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 → B: g^A, A
  B → A: g^B, sig_B( g^A, g^B, A )
  A → B: sig_A( g^A, g^B, B )

  > Shared secret: g^AB
  > Authenticated

Diffie-Hellman: Property
> Formula
  \[ \text{[ new } a \text{ ] Fresh}(\cdot, g^A) \]

> Explanation
  > Modal form: \[ \text{[ actions ]}_P \phi \]
  > Actions: \[ \text{[ new } a \text{ ] } \phi \]
  > Postcondition: Fresh(\cdot, g^A)

Component 1
> Diffie-Hellman
  A → B: g^A
  B → A: g^B

  > Shared secret (with someone)
  > A deduces:
    Knows(Y, g^AB) \implies (Y = A) \lor 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: \[ \phi[ \text{ actions } ]_P \psi \]
  > precondition: Fresh(\cdot, m)
  > actions: \[ \text{[ Initiator role actions ] } \phi \]
  > postcondition:
    Honest(B) \implies ActionsInOrder(
      send(\cdot, (A,B,m)),
      receive(\cdot, (A,B,m)),
      send(\cdot, (B,A,(n, sig_B( m, n, A )))),
      receive(\cdot, (B,A,(n, sig_B( m, n, A ))))
    )

Component 2
> Challenge Response:
  A → B: m, A
  B → A: n, sig_B( m, n, A )
  A → B: sig_A( m, n, B )

  > Shared secret (with someone)
  > Authenticated

Protocol Logic: Formulas
> Action formulas
  a ::= Send( P, m ) | Receive( P, m ) | New( P, t )
  | Decrypt( P, t ) | Verify( P, t )

> Formulas
  \[ \phi ::= a | Has( P, t ) | Fresh( P, t ) | Honest( N )
  | Contains( t_1, t_2 ) | \neg \phi | \phi \land \phi_2 | \exists x \phi
  | \neg \phi | \phi \]

> Example
  After(a, b) = \circ(b \land \circ(a)

Composition Rules
> Prove assertions from invariants
  \[ \Gamma \vdash \phi[ \text{ actions } ]_P \psi \]

> Invariant weakening rule
  \[ \Gamma \vdash \phi[ \text{ actions } ]_P \psi \]
  \[ \text{[ Initator role actions ] } \phi \]
  \[ \text{[ new } a \text{ ] } \phi \]

> Prove invariants from protocol
  \[ Q \mid \Gamma \quad Q' \mid \Gamma \]
  \[ Q \cdot Q' \mid \Gamma \]