

Models for Protocols

F. Javier Thayer

Why Security Protocols?

- Potentially enormous numbers of agents
- Adversaries with unknown or unspecified characteristics such as
 - Motivation
 - Money, Fun, Prestige, Boredom, Military Aggression?
 - Computational resources
 - Cryptographic skill
 - Eavesdropping capabilities
- Interlocuteurs (e.g., buyers and sellers) are rarely seen or heard in familiar ways.

Goals for this Presentation

- What's a security protocol. Examples.
- Models, Strand space model.
- What does protocol correctness mean?
- Will focus only on academic protocols. Why?
 - Real protocols are horrendous.
 - Propose and discuss threat models.
 - Formal correctness proof techniques
 - Qualify formal
- Stochastic models
 - Bundle Random Variables.
 - Application to pure authentication protocol.
- Conclusion. Tolerances for protocol failure.

Types of Protocols

- Networking protocols such as TCP:
 - Agents: Application programs.
 - Goal: Reliable communication.
- Authentication protocols:
 - Agents: Individuals or programs.
 - Goal: Ostensibly to mutually establish identity of agents.
- Key exchange protocols:
 - Agents: Programs.
 - Goal: Establish session encryption key.
- Key management Protocols:
 - Agents: Programs.
 - Goal: Manage key longevity, revocation etc.

Protocol Analysis

- Goals of security protocols
 - Exchange of session keys for encryption
 - Methods of authenticating interlocutors.
- How do security protocols work?
 - Use primitives such as cryptography or hashing.
 - Interlocutors attempt to prove they possess a secret or have received a message
- What can go wrong?
 - Timing delays, communication failures, agent failures,
 - Hostile attacks.

Approaches

- Many security protocols are in use currently.
- Classic works based on logical formalisms
 - Dolev, Yao, Karp (1982)
 - Burroughs, Abadi, Needham (1989)
- Strand Spaces: Models graphical structure of interactions in protocols (J. Guttman, J. Herzog, F. J. Thayer JCS 1999)
 - What is authentication, secrecy?
 - Explicitly formulate security goals.
 - Techniques applicable to a variety of protocols
- Allows formulation of probabilistic statements.

Authentication Example

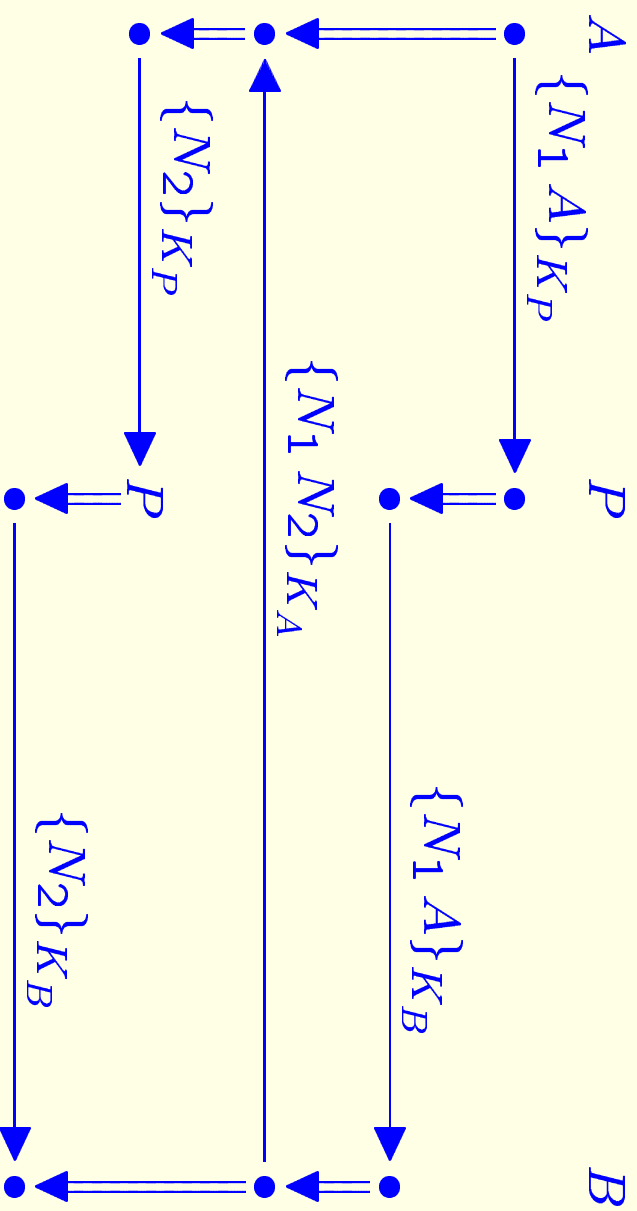
- Needham-Schroeder, using public key cryptography:



- B “proves” to A that he received nonce N_1 :
Only B has private key K_B^{-1} .
- A “proves” to B that she received N_2 :
- N_1, N_2 can be used to compose a session key.
Only A has private key K_A^{-1}

Protocol ‘Flaw’

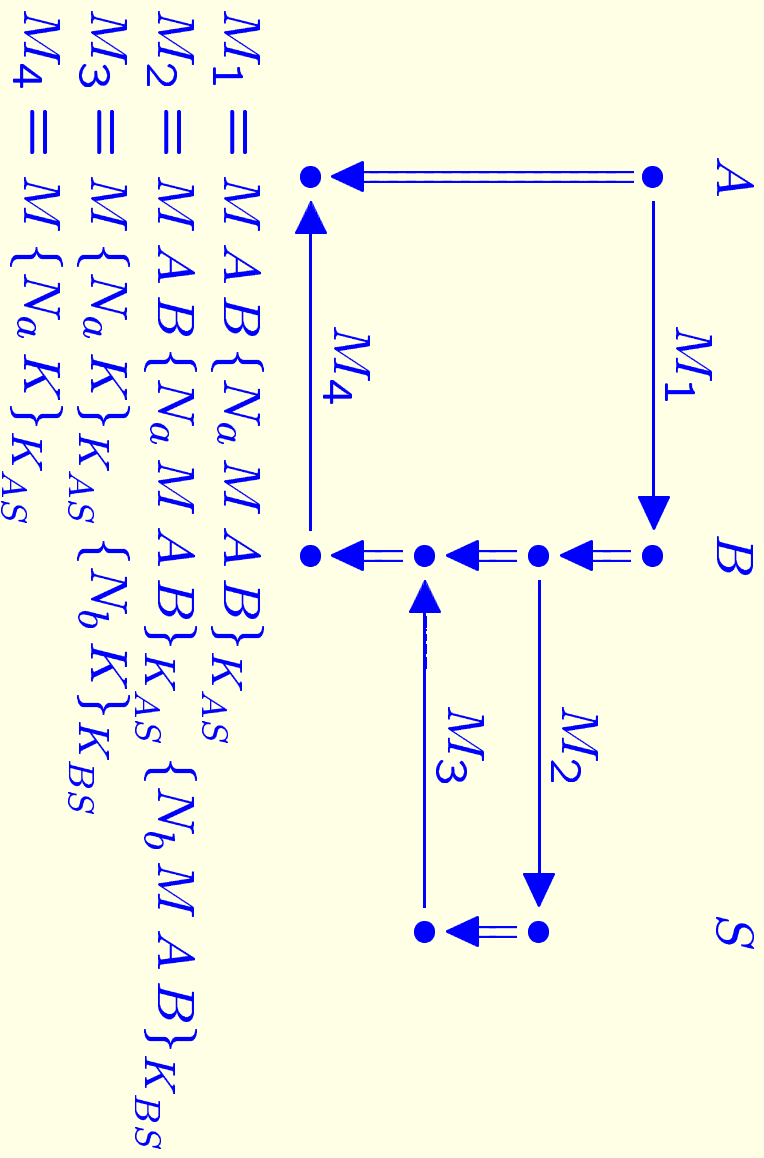
- Subverted Needham-Schroeder



- Illustrates protocol failure outside context of design assumptions:
 - All the potential interlocutors are trustworthy

Example: Otway-Rees

- Goal: Mutually authenticate, distribute session key K . K_{AS} is longterm shared key between A and S .



Parametric Form for Strands I

Needham Schroeder (Modified)

Node Schema	Fresh Value
Initiator $[A, B, N_a, N_b]$	
+	$\{N_a A\}_{K_B}$
-	$\{N_a N_b B\}_{K_A}$
+	$\{N_b\}_{K_B}$
Responder $[A, B, N_a, N_b]$	
-	$\{N_a A\}_{K_B}$
+	$\{N_a N_b B\}_{K_A}$
-	$\{N_b\}_{K_B}$

Parametric Form for Strands II

Otway Rees

Node Schema	Fresh Value
Initiator $[A, B, N_a, M, K]$	
+ $M A B \{N_a M A B\}_{K_A}$	N_a
- $M \{N_a K\}_{K_A}$	
Responder $[A, B, N_b, M, K, H, H']$	
- $M A B H$	
+ $M A B H \{N_b M A B\}_{K_B}$	N_b
- $M H' \{N_b K\}_{K_B}$	
+ $M H'$	
Server $[A, B, N_a, N_b, M, K]$	
- $M A B \{N_a M A B\}_{K_A} \{N_b M A B\}_{K_B}$	
+ $M \{N_a K\}_{K_A} \{N_b K\}_{K_B}$	K

General Protocol Assumptions

- Communication medium controlled by hostile agent.
- Adversary can
 - Intercept and examine all messages,
 - Replace messages by concatenating, decomposing and repeating other messages or discarding.
 - Encrypt or decrypt messages using keys known from the start.
 - Apply relations in cryptography,
 - Lots of guessing.
- Adversary cannot violate laws of Physics:
 - Cannot cause messages to be received before they are sent.
- Regular principals have only know what they send and receive.

Strand Spaces

- \mathbb{A} : possible messages in a protocol.
- Transmission of t is $+t$, reception of t is $-t$.
- *Strand Space* over \mathbb{A} :
 - Nodes \mathcal{N} partitioned into *strands* Σ .

Strand: One principal's experience of one run

– $\tau : \mathcal{N} \rightarrow \pm\mathbb{A}$.

– Two kinds of arrows

$n_1 \rightarrow n_2$: n_1 sends m and n_2 receives m

$n_1 \Rightarrow n_2$: n_1 immediately precedes n_2 on a strand

Message Algebra

- Message concatenation $\kappa : \mathbb{A} \times \mathbb{A} \rightarrow \mathbb{A}$
- Encryption $\epsilon : \mathbb{K} \times \mathbb{A} \rightarrow \mathbb{A}$
- Real encryption algebra has *many* non-trivial identities of the form $\{a\}_k = \{a'\}_{k'}$.
 - Any encryption algebra \mathbb{A} has a free “cover” $\pi : \mathbb{A}' \rightarrow \mathbb{A}$.
 - A protocol property fails for strand spaces over \mathbb{A}' , then the same protocol property fails for \mathbb{A} .
 - Protocol failures may exploit relations in \mathbb{A} which cannot be lifted to \mathbb{A}' .
 - Prevent failures based on protocol structure, not on particular properties of the message algebra.

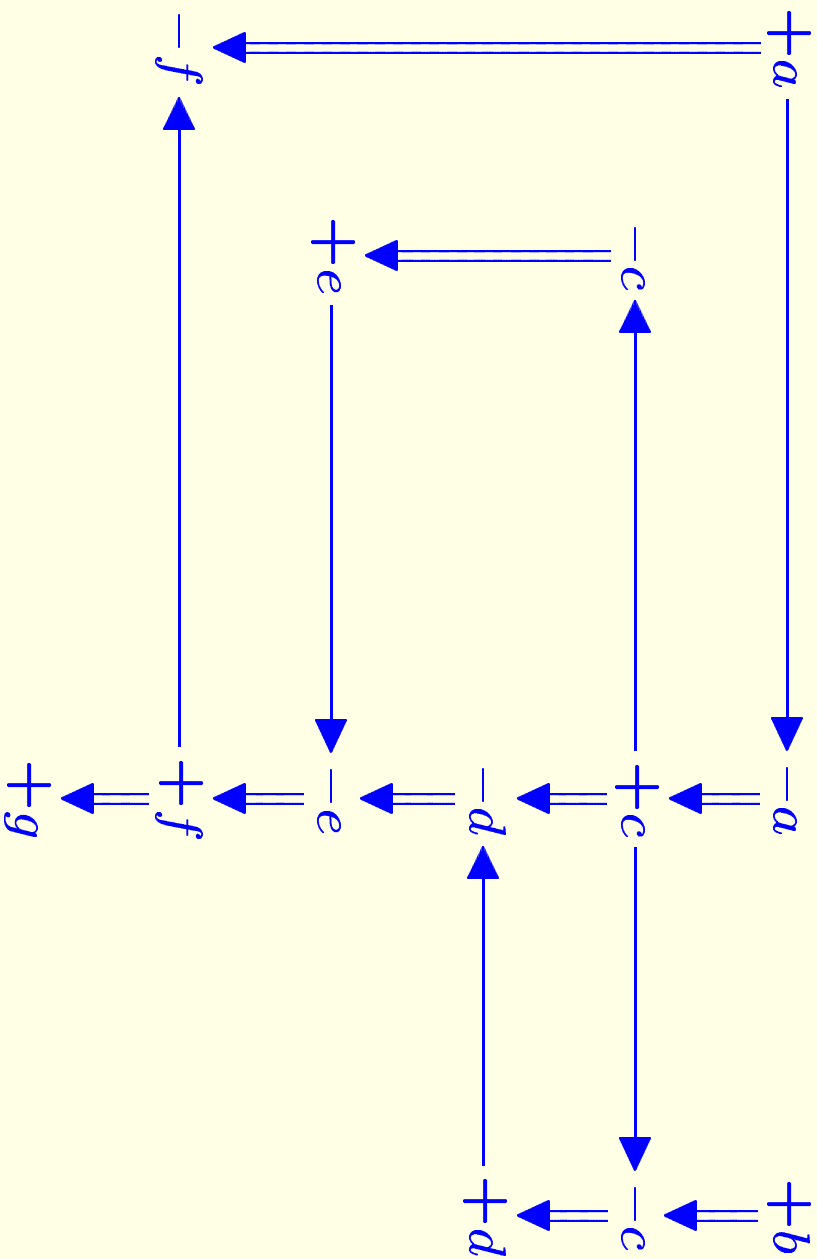
Strands

- Kinds of *regular* (= non-penetrator) strands depends on
 - Protocol
 - Roles in protocol (e.g., initiator, responder, server)
 - Usually given in parametric form.
- Penetrator: In simplest model, represented by short strands for
 - Concatenation, decomposition, repetition, encryption, decryption

Bundles

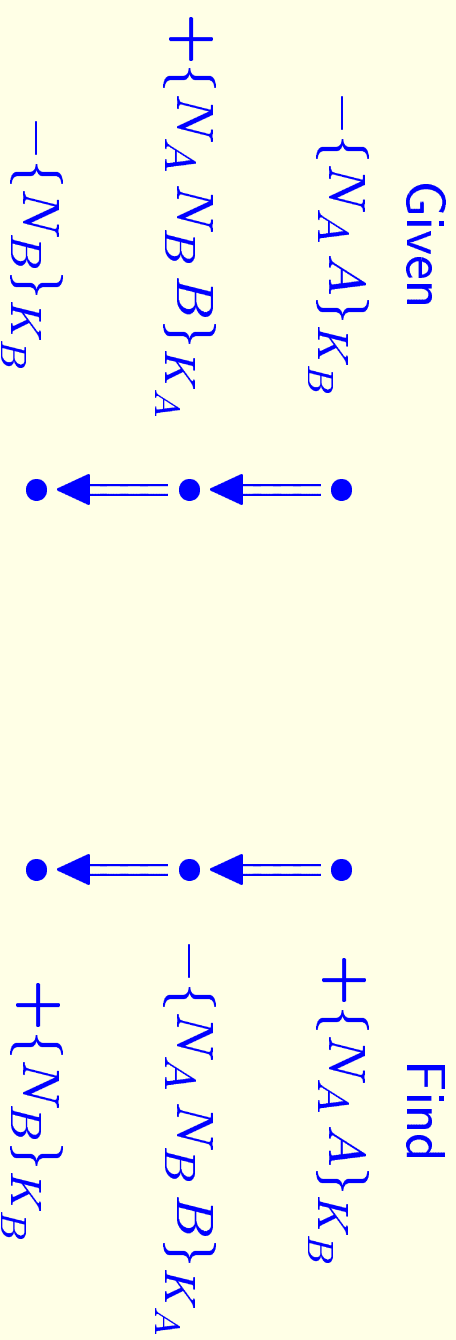
- A *bundle* is a finite subgraph \mathcal{C} of $(\mathcal{N}, \rightarrow, \Rightarrow)$ such that
 - If $n_2 \in \mathcal{C}$ and $\text{term}(n_2)$ is negative, then there is a unique n_1 such that $n_1 \rightarrow_{\mathcal{C}} n_2$.
 - If $n_2 \in \mathcal{C}$ and $n_1 \Rightarrow n_2$ then $n_1 \Rightarrow_{\mathcal{C}} n_2$.
 - \mathcal{C} is acyclic.
- Transitive reflexive closure of $\rightarrow \cup \Rightarrow$ is a partial order.

A Bundle



A Uniqueness Property

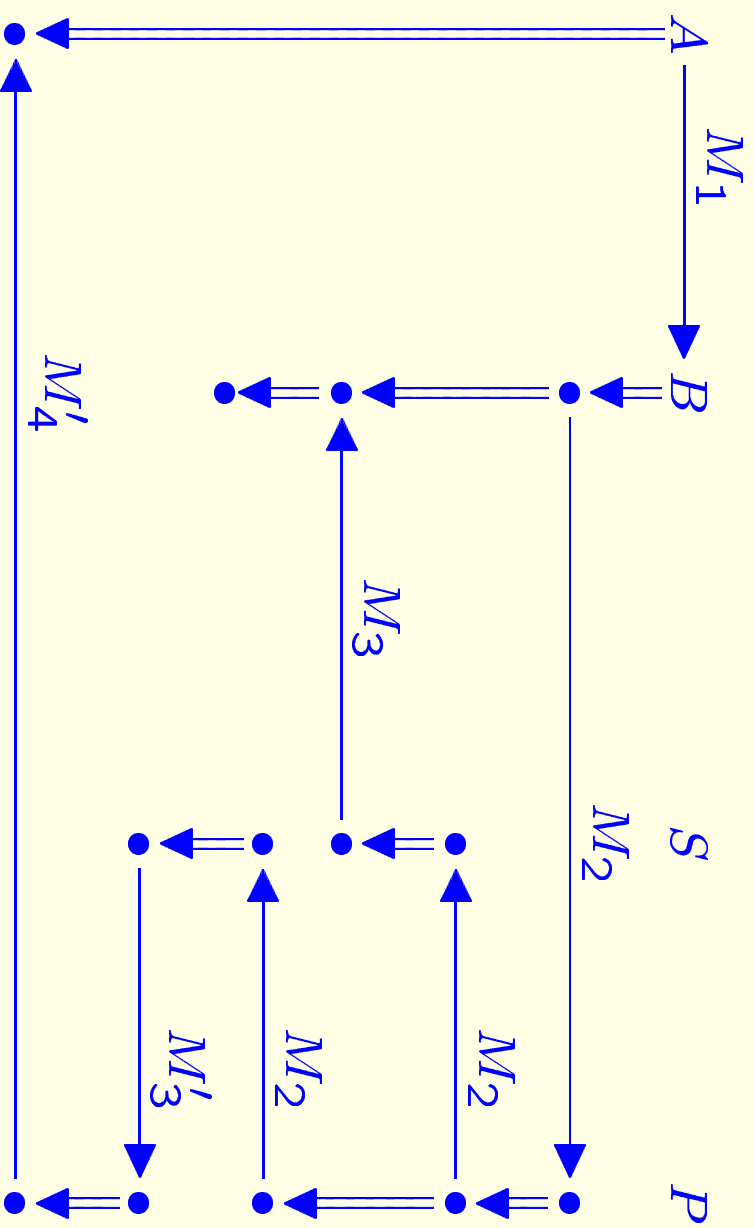
- Given an NSL bundle:



- Assuming:
 - K_A^{-1} not initially known to penetrator;
 - $N_a \neq N_b$ and N_b is fresh in bundle

Other Examples of Flaws

- Infiltrated Otway-Rees Bundle:

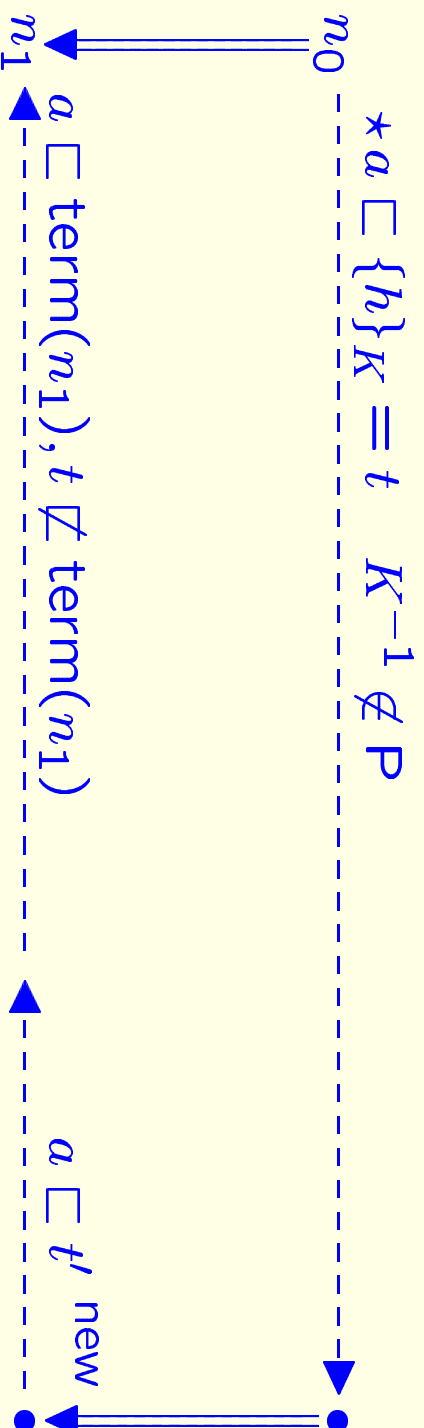


Summary

- Strand Spaces: Emphasizes global properties that follow from experience of one principal
- Geometric representation useful
 - Semantics of protocol correctness.
 - Suggesting singular situations/flaws
 - Emphasizes importance of protocol specification and protocol limits.
- General solution of correctness problem (assuming freeness) using Authentication Tests.

Authentication Test

- J. Guttman, F. J. Thayer, TCS 2001



- “ \bullet ” means the test shows this regular node exists

Limitations

- No account of collisions of nonces,
- Adversary is not allowed to make lots of guesses,
 - Potentially useful for faking signatures
- No relations between cryptography and the protocol.

Bundle-valued Random Variables

Current work (J. Guttman, F. J. Thayer, L. Zuck)

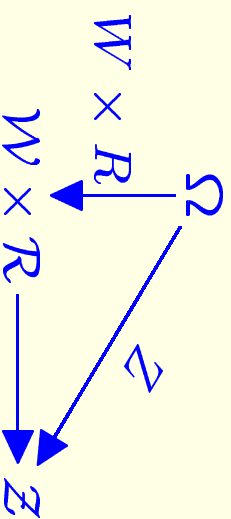
- View bundle as first class object.
- Bundle is “countably specified” object,
 - Finite labelled graph.
- \mathfrak{B} is set of bundles. \mathfrak{B} is a complete separable metric space.
- $(\Omega, \mathcal{A}, \mathbf{P})$ probability space.
 - Encapsulates choice of nonces, interlocutors, message delays and behavior of the penetrator.
- $B : \Omega \rightarrow \mathfrak{B}$ is measurable.
- $(\Omega, \mathcal{A}, \mathbf{P})$ is only constrained by independence assumptions on random variables.

Protocol Correctness: Possible meanings

- $B(\omega)$ is correct almost surely.
 - Require bundles of infinite size.
- $B(\omega)$ is correct almost surely tractable probability.
 - True in asymptotic sense.
- $B(\omega)$ is correct within tolerance.
 - Given bounds on size and some stochastic assumptions, what can be said about a specific bundle.

Behavior of Adversary

- Some random variable $Z : \Omega \rightarrow \mathcal{Z}$
- Depends on
 - Regular messages, $W : \Omega \rightarrow \mathcal{W}$
 - Other random input $R : \Omega \rightarrow \mathcal{R}$
- Diagram

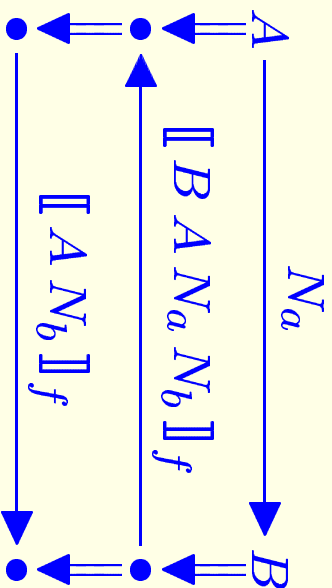


- R, W stochastically independent.
- \mathcal{Z} is set of forged messages.
- Adversary sees into future!

Pure Authentication Protocol

- Protocol of theoretical interest (Bellare-Rogaway)
- Z are hash guesses of adversary.
- Adversary wins if makes one correct guess.
- Using Carter-Wegman hashes, obtain upper estimates for likelihood of protocol failure.
 - Carter-Wegman hashing is unconditionally secure.
- Depends on size of bundle. Maximum of
 - ┌ Number of regular messages
 - └ Number of regular nonces
 - ∧ Number of adversary messages

An Authentication Protocol



- Nonces are independently uniformly chosen,
- Hash function f is chosen independently of penetrator behavior.

Conclusion

- Protocol correctness close to “social aspects” of network security,
 - Contrast to cryptographic aspects.
- Protocol tolerances: Probability of failure under conditions of Bundle size.
 - Limits key longevity.
 - Requires quality random number generation.
- Suggests protocol quality standard.