

# A Derivation System for Security Protocols and its Logical Formalization

Anupam Datta, Ante Derek, John C. Mitchell (Stanford University)\*

Dusko Pavlovic (Kestrel Institute)

\*Partially supported by the CIP/SW URI "Software Quality and Infrastructure Protection for Diffuse Computing" through ONR grant N00014-01-1-0795.

## Contributions

### Protocol Derivation System:

- Systematizes the practice of building protocols from standard sub-protocols. Useful for:
  - protocol analysis and understanding.
  - organizing related protocols in taxonomies.
  - protocol synthesis.

### Protocol Logic:

- Correctness proofs follow derivation steps.
- Rigorous treatment of protocol composition.

## Composition

### ISO 9798-3 protocol:

$A \rightarrow B: g^a, A$

$B \rightarrow A: g^b, \text{sig}_B\{g^a, g^b, A\}$

$A \rightarrow B: \text{sig}_A\{g^a, g^b, B\}$

- Shared secret:  $g^{ab}$
- Authenticated

## Diffie-Hellman: Property

### Formula

- $[ \text{new } a ]_A \text{ Fresh}(A, g^a)$

### Explanation

- Modal form:  $[ \text{actions} ]_p \varphi$
- Actions:  $[ \text{new } a ]_A$
- Postcondition:  $\text{Fresh}(A, g^a)$

## Component 1

### Diffie-Hellman

$A \rightarrow B: g^a$

$B \rightarrow A: g^b$

### Shared secret (with someone)

- A deduces:

$\text{Knows}(Y, g^{ab}) \supset (Y = A) \vee \text{Knows}(Y, b)$

### Authenticated

## Derivation Framework

### Protocols are constructed from:

- components

by applying a series of:

- composition, refinement and transformation operations.

### Properties accumulate as a derivation proceeds.

### Examples in paper [CSFW03; Invited submission JCS03]:

- STS, ISO-9798-3, JFKi, JFKr, IKE

## Challenge Response: Property

### Modal form: $\varphi [ \text{actions} ]_p \psi$

- precondition:  $\text{Fresh}(A, m)$

- actions:  $[ \text{Initiator role actions} ]_A$

- postcondition:

$\text{Honest}(B) \supset \text{ActionsInOrder}(\text{send}(A, \{A, B, m\}),$

$\text{receive}(B, \{A, B, m\}),$

$\text{send}(B, \{B, A, \{n, \text{sig}_B\{m, n, A\}\}\}),$

$\text{receive}(A, \{B, A, \{n, \text{sig}_B\{m, n, A\}\}\}))$

)

## Component 2

### Challenge Response:

$A \rightarrow B: m, A$

$B \rightarrow A: n, \text{sig}_B\{m, n, A\}$

$A \rightarrow B: \text{sig}_A\{m, n, B\}$

### Shared secret (with someone)

### Authenticated

- A deduces:  $\text{Received}(B, \text{msg1}) \wedge \text{Sent}(B, \text{msg2})$

## Protocol Logic: Formulas

### Action formulas

$a ::= \text{Send}(P, m) \mid \text{Receive}(P, m) \mid \text{New}(P, t)$   
 $\mid \text{Decrypt}(P, t) \mid \text{Verify}(P, t)$

### Formulas

$\varphi ::= a \mid \text{Has}(P, t) \mid \text{Fresh}(P, t) \mid \text{Honest}(N)$   
 $\mid \text{Contains}(t_1, t_2) \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \exists x \varphi$   
 $\mid \circ\varphi \mid \diamond\varphi$

### Example

$\text{After}(a, b) = \diamond(b \wedge \circ\Diamond a)$

## Composition Rules

### Prove assertions from invariants

$\Gamma \vdash \varphi [ \dots ]_p \psi$

### Invariant weakening rule

$\Gamma \vdash \varphi [ \dots ]_p \psi$

$\Gamma \cup \Gamma' \vdash \varphi [ \dots ]_p \psi$

### Prove invariants from protocol

$Q \triangleright \Gamma \quad Q' \triangleright \Gamma$

$Q \bullet Q' \triangleright \Gamma$