Operational Semantics of Security Protocols

Sjouke Mauw

joint work with Cas Cremers and Erik de Vink

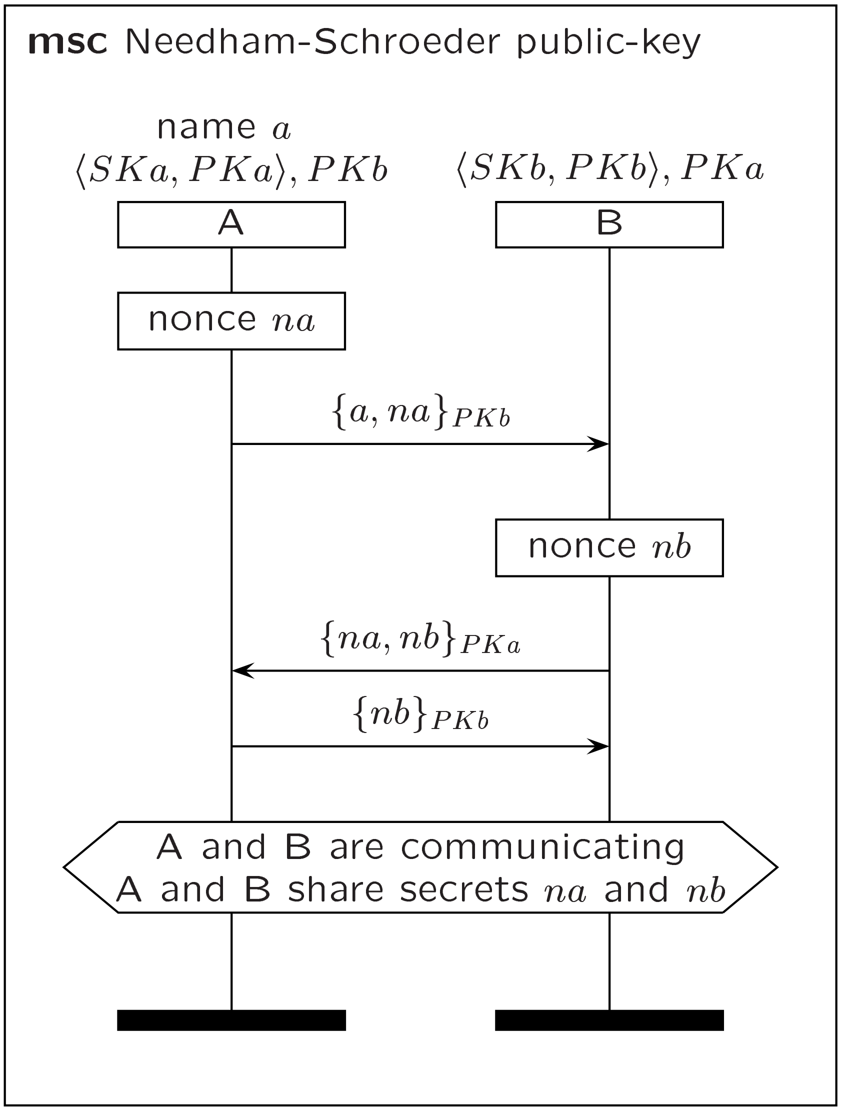
Eindhoven University of Technology
The Netherlands

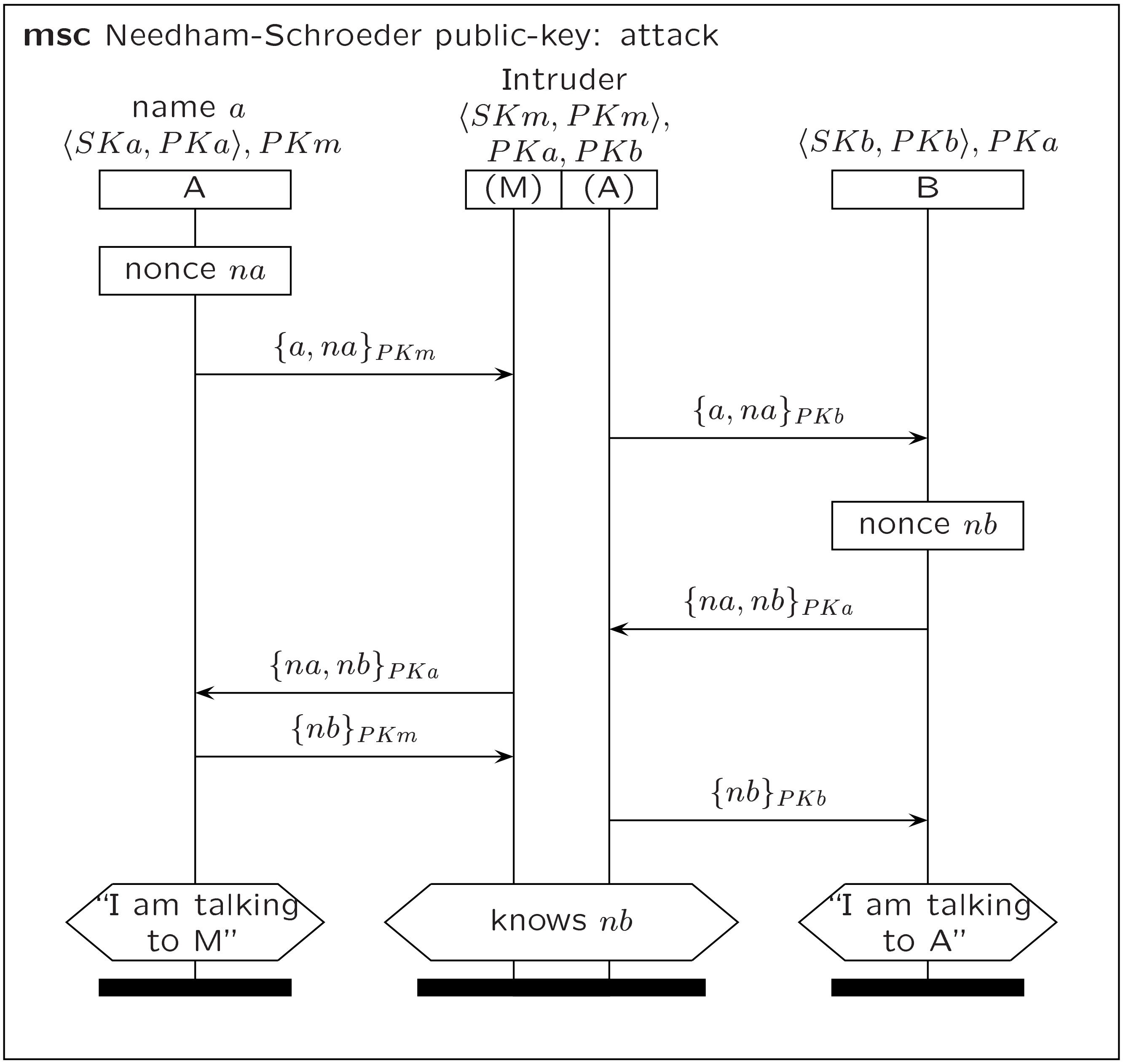
- Motivation.
- Black Box security protocols.
- Derivation rules.
- Some security properties.
- Conclusions and ongoing research.

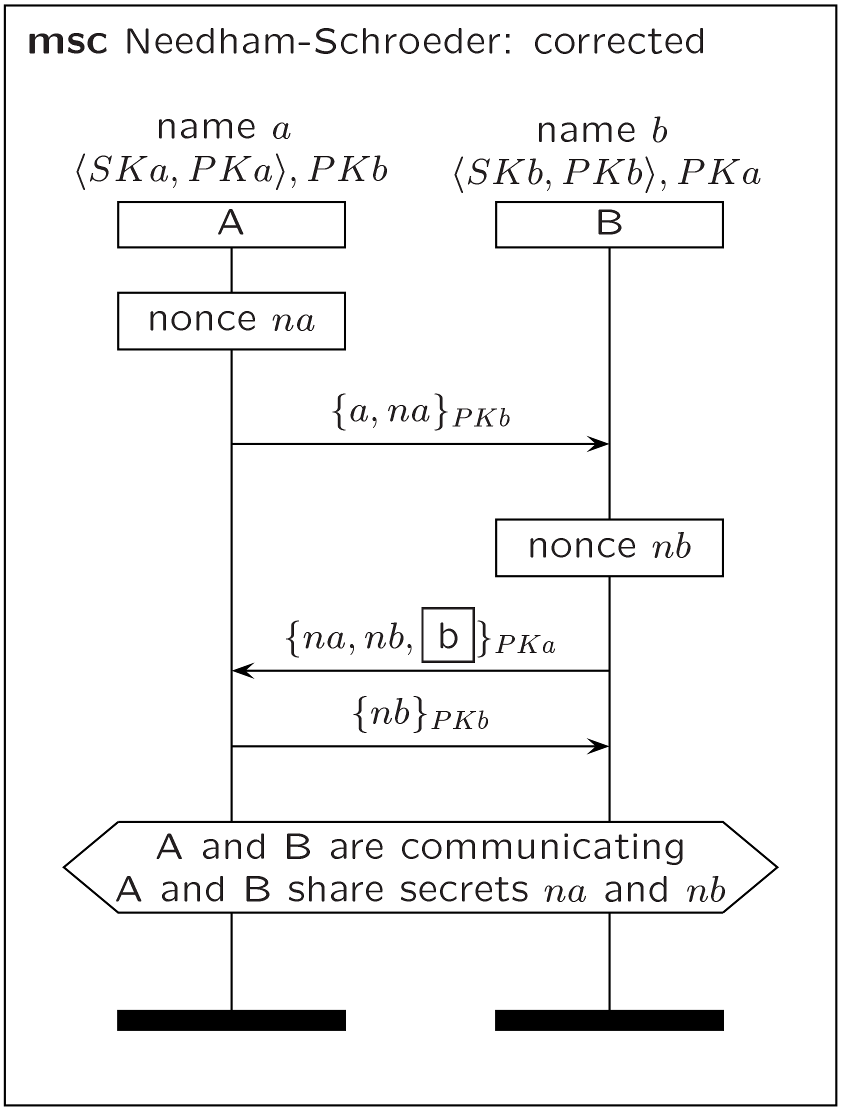
"Security protocols are three-line programs that people still manage to get wrong" (Roger Needham)

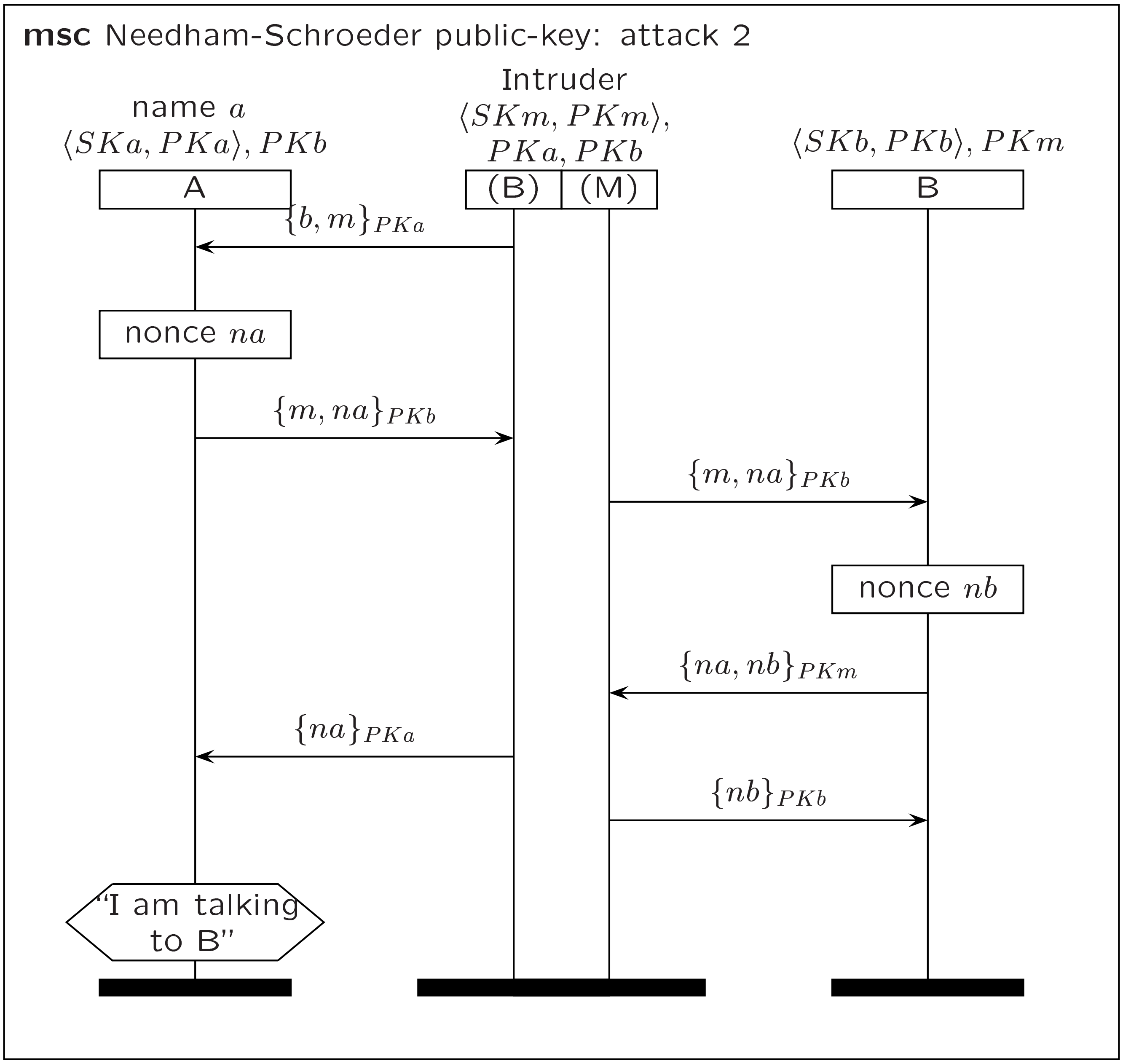
Security protocol = set of interaction rules to guarantee security property (plus some intended functionality).

Formal validation is imperative and feasible.


msc Needham-Schroeder public-key
name a
$\langle SKa, PKa\rangle, PKb$
$\langle SKb, PKb\rangle, PKa$
A
B
nonce na
$\{a, na\}_{PKb}$
nonce nb
$\{na, nb\}_{PKa}$
$\{nb\}_{PKb}$
A and B are communicating
A and B share secrets na and nb


msc Needham-Schroeder public-key: attack
name a
$\langle SKa, PKa\rangle, PKm$
Intruder
$\langle SKm, PKm\rangle,$
PKa, PKb
$\langle SKb, PKb\rangle, PKa$
A
(M)
(A)
B
nonce na
$\{a, na\}_{PKm}$
$\{a, na\}_{PKb}$
nonce nb
$\{na, nb\}_{PKa}$
$\{na, nb\}_{PKa}$
$\{nb\}_{PKm}$
$\{nb\}_{PKb}$
"I am talking to M"
knows nb
"I am talking to A"


msc Needham-Schroeder: corrected
name a
$\langle SKa, PKa\rangle, PKb$
A
name b
$\langle SKb, PKb\rangle, PKa$
B
nonce na
$\{a, na\}_{PKb}$
nonce nb
$\{na, nb, \boxed{\text{b}}\}_{PKa}$
$\{nb\}_{PKb}$
A and B are communicating
A and B share secrets na and nb


msc Needham-Schroeder public-key: attack 2
name a
$\langle SKa, PKa\rangle, PKb$
Intruder
$\langle SKm, PKm\rangle,$
PKa, PKb
$\langle SKb, PKb\rangle, PKm$
A
(B)
(M)
B
$\{b, m\}_{PKa}$
nonce na
$\{m, na\}_{PKb}$
$\{m, na\}_{PKb}$
nonce nb
$\{na, nb\}_{PKm}$
$\{na\}_{PKa}$
$\{nb\}_{PKb}$
"I am talking to B"

Protocol verification
vs.
Security Protocol verification

Extra structure:

- execution model,
- intruder model,
- selected security properties,
- closed world assumption.

Additional opinions sollicited!

- BAN logic,
- Casper/FDR,
- Strand spaces,
- etc.

All have their pro's and con's.

- Only isolated protocols (no protocol sets).
- No proper definition of security properties (confidentiality, authentication, non-repudiation, etc). And where proper, no consensus.
- Can only deal with single intruder model (Dolev-Yao).
- No type flaw attacks.
- No forward secrecy/backward security.
- Model checking is incomplete.
- Trade-off between precision and useability.

So: develop general formal framework.
(Yes, this is ambitious, I know!)

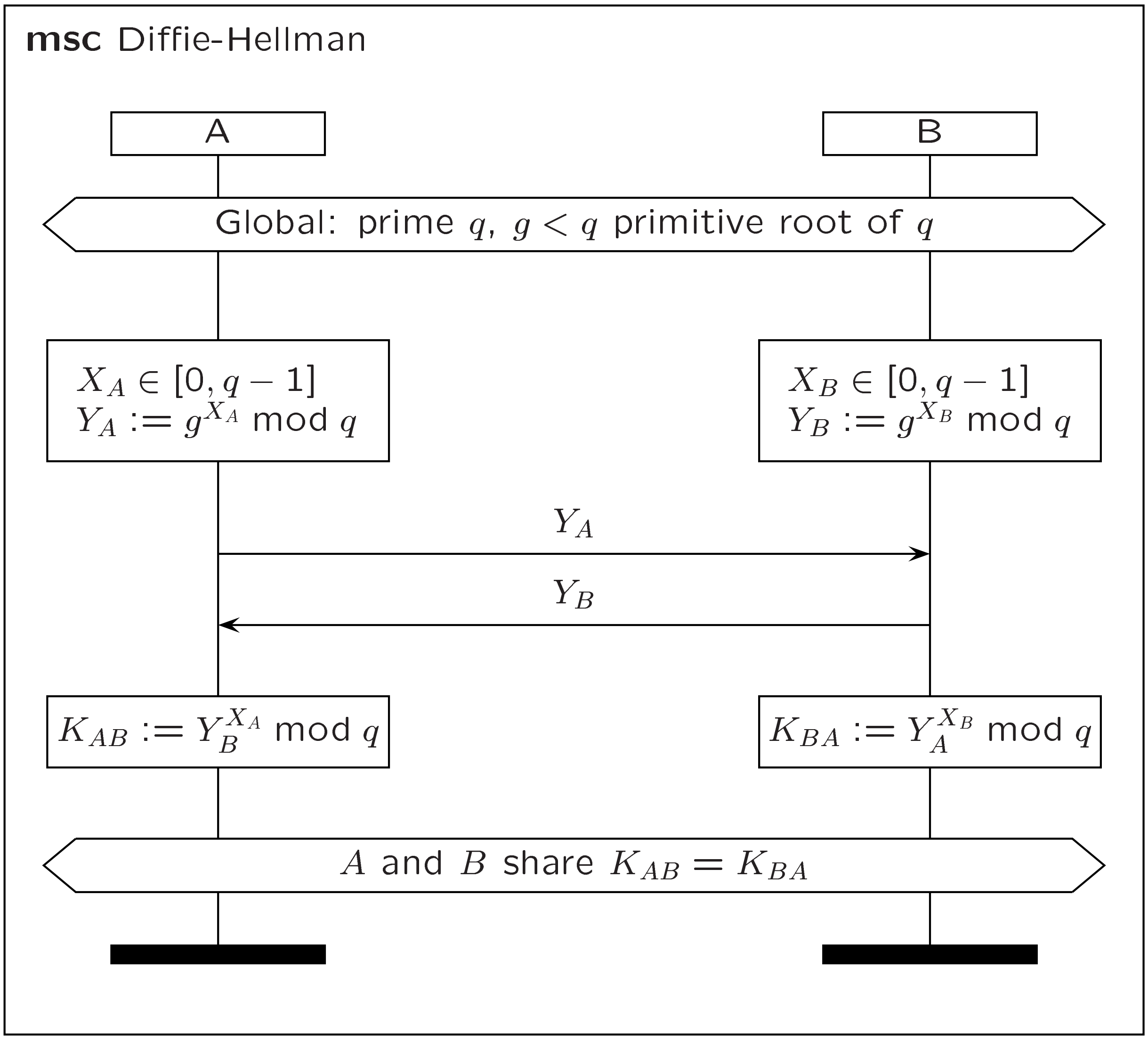
Develop a modular general operational semantics for security protocol sets having the required merits.

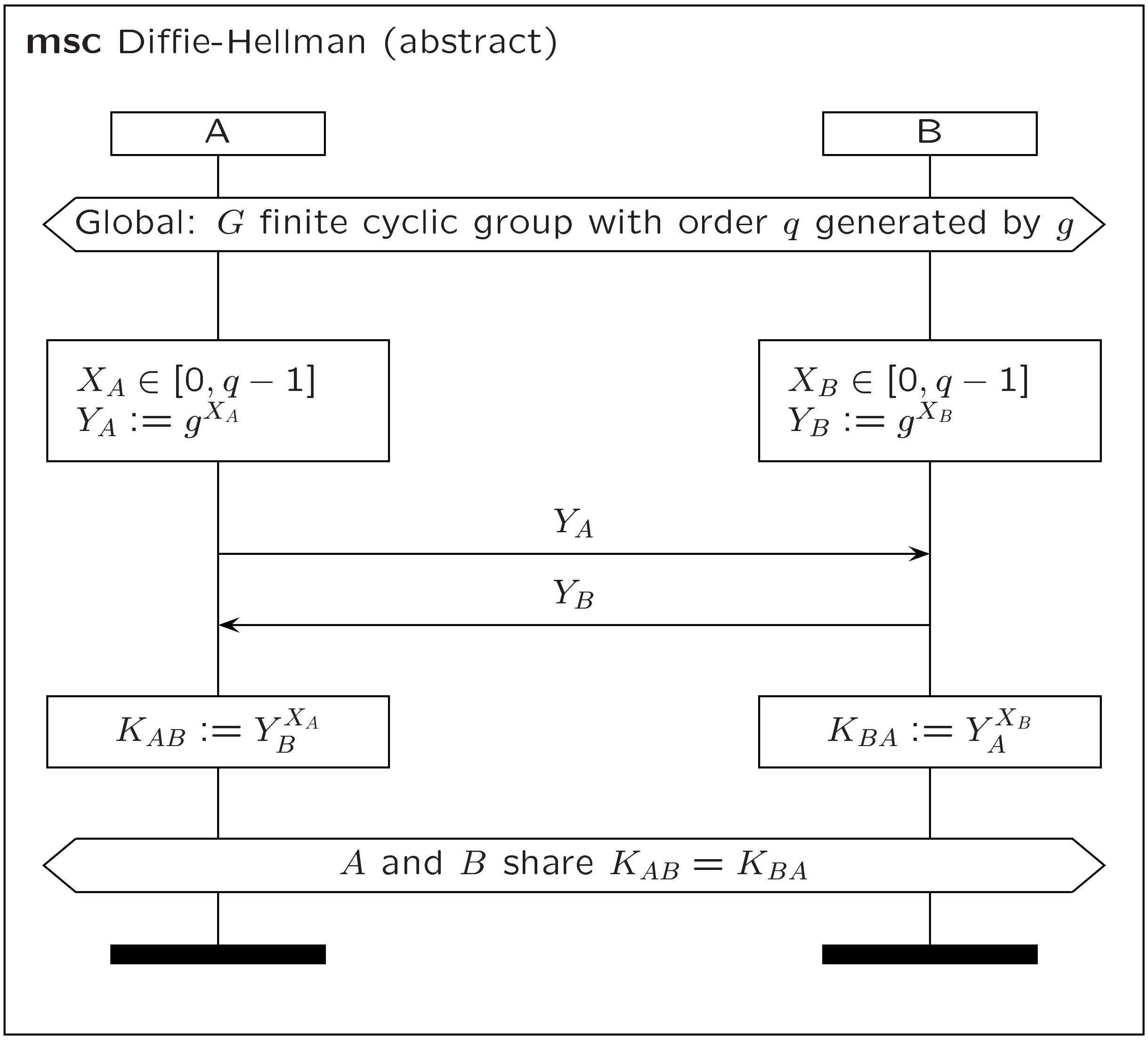
Assume underlying set of cryptographic primitives, from which we only know the relevant properties.

Example: $\{\{m\}_{PK}\}_{SK} = \{\{m\}_{SK}\}_{PK} = m$

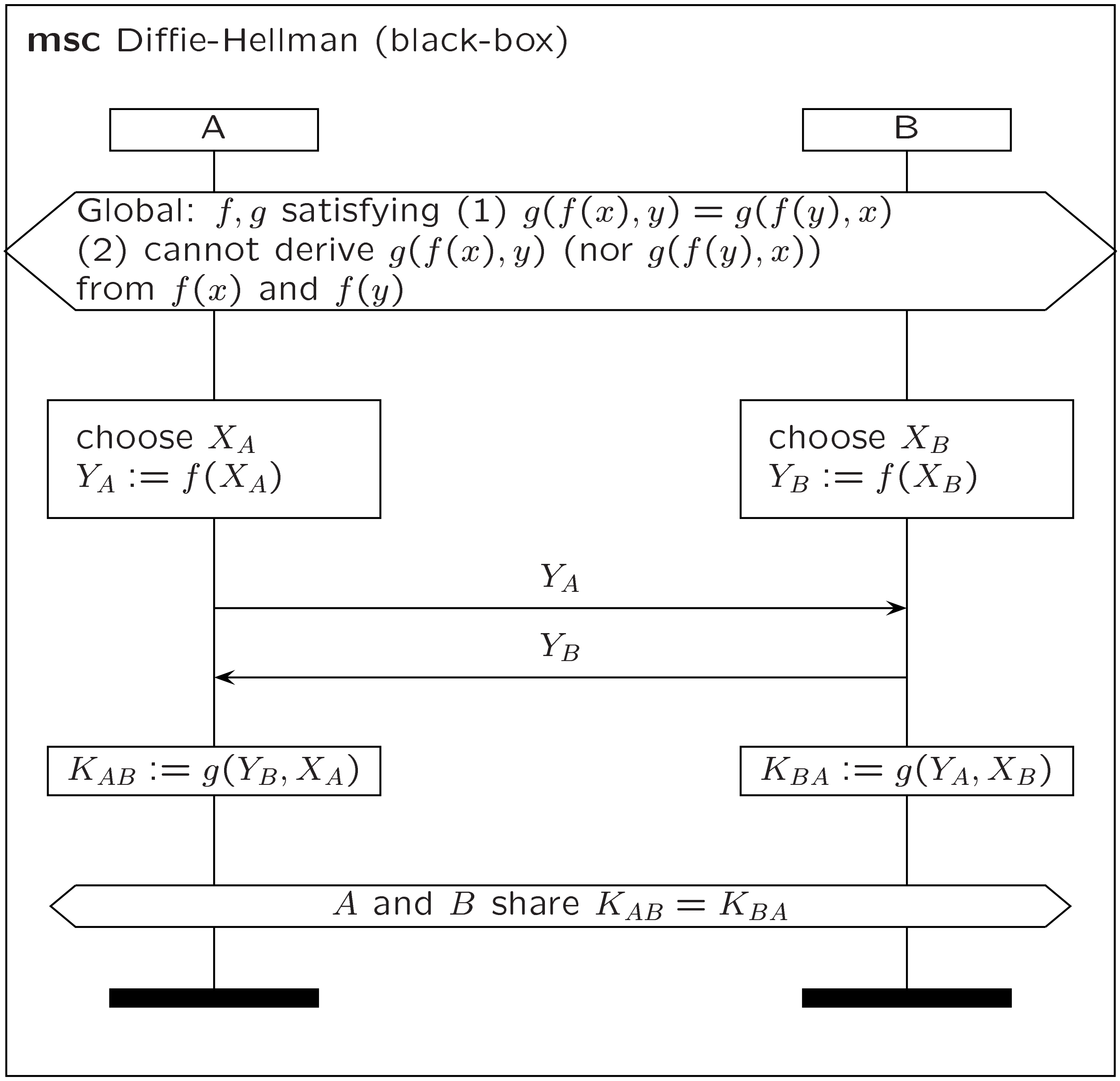
Advantages:

- Separation of concerns.
- Substitute any mathematical object satisfying the required properties.
- Develop protocols based on hypothetical primitives.


msc Diffie-Hellman
A
B
Global: prime q, $g < q$ primitive root of q
$X_A \in [0, q-1]$
$Y_A := g^{X_A} \bmod q$
$X_B \in [0, q-1]$
$Y_B := g^{X_B} \bmod q$
Y_A
Y_B
$K_{AB} := Y_B^{X_A} \bmod q$
$K_{BA} := Y_A^{X_B} \bmod q$
A and B share $K_{AB} = K_{BA}$



msc Diffie-Hellman (abstract)
A
B
Global: G finite cyclic group with order q generated by g
$X_A \in [0, q-1]$
$Y_A := g^{X_A}$
$X_B \in [0, q-1]$
$Y_B := g^{X_B}$
Y_A
Y_B
$K_{AB} := Y_B^{X_A}$
$K_{BA} := Y_A^{X_B}$
A and B share $K_{AB} = K_{BA}$


msc Diffie-Hellman (black-box)
A
B
Global: f, g satisfying (1) $g(f(x), y) = g(f(y), x)$
(2) cannot derive $g(f(x), y)$ (nor $g(f(y), x)$)
from $f(x)$ and $f(y)$
choose X_A
$Y_A := f(X_A)$
choose X_B
$Y_B := f(X_B)$
Y_A
Y_B
$K_{AB} := g(Y_B, X_A)$
$K_{BA} := g(Y_A, X_B)$
A and B share $K_{AB} = K_{BA}$

- Set of States S.
- Set of Events E.
- Transition relation $s \xrightarrow{e} s'$
  Determine for every state $s \in S$ all possible executable events $e \in E$ and the resulting state $s' \in S$.
- Gives set of traces (or graph):
  $s_0 \xrightarrow{e_0} s_1 \xrightarrow{e_1} s_2 \xrightarrow{e_2} \ldots$
- Defined by derivation rules $\frac{Hypothesis}{s \xrightarrow{e} s'}$

create$(a, initiator(a, m)) \circ$

create$(b, responder(a, b)) \circ$

nonce$(a, na) \circ$

$s(a, m, \{a, na\}_{PKm}) \circ$

deflect$(s(a, m, \{a, na\}_{PKm})) \circ$

inject$(s(a, b, \{a, na\}_{PKb})) \circ$

$r(a, b, \{a, na\}_{PKb}) \circ$

nonce$(b, nb) \circ$

$s(b, a, \{na, nb\}_{PKa}) \circ$

deflect$(s(b, a, \{na, nb\}_{PKa})) \circ$

inject$(s(m, a, \{na, nb\}_{PKa})) \circ$

$r(m, a, \{na, nb\}_{PKa}) \circ$

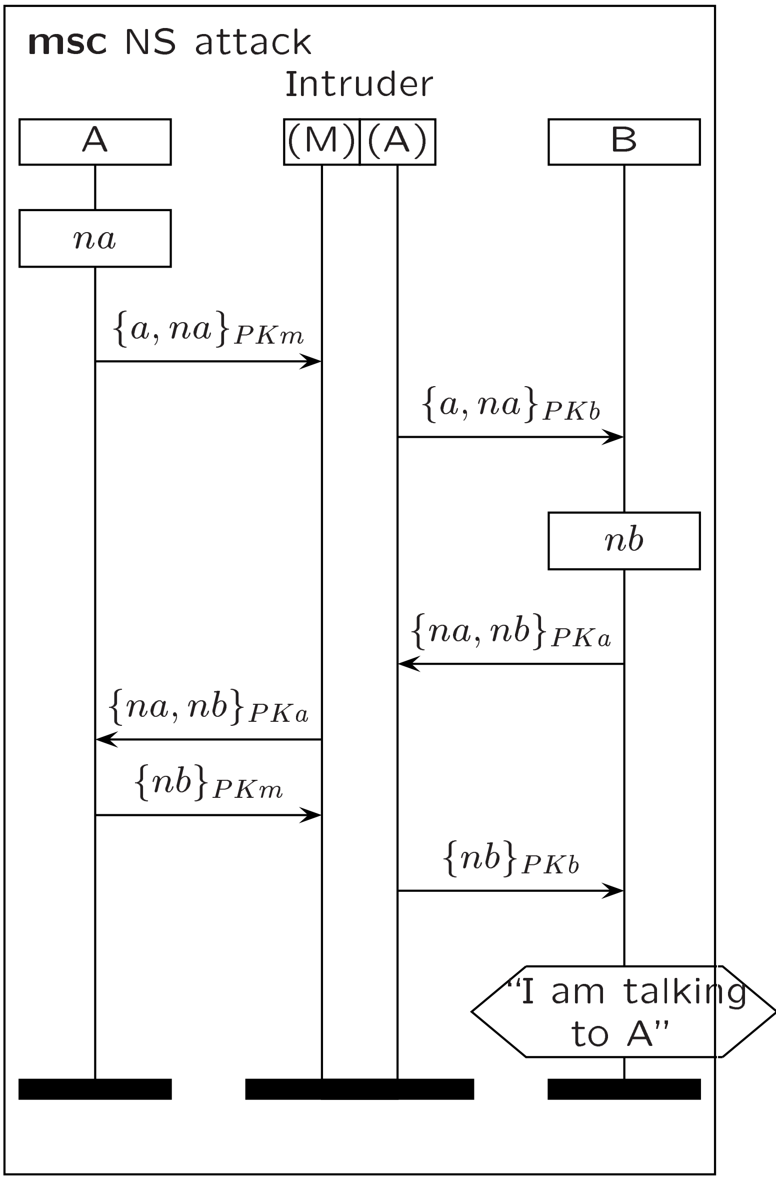
$s(a, m, \{nb\}_{PKm}) \circ$

deflect$(s(a, m, \{nb\}_{PKm})) \circ$

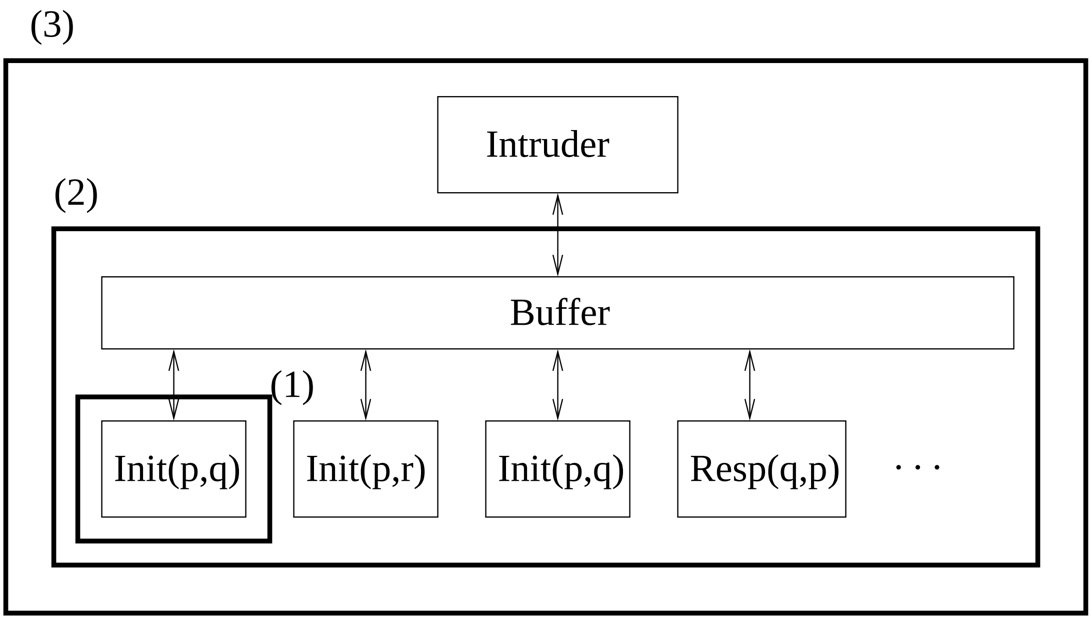
inject$(s(a, b, \{nb\}_{PKb})) \circ$

$r(a, b, \{nb\}_{PKb}) \circ$

$claim(auth, b, a)$



1. One agent executing protocol role: $\rightsquigarrow$
2. Network of agents: $\cdots\!\rightarrow$
3. Network of agents plus intruder: $\rightarrow$



- $Act = \{s(x,y,m), r(x,y,m), nonce(x,nx), claim(prop,x,y)\}$
- State: $\Sigma^{run} = Act^*$
- Initial state: full role description form $RoleDef$.
- Events: $E^{run} = Act$
- Transitions: $\alpha \circ t \stackrel{\alpha}{\rightsquigarrow} t$

Example:

$$nonce(a,na) \circ s(a,b,\{a,na\}_{PKb}) \circ \ldots$$

$$\stackrel{nonce(a,na)}{\rightsquigarrow}$$

$$s(a,b,\{a,na\}_{PKb}) \circ \ldots$$

- Buffer: $\mathbb{B} = \mathcal{M}(\{s(x, y, m)\})$
- Run identifiers: $RunId$
- Runs: $\mathbb{F} = RunId \rightarrow \Sigma^{\mathsf{run}}$ (partial)
- State: $\Sigma^{\mathsf{network}} = \mathbb{B} \times \mathbb{F}$
- Initial state: $\sigma_0^{network} = \emptyset \times \emptyset$
- Events: $E^{\mathsf{network}} = \mathsf{Act} \setminus \{nonce(x, nx)\} \cup \{nonce(x, nx\sharp rid)\}$

$$\frac{t \overset{s(a,b,m)}{\rightsquigarrow} t', (rid, t) \in F}{\langle B, F\rangle \overset{s(a,b,m)}{\cdots\!\longrightarrow} \langle B \cup \{s(a,b,m)\}, F[rid := t']\rangle}$$

$$\frac{t \overset{r(a,b,m)}{\rightsquigarrow} t', (rid, t) \in F, s(a,b,m) \in B}{\langle B, F\rangle \overset{r(a,b,m)}{\cdots\!\longrightarrow} \langle B \setminus \{s(a,b,m)\}, F[rid := t']\rangle}$$

$$\frac{t \in \mathsf{RoleDef}, rid \notin runids(F)}{\langle B, F\rangle \overset{\mathsf{create}}{\cdots\!\longrightarrow} \langle B, F \cup (rid, t)\rangle}$$

$$\frac{t \overset{nonce(a,N)}{\rightsquigarrow} t', (rid, t) \in F}{\langle B, F\rangle \overset{nonce(a,N\sharp rid)}{\cdots\!\longrightarrow} \langle B, F[rid := t'[N\sharp rid/N]]\rangle}$$

- Intruder knowledge: $K =$ set of terms.
- Closedness: if $d_1, d_2, \ldots d_n \in K$ then also $f(d_1, d_2, \ldots d_n) \in K$ (for appropriately typed selected functions f).
- $K + d$ means closure of $K \cup \{d\}$

Example: If $\{m\}_{PK} \in K$ and $SK \in K$ then $\{\{m\}_{PK}\}_{SK} = m \in K$

- State: $\Sigma^{inetw} = K \times \Sigma^{network}$
- Initial state: $K_0 \times \sigma_0^{network}$, where K_0 is the initial knowledge of the intruder

$$\frac{S \stackrel{\alpha}{\cdots\longrightarrow} S'}{\langle K, S\rangle \xrightarrow{\alpha} \langle K, S'\rangle}$$

$$\frac{S \stackrel{s(a,b,m)}{\cdots\longrightarrow} S'}{\langle K, S\rangle \xrightarrow{s(a,b,m)} \langle K + m, S'\rangle}$$

$$\frac{s(a,b,m) \in B}{\langle K, \langle B, F\rangle\rangle \xrightarrow{\textit{deflect}} \langle K, \langle B \setminus \{s(a,b,m)\}, F\rangle\rangle}$$

$$\frac{a, b, m \in K}{\langle K, \langle B, F\rangle\rangle \xrightarrow{\textit{inject}} \langle K, \langle B \cup \{s(a,b,m)\}, F\rangle\rangle}$$

$$\frac{m' \in K, s(a,b,m) \in B}{\langle K, \langle B, F\rangle\rangle \xrightarrow{\textit{modify}} \langle K, \langle (B \setminus \{s(a,b,m)\}) \cup \{s(a,b,m')\}, F\rangle\rangle}$$

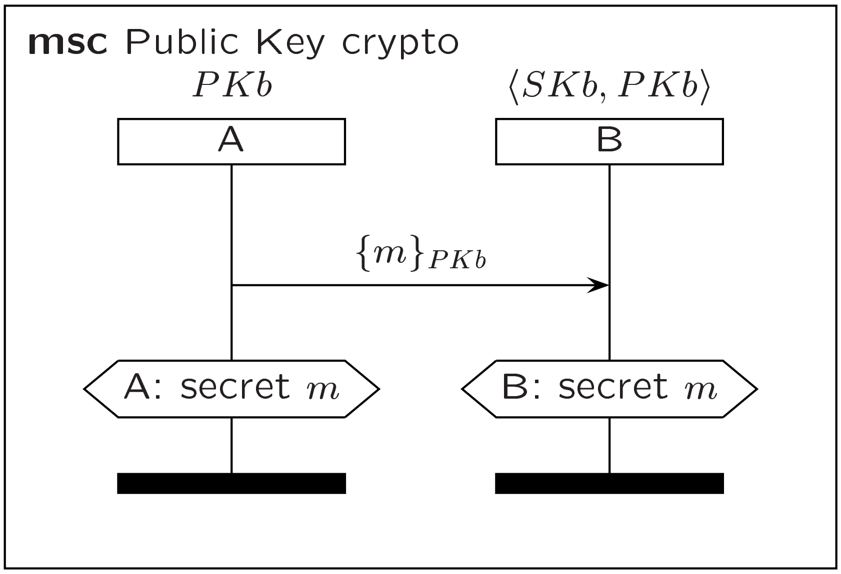
$$\frac{s(a,b,m) \in B,\ p,q \in K}{\langle K, \langle B, F\rangle\rangle \xrightarrow{\textit{reroute}} \langle K, \langle (B \setminus \{s(a,b,m)\}) \cup \{s(p,q,m)\}, F\rangle\rangle}$$

$$\frac{s(a,b,m) \in B}{\langle K, \langle B, F\rangle\rangle \xrightarrow{\textit{duplicate}} \langle K, \langle B \cup \{s(a,b,m)\}, F\rangle\rangle}$$

- Confidentiality.
- Authentication
- Non-repudiation.
- Anonymity.
- Etc.

For all traces of protocol p, if a term t is claimed to be secret, the intruder will never learn (deduce) this term.

$\forall_{\alpha \in Traces(p)}$ if $\alpha_i = \textit{secret}(a,t)$ then $\forall_{j>i} t \notin K_j$



Proof of A's claim (sketch):

1. $\forall_j SKb \notin K_j$.
2. Inspection of derivation rules learns that K is only extended with $\{m\}_{PKb}$.

Proof of B's claim:

For instance: aliveness. If A reaches the claim that B has been alive, then B has once sent a message.

$\forall_{\alpha \in Traces(p)}$ if $\alpha_i = alive(a, b)$ then
$\exists_{j<i} \alpha_j = s(b, x, m)$

Stronger forms of authentication: await upcoming research note.

- Extending/finishing/simplifying the model
  - type flaw attacks
  - forward secrecy
  - several forms of authentication
  - other security claims
- Relation to other approaches
  (strand spaces, Casper/FDR, BAN logic)
- Case studies
  (experimenting with intruder models, protocol sets)
- Tool support
  - model checker
  - proof assistent

- Preliminary results are encouraging.
- Modular and general.
- Framework for proving
  - correctness of security protocols,
  - theoretical properties.
- Better formal basis than the methods mentioned earlier.