

University of Stuttgart
Institute of
Information Security

Carnegie
Mellon
University

Inria



DY*: A Modular Symbolic Verification Framework for Executable Cryptographic Protocol Code

EuroSP'21 | reprosec.org

SEC

Bhargavan, Bichhawat, Do, Hosseyni, Küsters, Schmitz, Würtele

Cryptographic Protocols are Everywhere: Golden Era of Crypto

- Ubiquitous HTTPS: TLS 1.3, QUIC, ACME/Let's Encrypt, ...
- Secure Messaging: Signal, MLS, ...
- Single-Sign On: OAuth, OIDC, SAML, ...
- Wireless: Wifi/WPA, 4G, 5G, Zigbee, ...
- Payment: EMV, W3C Web Payments, ...
- Post-Quantum Crypto: NIST KEMs, Signature, ...
- Lightweight Crypto: IETF LAKE, NIST LWC



Cryptographic Protocols are Everywhere: Golden Era of Crypto

COMPUTERWORLD UNITED STATES INSIDER

NEWS

EMV flaw allows 'pre-play' attacks on chip-enabled payment cards

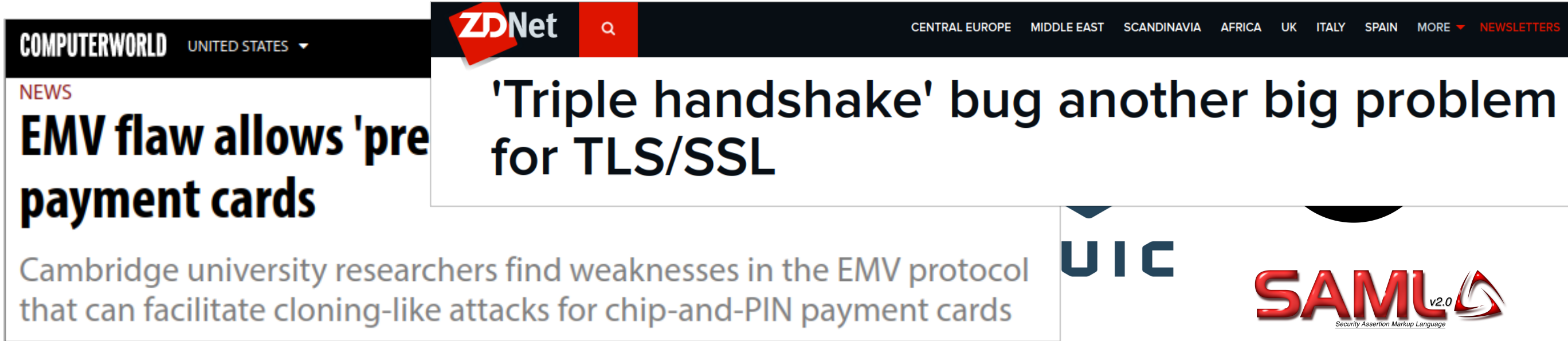
Cambridge university researchers find weaknesses in the EMV protocol that can facilitate cloning-like attacks for chip-and-PIN payment cards



- Payment: EMV, v3C web Payments, ...
- Post-Quantum Crypto: NIST KEMs, Signature, ...
- Lightweight Crypto: IETF LAKE, NIST LWC



Cryptographic Protocols are Everywhere: Golden Era of Crypto



The screenshot shows a ZDNet news article. The main headline is "'Triple handshake' bug another big problem for TLS/SSL". To the left, there is a secondary headline: "EMV flaw allows 'pre payment cards'". Below the headlines, there is a sub-headline: "Cambridge university researchers find weaknesses in the EMV protocol that can facilitate cloning-like attacks for chip-and-PIN payment cards". The ZDNet logo and navigation menu are visible at the top.

- Payment: EMV, v3C web Payments, ...
- Post-Quantum Crypto: NIST KEMs, Signature, ...
- Lightweight Crypto: IETF LAKE, NIST LWC



Cryptographic Protocols are Everywhere: Golden Era of Crypto

The collage features several elements:

- ZDNet** logo with a search icon.
- Navigation links: CENTRAL EUROPE, MIDDLE EAST, SCANDINAVIA, AFRICA, UK, ITALY, SPAIN, MORE, NEWSLETTERS.
- COMPUTERWORLD** logo with "UNITED STATES" dropdown.
- NEWS** section with a snippet: "EMV flaw allows 'pre payment cards'".
- Article snippet: "'Triple handshake' bug another big problem for TLS/SSL".
- CLOUDFLARE** logo and "The Cloudflare Blog" header.
- Cloudflare navigation: Product News, Speed & Reliability, Security, Serverless, Zero Trust, Developers, Deep Dive, Life @Cloudflare.
- Article snippet: "Logjam: the latest TLS vulnerability explained" dated 21/05/2015.
- UIC** logo.
- SAML v2.0** logo with "Security Assertion Markup Language" text.
- Let's Encrypt** logo featuring a sun and a padlock.
- Communication logos: WhatsApp, Messenger, Skype, and **Signal**.
- zigbee** logo.
- Visuals of overlapping credit cards (orange and green).
- OAuth 2.0** logo.

Cryptographic Protocols are Everywhere: Golden Era of Crypto

The collage features several overlapping elements:

- COMPUTERWORLD** header with "UNITED STATES" and a dropdown arrow.
- NEWS** section with the headline: "EMV flaw allows 'pre payment cards'".
- ZDNet** logo and a search icon.
- Headline: "'Triple hand for TLS/SSL'".
- SearchSecurity** header with a search icon and a menu icon.
- CLOUDFLARE** logo and "The Cloudflare Blog" header.
- Navigation links: "Product News", "Speed & Reliability", "Security", "Serverless", "Zero Trust", "Developers", "Deep Dive".
- Headline: "Logjam: the latest TLS vulnerability explained".
- Date: "21/05/2015".
- Headline: "OAuth vulnerabilities must be fixed in the standard".
- Text: "Researchers in Germany have found two OAuth vulnerabilities, which could allow attackers to break the authorization and authentication standard. And an expert said the fix must be made to the standard itself."
- Byline: "By Michael Heller, Senior Reporter".
- Published: "12 Jan 2016".
- Logos for **Signal** and **zigbee**.
- Icons for WhatsApp, Messenger, and Signal.
- Icons for a credit card and a coin with the number "2".

Cryptographic Protocols are Everywhere: Golden Era of Crypto

COMPUTERWORLD UNITED STATES

NEWS

EMV flaw allows 'pre payment cards

ZDNet

'Triple hand for TLS/SSL

SearchSecurity

PIXEL_DREAMS - FOTOLIA

NEWS

OAuth vulnerabilities must be fixed in the standard

have found two OAuth vulnerabilities, which break the authorization and authentication and said the fix must be made to the standard itself.

Published: 12 Jan 2016

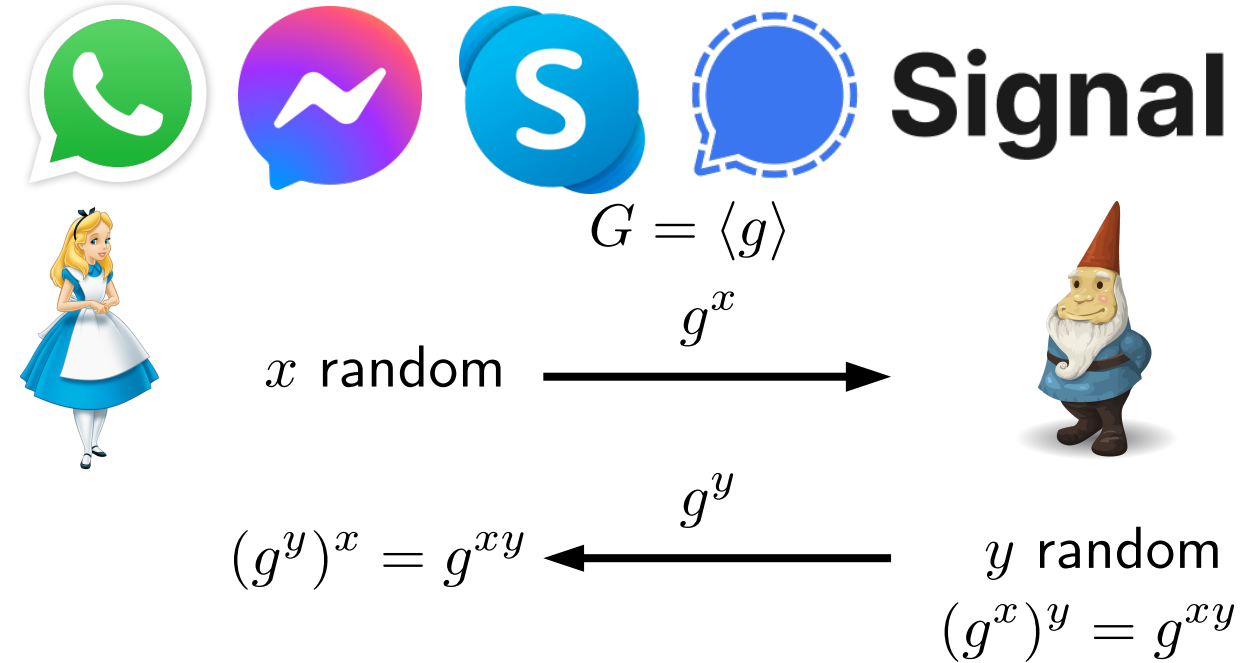
ars TECHNICA

*KRACK*TOA —

How the KRACK attack destroys nearly all Wi-Fi security

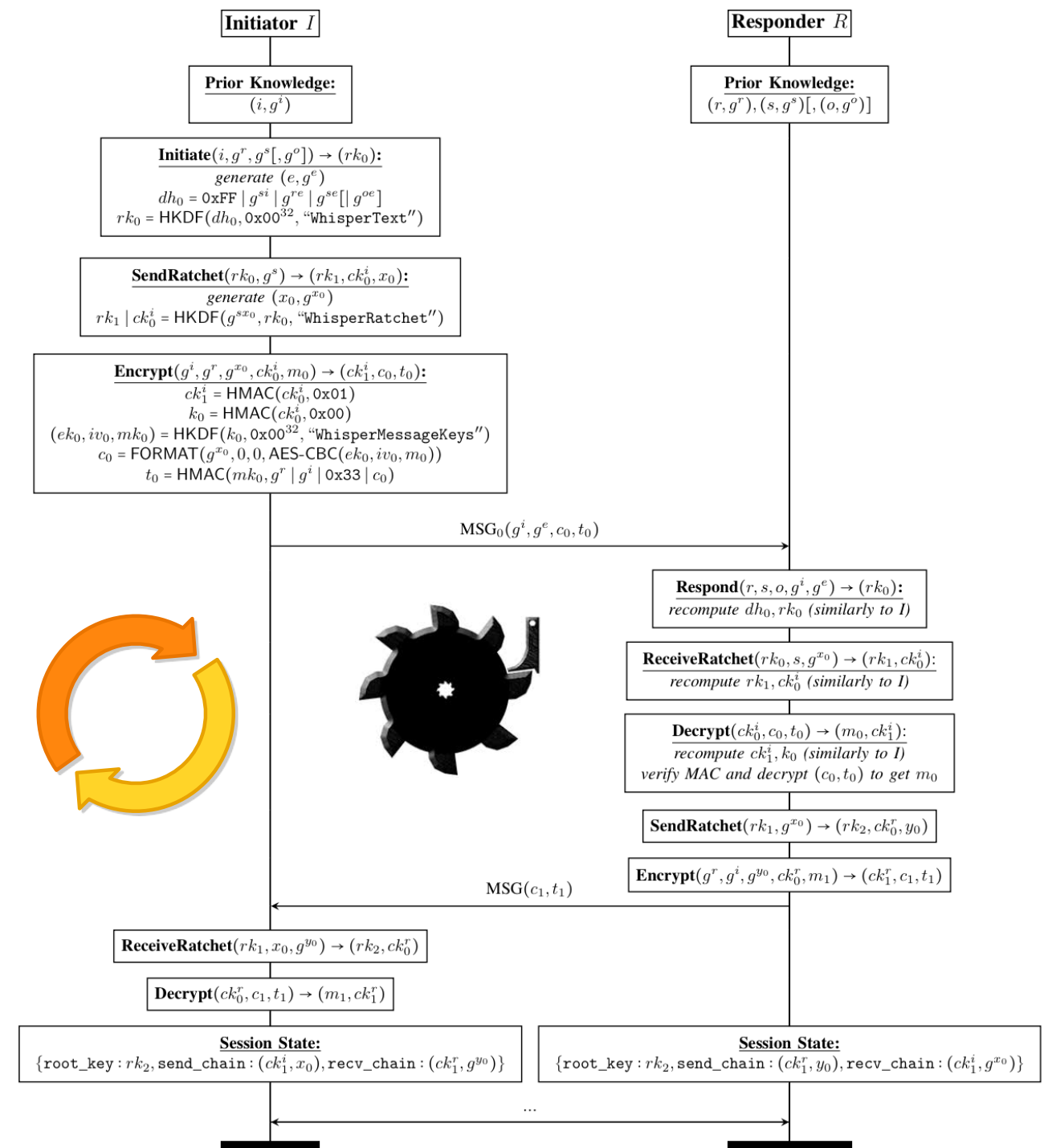
Signal Messaging Protocol

- Asynchronous continuous key exchange



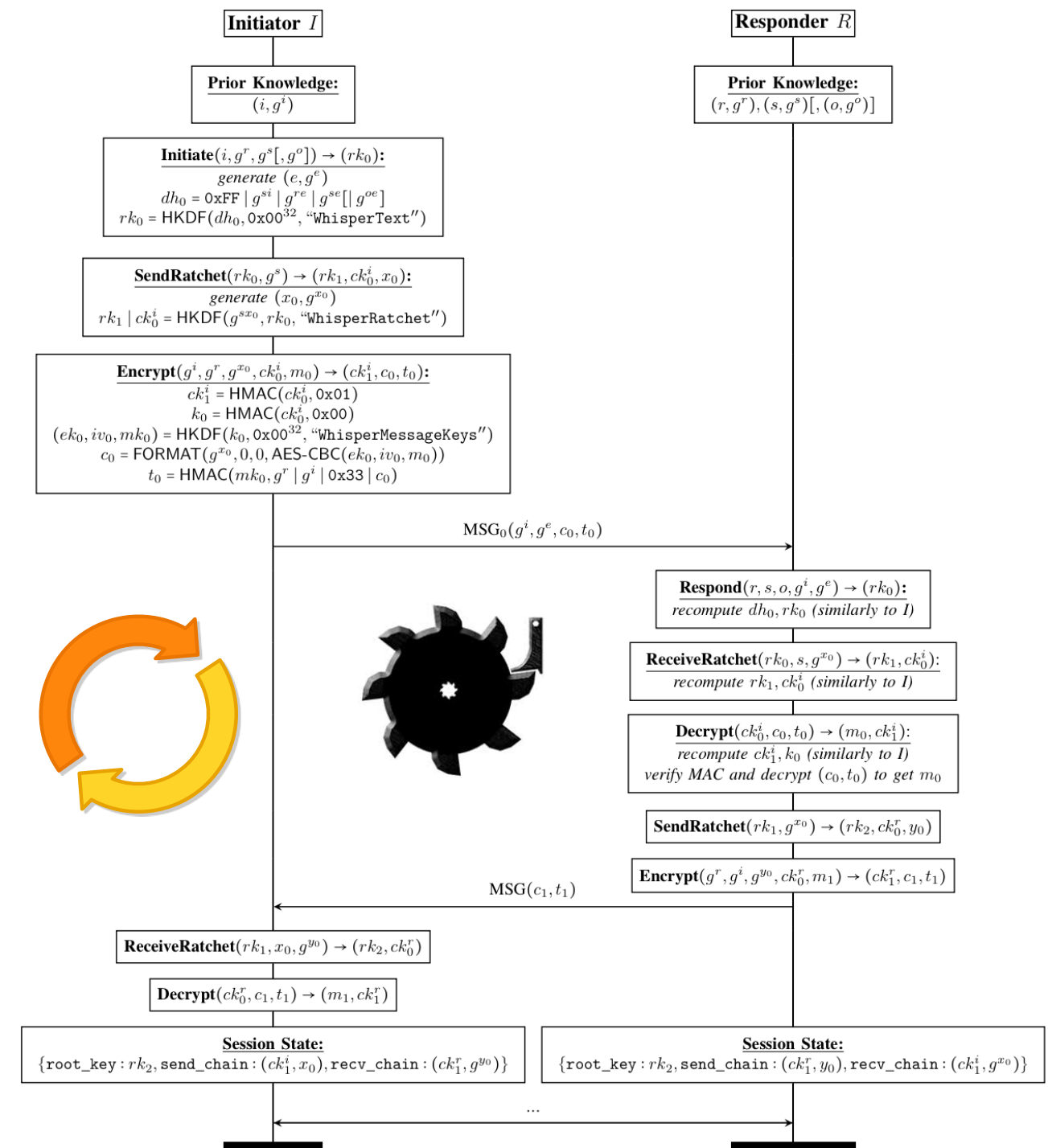
Signal Messaging Protocol

- Asynchronous continuous key exchange



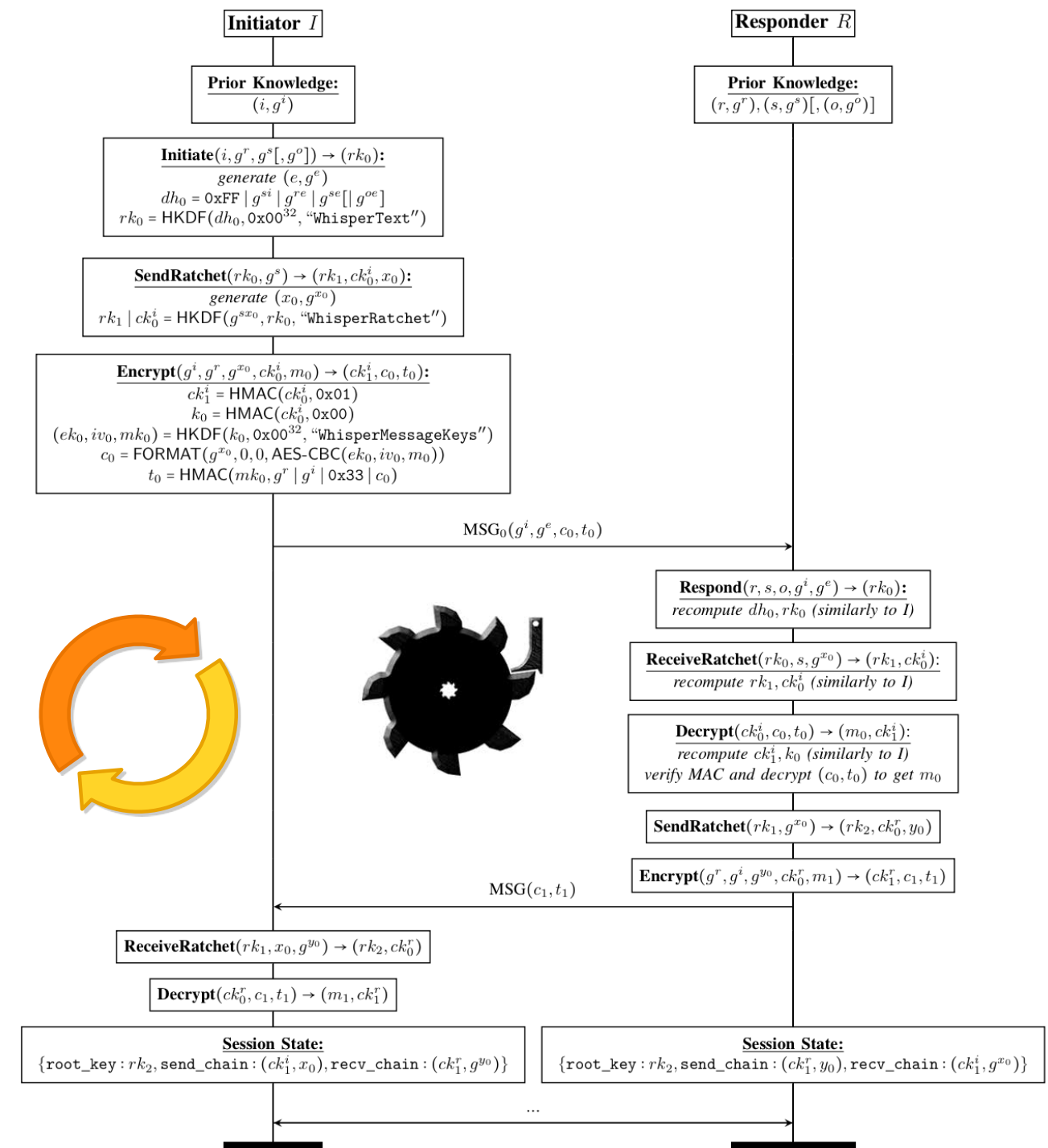
Signal Messaging Protocol

- Asynchronous continuous key exchange
- Multiple subprotocols
 - X3DH (initial key exchange)
 - DH Ratchet (post-compromise security)
 - Hash Ratchet (forward security)
 - Authenticated Encryption (message security)



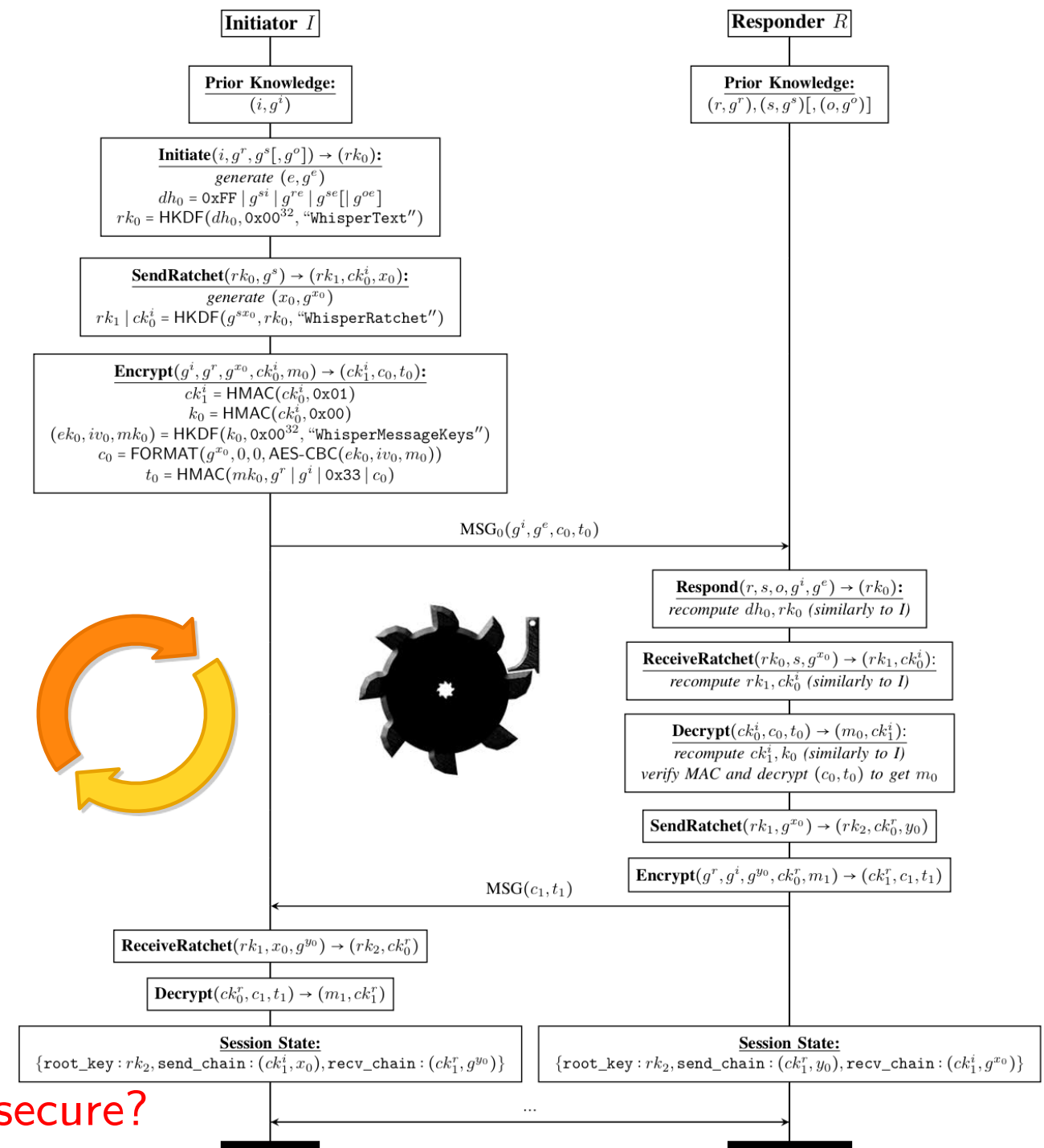
Signal Messaging Protocol

- Asynchronous continuous key exchange
- Multiple subprotocols
 - X3DH (initial key exchange)
 - DH Ratchet (post-compromise security)
 - Hash Ratchet (forward security)
 - Authenticated Encryption (message security)
- Inherently recursive
 - Security of each message depends on a chain of derived keys

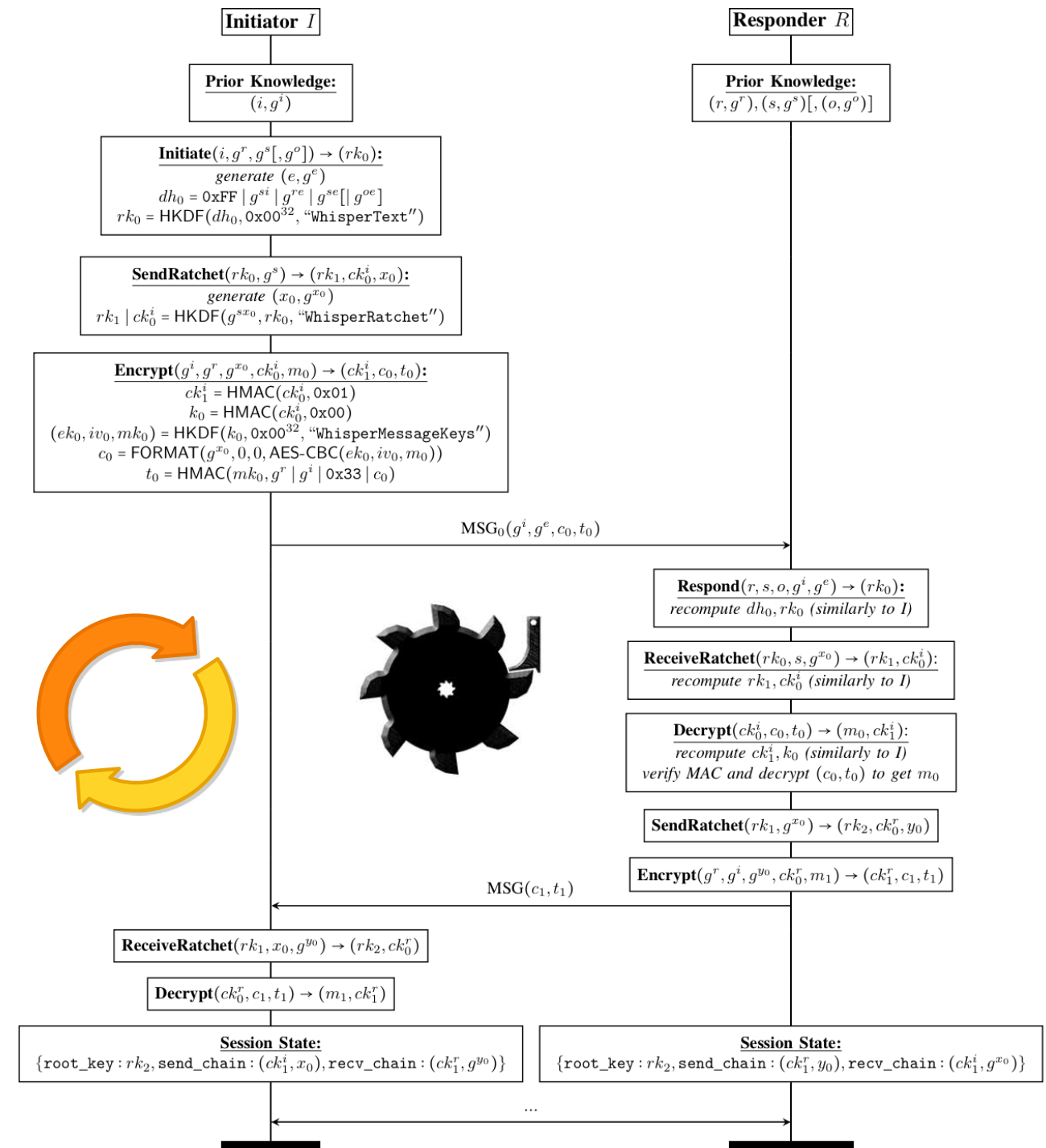


Signal Messaging Protocol

- Asynchronous continuous key exchange
- Multiple subprotocols
 - X3DH (initial key exchange)
 - DH Ratchet (post-compromise security)
 - Hash Ratchet (forward security)
 - Authenticated Encryption (message security)
- Inherently recursive
 - Security of each message depends on a chain of derived keys
- Can we mechanically verify that the protocol is secure?



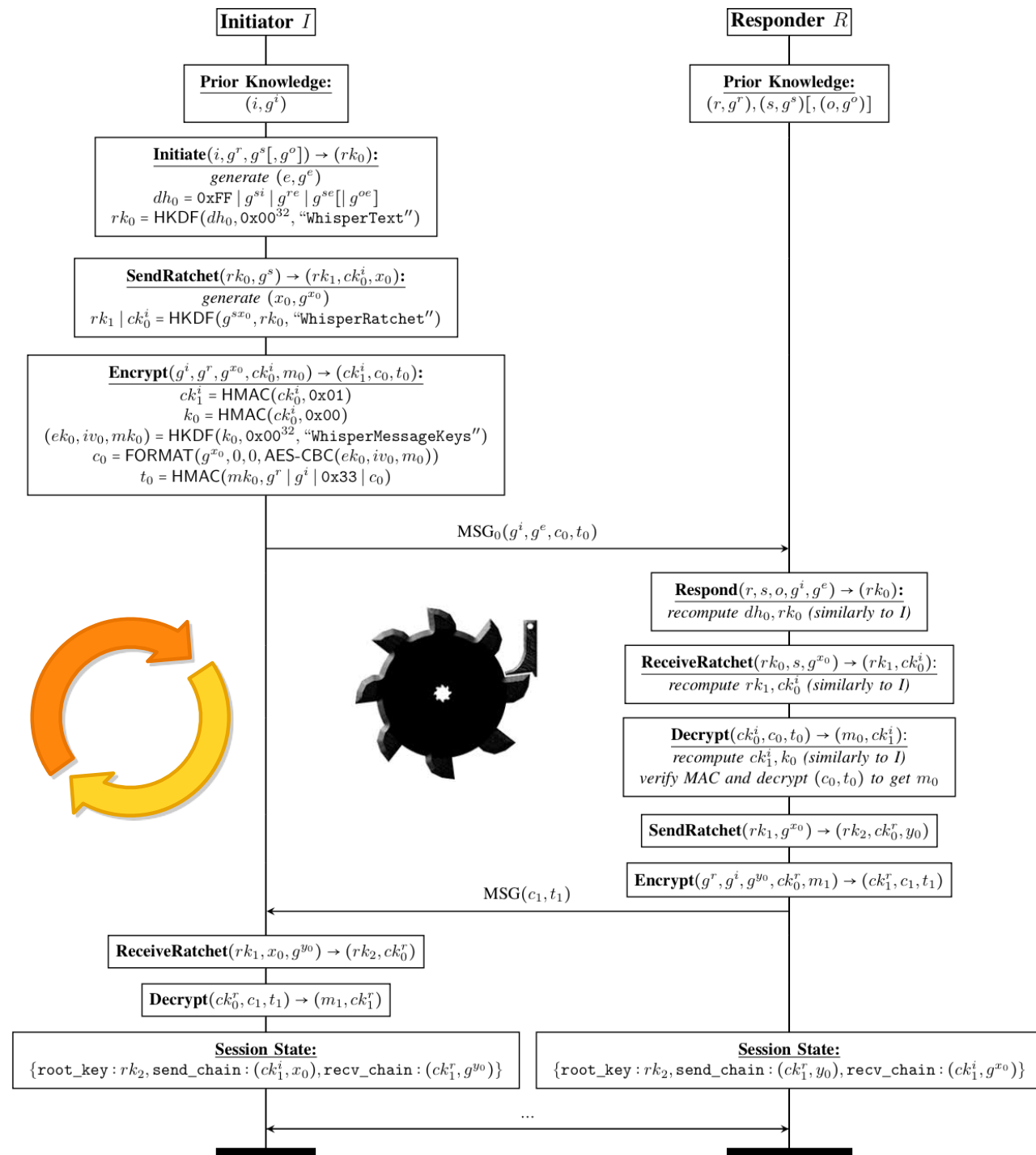
Formalizing Signal



Formalizing Signal

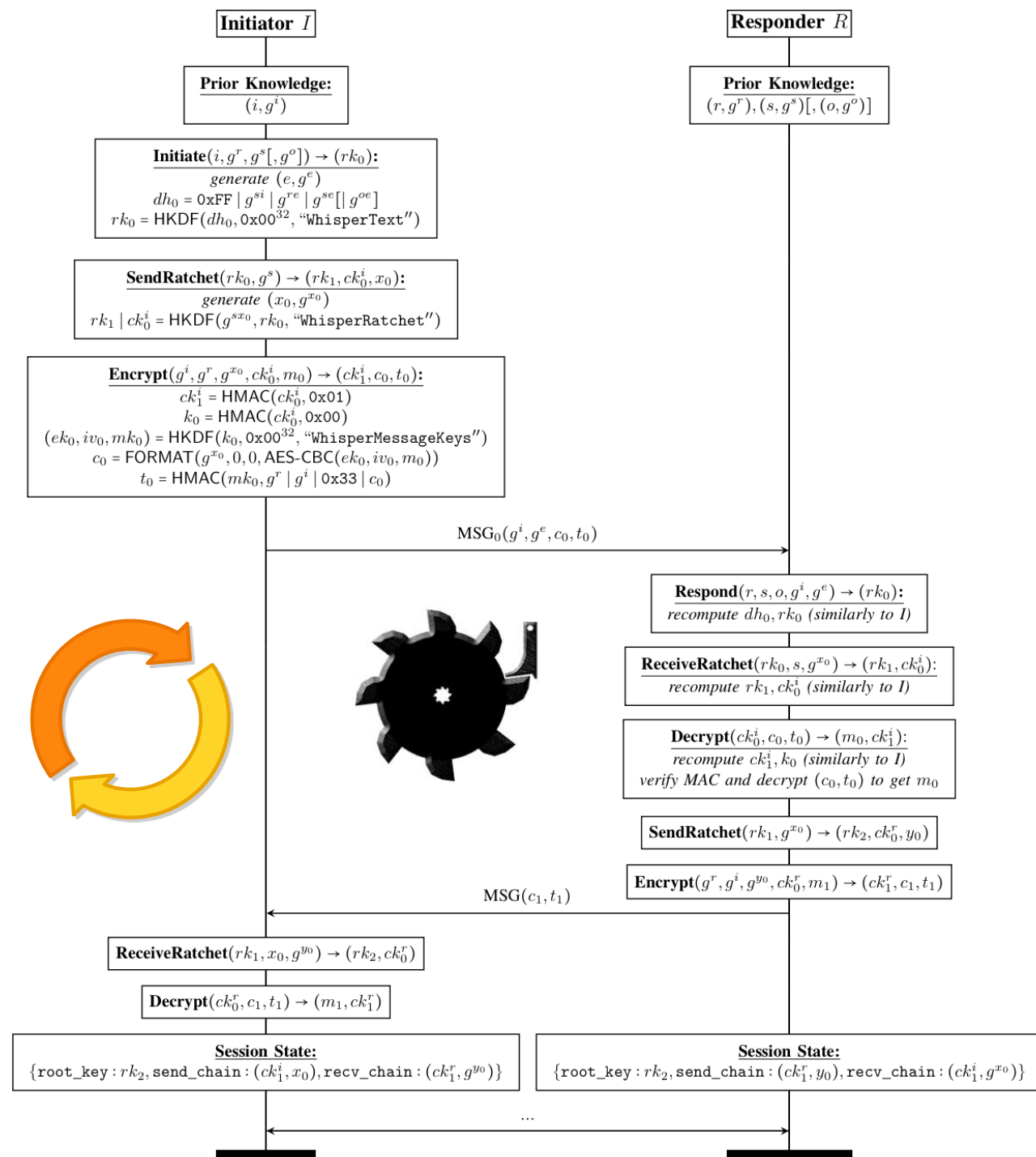
- Existing Analyses

- Using ProVerif and CryptoVerif
- Model X3DH, Double Ratchet
- Few hundred lines written in applied pi calculus



Formalizing Signal

- Existing Analyses
 - Using ProVerif and CryptoVerif
 - Model X3DH, Double Ratchet
 - Few hundred lines written in applied pi calculus
- One major limitation of existing analyses: Proofs for only 3 message rounds due to recursion



Analysis of Security Protocols: Tools

Computational Tools:
CryptoVerif, EasyCrypt, ...

- Focus on cryptographic core
- Messages are bitstrings
- Probabilistic

Symbolic Tools:
ProVerif, Tamarin, RCF, ...

- Abstract cryptography
- Messages are formal terms

Analysis of Security Protocols: Tools

Computational Tools:
CryptoVerif, EasyCrypt, ...

- Focus on cryptographic core
- Messages are bitstrings
- Probabilistic

Symbolic Tools:
ProVerif, Tamarin, RCF, ...

- Abstract cryptography
- Messages are formal terms

Existing Symbolic Approaches and DY*

DY-style tools:
Tamarin, ProVerif, ...

Dependent Types:

Existing Symbolic Approaches and DY*

DY-style tools:
Tamarin, ProVerif, ...

Dependent Types:
RCF, F7, ...

Existing Symbolic Approaches and DY*

DY-style tools:
Tamarin, ProVerif, ...

Dependent Types:
RCF, F7, ...

focus on protocol core

- | | |
|-------------------------------|-------------------------------------|
| ✗ abstract models | ✓ automated analysis |
| ✗ bounded data structures | (potentially some user interaction) |
| ✗ no modularity | ✓ global trace & |
| ✗ limited inductive reasoning | properties |
| ✗ interoperability | ✓ equational theories |

Existing Symbolic Approaches and DY*

DY-style tools:
Tamarin, ProVerif, ...

focus on protocol core

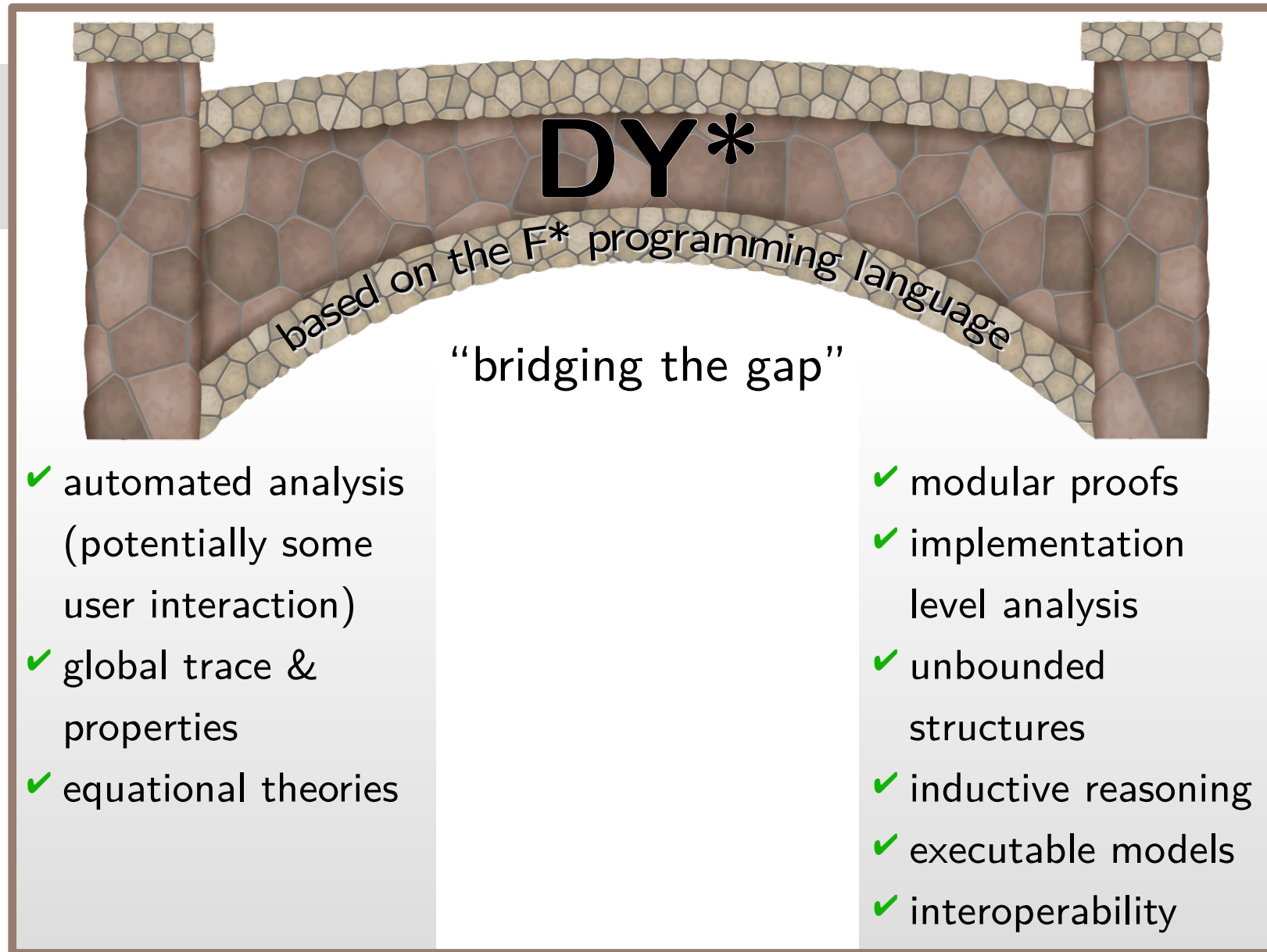
- ✗ abstract models
- ✗ bounded data structures
- ✗ no modularity
- ✗ limited inductive reasoning
- ✗ interoperability
- ✓ automated analysis (potentially some user interaction)
- ✓ global trace & properties
- ✓ equational theories

Dependent Types:
RCF, F7, ...

focus on
implementation aspects

- ✓ modular proofs
- ✓ implementation level analysis
- ✓ unbounded structures
- ✓ inductive reasoning
- ✓ executable models
- ✓ interoperability
- ✗ missing global view
- ✗ limited expressivity w.r.t. security prop.
- ✗ limited support for mutable state
- ✗ less automation
- ✗ no equational theories (e.g., DH)

Existing Symbolic Approaches and DY*



DY-style tools:
Tamarin, ProVerif, ...

focus on protocol core

- ✗ abstract models
- ✗ bounded data structures
- ✗ no modularity
- ✗ limited inductive reasoning
- ✗ interoperability

Dependent Types:
RCF, F7, ...

focus on
implementation aspects

- ✗ missing global view
- ✗ limited expressivity w.r.t. security prop.
- ✗ limited support for mutable state
- ✗ less automation
- ✗ no equational theories (e.g., DH)

What is F*?

- **Functional programming language** aimed at program verification
 - Can be used to precisely express strong (security) properties
- Developed and actively supported by **Microsoft Research, INRIA**, and others
- Already used for computational protocol analysis (for example, parts of **TLS 1.3**)
- Rich, versatile **type system**
 - Dependent and refinement types
 - Backed by SMT-Solver Z3
 - Pre/post conditions
 - Allow modeling unbounded and recursive data structures



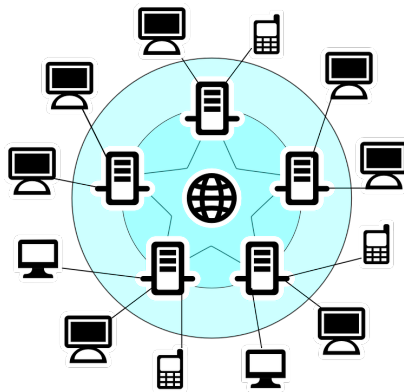
Dolev-Yao* (DY*): Architecture

Append-only log that captures relevant interaction with the framework.

Runtime Model



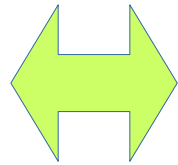
Crypto



Network
Communication



Application
State



Global Trace

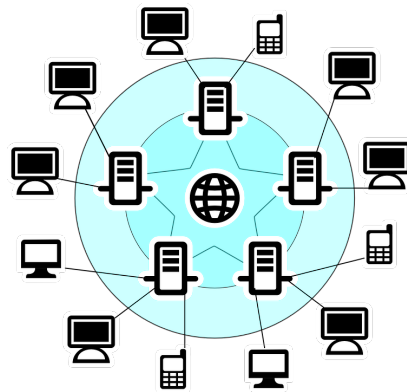
Dolev-Yao* (DY*): Architecture

Append-only log that captures relevant interaction with the framework.

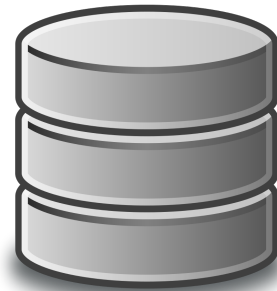
Runtime Model



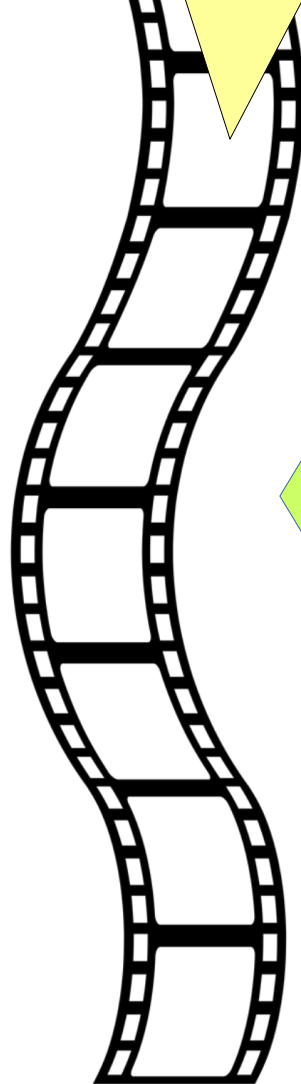
Crypto



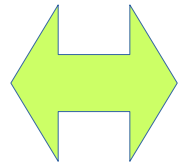
Network
Communication



Application
State



Global Trace



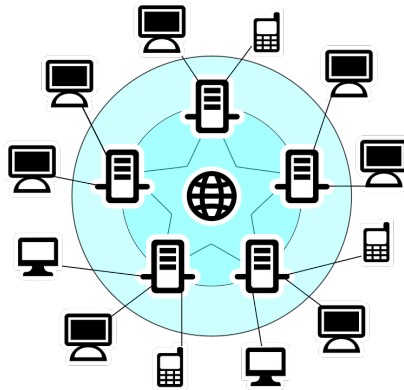
Dolev-Yao* (DY*): Architecture

Append-only log that captures relevant interaction with the framework.

Runtime Model



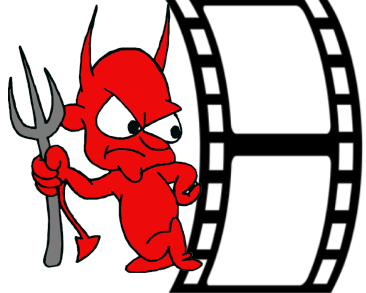
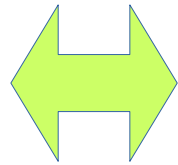
Crypto



Network
Communication



Application
State



Global Trace

Dolev-Yao* (DY*): Architecture

Append-only log that captures relevant interaction with the framework.

Runtime Model

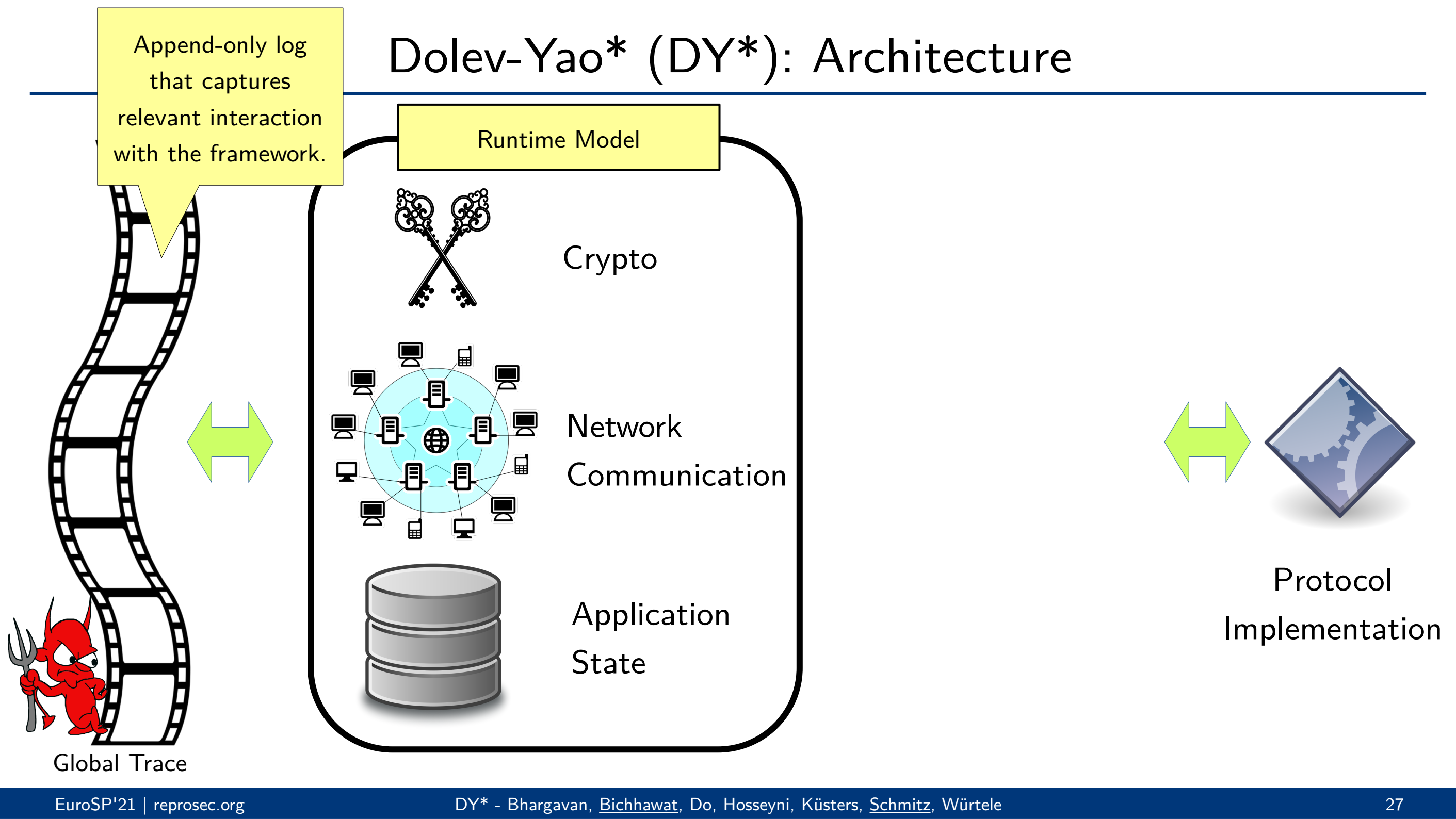
Crypto

Network Communication

Application State

Protocol Implementation

Global Trace



Dolev-Yao* (DY*): Architecture

Append-only log that captures relevant interaction with the framework.

Runtime Model

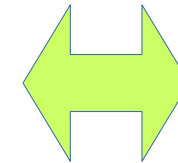
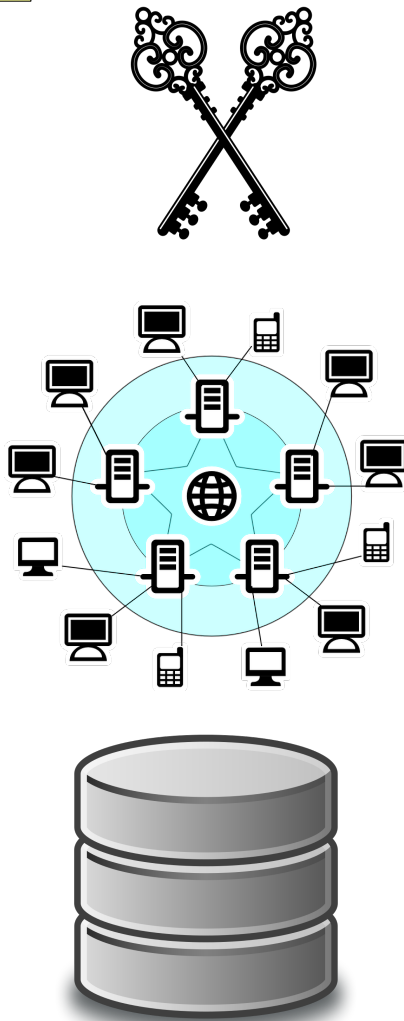
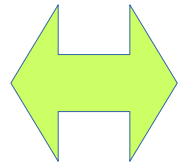
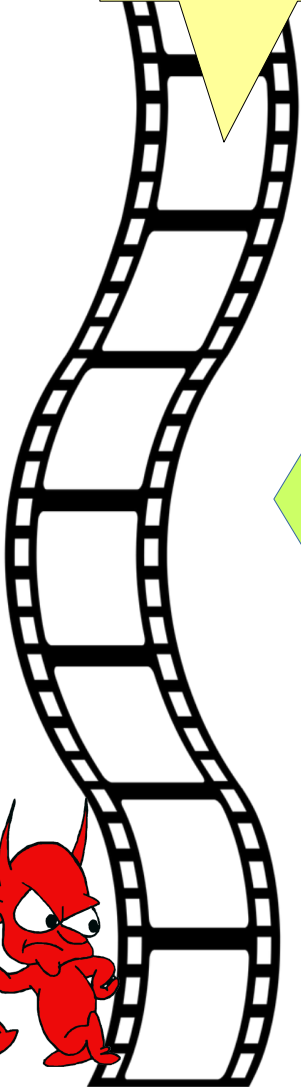
Crypto

Network Communication

Application State

Protocol Implementation

Global Trace

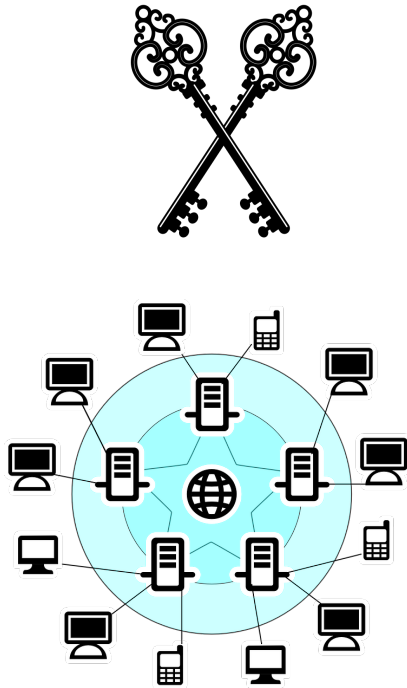


Dolev-Yao* (DY*): Architecture

Append-only log that captures relevant interaction with the framework.

Runtime Model

Labeling Layer



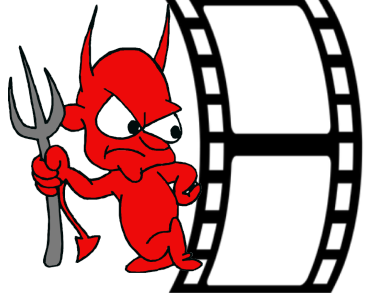
Crypto

Network Communication

Application State

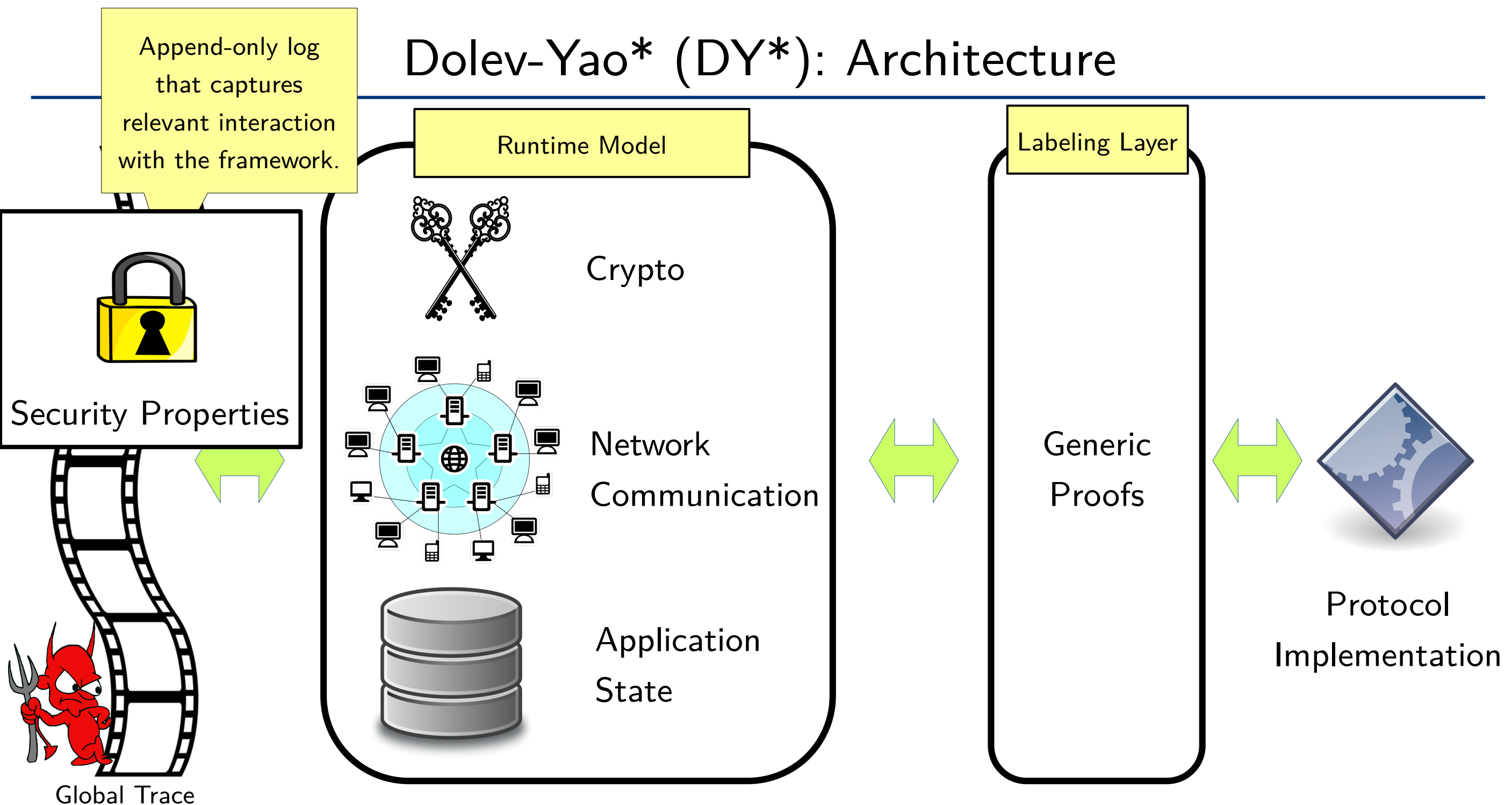
Generic Proofs

Protocol Implementation

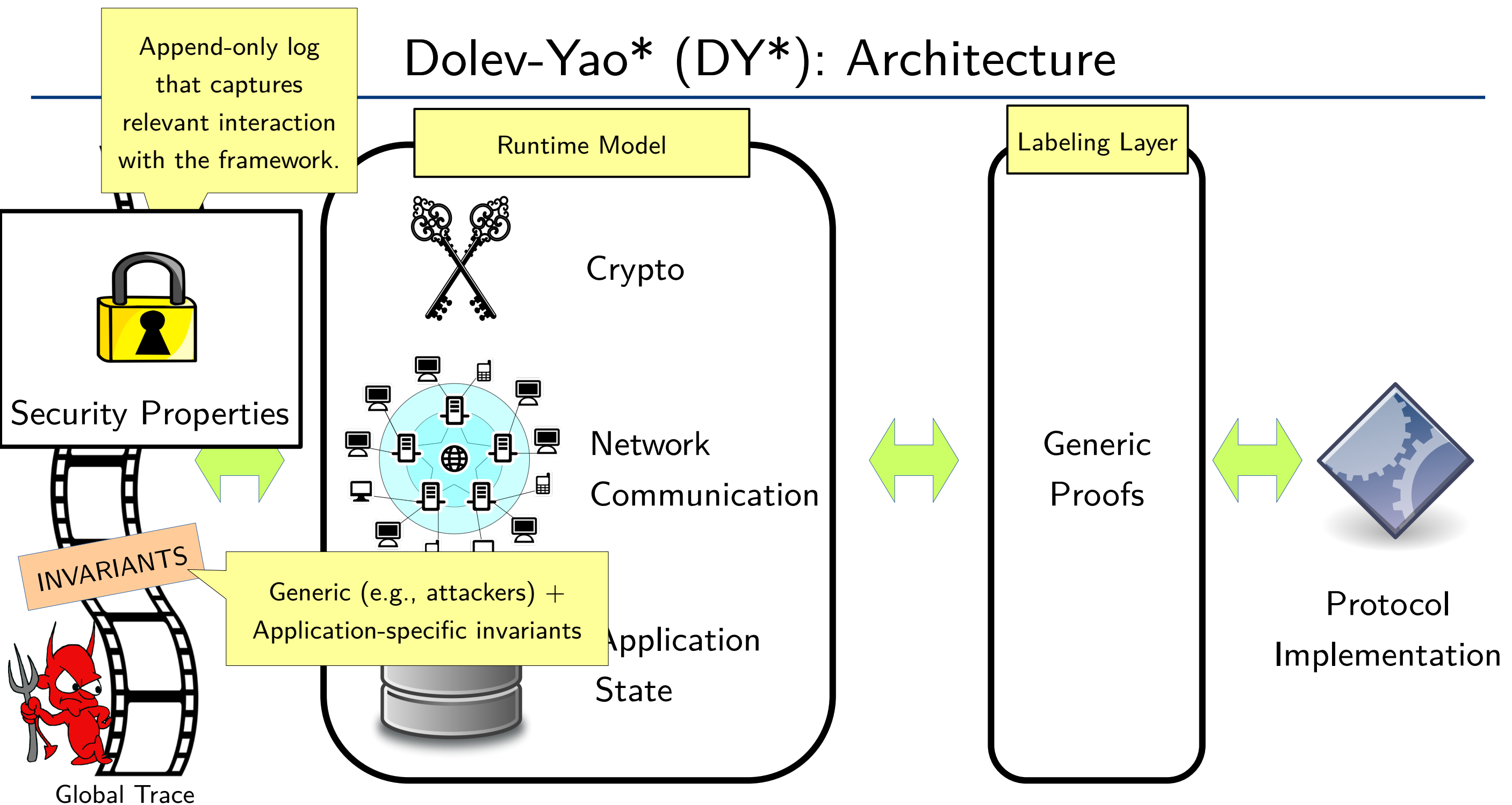


Global Trace

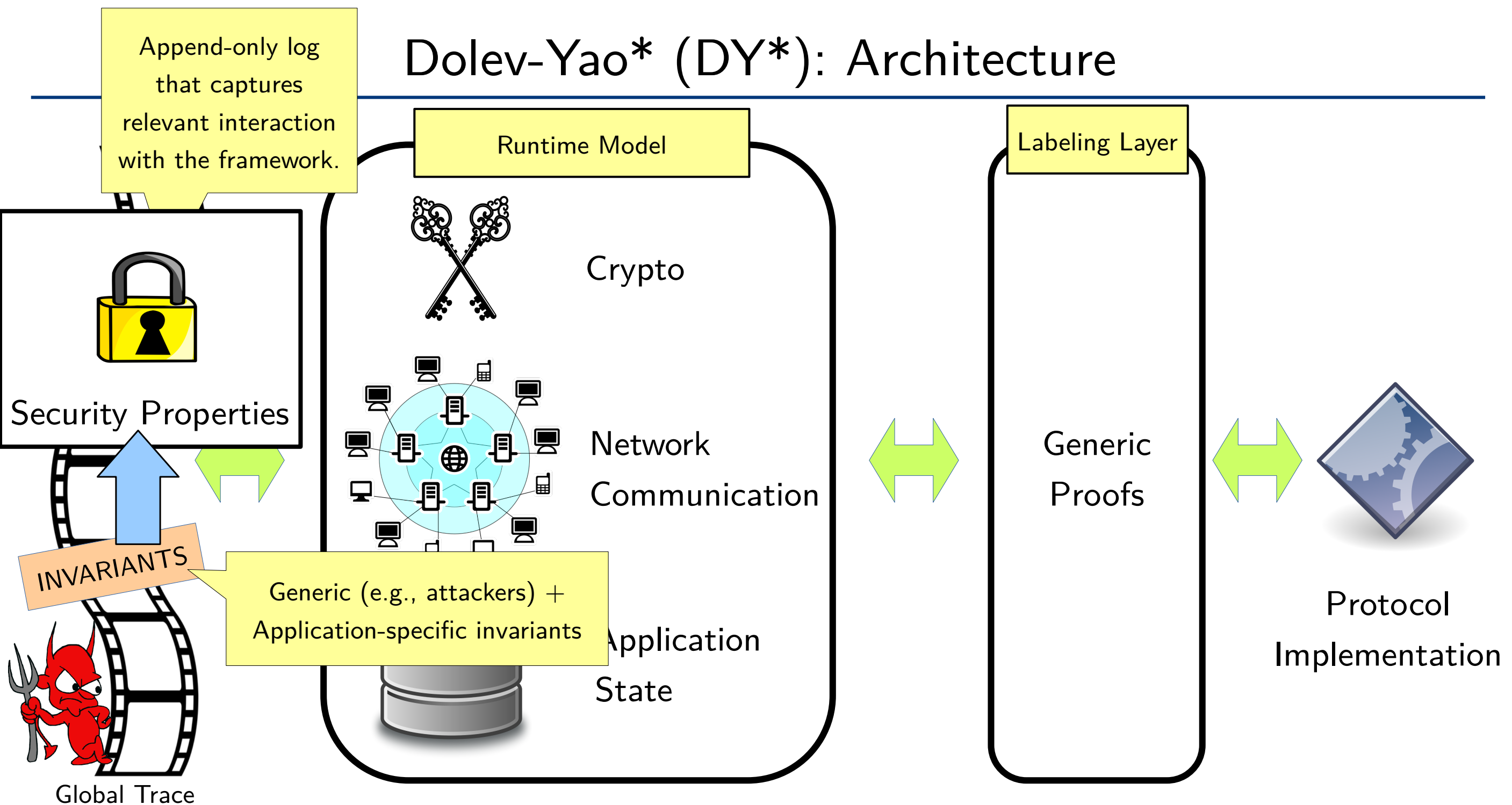
Dolev-Yao* (DY*): Architecture



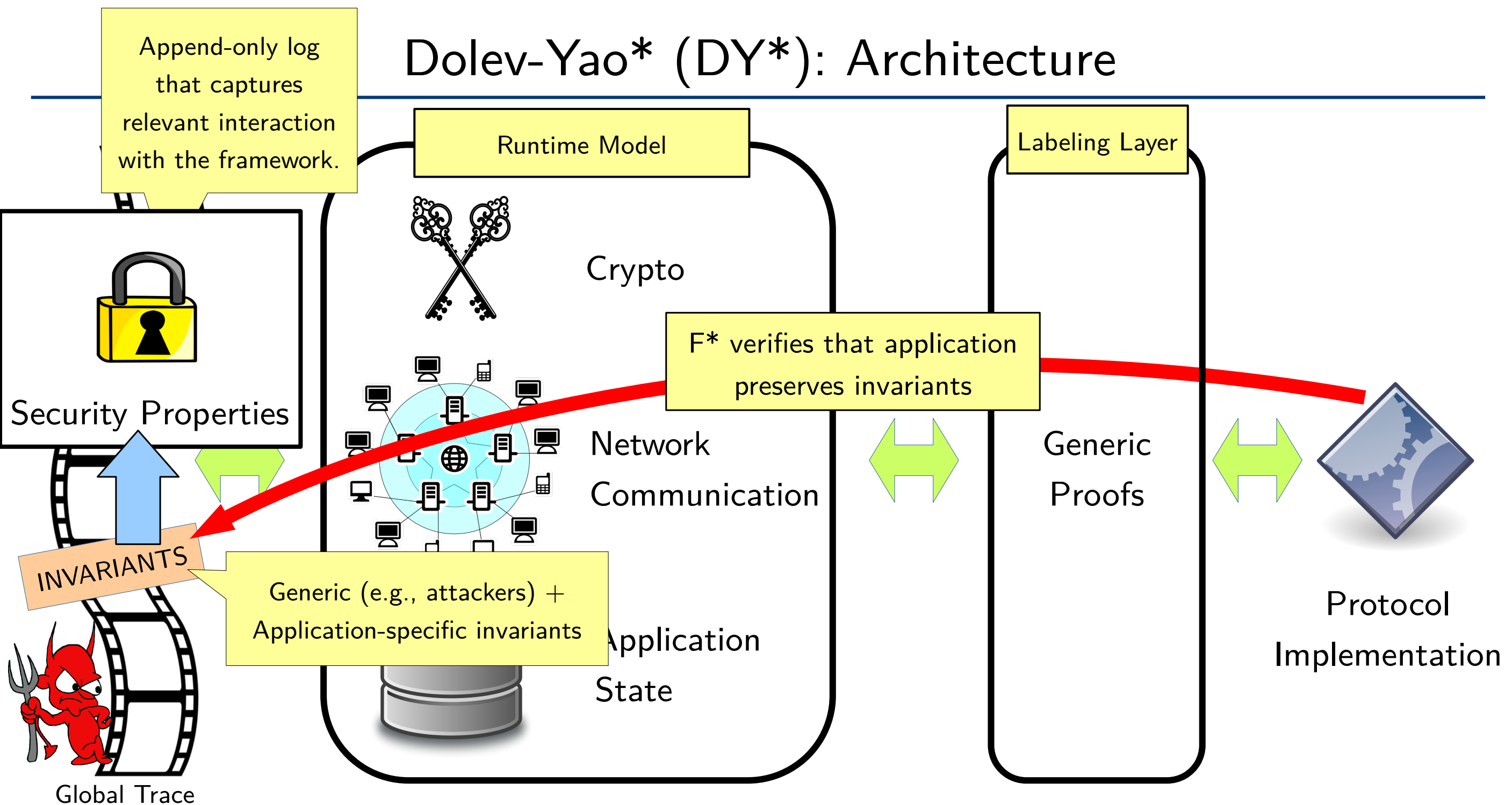
Dolev-Yao* (DY*): Architecture



Dolev-Yao* (DY*): Architecture



Dolev-Yao* (DY*): Architecture



Case Studies

- Signal Messaging Protocol



Signal

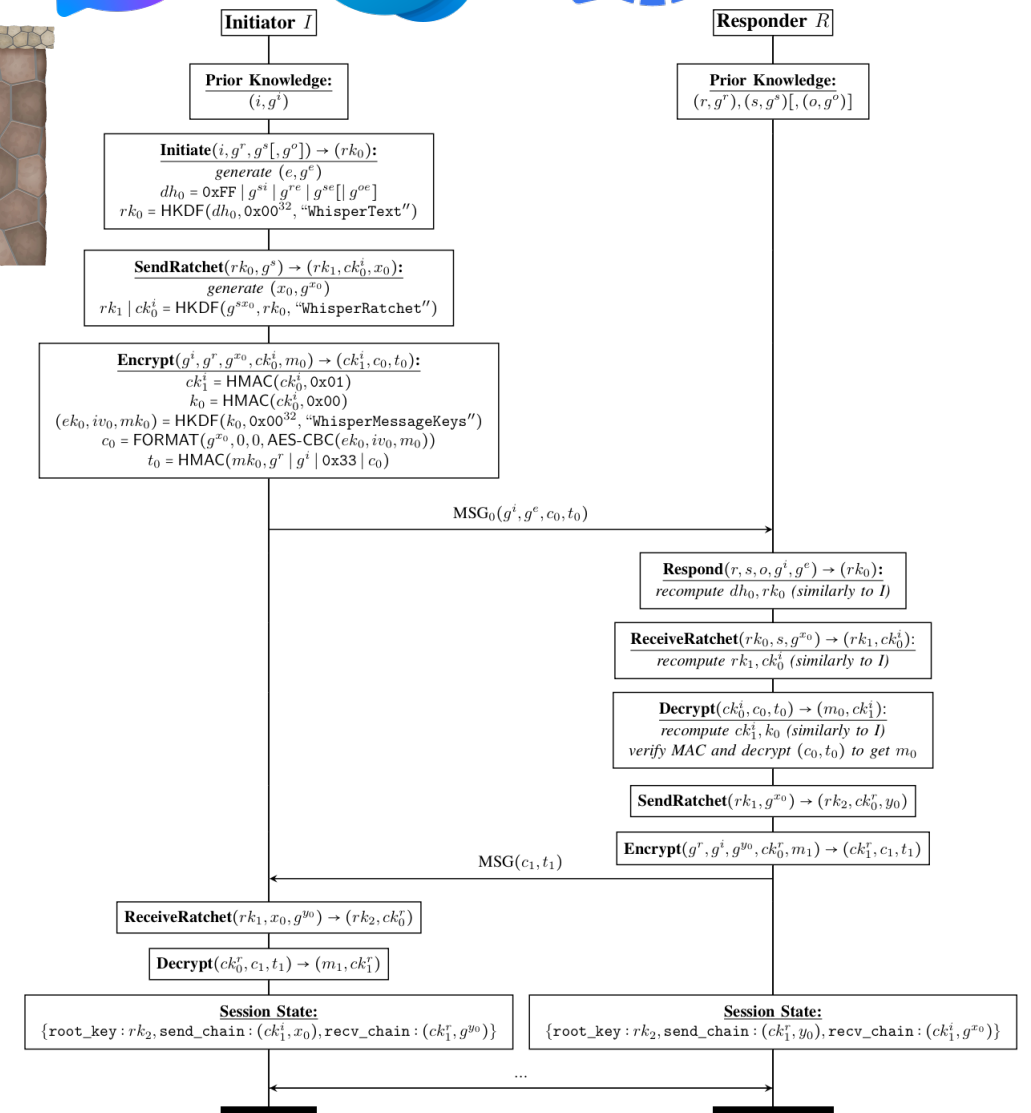
Signal Messaging Protocol

- First mechanized proof accounting for
 - Forward Secrecy
 - Post-compromise Security
 - Unbounded number of protocol rounds



at the same time

- First type-based formulation and proof of post-compromise security for any protocol
- First analysis of Signal based on dependent types



Case Studies

- Signal Messaging Protocol

- Unbounded number of rounds (ratcheting)
- Forward Secrecy & Post Compromise Security



Signal

- Needham-Schroeder(-Lowe), ISO-DH, and ISO-KEM

Conclusion & Future Work

- **Golden era** of cryptographic protocols
- We recently proposed DY*, a **new mechanized symbolic verification framework** for protocols and their code



- Overcomes many limitations of existing tools
- Precise reasoning on global properties
- Account for low-level protocol details
- Protocol models can even be interoperable

Conclusion & Future Work

- **Golden era** of cryptographic protocols
- We recently proposed DY*, a **new mechanized symbolic verification framework** for protocols and their code



- Overcomes many limitations of existing tools
- Precise reasoning on global properties
- Account for low-level protocol details
- Protocol models can even be interoperable

- **Lots of interesting work to be done!**

- Equivalence properties
- Computational analysis
- WIM*: mechanize the **Web Infrastructure Model**

See [S&P '14, ESORICS '15, CCS '15, CCS '16, CSF '17, S&P '19]

Conclusion & Future Work

- **Golden era** of cryptographic protocols
- We recently proposed DY*, a **new mechanized symbolic verification framework** for protocols and their code



- Overcomes many limitations of existing tools
- Precise reasoning on global properties
- Account for low-level protocol details
- Protocol models can even be interoperable

- **Lots of interesting work to be done!**

- Equivalence properties
- Computational analysis
- WIM*: mechanize the **Web Infrastructure Model**

See [S&P '14, ESORICS '15, CCS '15, CCS '16, CSF '17, S&P '19]

Find more information on: **reprosec.org**

Thank you!