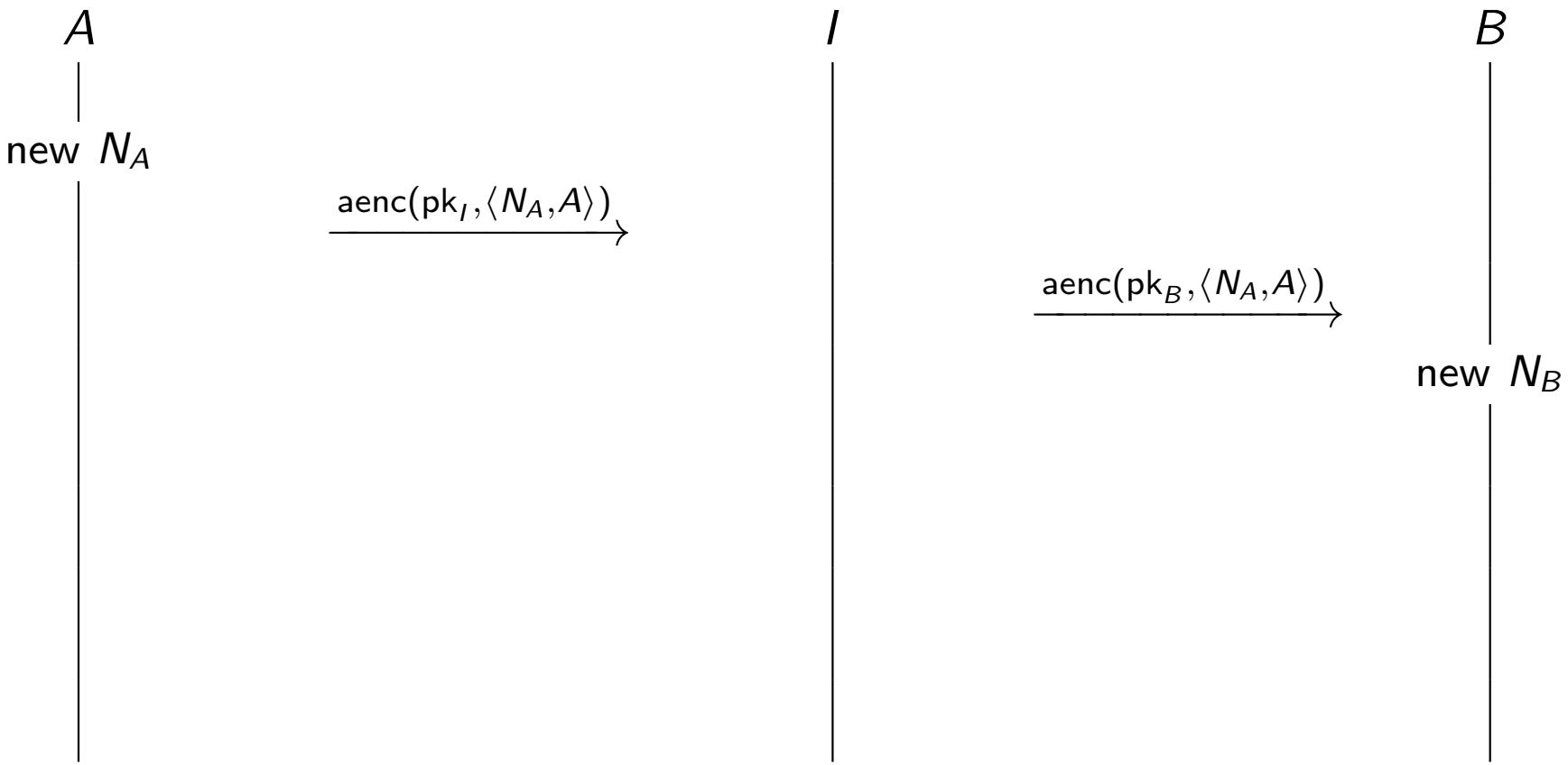
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

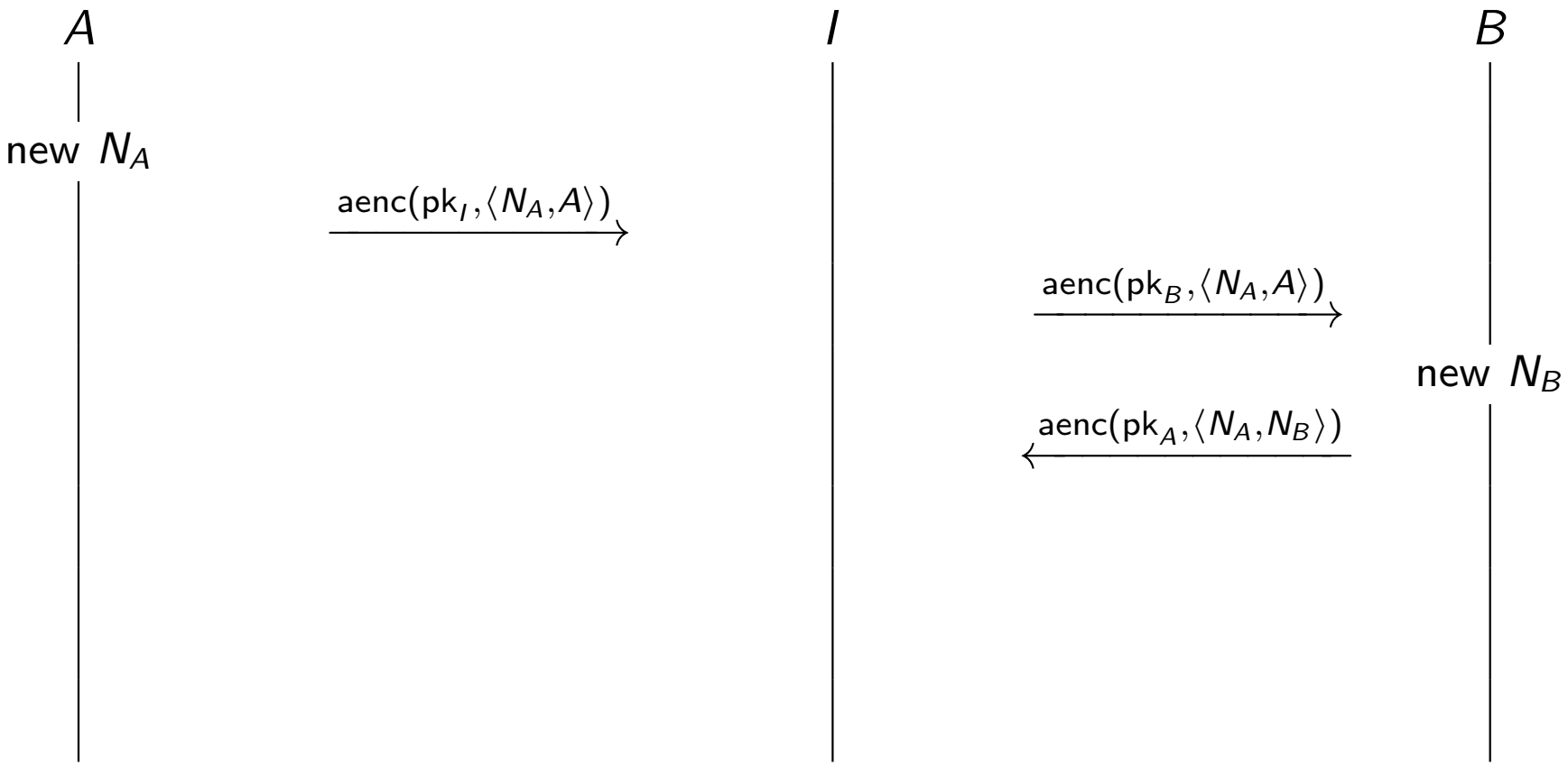
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

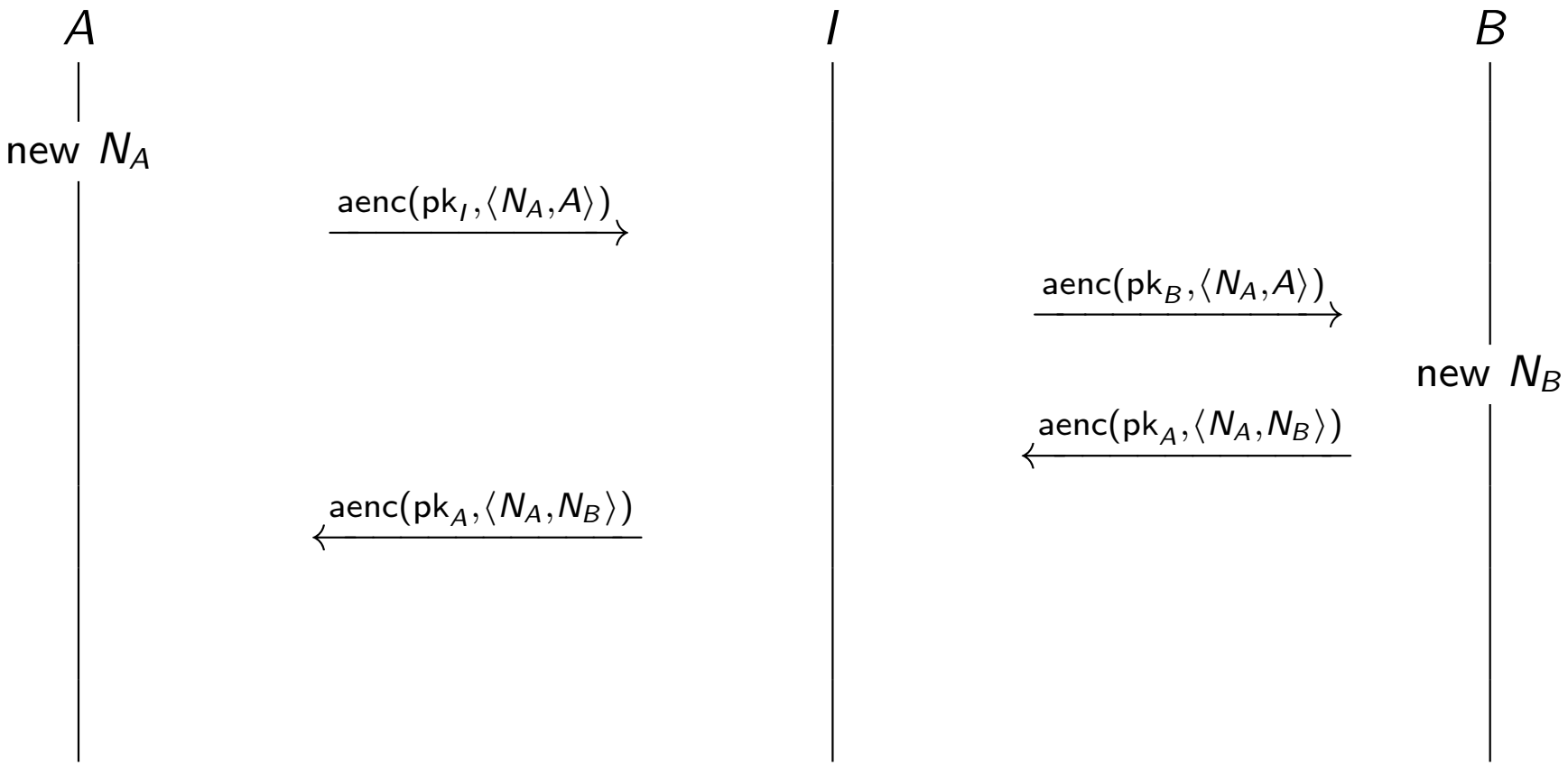
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

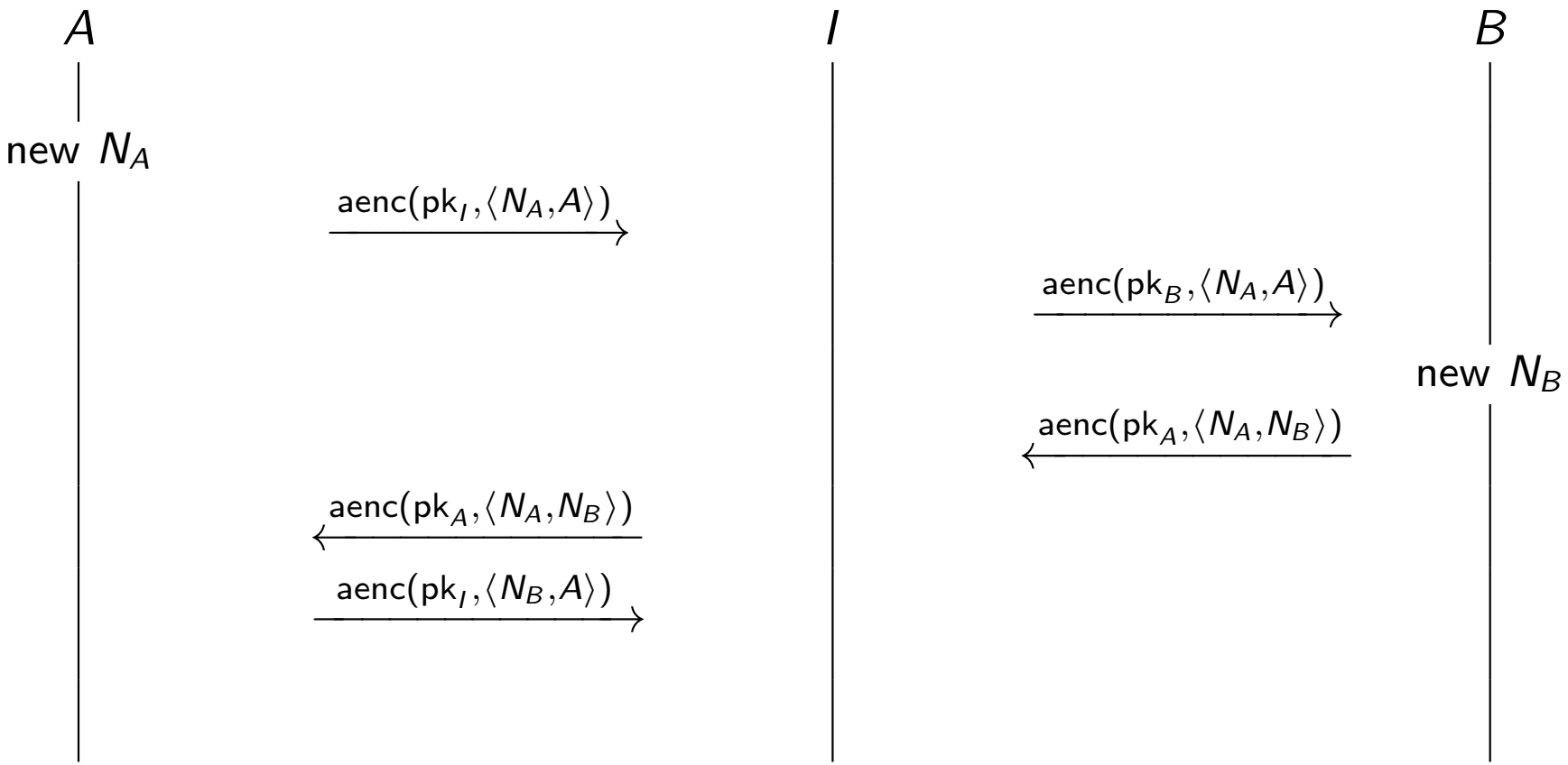
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

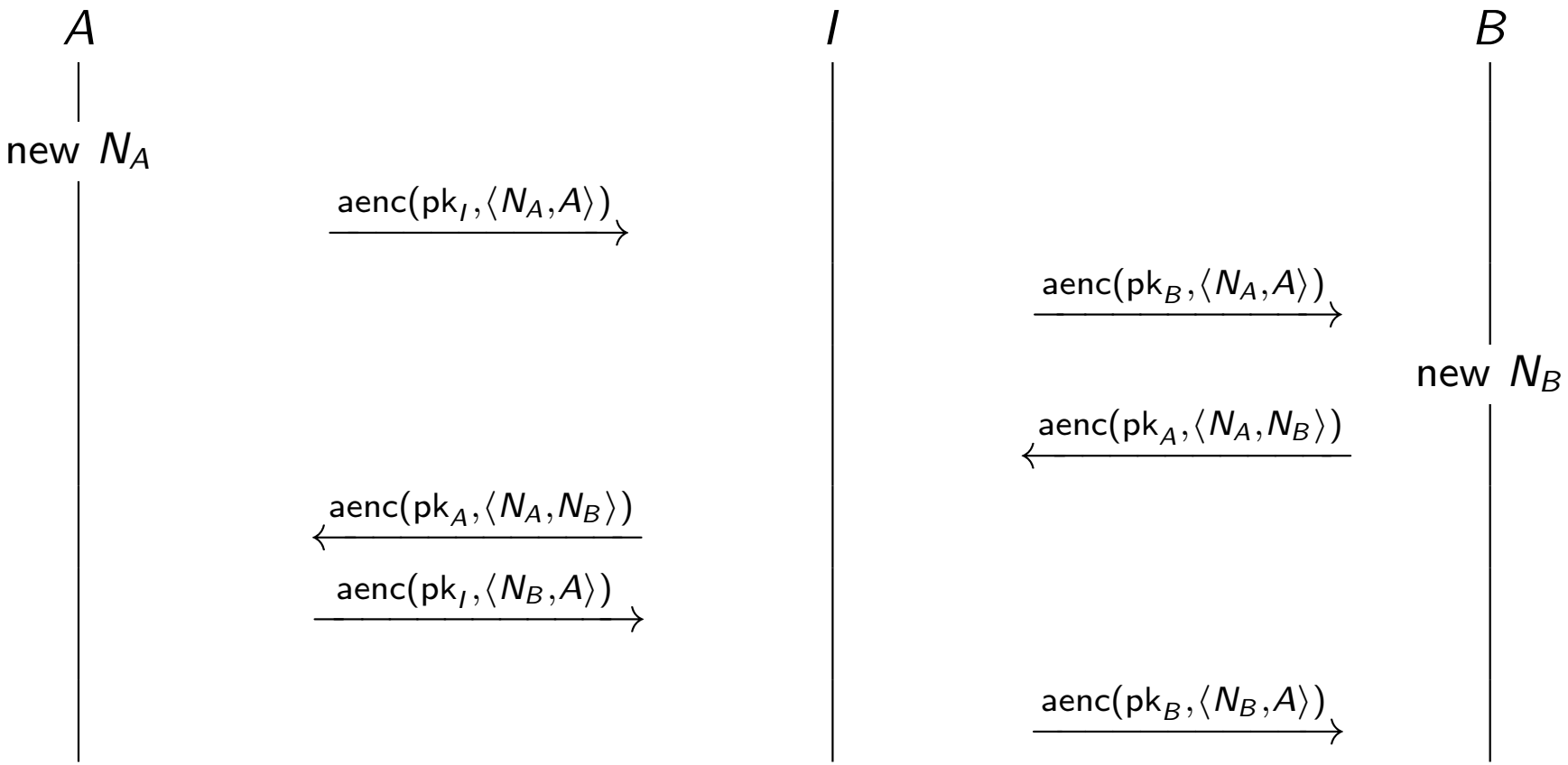
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

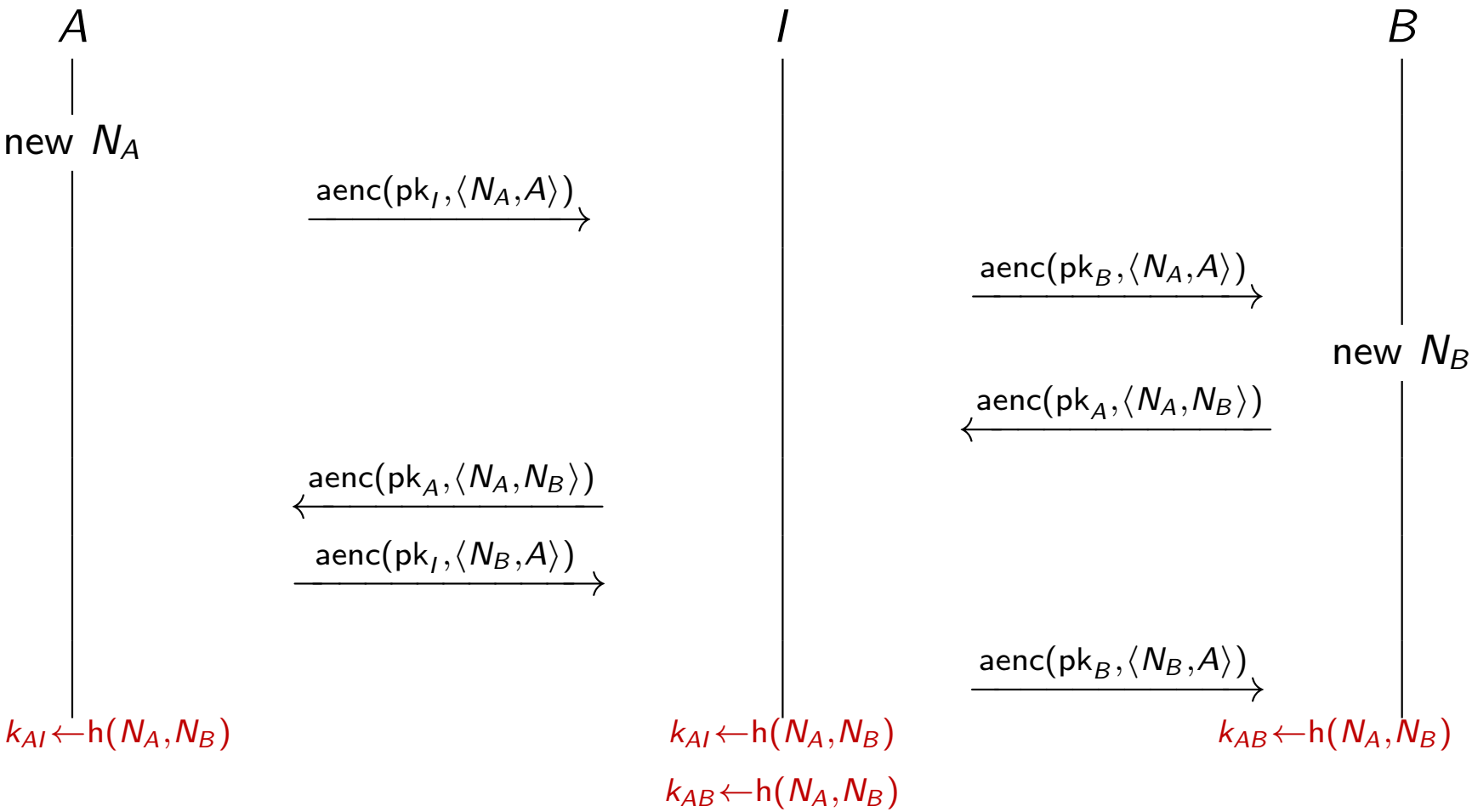
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's attack on authentication

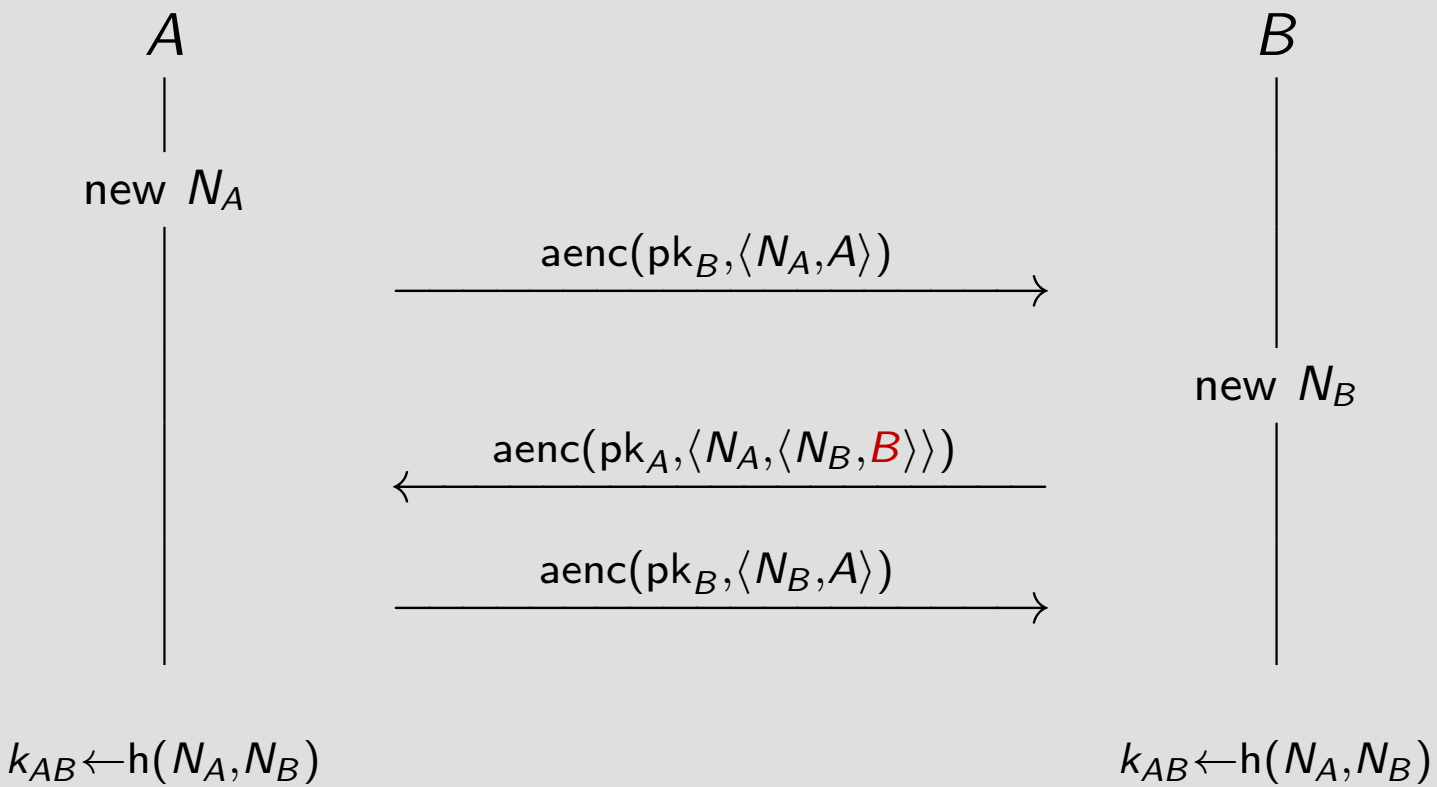
Attack found 17 years after the publication of the NS protocol!!



[G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol". Information Processing Letters (November 1995)]

NSPK: Lowe's fix

The Needham-Schroeder-Lowe (NSL) protocol



Forward secrecy

- The NSL protocol is secure against an attacker that controls the network.
- What if the Alice's and Bob's private keys get compromised?
- What if the government forces Alice and Bob to reveal their private keys?
- Can we still protect confidentiality?

Forward secrecy

A protocol ensures forward secrecy, if even if long-term keys are compromised, past sessions of the protocol are still kept confidential, and this even if an attacker actively interferred.

The Station-to-Station (StS) protocol

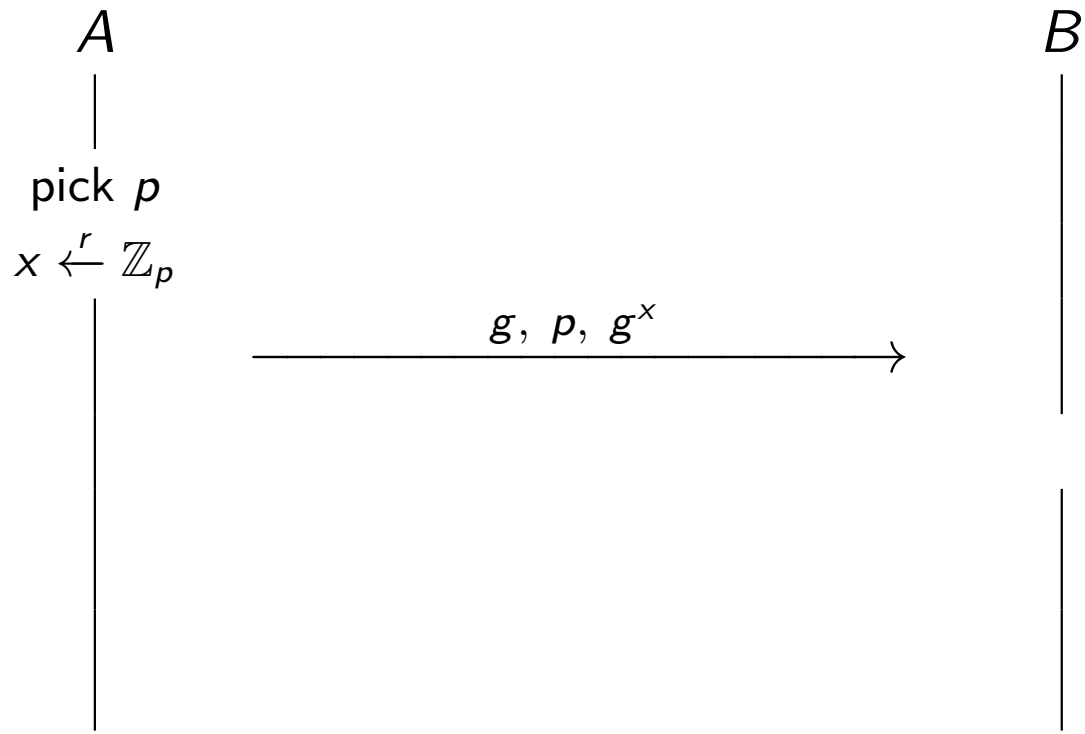
The Station-to-Station (StS) protocol

- where p is a large prime
- and g a generator of $\mathbb{Z}_p^*$

The Station-to-Station (StS) protocol

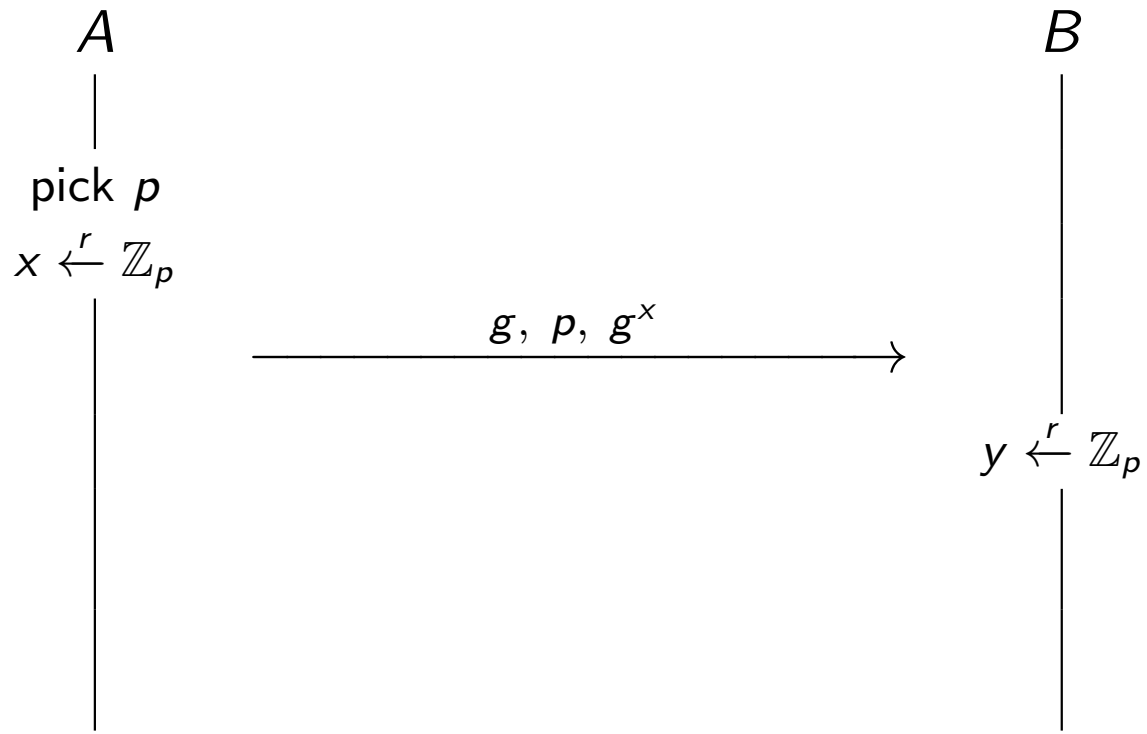
- where p is a large prime
- and g a generator of $\mathbb{Z}_p^*$

The Station-to-Station (StS) protocol



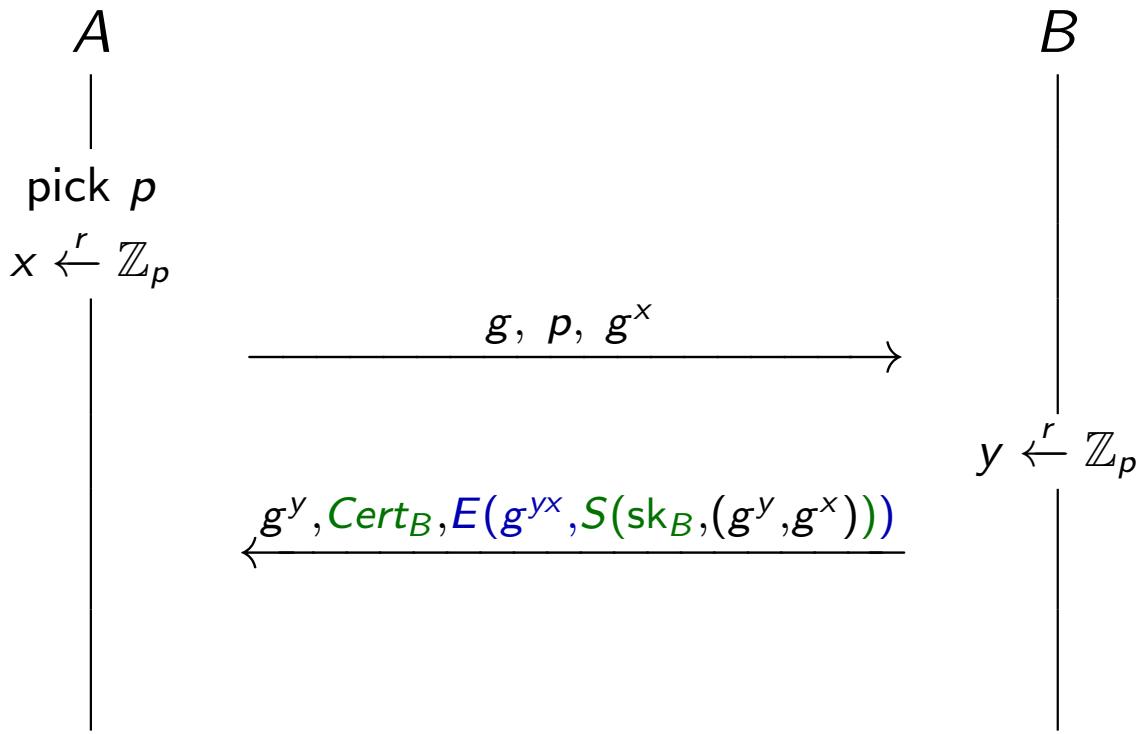
- where p is a large prime
- and g a generator of $\mathbb{Z}_p^*$

The Station-to-Station (StS) protocol



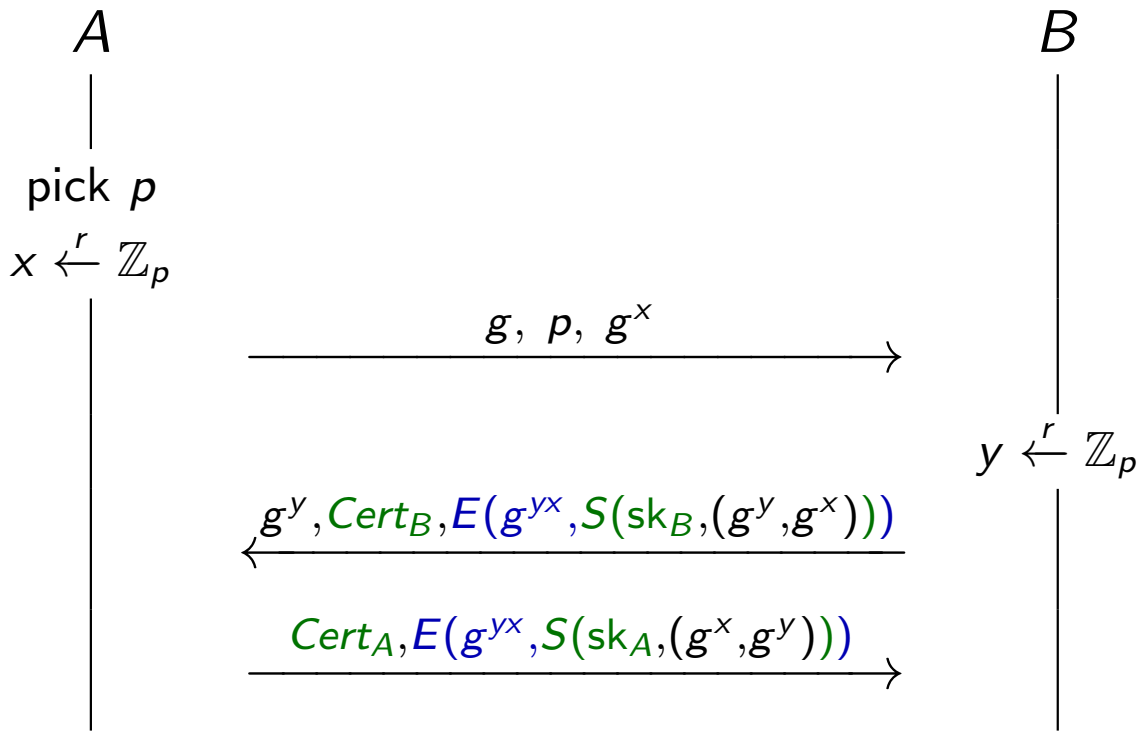
- where p is a large prime
- and g a generator of $\mathbb{Z}_p^*$

The Station-to-Station (StS) protocol



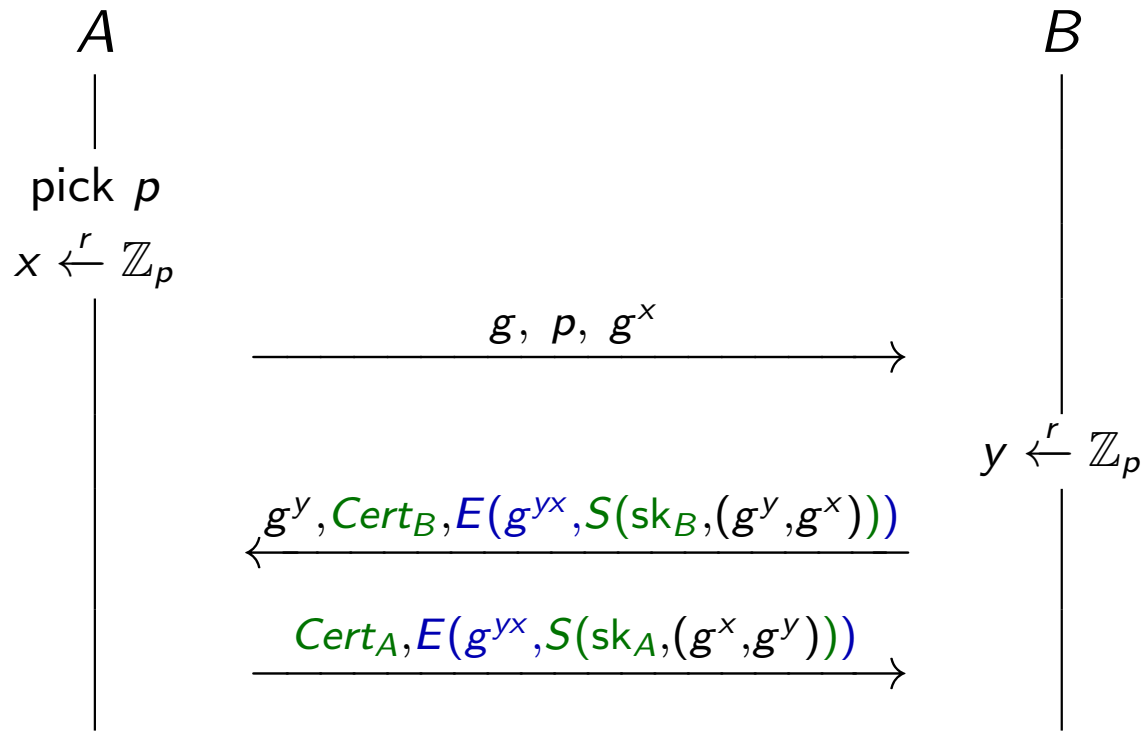
- where p is a large prime
- and g a generator of $\mathbb{Z}_p^*$

The Station-to-Station (StS) protocol



- where p is a large prime
- and g a generator of $\mathbb{Z}_p^*$

The Station-to-Station (StS) protocol



- where p is a large prime
- and g a generator of $\mathbb{Z}_p^*$

The StS ensures mutual authentication, key agreement, and forward secrecy

The Basic Access Control (BAC) protcol

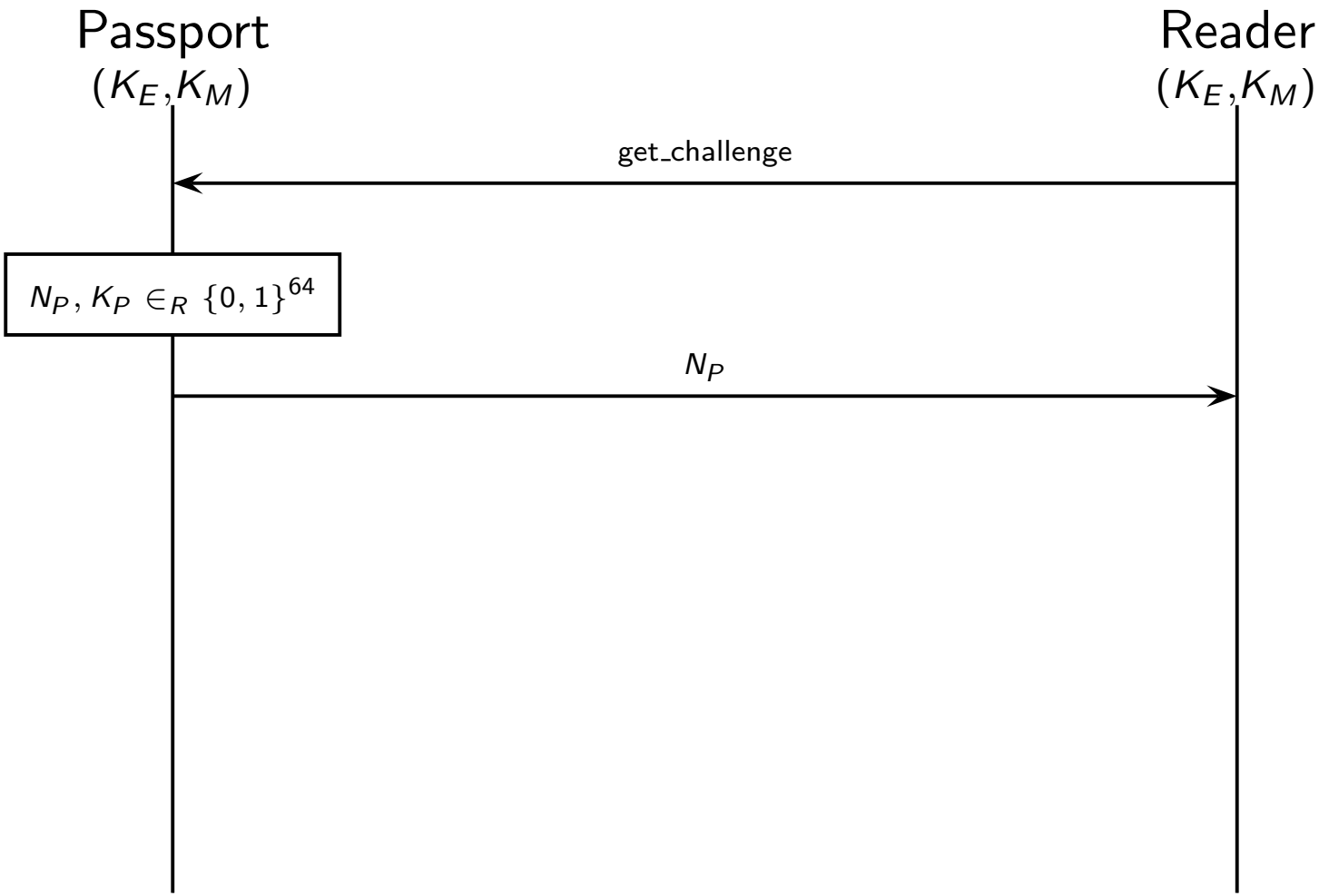
An e-Passport is a passport with an RFID tag embedded in it.

The RFID tag stores:

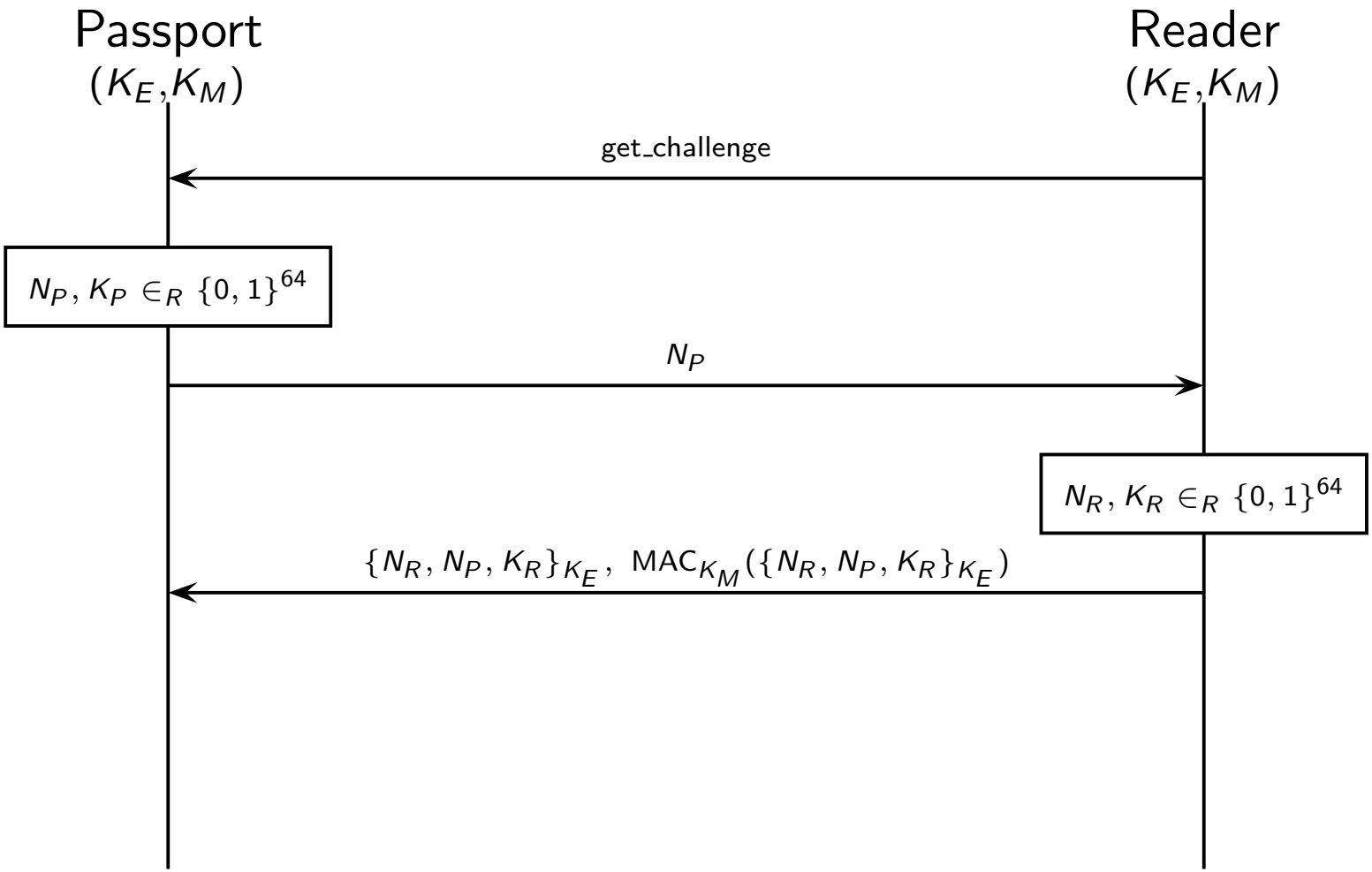
- the information printed on the passport,
- a JPEG copy of the picture

BAC: authentication and key agreement protocol implemented on e-Passports

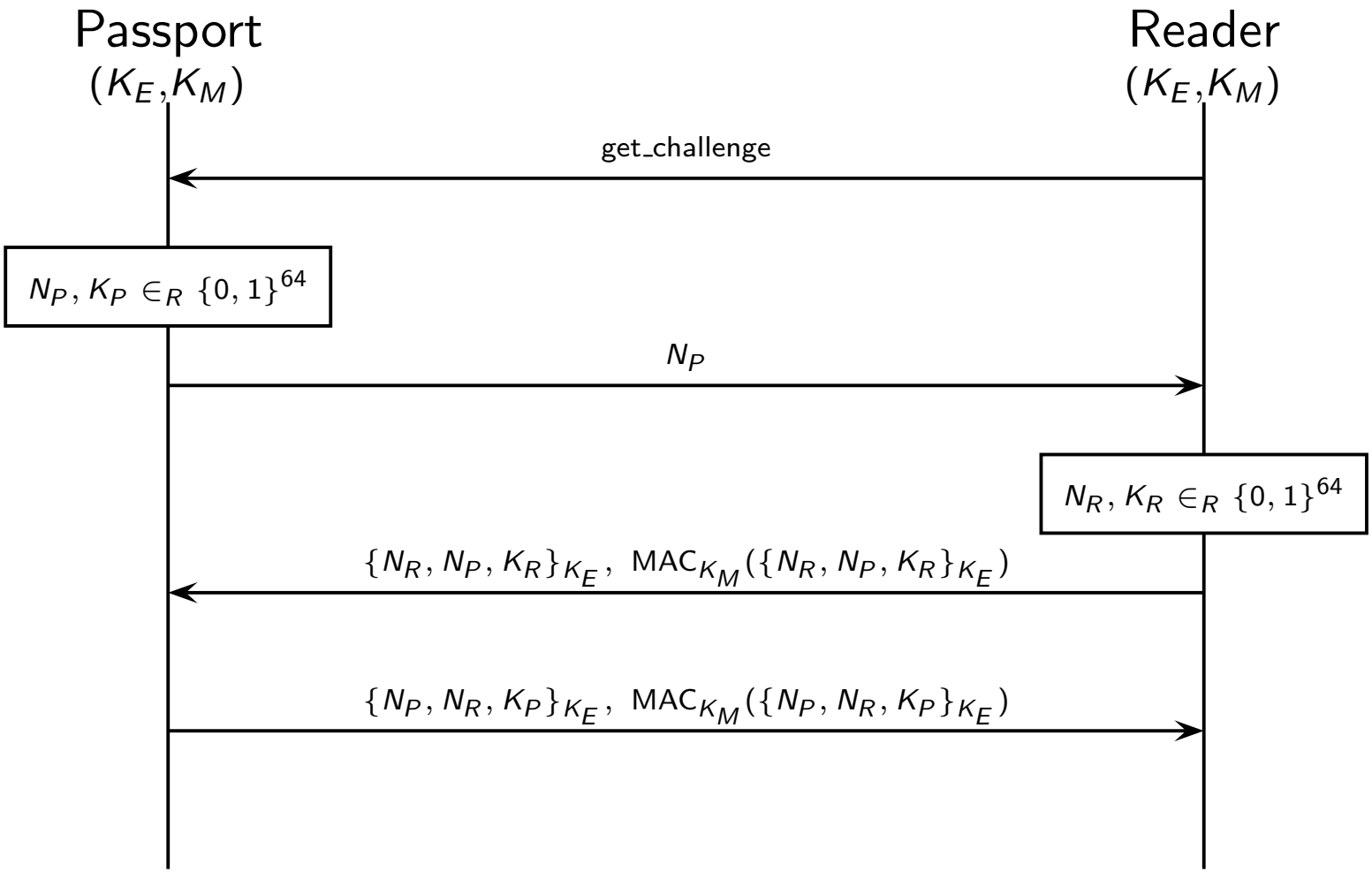
The Basic Access Control protocol (BAC)



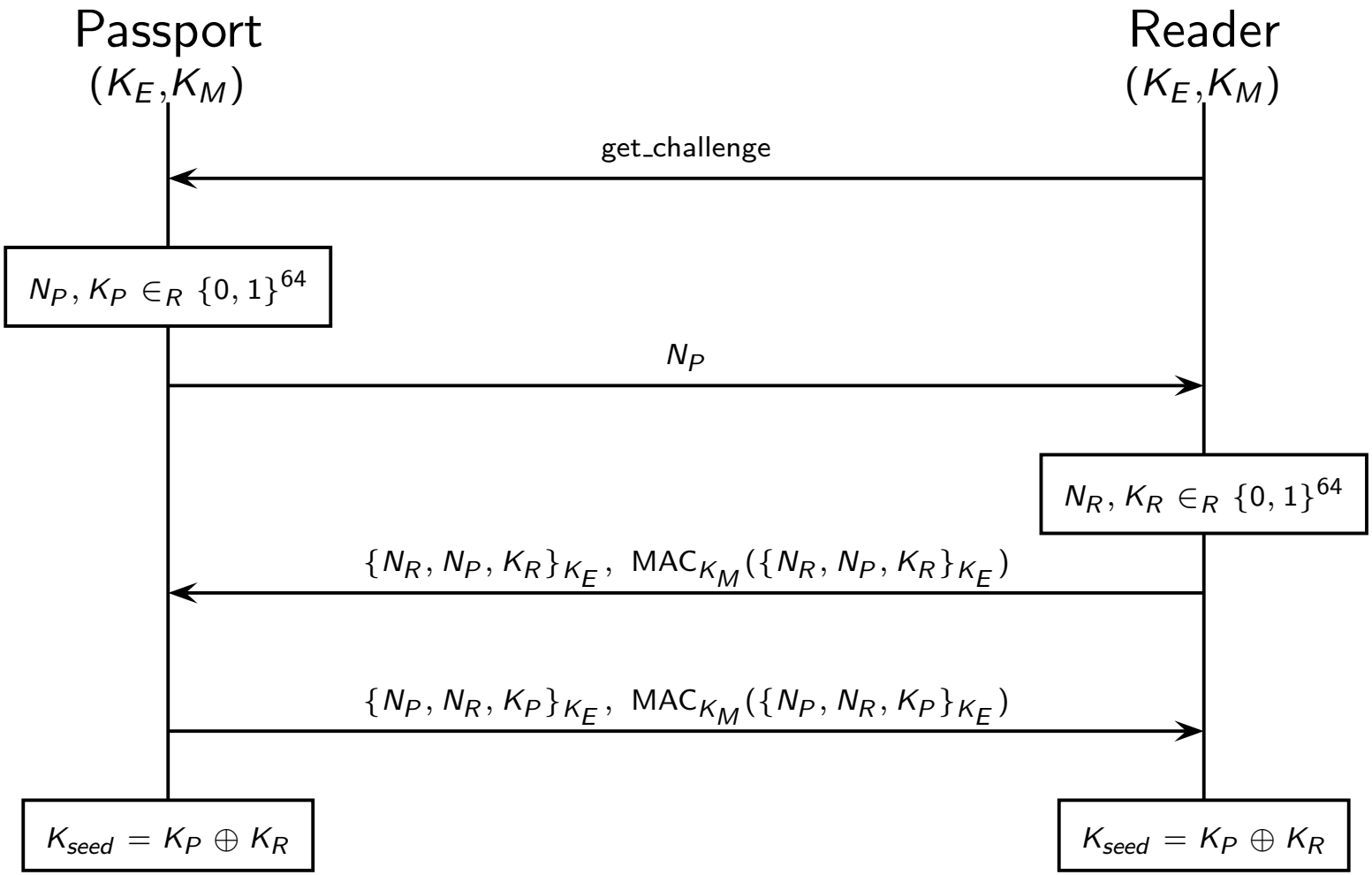
The Basic Access Control protocol (BAC)



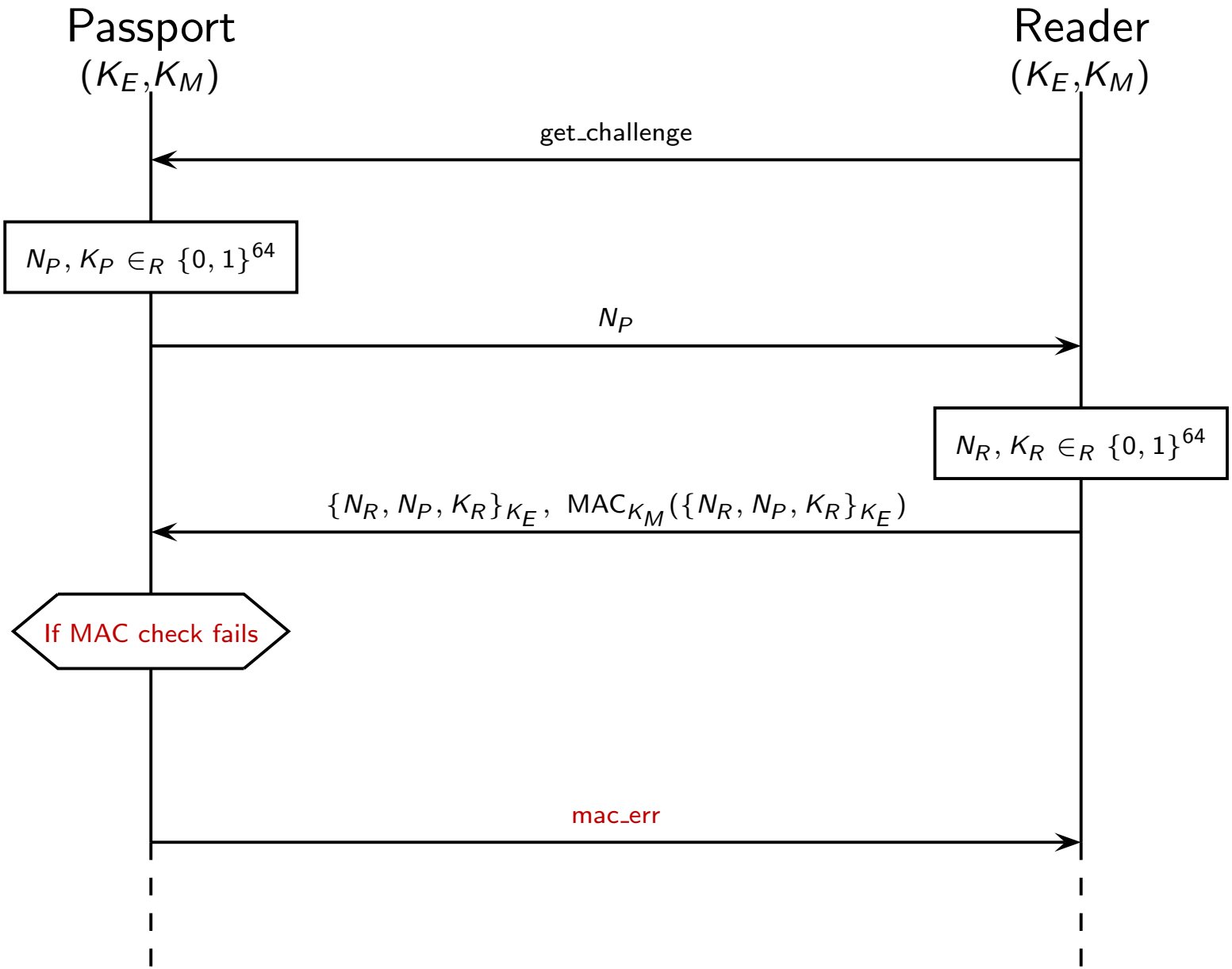
The Basic Access Control protocol (BAC)



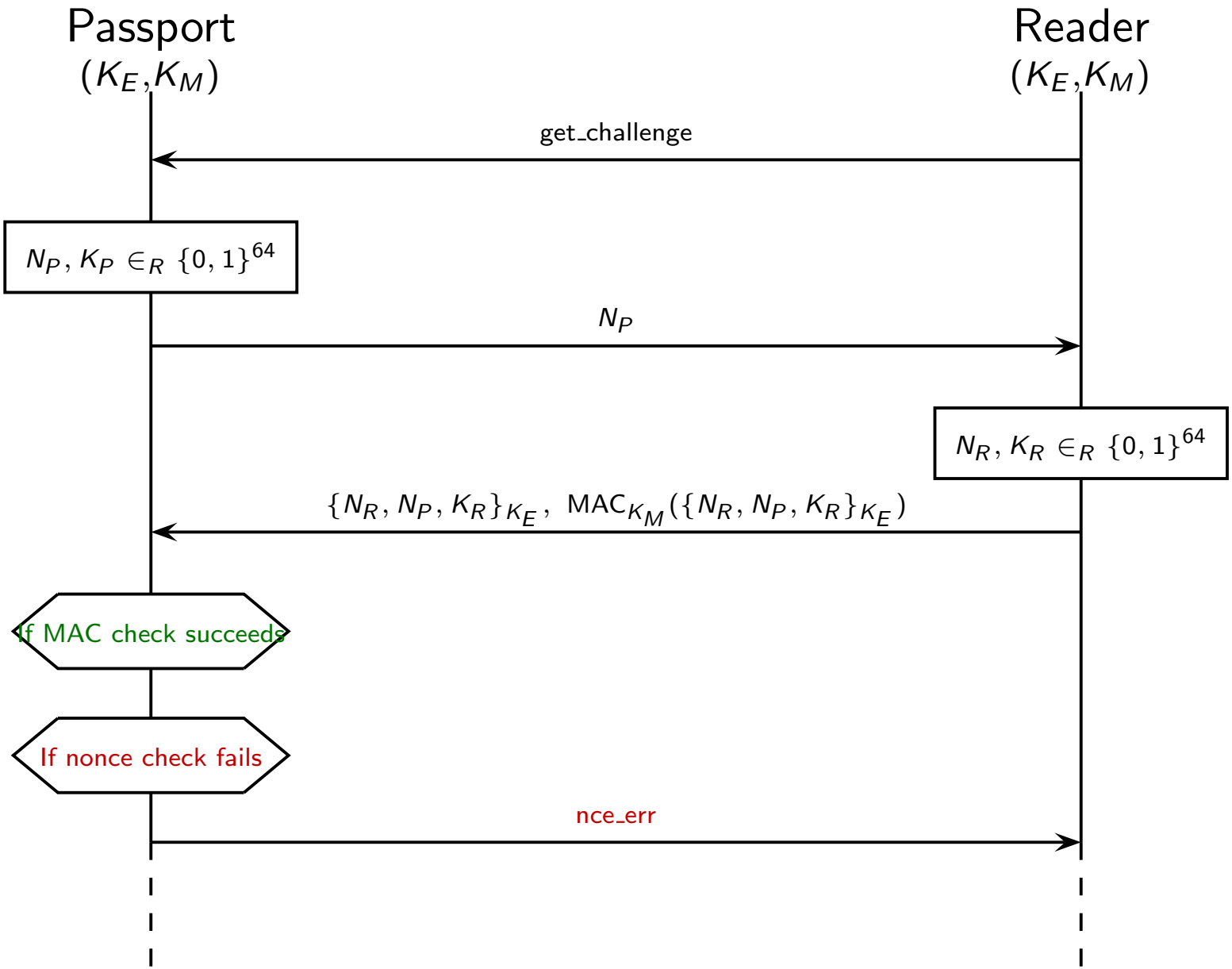
The Basic Access Control protocol (BAC)



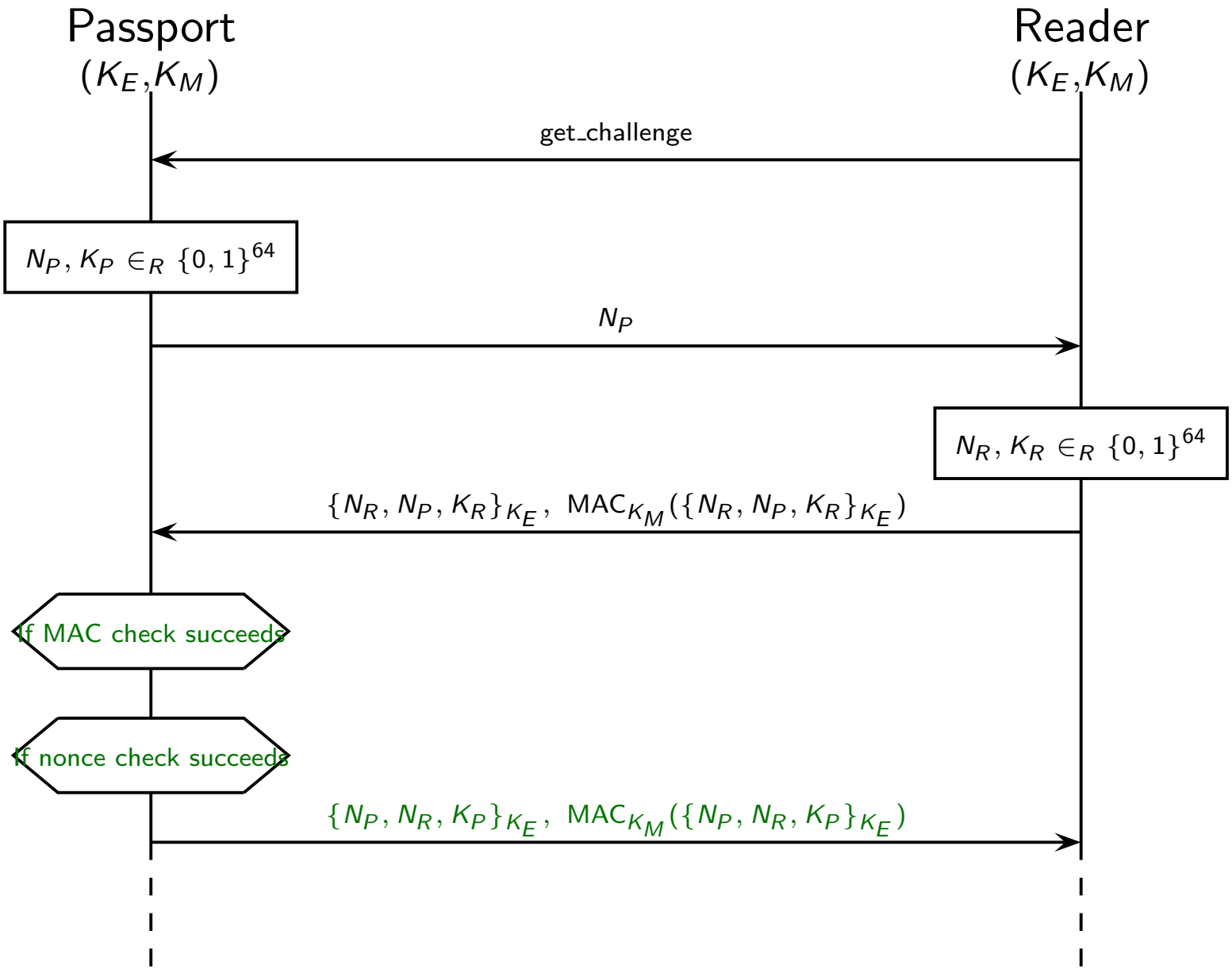
The passport must reply to all received messages



The passport must reply to all received messages



The passport must reply to all received messages



e-Passports and privacy

- The BAC protocol provides mutual authentication, key agreement, and confidentiality of subsequent communication
- e-Passports further aim at providing anonymity and unlinkability to their bearers

Definition (ISO 15408)

Anonymity ensures that a user may use of a resource or service without disclosing the user's identity.

Definition (ISO 15408)

Unlinkability ensures that a user may make multiple uses of a resource or service without other users being able to link these uses together.

Different implementations of the BAC protocol

The ICAO e-Passport standard doesn't specify what the error messages should be. Each nation has implemented its own version:

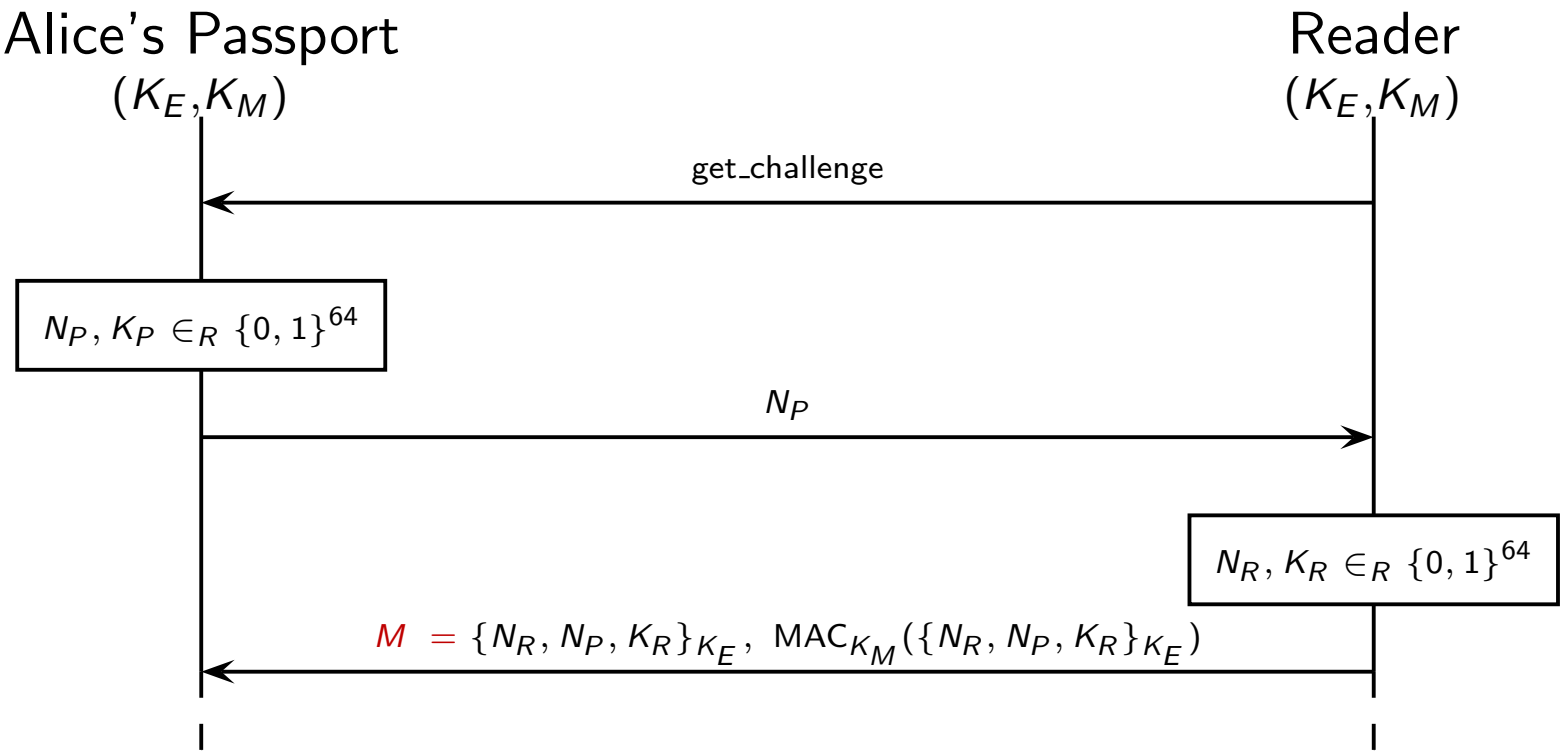
- French e-Passport: mac_err $\neq$ nce_err
  $\longrightarrow$ French implementation allows an attacker to **track a passport**, provided he has once witnessed a successful authentication.

- British e-Passport: mac_err $=$ nce_err
  $\longrightarrow$ The British version of the BAC protocol **satisfies unlinkability**.

[T. Chothia, V. Smirnov. "A traceability attack against e-Passports". 14th International Conference on Financial Cryptography and Data Security 2010.]

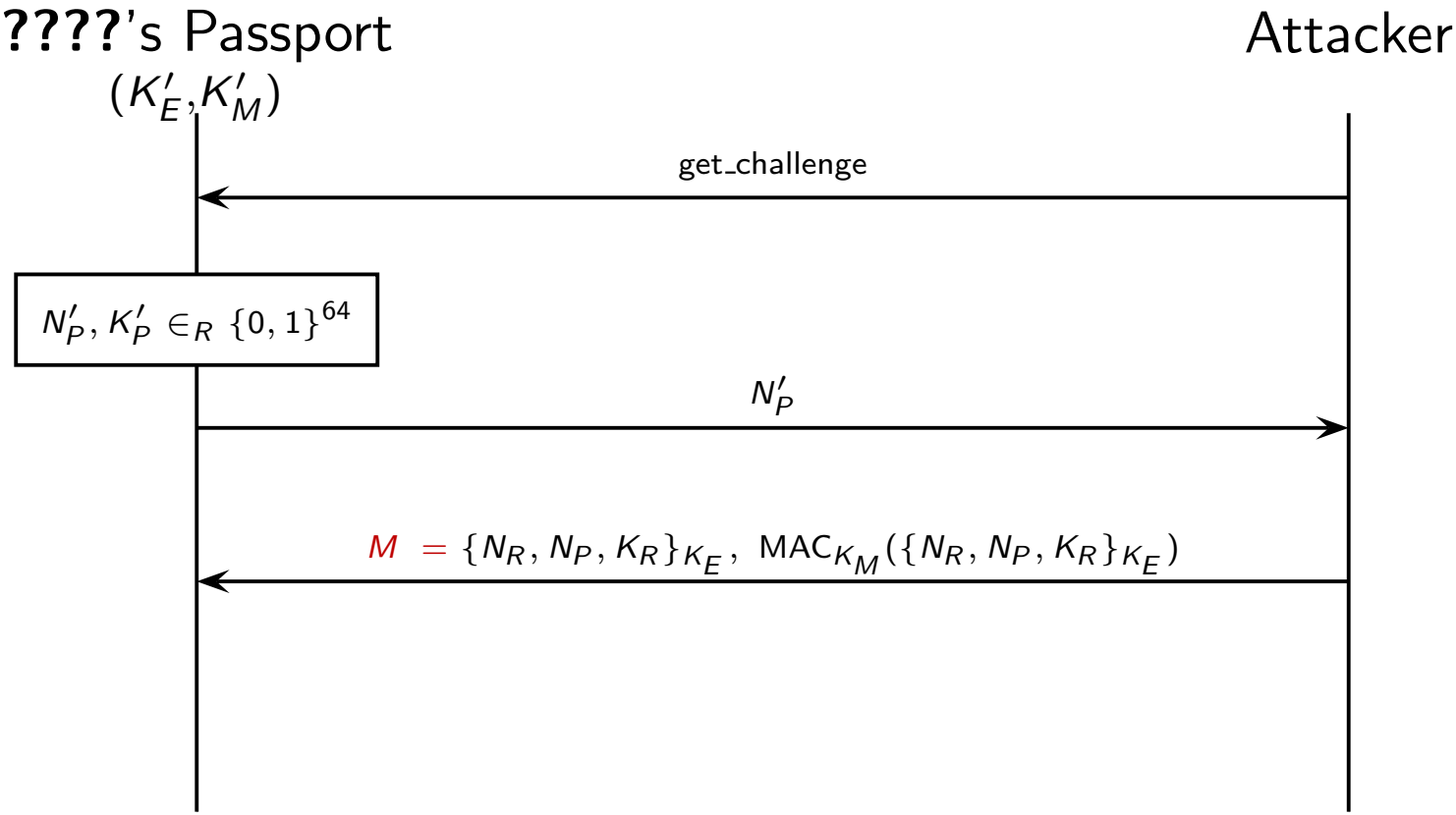
An attack on the French e-Passport (part 1)

The attacker eavesdrop on Alice using her passport

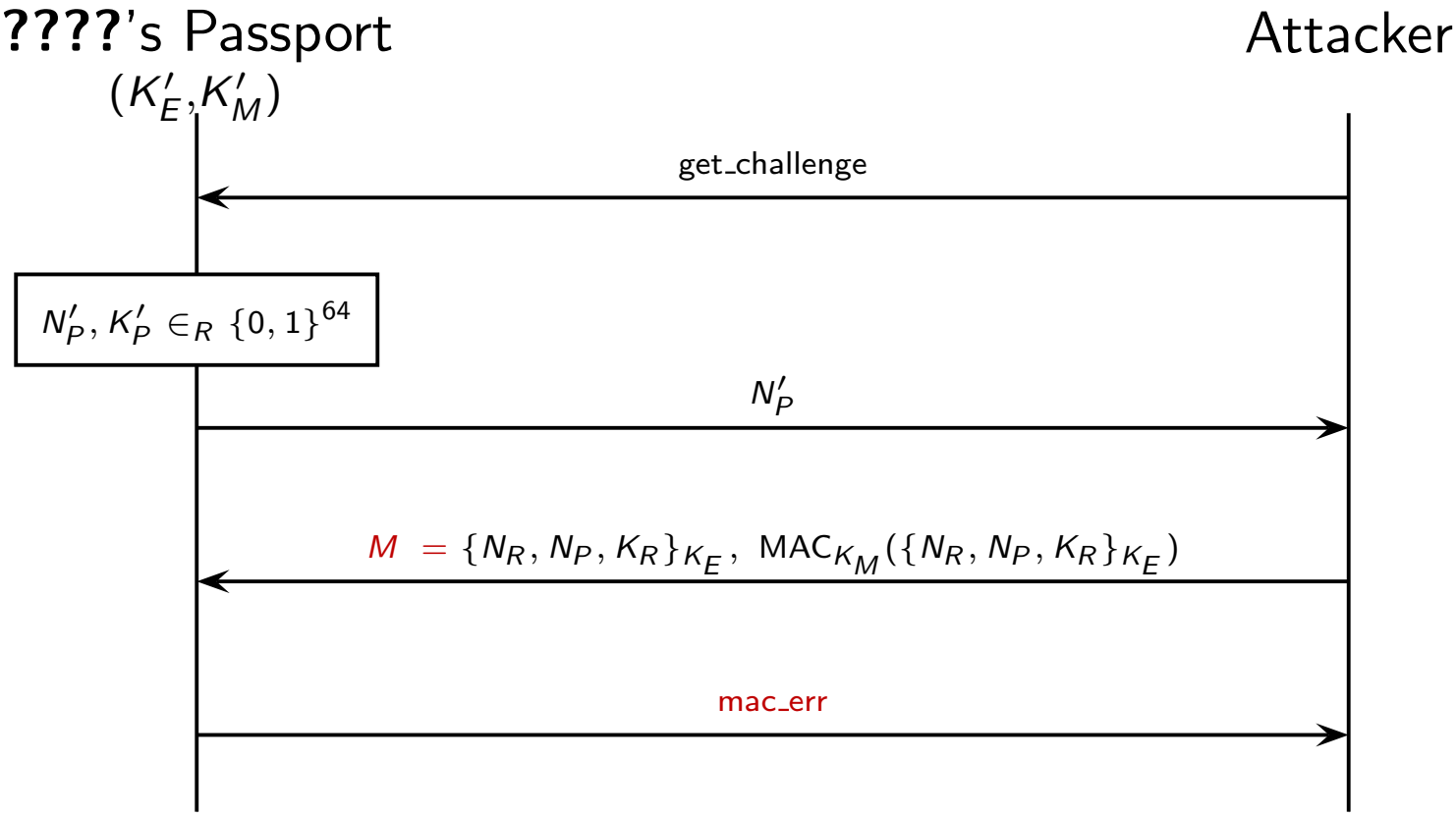


and records message M

An attack on the French e-Passport (part 2)

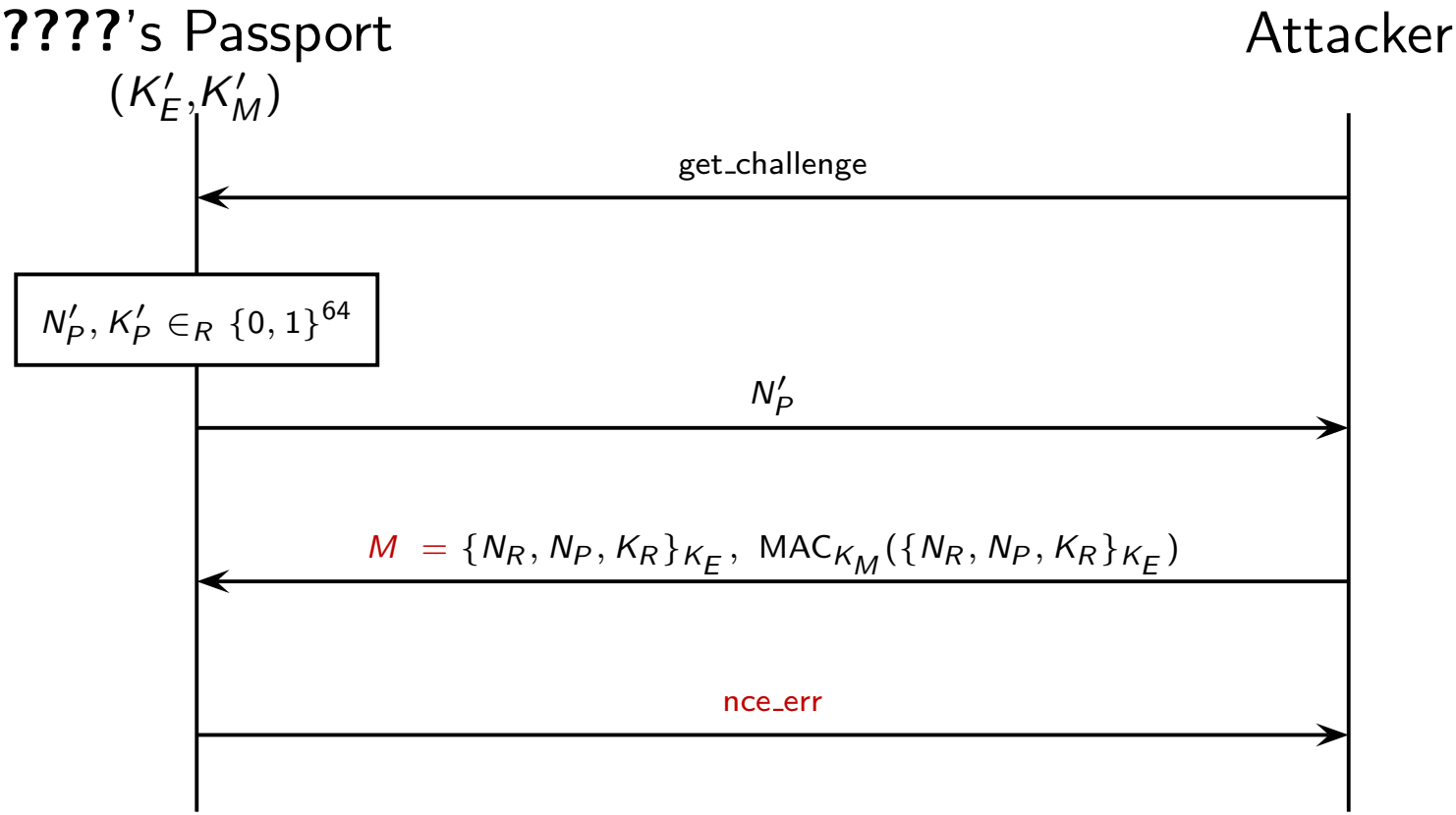


An attack on the French e-Passport (part 2)



$\Rightarrow$ MAC check failed $\Rightarrow$ $K'_M \neq K_M$ $\Rightarrow$ **????** is not Alice

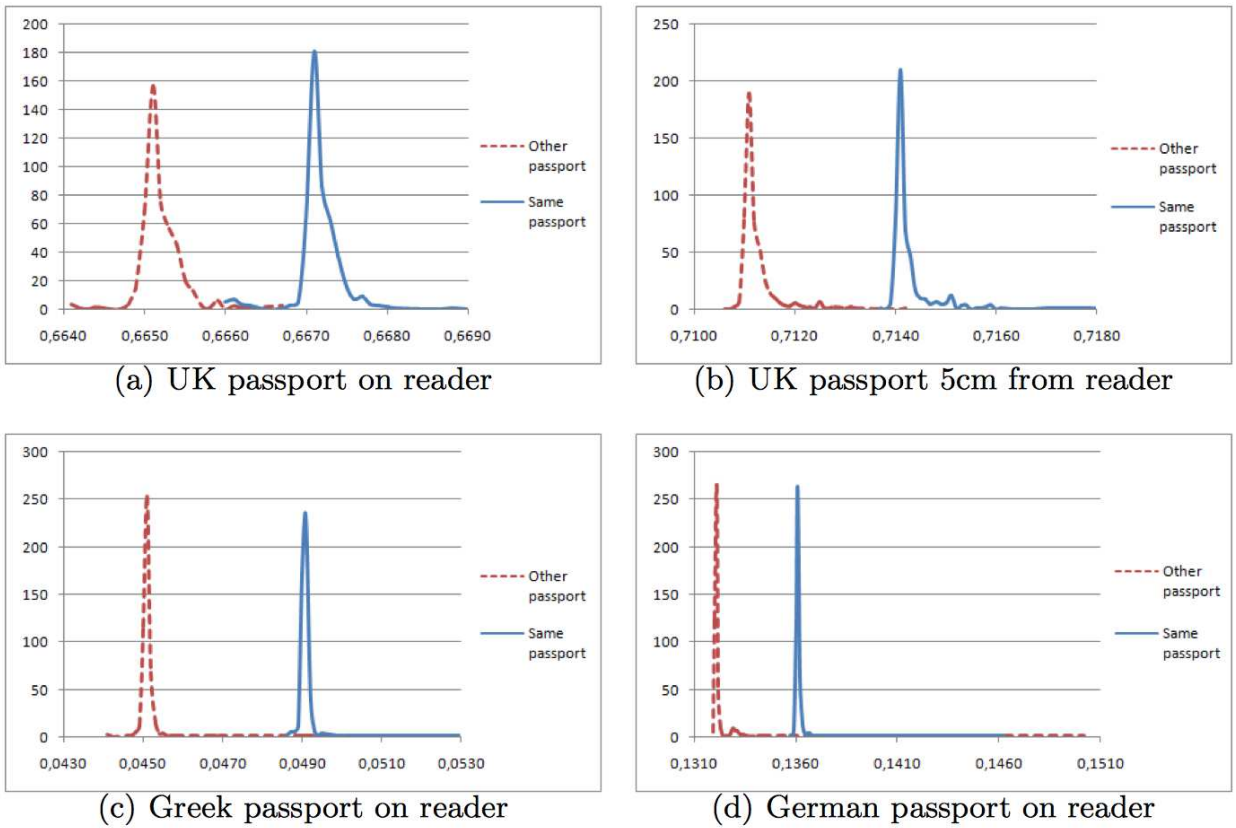
An attack on the French e-Passport (part 2)



$\Rightarrow$ MAC check succeeded $\Rightarrow$ $K'_M = K_M$ $\Rightarrow$ **????** is Alice

Timing attack: the failed MAC is rejected sooner

- UK, Greek, German passports return the same error in both situations, but still...



(a) UK passport on reader

(b) UK passport 5cm from reader

(c) Greek passport on reader

(d) German passport on reader

Fig. 4. Sampled Times from Replaying a Message to the Same or a Different Passport

[T. Chothia, V. Smirnov. "A traceability attack against e-Passports". 14th International Conference on Financial Cryptography and Data Security 2010.]