Tracking knowledge in security protocols: Verification via action models

Cosimo Perini Brogi
IMT School for Advanced Studies Lucca

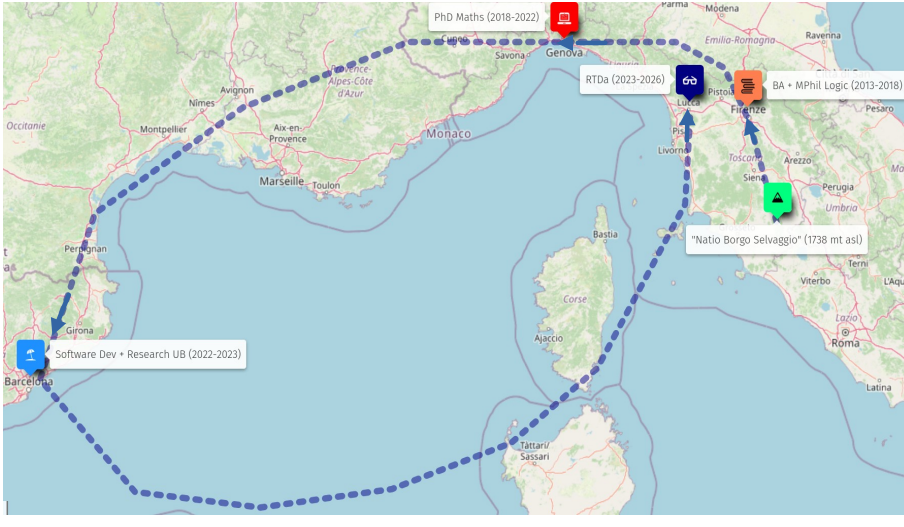
Spring Meeting
VRAIN-ELP & IMT-SYSMA
March 7, 2025 @ Universitat Politècnica de València

IMT SCUOLA ALTI STUDI LUCCA

About me

Westward Ho, and Return

$$|\text{Logician}\rangle \approx \tfrac{1}{3}|\text{Mathlete}\rangle + \tfrac{1}{3}|\text{Geek}\rangle + \tfrac{1}{3}|\text{Thinker}\rangle$$



Our project

Long term

- Establish a new methodology based on *Dynamic Epistemic Logic* (DEL) to analyse and verify "functional properties" and potential vulnerabilities of communication protocols, formalised in a *simplest specification language* (SPEC).

This is a joint work with

- Gabriele Costa (Associate Professor @ IMT)
- Hira Zaheer (PhD Student of the National PhD Programme in Cybersecurity @ IMT)

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Our goal

For today

- Illustrate our DEL-verification approach to a specific new protocol, named Broken Key Protocol (BKP), verifying that the evolution of epistemic states along the protocol execution from the view-points of *each participant* (*honest* prover and verifier) satisfies (forms of):

$$\left.\begin{array}{l} \Rightarrow \textit{ Zero-knowledge} \\ \Rightarrow \textit{ Proof of knowledge} \\ \Rightarrow \textit{ No repudiation} \end{array}\right\} \textit{ expressed as formulas of DEL}$$

More details in our conference paper:

- ✓ G. Costa, C. Perini Brogi. *Toward dynamic epistemic verification of zero-knowledge protocols*, in Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024), Salerno, Italy, April 8-12, 2024, CEUR Workshop Proceedings Vol. 3731, Open Access .

Our goal

For today

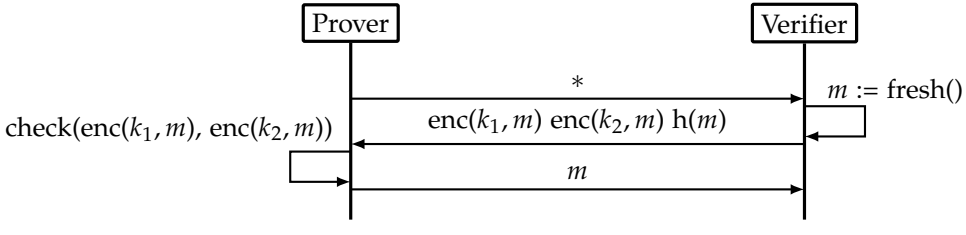
- Illustrate our DEL-verification approach to a specific new protocol, named Broken Key Protocol (BKP), verifying that the evolution of epistemic states along the protocol execution from the view-points of *each participant* (*honest* prover and verifier) satisfies (forms of):

$$\left.\begin{array}{l} \Rightarrow \textit{ Zero-knowledge} \\ \Rightarrow \textit{ Proof of knowledge} \\ \Rightarrow \textit{ No repudiation} \end{array}\right\} \textit{ expressed as formulas of DEL}$$

More details in our conference paper:

- ✓ G. Costa, C. Perini Brogi. *Toward dynamic epistemic verification of zero-knowledge protocols*, in Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024), Salerno, Italy, April 8-12, 2024, CEUR Workshop Proceedings Vol. 3731, Open Access .

Broken Key Protocol



Simple Protocol Epistemic Calculus

Statements

A *protocol statement* S is a term generated through the following grammar.

$$S ::= x := e \mid \rightarrow_A : e \mid \leftarrow_B : x \mid [g]S \mid S; S'$$

Structural Operational Semantics

$$\frac{\langle \sigma, S \rangle \longrightarrow \langle \sigma', S'' \rangle}{\langle \sigma, S; S' \rangle \longrightarrow \langle \sigma', S''; S' \rangle} \text{ (Seq 1)} \qquad \frac{\langle \sigma, S \rangle \longrightarrow \langle \sigma', \cdot \rangle}{\langle \sigma, S; S' \rangle \longrightarrow \langle \sigma', S' \rangle} \text{ (Seq 2)}$$

$$\frac{[\![g]\!]_\sigma = \mathbf{1}}{\langle \sigma, [g]S \rangle \longrightarrow \langle \sigma, S \rangle} \text{ (Cond 1)} \qquad \frac{[\![g]\!]_\sigma = \mathbf{0}}{\langle \sigma, [g]S \rangle \longrightarrow \text{☠}} \text{ (Cond 2)} \qquad \frac{[\![e]\!]_\sigma = v}{\langle \sigma, x := e \rangle \longrightarrow \langle \sigma[v/x], \cdot \rangle} \text{ (Asgn)}$$

$$\frac{[\![e]\!]_\sigma = v}{\langle \sigma, \rightarrow_A : e \rangle \longrightarrow \langle \sigma, \cdot \rangle \uparrow_{A,v}} \text{ (Send)} \qquad \frac{\langle \sigma, S \rangle \longrightarrow \langle \sigma', S'' \rangle \uparrow_{A,v}}{\langle \sigma, S; S' \rangle \longrightarrow \langle \sigma', S''; S' \rangle \uparrow_{A,v}} \text{ (Send-P)}$$

$$\frac{}{\langle \sigma, \leftarrow_B : x \rangle \longrightarrow \langle \sigma, \cdot \rangle \downarrow_{B,x}} \text{ (Recv)} \qquad \frac{\langle \sigma, S \rangle \longrightarrow \langle \sigma', S'' \rangle \downarrow_{B,x}}{\langle \sigma, S; S' \rangle \longrightarrow \langle \sigma', S''; S' \rangle \downarrow_{B,x}} \text{ (Recv-P)}$$

SPEC-description of BKP

Honest prover

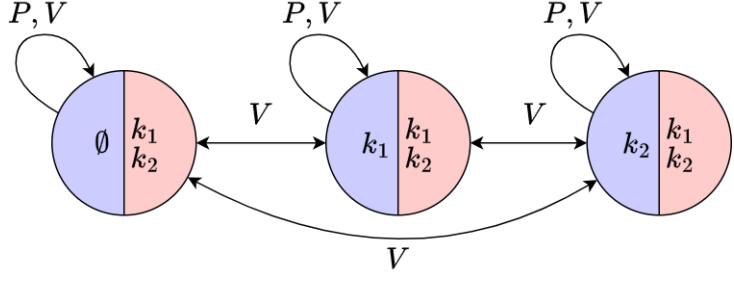
$$S_P \triangleq \quad \rightarrow_V : *; \leftarrow_V : x, y, z; [\texttt{comp}(x, y)][z = \texttt{h}(\texttt{trydec}(k, x, y))] \rightarrow_V : \texttt{trydec}(k, x, y)$$

Honest verifier

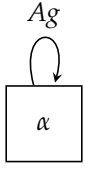
$$S_V \triangleq \quad \leftarrow_P : *; m := \texttt{fresh}(); \rightarrow_P : \texttt{enc}(k_1, m), \texttt{enc}(k_2, m), \texttt{h}(m); \leftarrow_P : x; [x = m]\texttt{skip}$$

Dynamic epistemic logic

Models for states

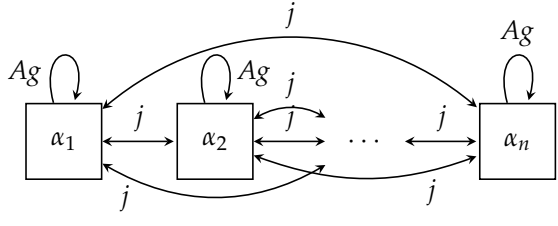


The action model $\langle\langle \rightarrow_i : e \rangle\rangle_j$ for agent j sending e to agent i:



"Sending an expression is a public action that can be performed whenever the sender is able to construct the value of that expression; after the event, that value is stored in the local information of the receiver."

The action model $\langle\langle \leftarrow_i : x \rangle\rangle_j$ for agent j receiving values on variable x from agent i:

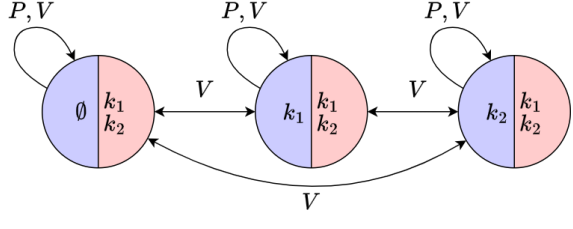


"Receiving information from the agent i as an equivalence class of sending statements from the same agent."

DEL-verification

Performing S_P

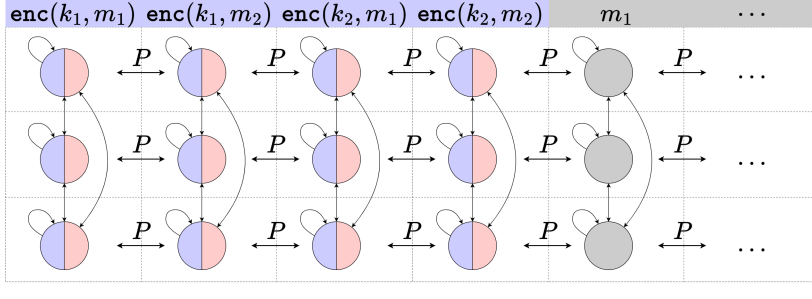
$$S_P \triangleq \twoheadrightarrow_V : *; \twoheadleftarrow_V : x, y, z; [\mathtt{comp}(x, y)][z = \mathtt{h}(\mathtt{trydec}(k, x, y))] \twoheadrightarrow_V : \mathtt{trydec}(k, x, y)$$



DEL-verification

Performing S_P

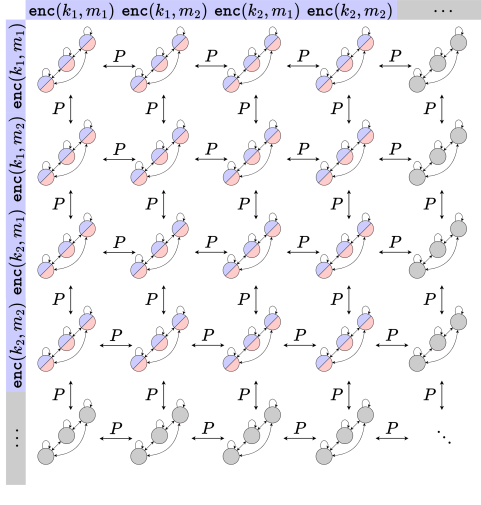
$$S_P \triangleq \twoheadrightarrow_V : *; \twoheadleftarrow_V : x, y, z; [\mathtt{comp}(x, y)][z = \mathtt{h}(\mathtt{trydec}(k, x, y))] \twoheadrightarrow_V : \mathtt{trydec}(k, x, y)$$



DEL-verification

Performing S_P

$$S_P \triangleq \twoheadrightarrow_V : *; \twoheadleftarrow_V : x, y, z; [\mathtt{comp}(x,y)][z = \mathtt{h}(\mathtt{trydec}(k,x,y))] \twoheadrightarrow_V : \mathtt{trydec}(k,x,y)$$



DEL-verification

Performing S_P

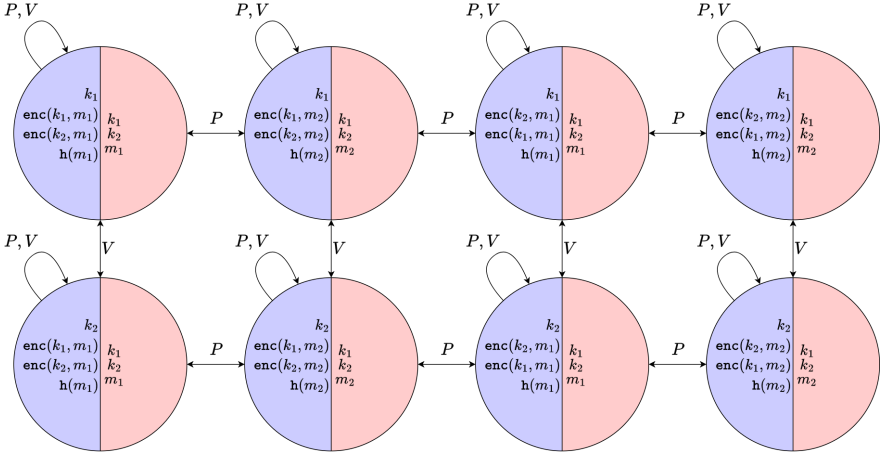
$$S_P \triangleq \twoheadrightarrow_V : *; \twoheadleftarrow_V : x, y, z; [\mathtt{comp}(x, y)][z = \mathtt{h}(\mathtt{trydec}(k, x, y))] \twoheadrightarrow_V : \mathtt{trydec}(k, x, y)$$

• • •

DEL-verification

Performing S_P

$$S_P \triangleq \twoheadrightarrow_V : *; \twoheadleftarrow_V : x, y, z; [\mathtt{comp}(x,y)][z = \mathtt{h}(\mathtt{trydec}(k,x,y))] \twoheadrightarrow_V : \mathtt{trydec}(k,x,y)$$



Zero knowledge: $\varphi_{\mathrm{ZK}} \triangleq \neg K_V(\mathsf{has}_P(k_1)) \wedge \neg K_V(\mathsf{has}_P(k_2))$

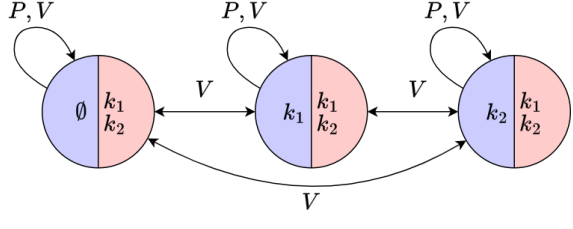
Proof of knowledge: $\varphi_{\mathrm{PoK}} \triangleq K_V(\mathsf{has}_P(k_1) \vee \mathsf{has}_P(k_2))$

No repudiation: $\varphi_{\mathrm{NR}} \triangleq K_V(K_P(K_V(\mathsf{has}_P(k_1) \vee \mathsf{has}_P(k_2))))$

DEL-verification

Performing S_V

$$S_V \triangleq \leftarrow_P : *; m := \texttt{fresh}(); \rightarrow_P : \texttt{enc}(k_1, m), \texttt{enc}(k_2, m), \texttt{h}(m); \leftarrow_P : x; [x = m]\texttt{skip}$$



DEL-verification

Performing S_V

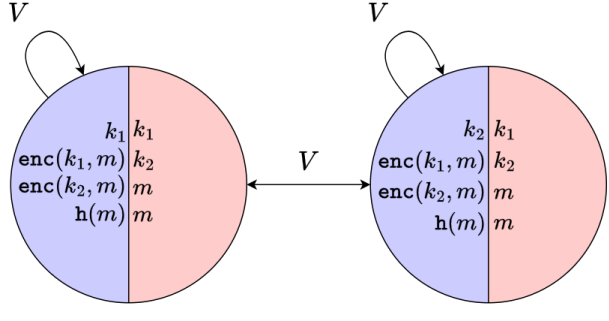
$$S_V \triangleq \leftarrow_P : *; m := \texttt{fresh}(); \rightarrow_P : \texttt{enc}(k_1, m), \texttt{enc}(k_2, m), \texttt{h}(m); \leftarrow_P : x; [x = m]\texttt{skip}$$

• • •

DEL-verification

Performing S_V

$$S_V \triangleq \leftarrow_P\colon *; m := \texttt{fresh}(); \rightarrow_P\colon \texttt{enc}(k_1, m), \texttt{enc}(k_2, m), \texttt{h}(m); \leftarrow_P\colon x; [x = m]\texttt{skip}$$



Proof of knowledge: $\varphi_{\text{PoK}} \triangleq K_V(\mathsf{has}_P(k_1) \vee \mathsf{has}_P(k_2))$

Put in perspective

- Employ the capabilities and flexibility of non-classical logics, and, in particular, dynamic epistemic logic, in
  - formalising knowledge dynamics in communication scenarios and security protocols;
  - abstracting the logical structure behind cryptographic and mathematical aspects of information flow;
  - verifying security desiderata of communication protocols.
- Store meta-theoretical results for the combination SPEC+DEL.
- Integrate existing models and automated tools for protocol verification with efficient and DEL-based modelling techniques (modulo some engineering adjustments).

Many thanks for listening!