

Key-Exchange Protocols in Strand Spaces

Joshua D Guttman

Jonathan C. Herzog F. Javier Thayer

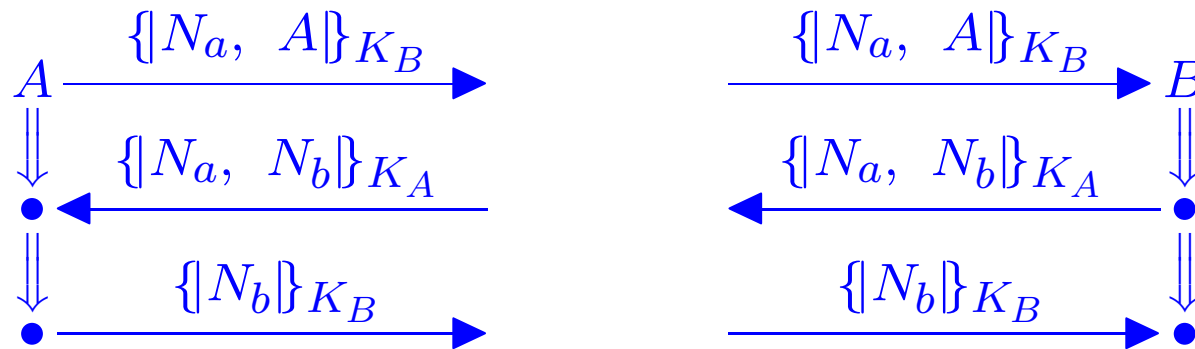
The MITRE Corporation

guttman@mitre.org

<http://www.ccs.neu.edu/home/guttman>

Thanks to support from: National Security Agency
MITRE-Sponsored Research

Needham-Schroeder



K_A, K_B

Public (asymmetric) keys of A, B

N_a, N_b

Nonces, one-time random bitstrings

$\{t\}_K$

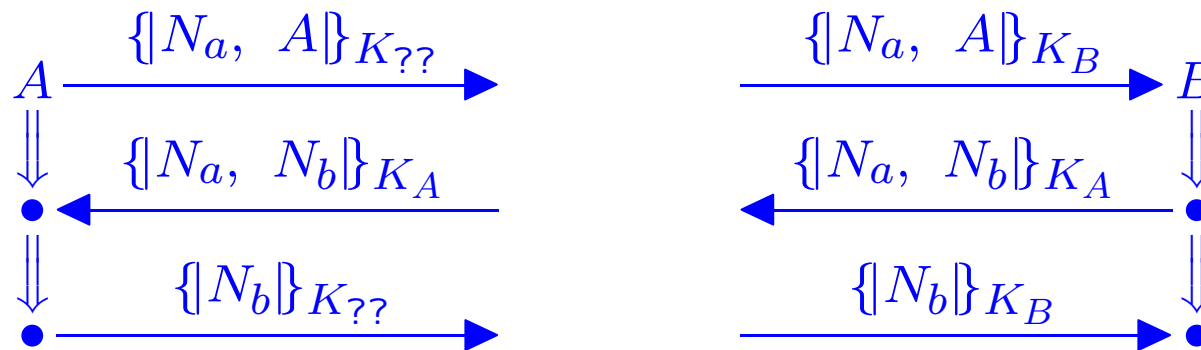
Encryption of t with K

$N_a \oplus N_b$

New shared secret

Needham-Schroeder: How does it work?

Assume A 's private key K_A^{-1} uncompromised



K_A, K_B

Public (asymmetric) keys of A, B

N_a, N_b

Nonces, one-time random bitstrings

$\{t\}_K$

Encryption of t with K

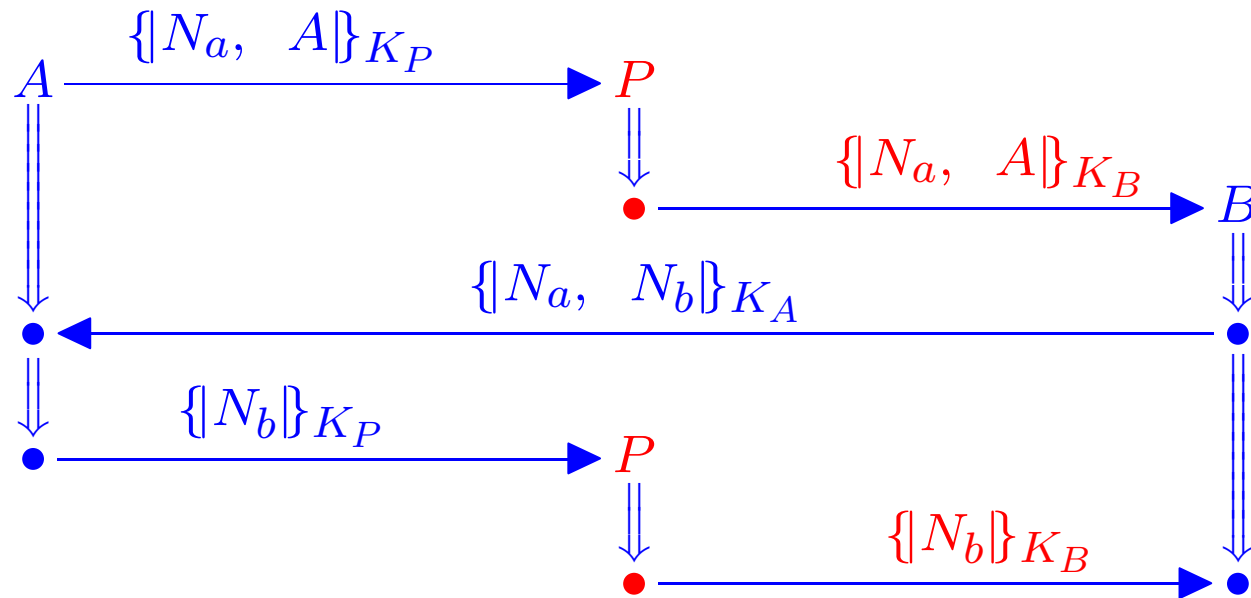
$N_a \oplus N_b$

New shared secret

Whoops

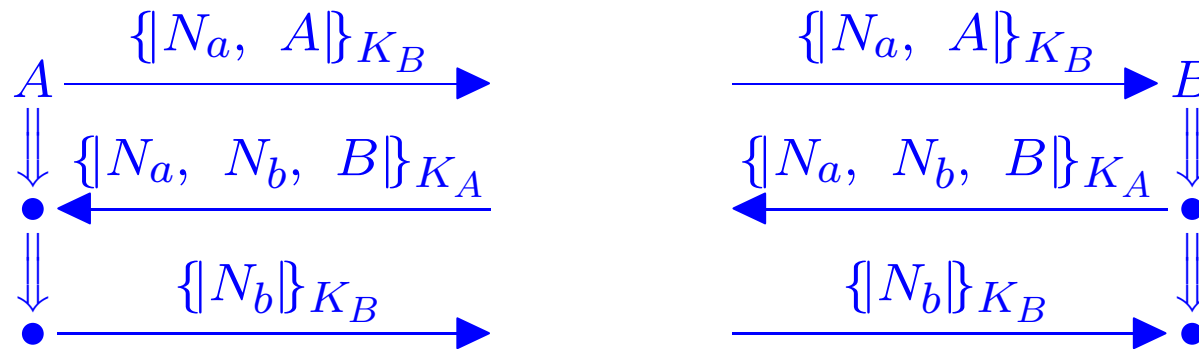
Needham-Schroeder Failure

If $?? = P$,



(Gavin Lowe)

Needham-Schroeder-Lowe



K_A, K_B

N_a, N_b

$\{t\}_K$

$N_a \oplus N_b$

Public (asymmetric) keys of A, B

Nonces, one-time random bitstrings

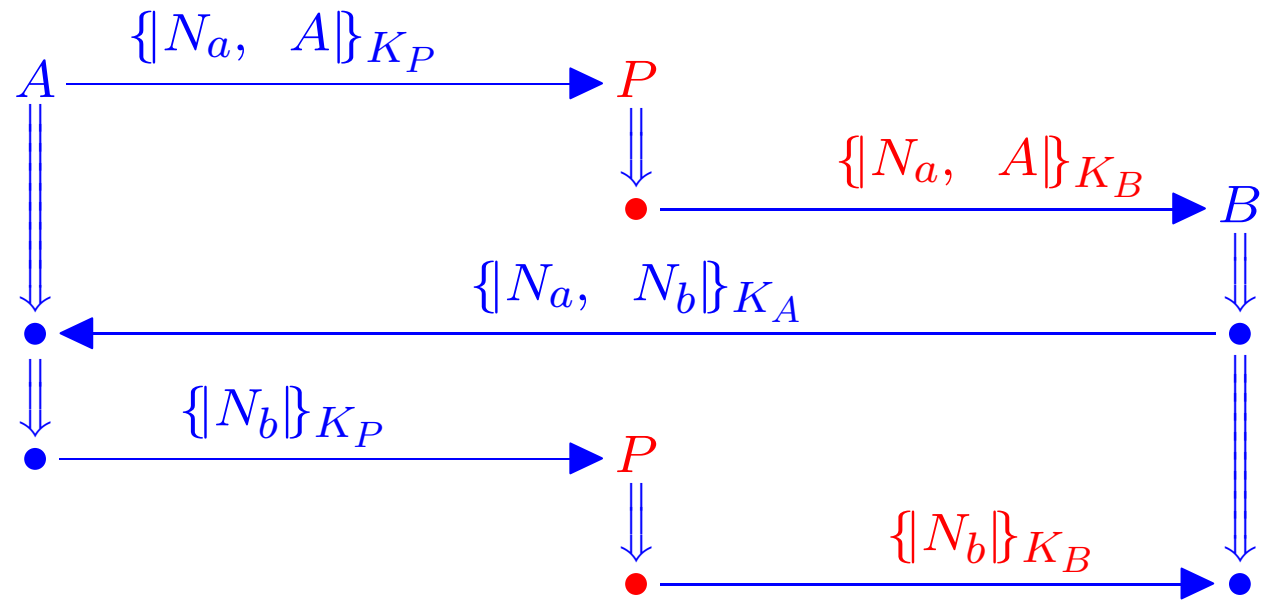
Encryption of t with K

New shared secret

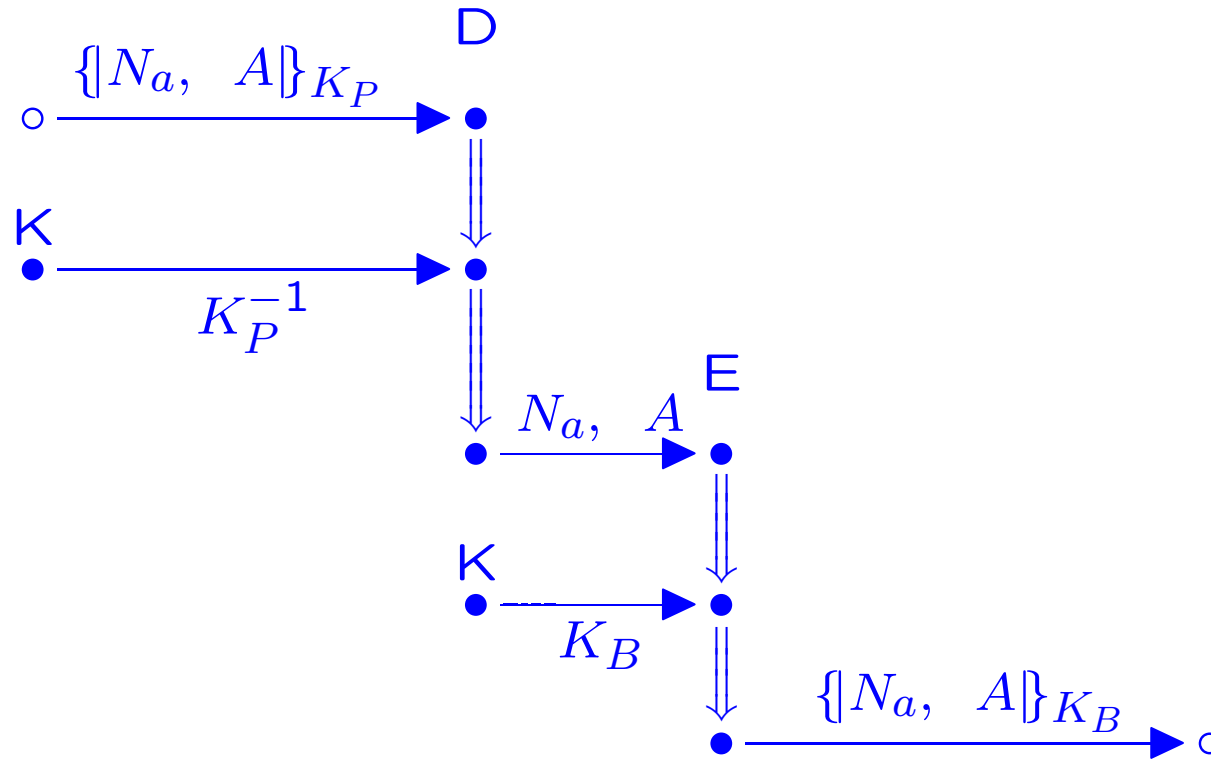
Protocol Executions are Bundles

- Send, receive events on strands called “nodes”
 - Positive for send
 - Negative for receive
- Bundle \mathcal{B} : Finite graph of nodes and edges representing causally well-founded execution; Edges are arrows \rightarrow, \Rightarrow
 - For every reception $-t$ in \mathcal{B} , there’s a unique transmission $+t$ where $+t \rightarrow -t$
 - When nodes $n_i \Rightarrow n_{i+1}$ on same strand, if n_{i+1} in \mathcal{B} , then n_i in \mathcal{B}
 - \mathcal{B} is acyclic

A Bundle

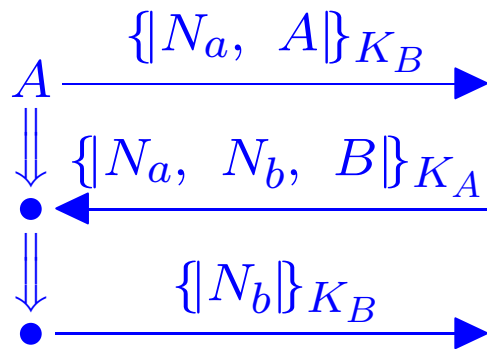


NS Attack: Adversary Activity

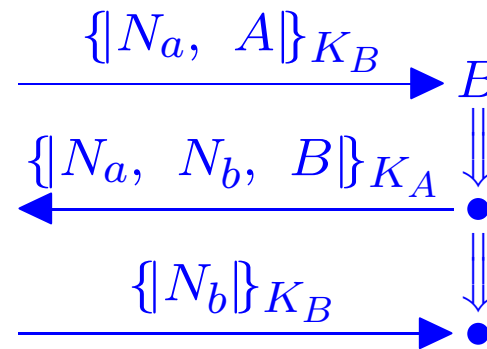


Bundles built from adversary strands
and regular strands

Regular Strands for NSL



NSInit[A, B, N_a, N_b]



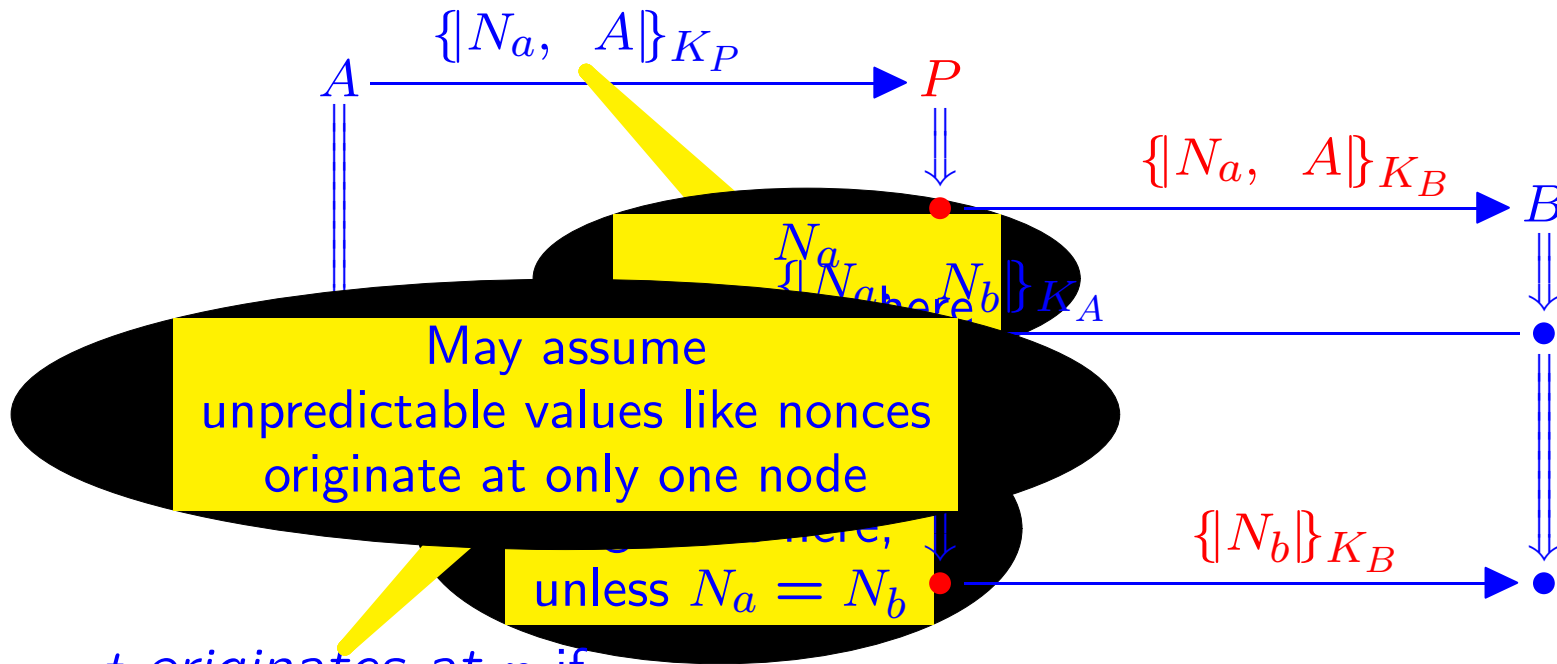
NSResp[A, B, N_a, N_b]

A **protocol** is a finite set of parametric strands, called the roles of the protocol

Precedence within a Bundle

- Bundle precedence ordering $\preceq_{\mathcal{B}}$
 - $n \preceq_{\mathcal{B}} n'$ means sequence of 0 or more arrows \rightarrow, \Rightarrow lead from n to n'
 - $\preceq_{\mathcal{B}}$ is a partial order by acyclicity
 - $\preceq_{\mathcal{B}}$ is well-founded by finiteness
- Bundle induction: Every non-empty subset of \mathcal{B} has $\preceq_{\mathcal{B}}$ -minimal members
- Reasoning about protocols combines
 - Bundle induction
 - Induction on message structure
 - Taking cases on
 - Regular strands for protocol
 - Adversary strands

Origination



t originates at n if

- n positive
- t is part of ultimate plaintext of term transmitted: $t \sqsubset \text{term}(n)$
- $t \not\sqsubset \text{term}(m)$ if $m \Rightarrow^+ n$

Private decryption keys K_A^{-1}, K_B^{-1} are used, but originate nowhere in this run

A Secrecy Goal

- Suppose:
 - Bundle \mathcal{B} contains a strand $\text{Resp}[A, B, N_a, N_b]$
 - K_A^{-1}, K_B^{-1} non-originating
 - N_b originates uniquely in \mathcal{B} , with $N_b \neq N_a$
- Then:
 - There is no node $n \in \mathcal{B}$ with $\text{term}(n) = N_b$

Form: \forall . This is false for NS, true for NSL

- To prove secrecy:
- (1) non-originating values are safe
 - (2) if a originates, but always inside $\{\dots a \dots\}_K$ with K^{-1} safe then a also safe

An Authentication Goal

- Suppose:
 - Bundle \mathcal{B} contains a strand $\text{Resp}[A, B, N_a, N_b]$
 - K_A^{-1} non-originating
 - N_b originates uniquely in \mathcal{B}
 - $N_b \neq N_a$
- Then:
 - There is a strand $\text{Init}[A, B, N_a, N_b]$ in \mathcal{B}

Authentication: correspondence assertions (of form $\forall\exists$)
This is false for NS: Only have

$\text{Init}[A, X, N_a, N_b]$ in \mathcal{B}

for some X