

# Term-based composition of Security Protocols

---

Genge Bela<sup>1</sup>, Haller Piroska<sup>2</sup>, Răţoi Ovidiu<sup>3</sup>, Iosif Ignat<sup>4</sup>



<sup>1,2,3</sup> “Petru Maior” University of Târgu Mures, Electrical Engineering department

<sup>4</sup> Technical University of Cluj Napoca, Computer Science department

Contact: {<sup>1</sup>bgenge, <sup>2</sup>phaller, <sup>3</sup>oratoi}@upm.ro, <sup>4</sup>iosif.ignat@cs.utcluj.ro

# Summary

---

- ❑ Introduction to security protocols and composition
  - ❑ Existent protocol specifications
  - ❑ Extending the strand space model
  - ❑ Composition requirements
  - ❑ Model term-connections
  - ❑ Example composition
  - ❑ Conclusion and future work
-

# Introduction

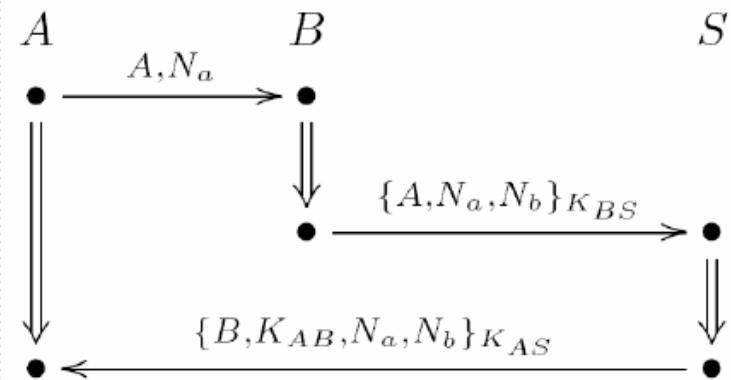
---

- Security protocols?
    - Communication protocols + cryptography
    - Example message specification:  $\{A, B, Na, K\}_{Kab}$
  - Composition?
    - Combining two or more protocols
    - Useful in design process
    - Known composition types:
      - Parallel
      - Sequential
      - *Term-based*
  - Parallel composition?
    - Protocol messages are run in parallel
  - Sequential composition?
    - Protocol messages are run sequentially
  - *Term-based* composition
    - Message components (i.e. terms) are combined together
-

# Existent specification models

- Existing message specification models are not satisfying because:
  - They are simplistic
  - Message specification does not contain sufficient information for formal reasoning
- Informal specification (a):
  - Inexistent formal reasoning language
- Strand space model (b):
  - Provides a formal reasoning language
  - Informal message specification
- Operational semantics (c):
  - Message components are made explicit
  - Message-term links are not made explicit

$A \rightarrow S: A, \{Ta, B, Kab\}Kas$   
 (a)  $S \rightarrow B: \{Ts, A, Kab\}Kbs$   
 $B \rightarrow A: \{Nb\}Kab$   
 $A \rightarrow B: \{Nb+1\}Kab$



$$ns(i) = (\{i, r, ni, sk(i), pk(i), pk(r)\}, \\
 send_1(i, r, \{i, ni\}_{pk(r)}) \cdot \\
 read_2(r, i, \{ni, V\}_{pk(i)}) \cdot \\
 send_3(i, r, \{V\}_{pk(r)}))$$

# Why extending the strand space model?

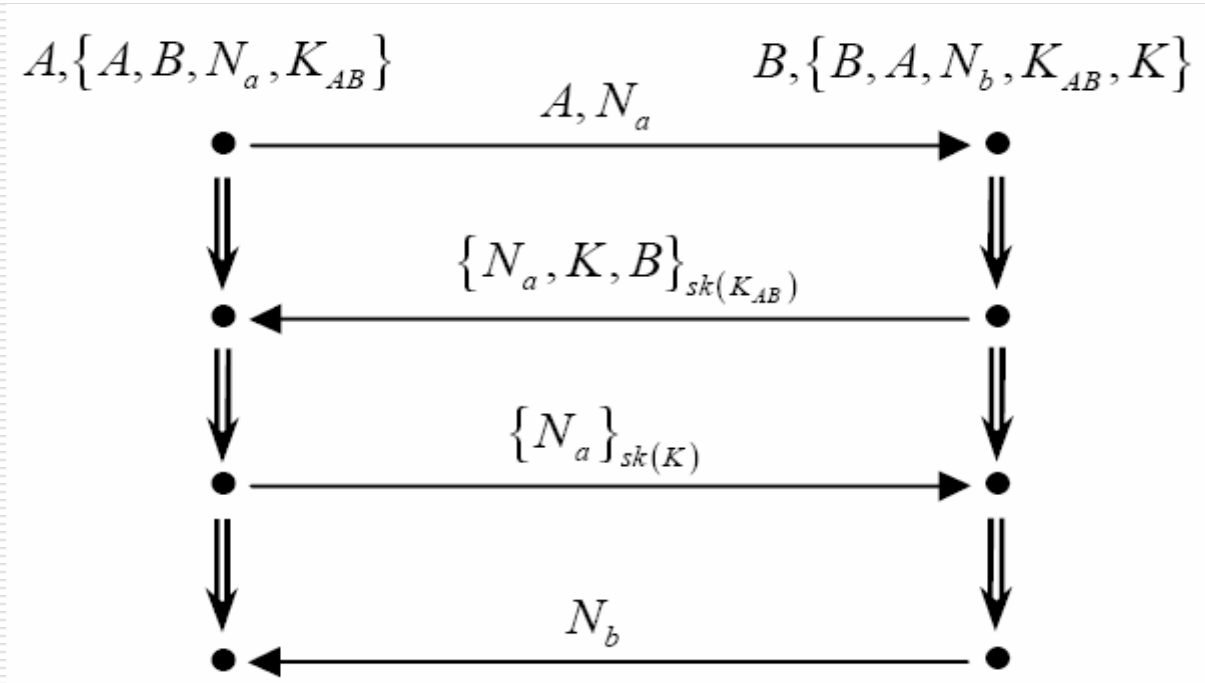
---

- Strand:
    - A sequence of send and receive events
    - Model protocol participants
  - Strand spaces:
    - A collection of strands
    - Model security protocols
  - Why extending the strand space model?
    - Highly general specification
    - Allows the modeling of internal mechanisms: encryption, decryption, key generation
    - Flexibility
-

# Example protocol specification

---

- Lowe's BAN Concrete Secure RPC protocol:



# Term-based composition requirements

---

- Eliminate duplicate terms:
  - Compose terms with the same encryption context (i.e. encryption key and function)
- Minimize the number of applied encryption functions
- Maintain security properties:
  - Model term-connections
  - Ensure that connections are maintained

$$\begin{aligned} & \_ \mapsto_P \_ : \langle (\pm T) \times T \times \Sigma_k \rangle \times \langle (\pm T) \times T \times \Sigma_k \rangle \\ & \_ \mapsto_C \_ : \langle (\pm T) \times T \times \Sigma_k \rangle \times \langle (\pm T) \times T \times \Sigma_k \rangle \end{aligned}$$

---

# Term composition example

## - Motivating term-connections -

---

### □ First term:

- $\{A, B, Na, Nb\}_{sk(Kab)}, \{A, B, Na, Nb\}_{h(.)}$

### □ Second term:

- $\{A, N'b\}_{sk(Kab)}$

### □ Result (at the first glance):

- $\{A, B, Na, Nb, N'b\}_{sk(Kab)}, \{A, B, Na, Nb\}_{h(.)}$

### □ The problem:

- The first term loses the integrity property
-

# Term composition example

## - Introducing term-connections -

---

□ Based on Guttman's authentication tests

□ For the previous example:

$$\langle n, \{A, B, Na, Nb\}_{sk(K_{ab})}, S_k \rangle \mapsto_C \langle n, \{A, B, Na, Nb\}_{h(.)}, S_k \rangle$$

□ The composed term becomes:

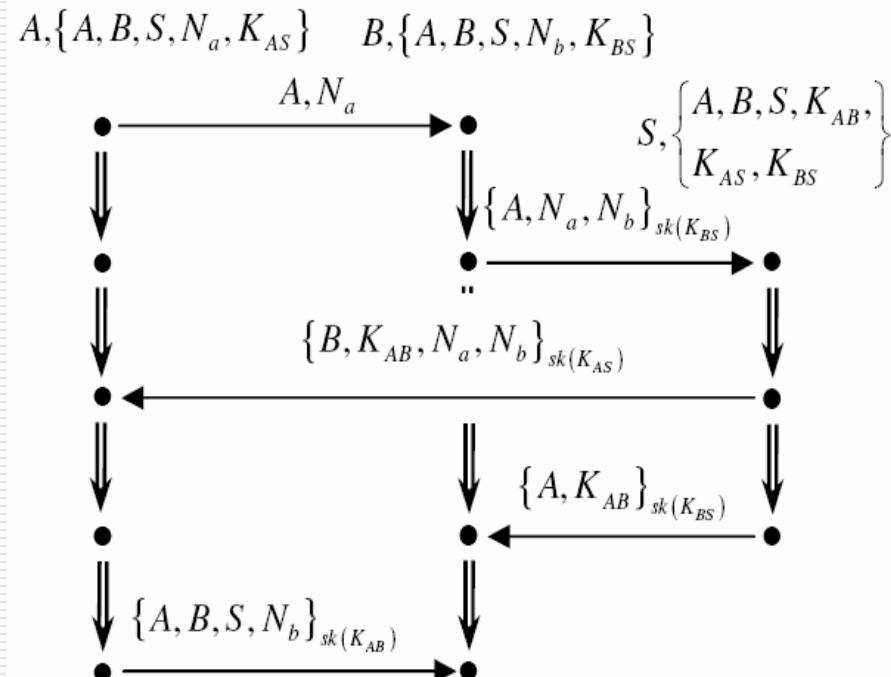
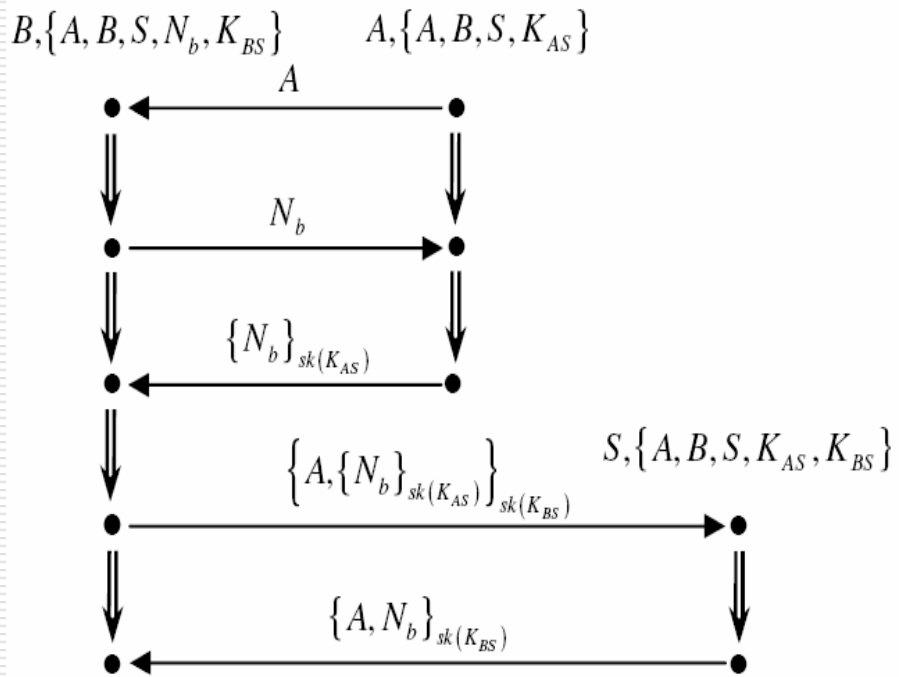
■  $\{A, B, Na, Nb, N'b\}_{sk(K_{ab})}, \{A, B, Na, Nb, N'b\}_{h(.)}$

---

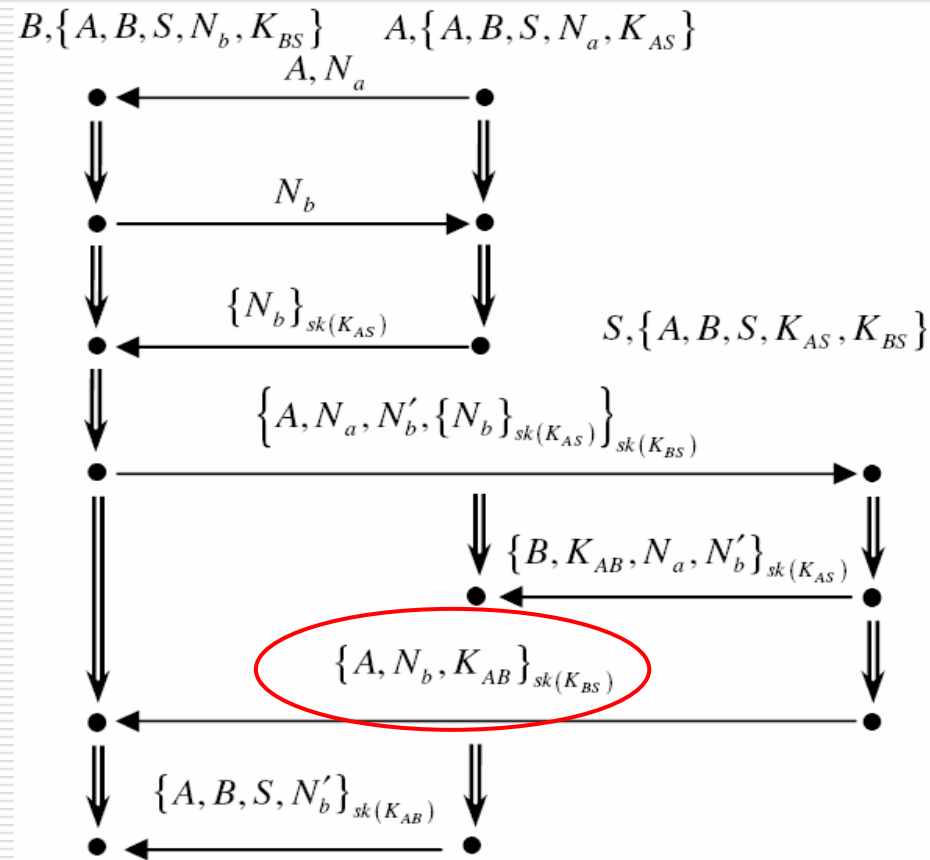
# Protocol composition example

□ Woo and Lam Pi

□ Yahalom



# Resulting protocol



# Future work

---

- ❑ Add performance-related information to optimize the performance of the created protocols
  - ❑ Implement a tool for the automated composition of security protocols
-

# Thanks for your attention!

---

Questions?

---