University of Stuttgart
Institute of
Information Security

Carnegie Mellon University

Inria

Indian Institute of Technology Gandhinagar

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

EuroSP'21 | reprosec.org

SEC

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

Cryptographic Protcols 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 Protcols 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, W3C Web Payments, ...
- Post-Quantum Crypto: NIST KEMs, Signature, ...
- Lightweight Crypto: IETF LAKE, NIST LWC

Cryptographic Protcols are Everywhere: Golden Era of Crypto

COMPUTERWORLD UNITED STATES

NEWS

EMV flaw allows 'pre... payment cards

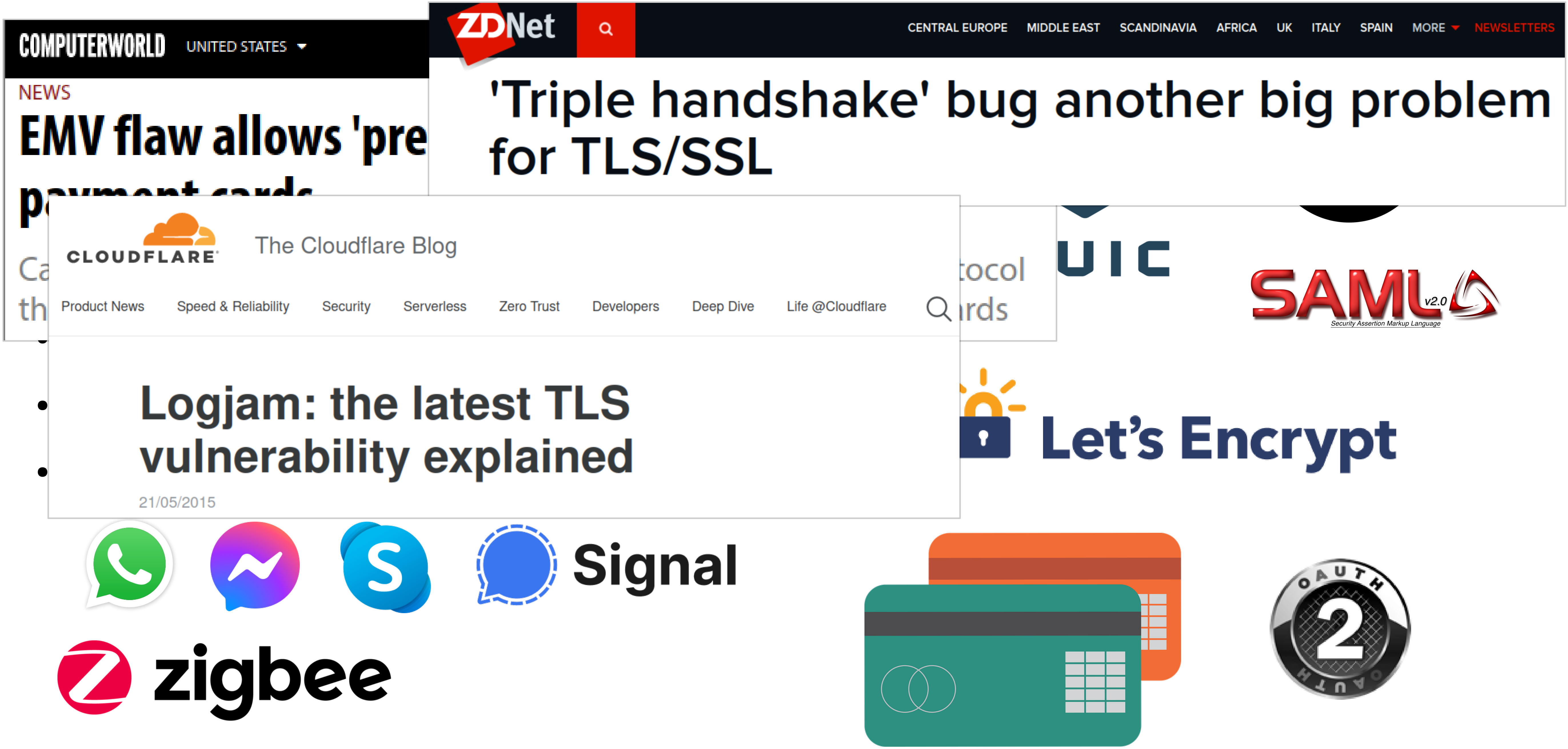
Cambridge university researchers find weaknesses in the EMV protocol that can facilitate cloning-like attacks for chip-and-PIN payment cards

ZDNet — CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS

'Triple handshake' bug another big problem for TLS/SSL

- Payment: EMV, W3C Web Payments, ...
- Post-Quantum Crypto: NIST KEMs, Signature, ...
- Lightweight Crypto: IETF LAKE, NIST LWC

Cryptographic Protcols are Everywhere: Golden Era of Crypto



Cryptographic Protcols are Everywhere: Golden Era of Crypto

COMPUTERWORLD UNITED STATES

NEWS

EMV flaw allows 'pre
payment cards

ZDNet

'Triple hand
for TLS/SSL

The Cloudflare Blog

Product News | Speed & Reliability | Security | Serverless | Zero Trust | Developers | Deep Dive

Logjam: the latest TLS vulnerability explained

21/05/2015

SearchSecurity

PIXEL_DREAMS - FOTOLIA

NEWS

OAuth vulnerabilities must be fixed in the standard

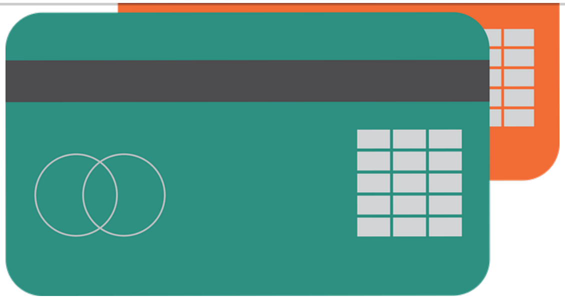
Researchers in Germany have found two OAuth vulnerabilities, which could allow attackers to break the authorization and authentication standard. And an expert said the fix must be made to the standard itself.

By Michael Heller, Senior Reporter

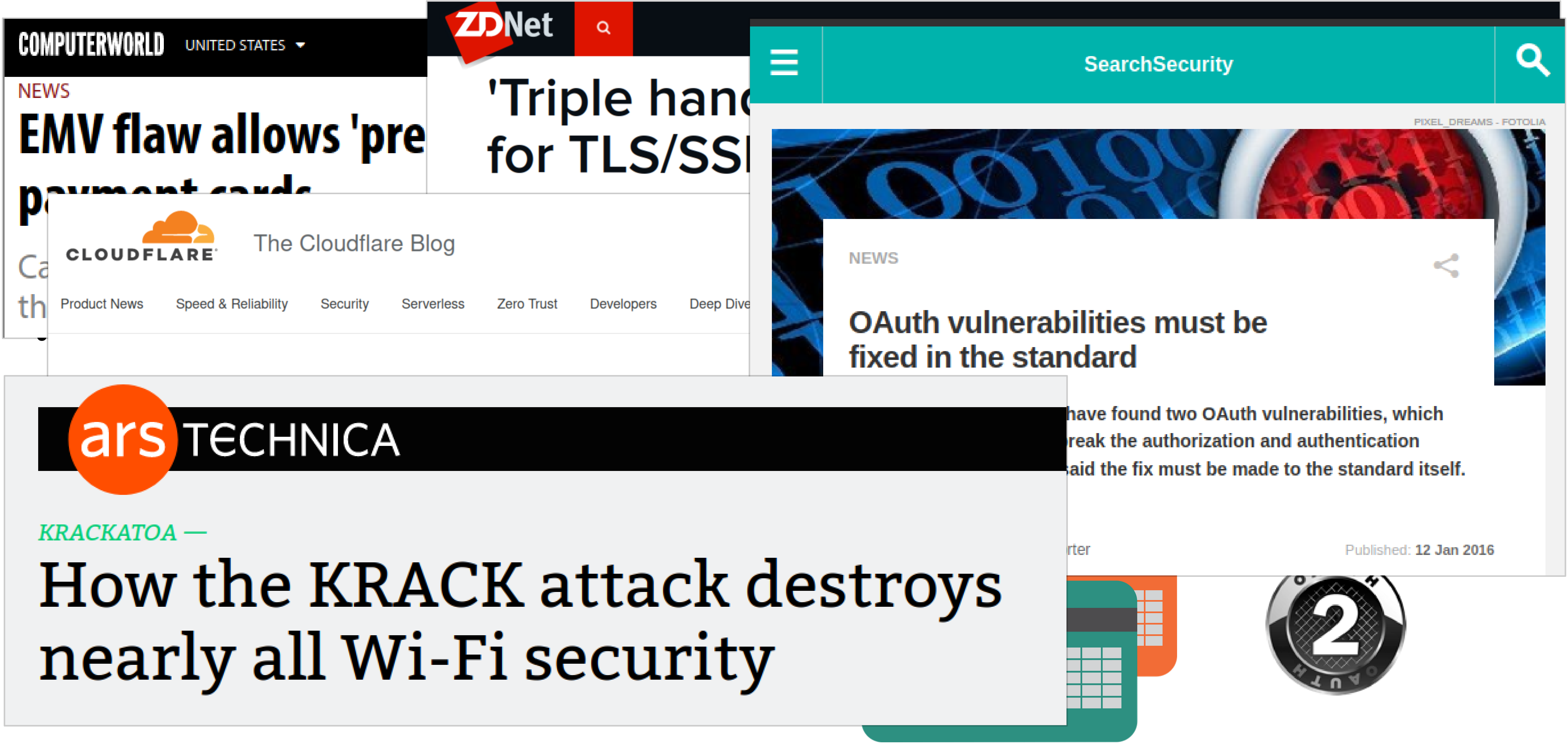
Published: 12 Jan 2016

Signal

zigbee



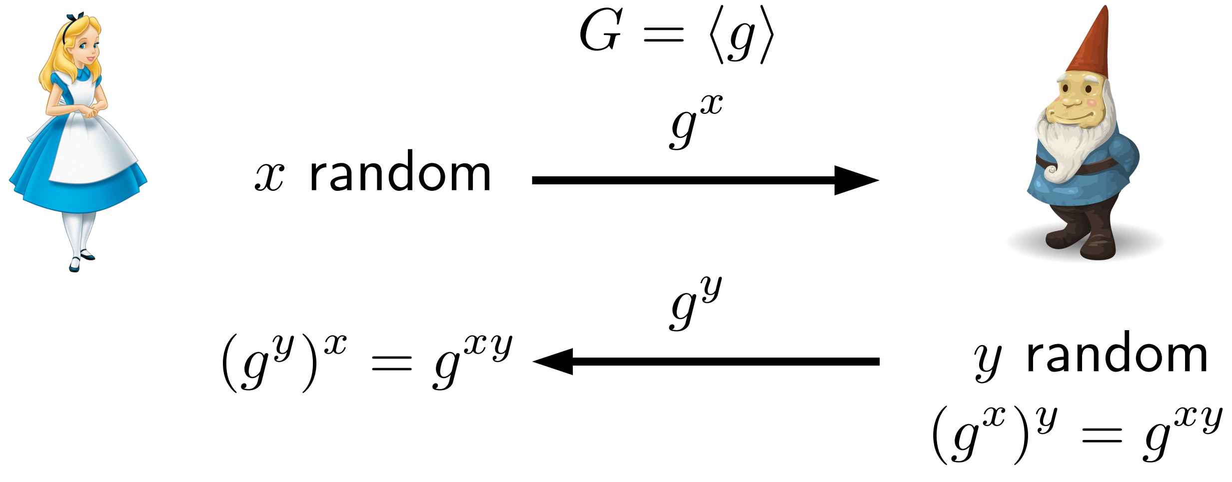
Cryptographic Protcols are Everywhere: Golden Era of Crypto



Signal Messaging Protocol

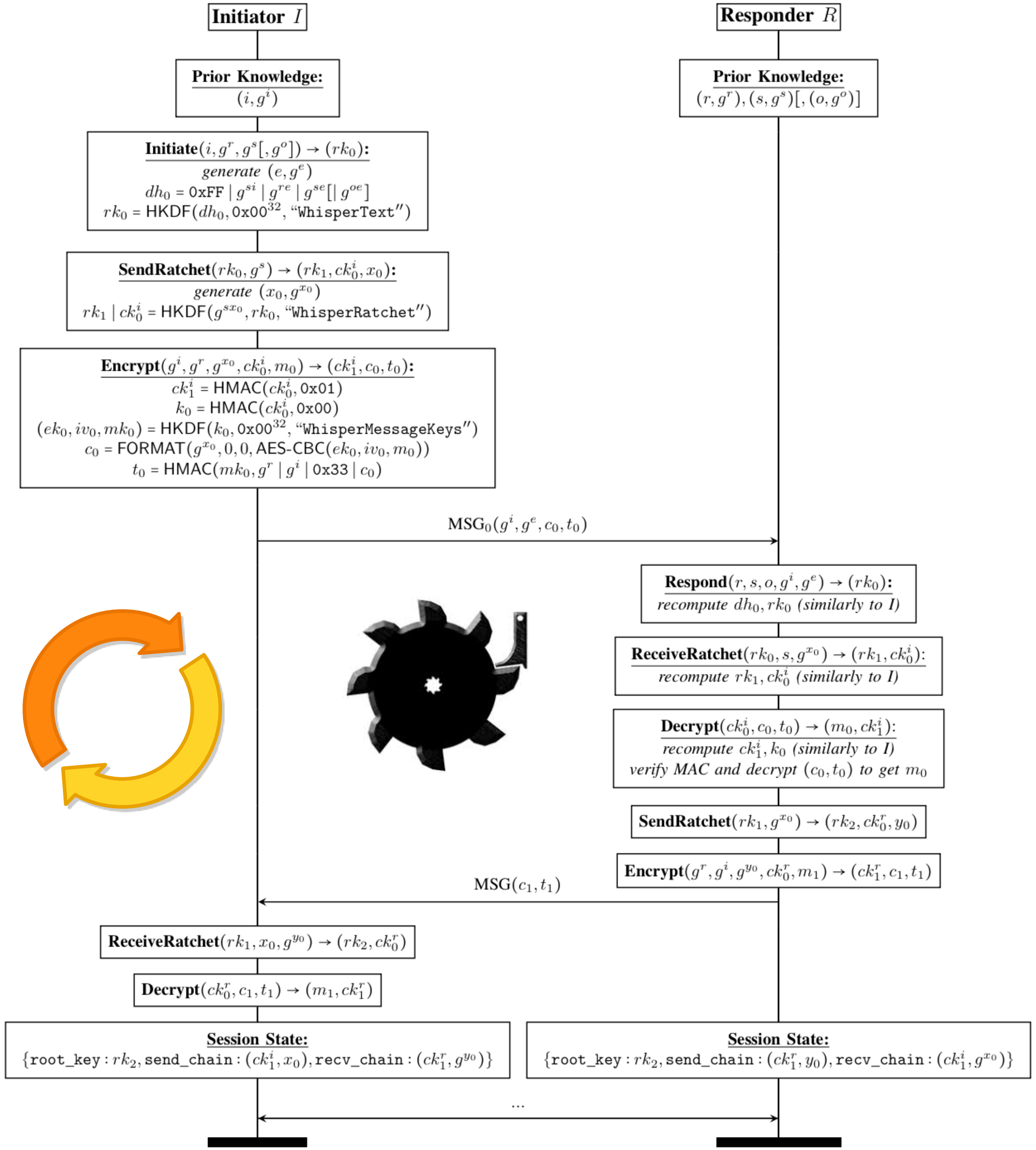
- Asynchronous continuous key exchange

Signal



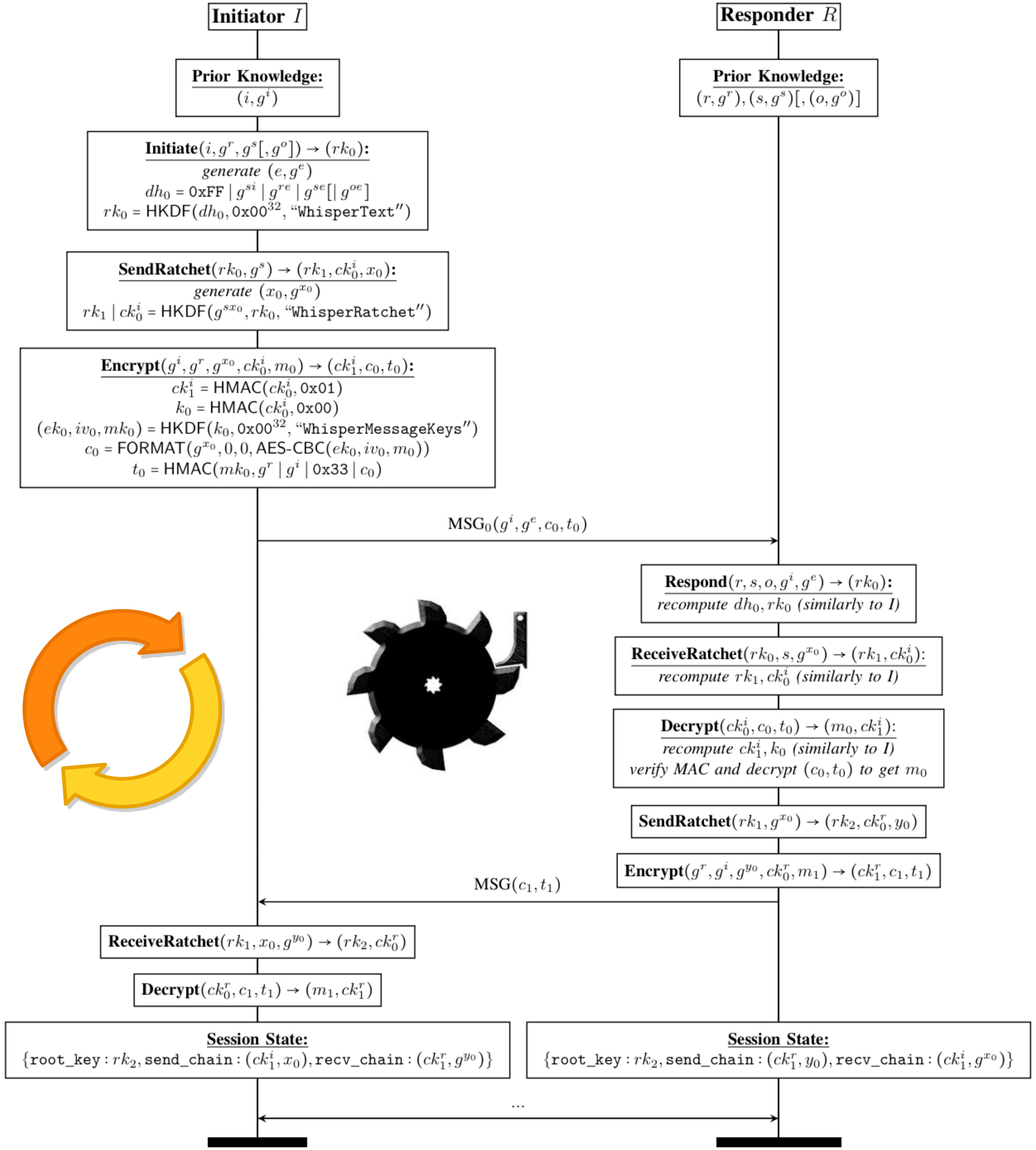
Signal Messaging Protocol

- Asynchronous continuous key exchange



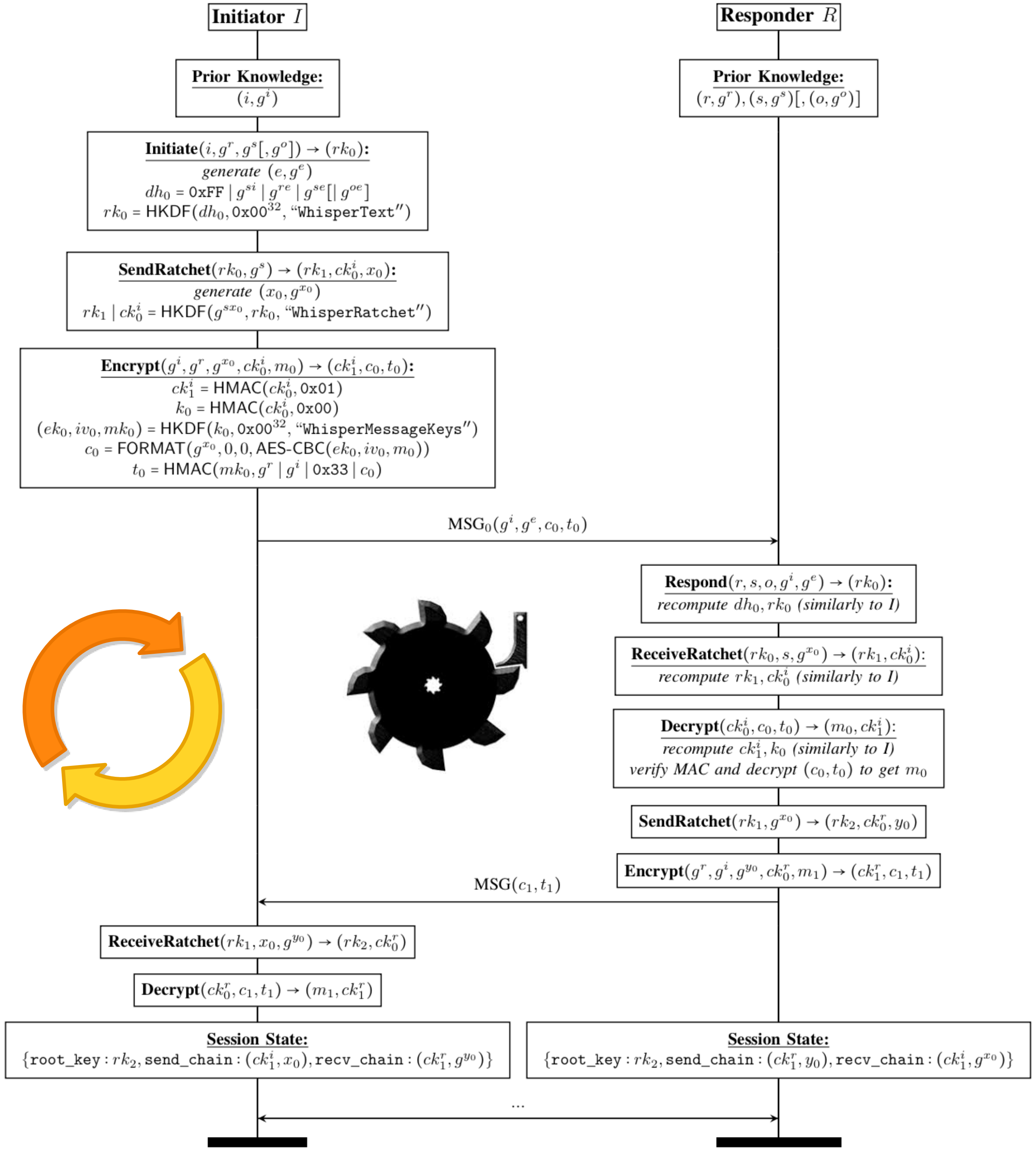
Signal Messaging Protocol

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



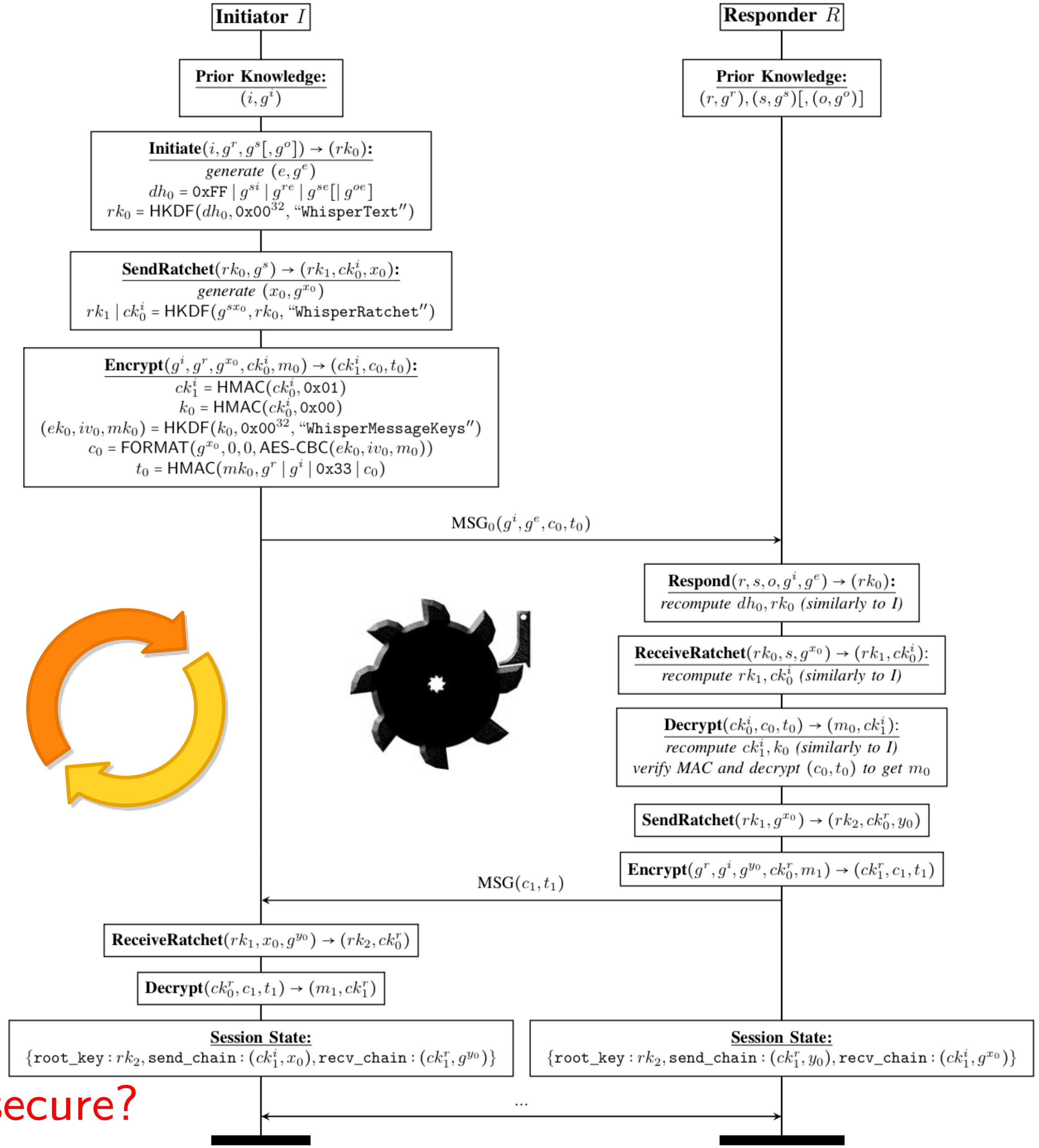
Signal Messaging Protocol

- 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



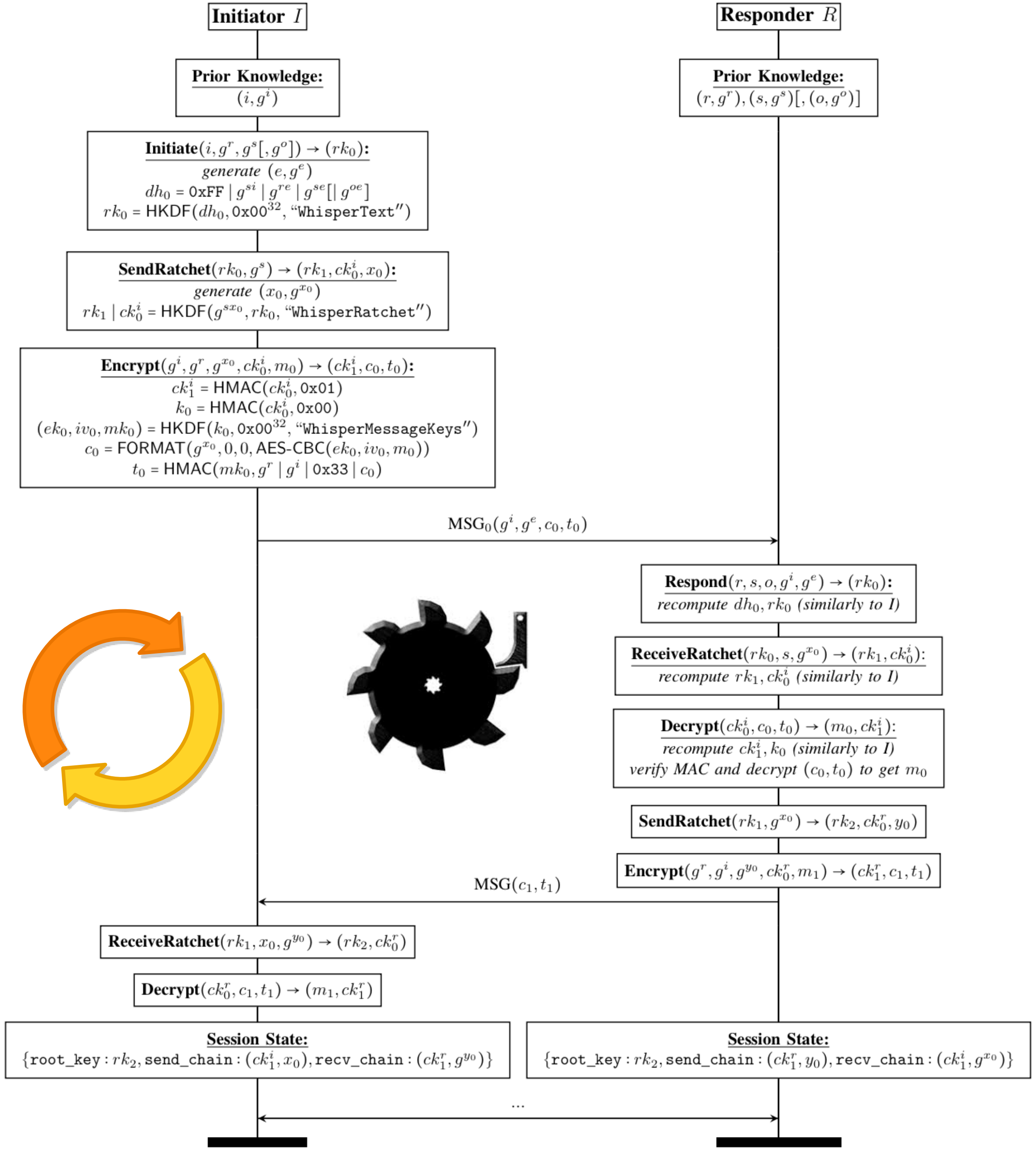
Signal Messaging Protocol

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



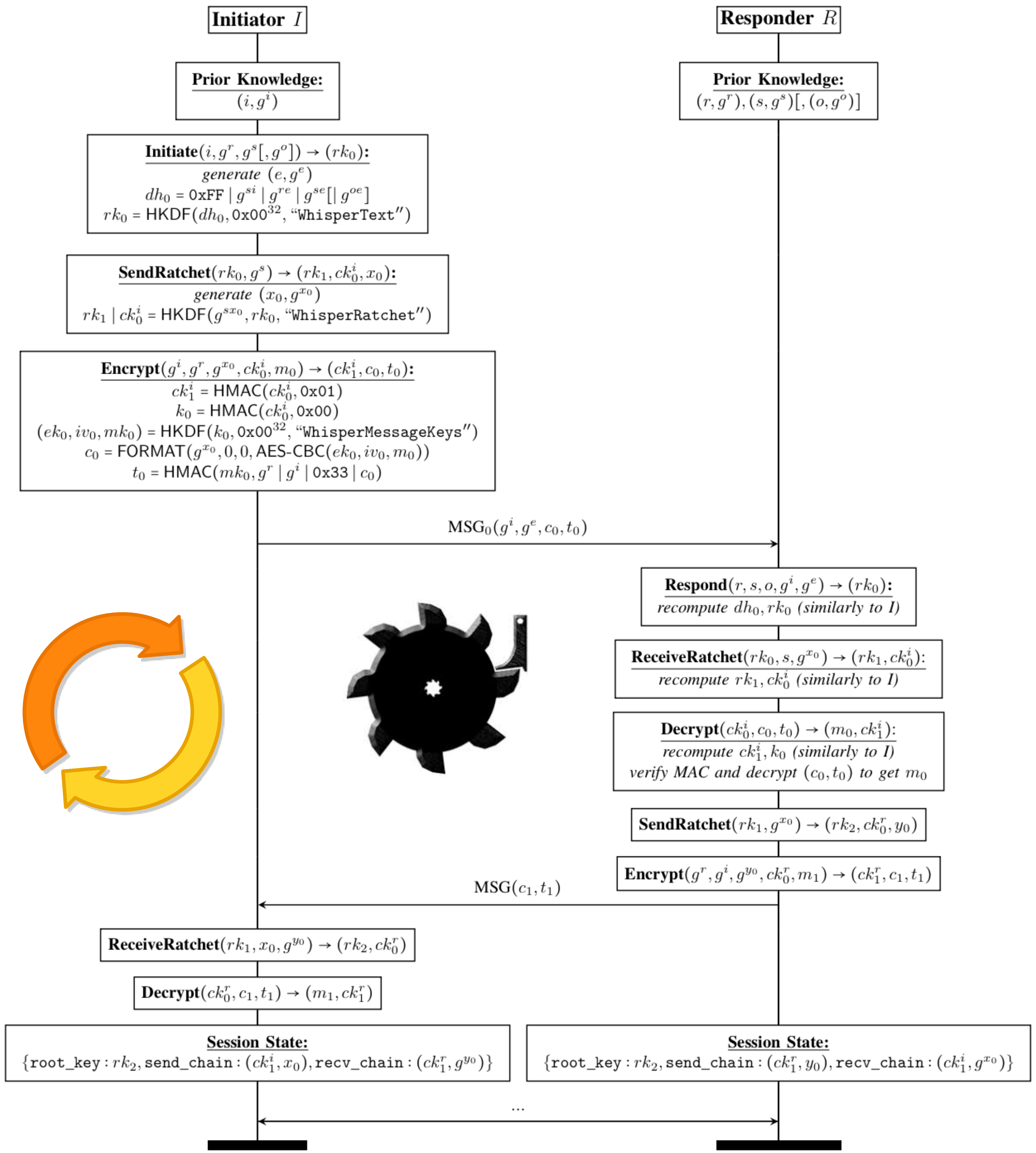
- Inherently recursive
  - Security of each message depends on a chain of derived keys
- Can we mechanically verify that the protocol is secure?

Formalizing Signal



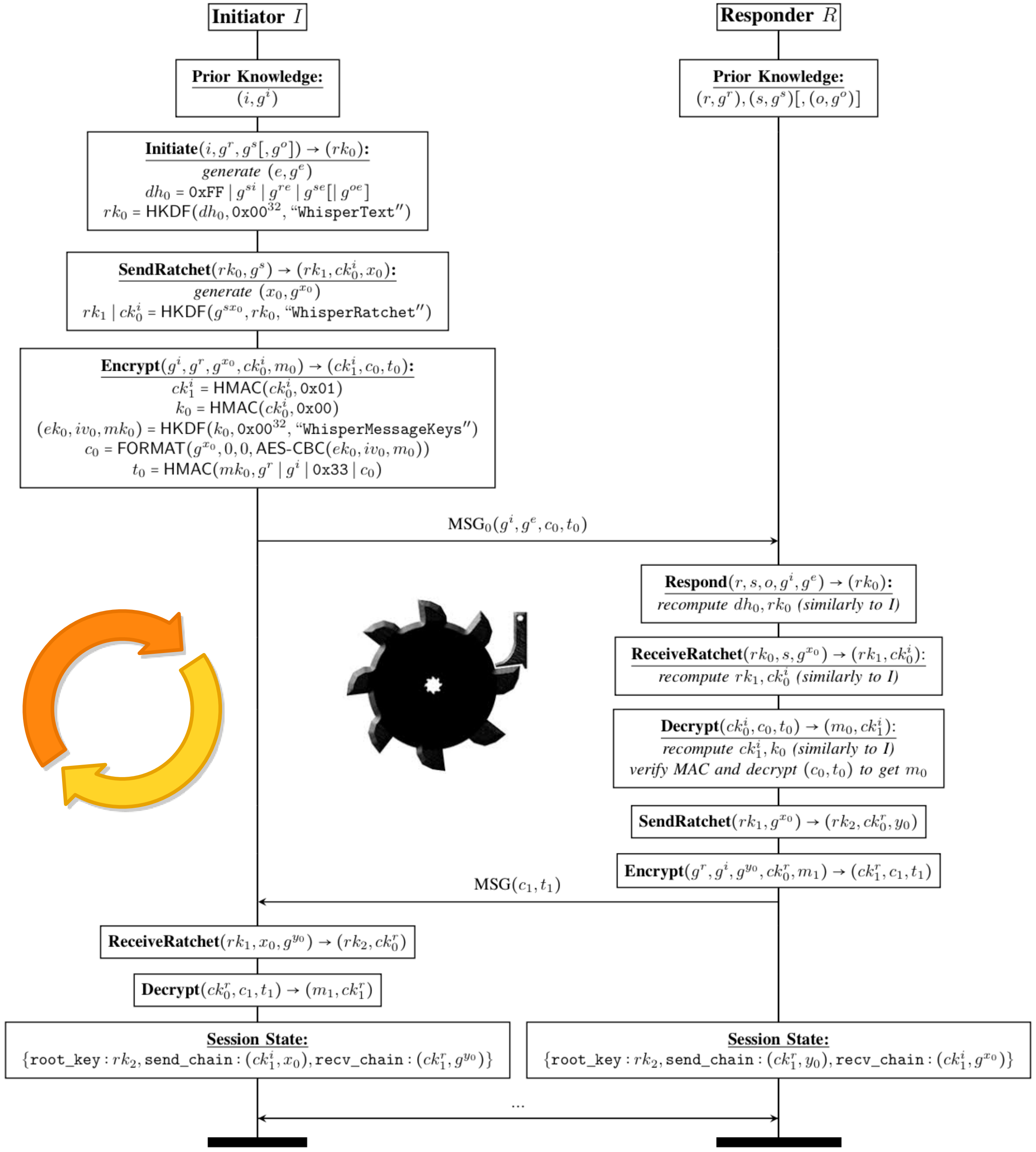
Formalizing Signal

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

- ✔ automated analysis (potentially some user interaction)
- ✔ global trace & properties
- ✔ 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

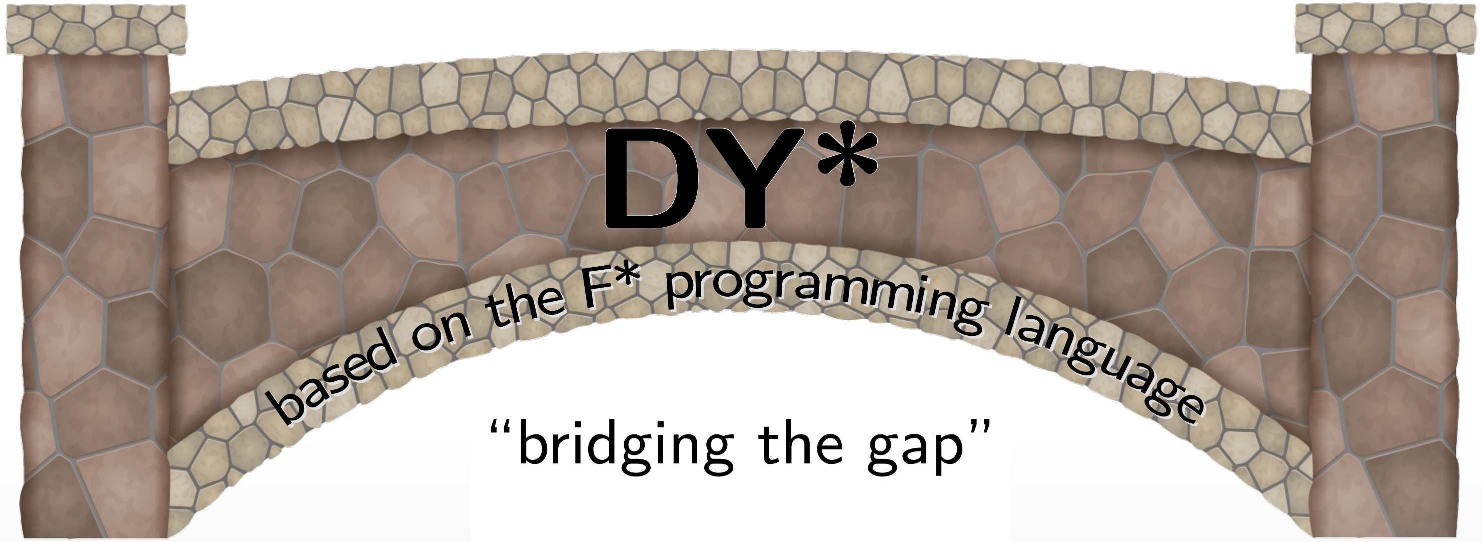
Dependent Types:
RCF, F7, ...

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*



"bridging the gap"

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

focus on protocol core

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

DY* (from DY-style tools):

- ✔ automated analysis (potentially some user interaction)
- ✔ global trace & properties
- ✔ equational theories

DY* (from dependent types):

- ✔ modular proofs
- ✔ implementation level analysis
- ✔ unbounded structures
- ✔ inductive reasoning
- ✔ executable models
- ✔ interoperability

Dependent Types: RCF, F7, ...

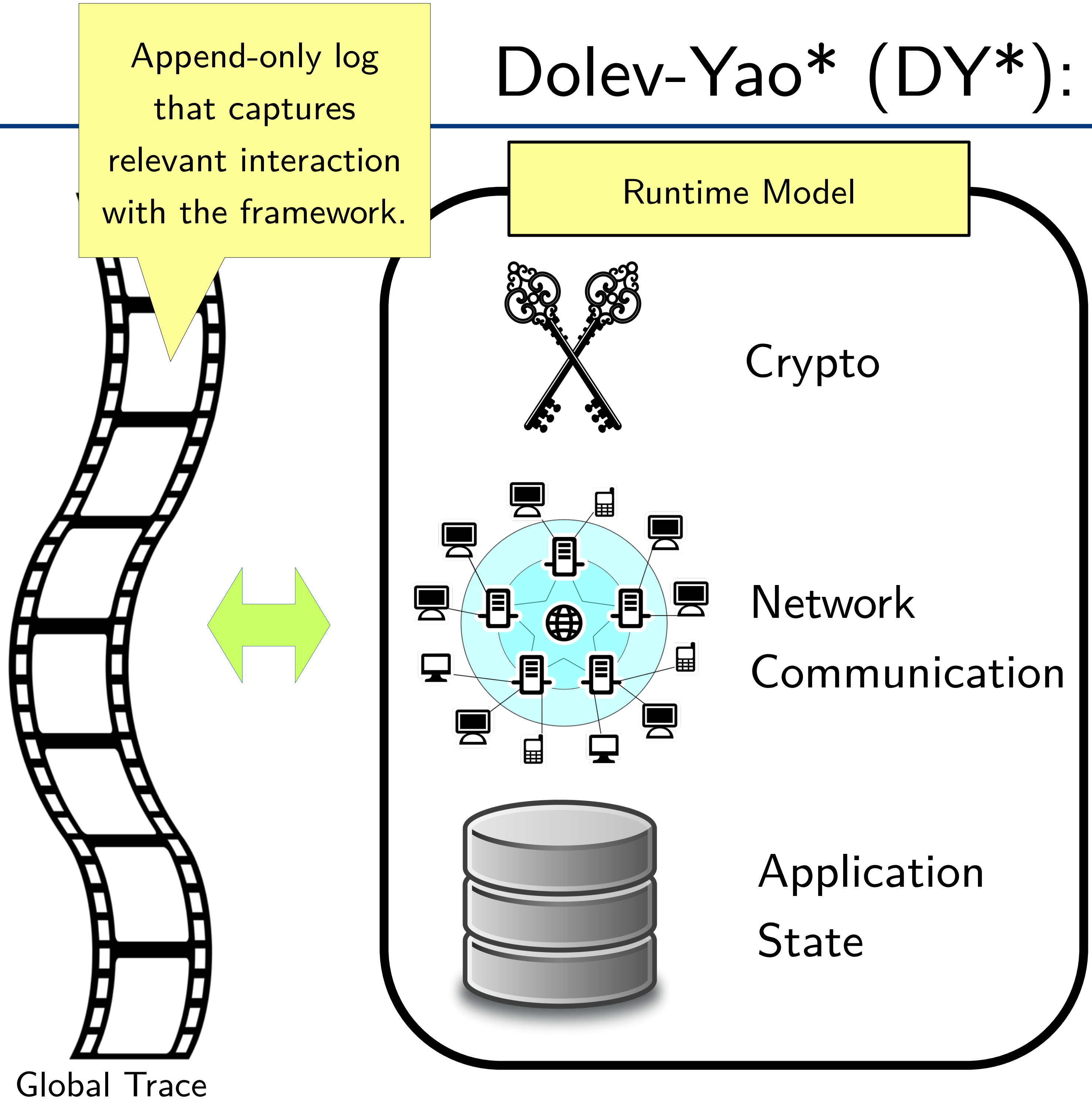
focus on implementation aspects

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

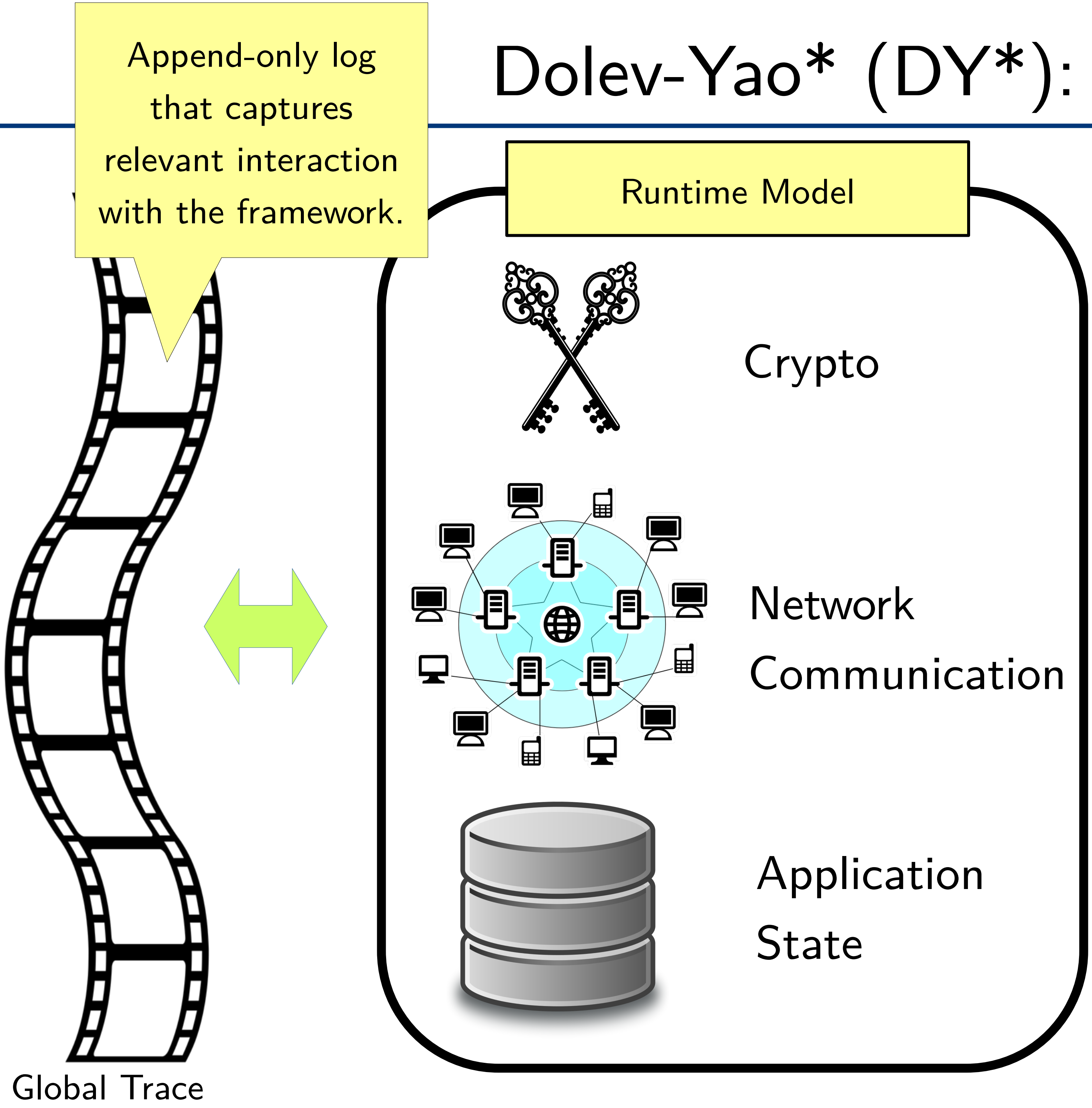
What is F*?

- 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

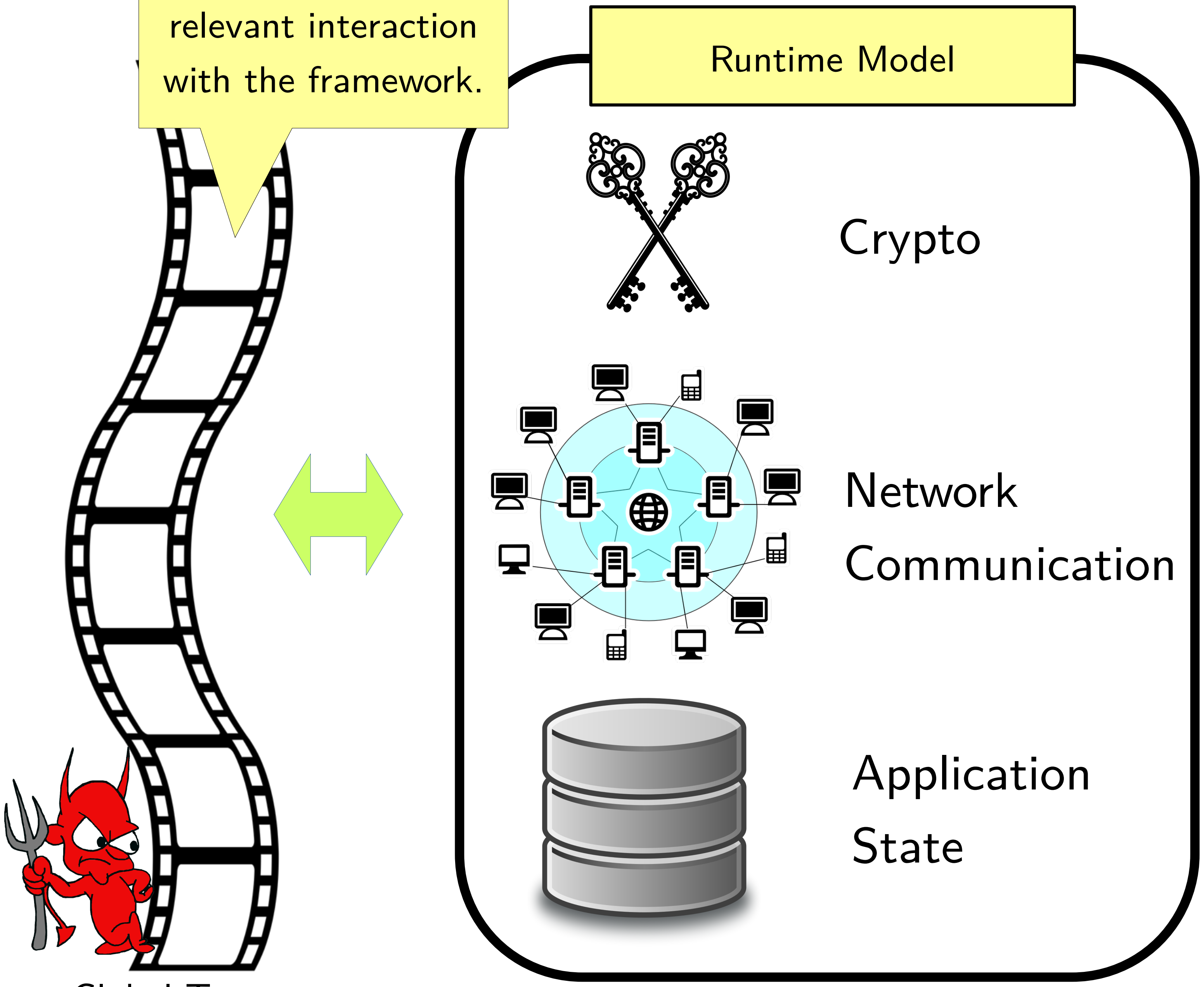


Dolev-Yao* (DY*): Architecture



Dolev-Yao* (DY*): Architecture

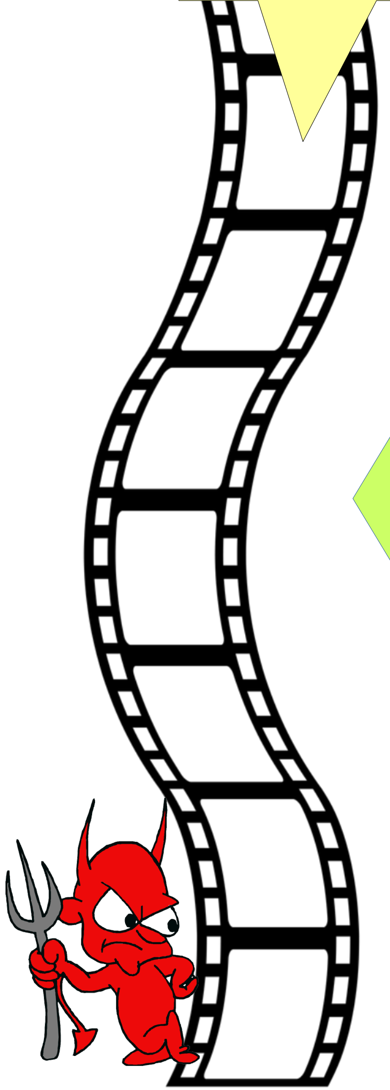
Append-only log that captures relevant interaction with the framework.



Global Trace

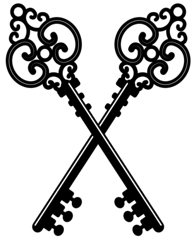
Dolev-Yao* (DY*): Architecture

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

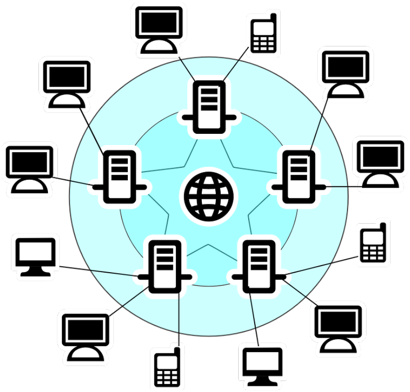


Global Trace

Runtime Model



Crypto

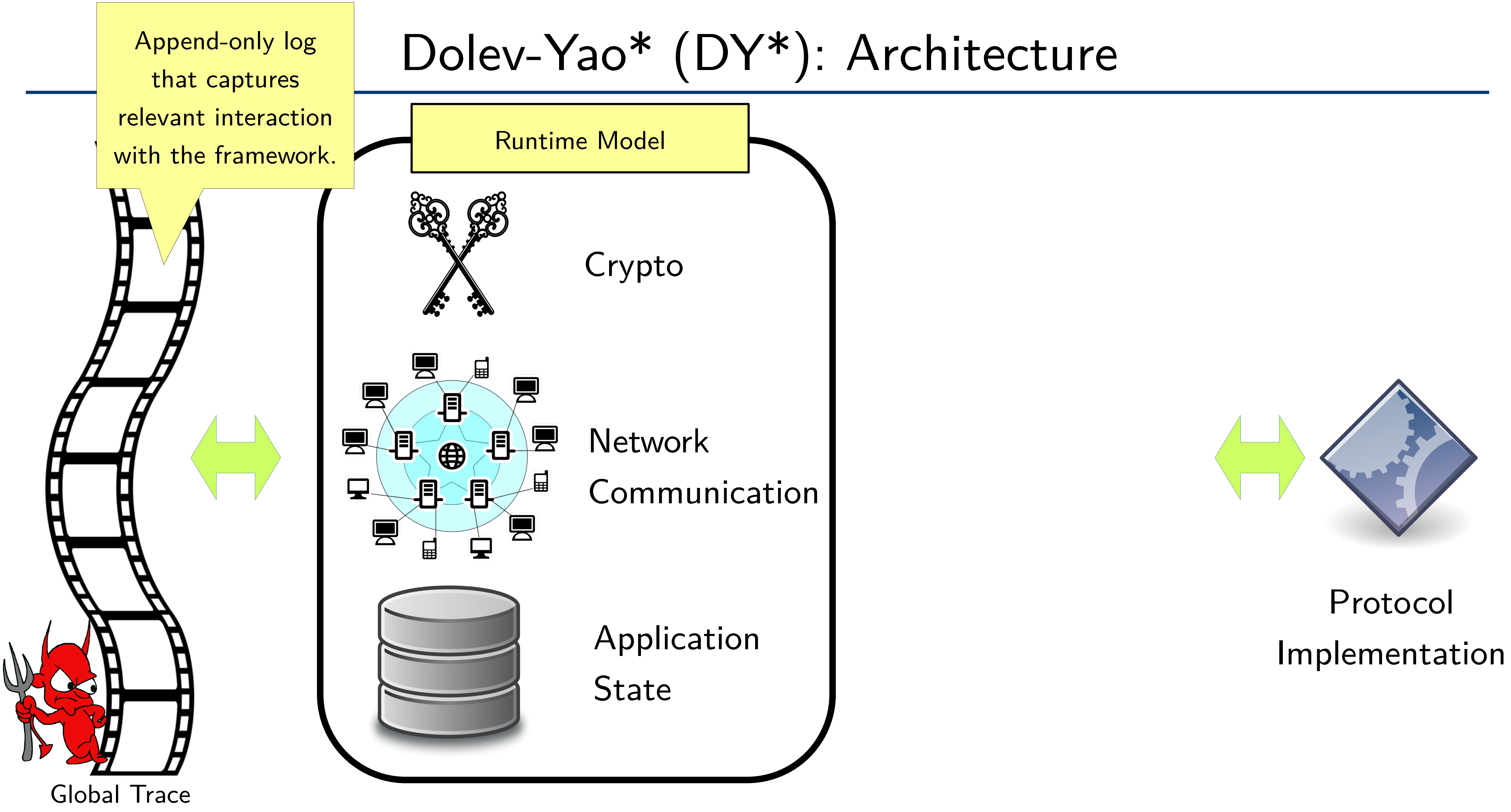


Network Communication

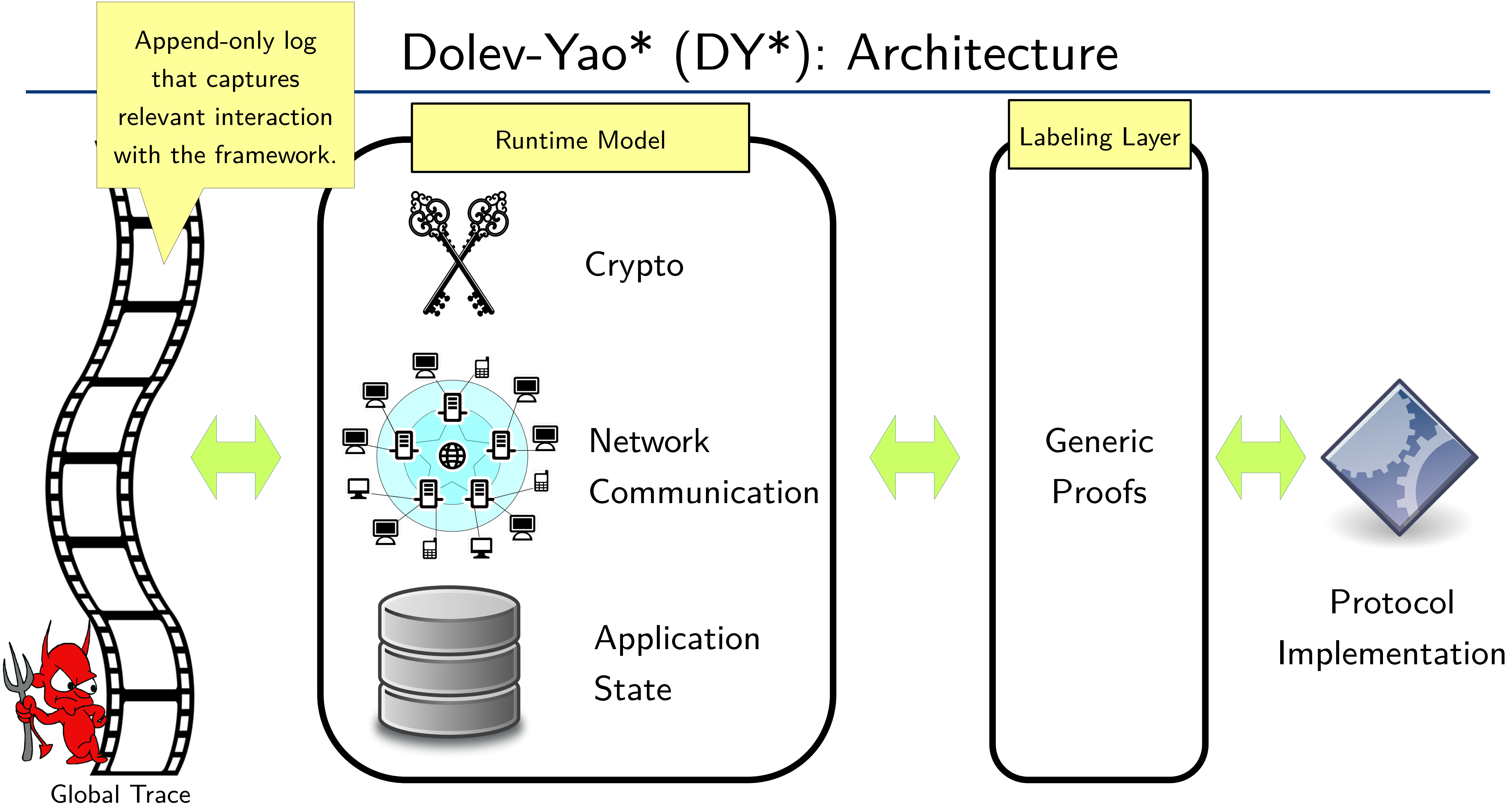
Application State

Protocol Implementation

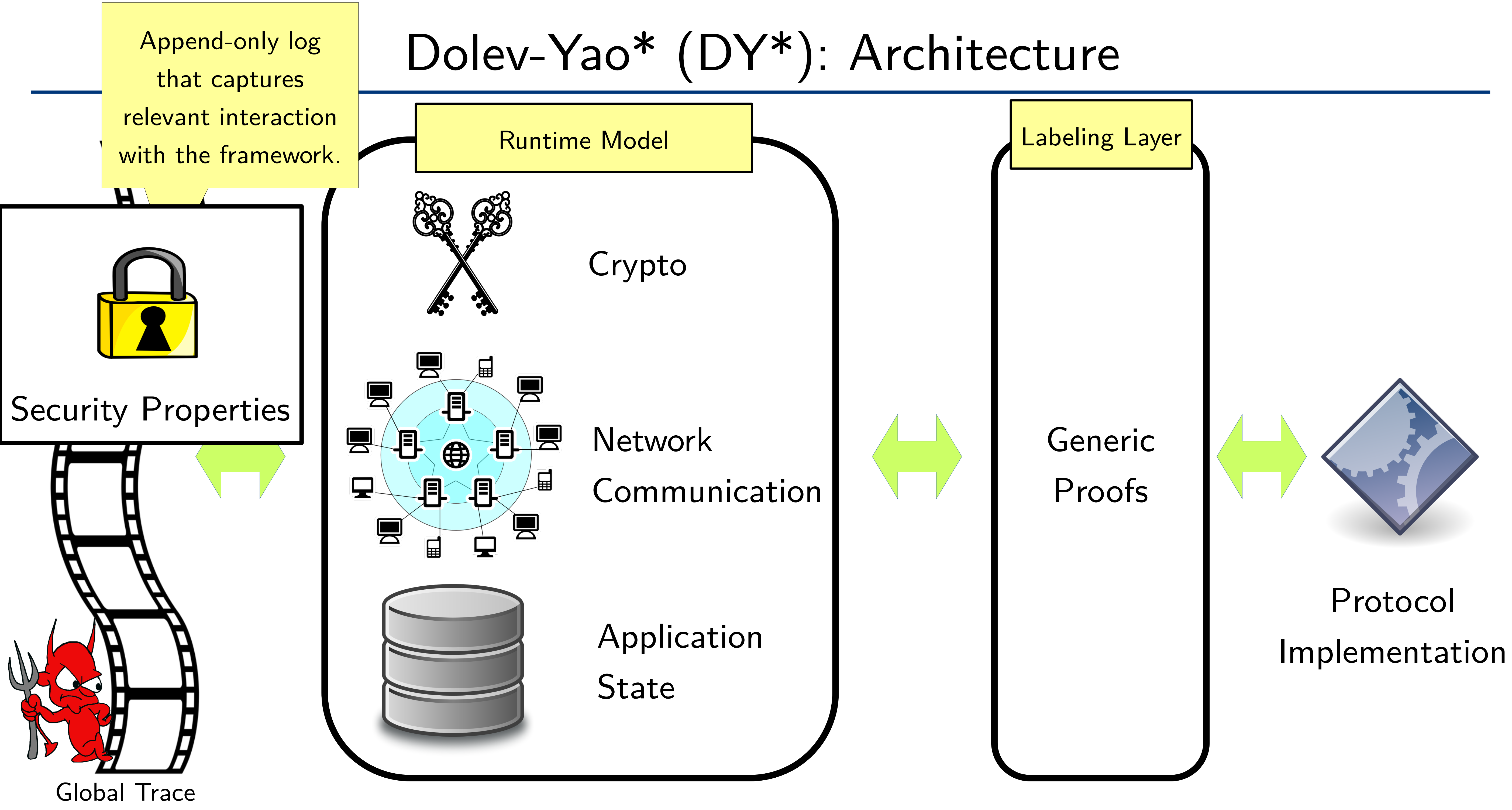
Dolev-Yao* (DY*): Architecture



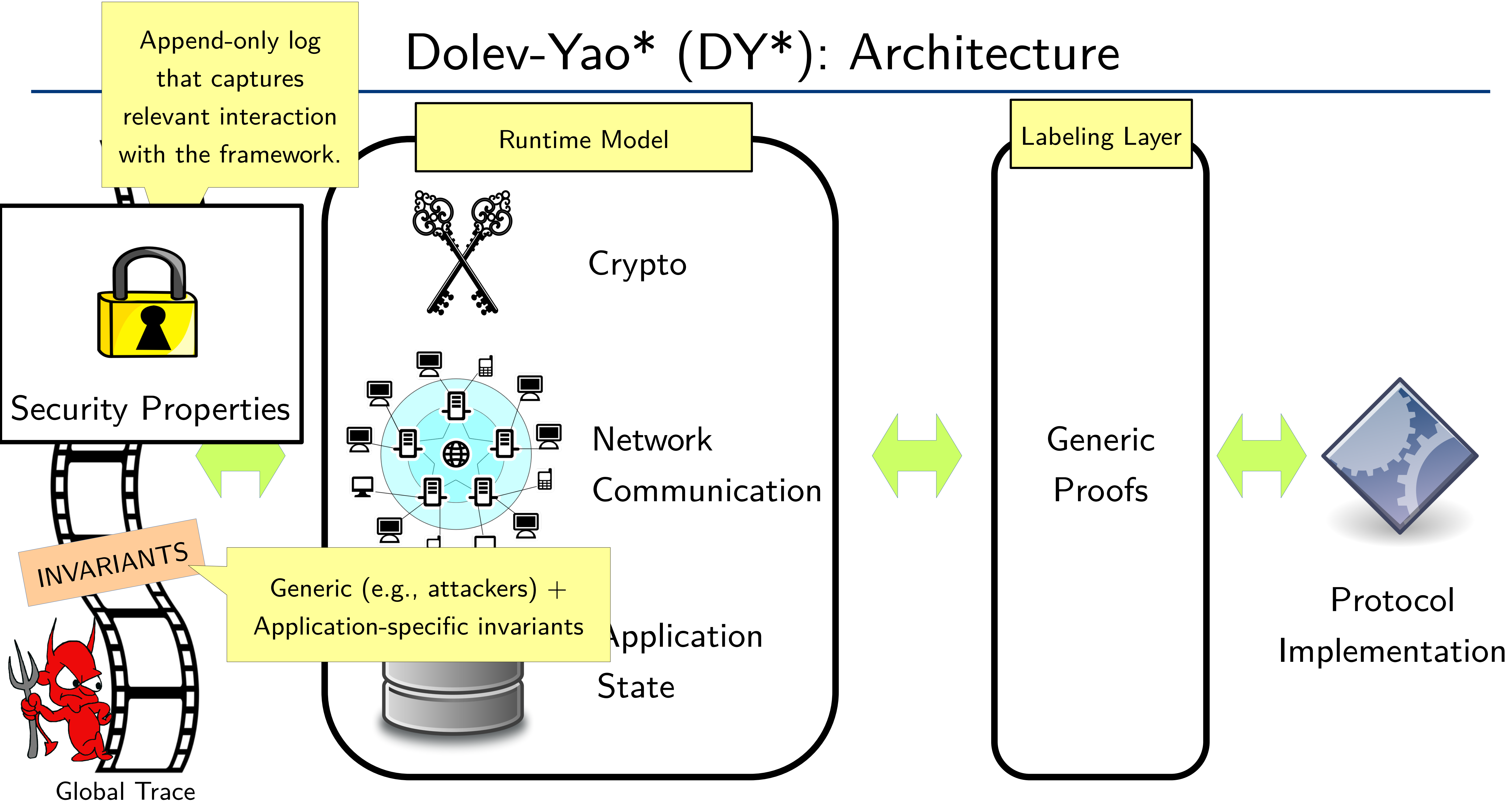
Dolev-Yao* (DY*): Architecture



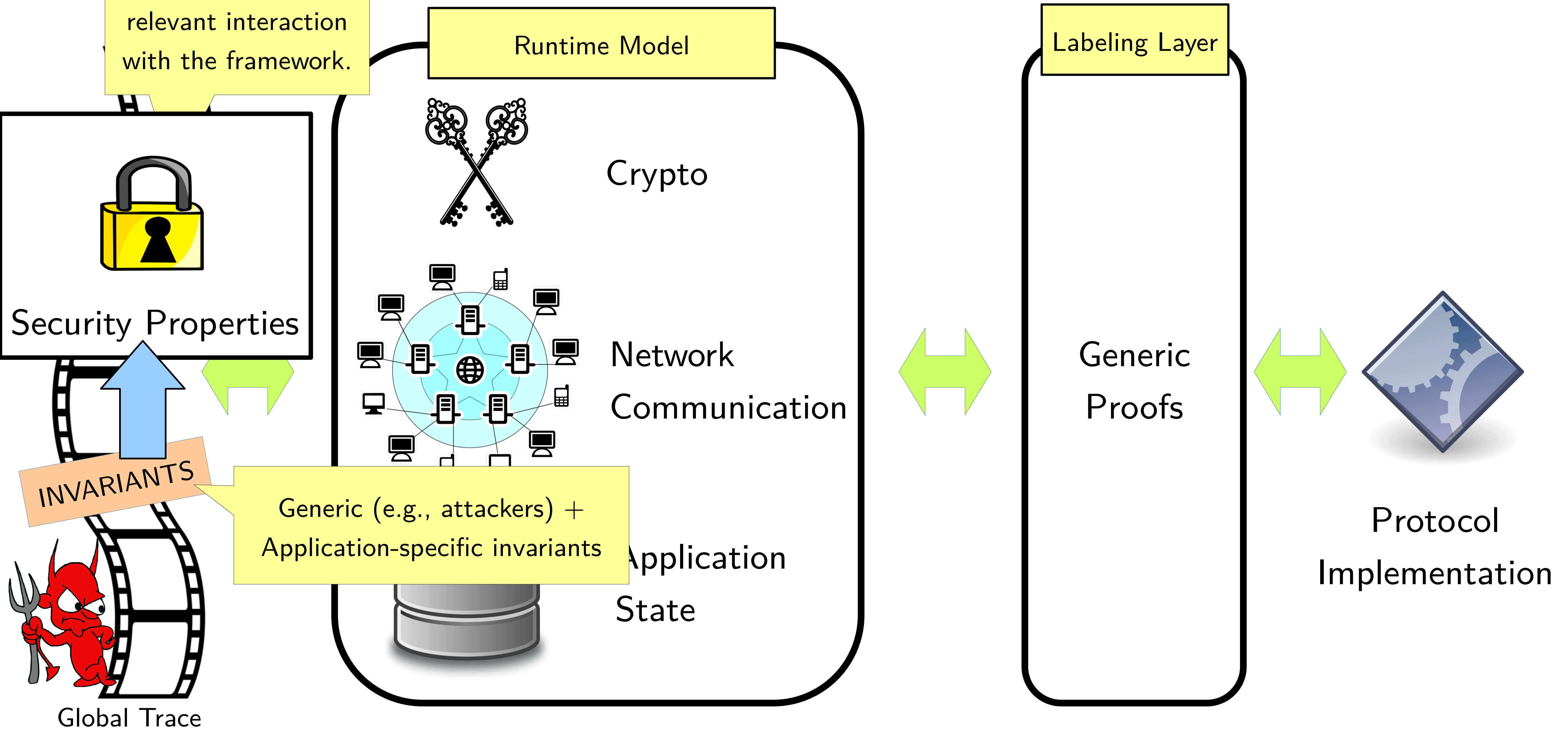
Dolev-Yao* (DY*): Architecture



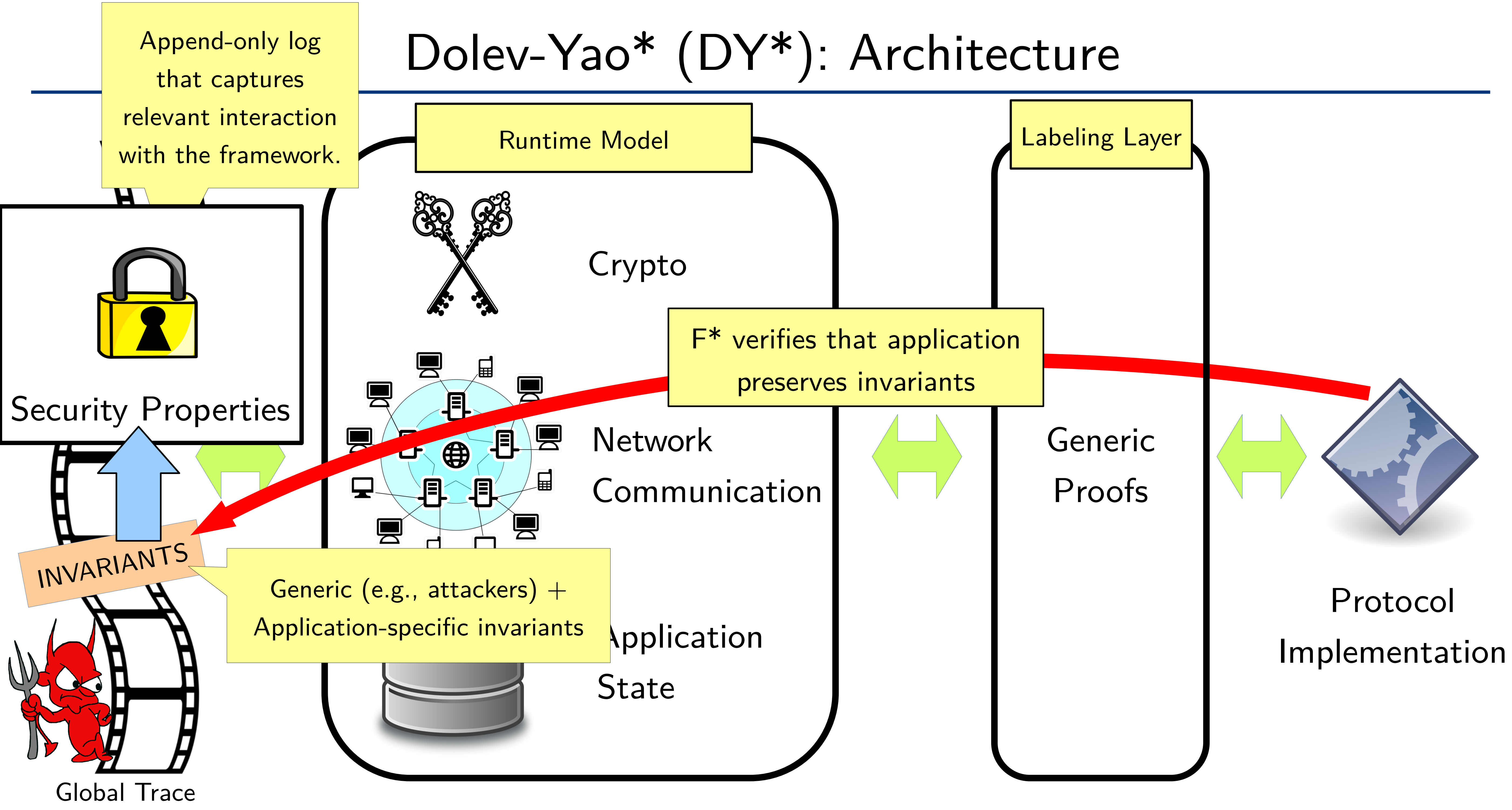
Dolev-Yao* (DY*): Architecture



Dolev-Yao* (DY*): Architecture



Dolev-Yao* (DY*): Architecture



Case Studies

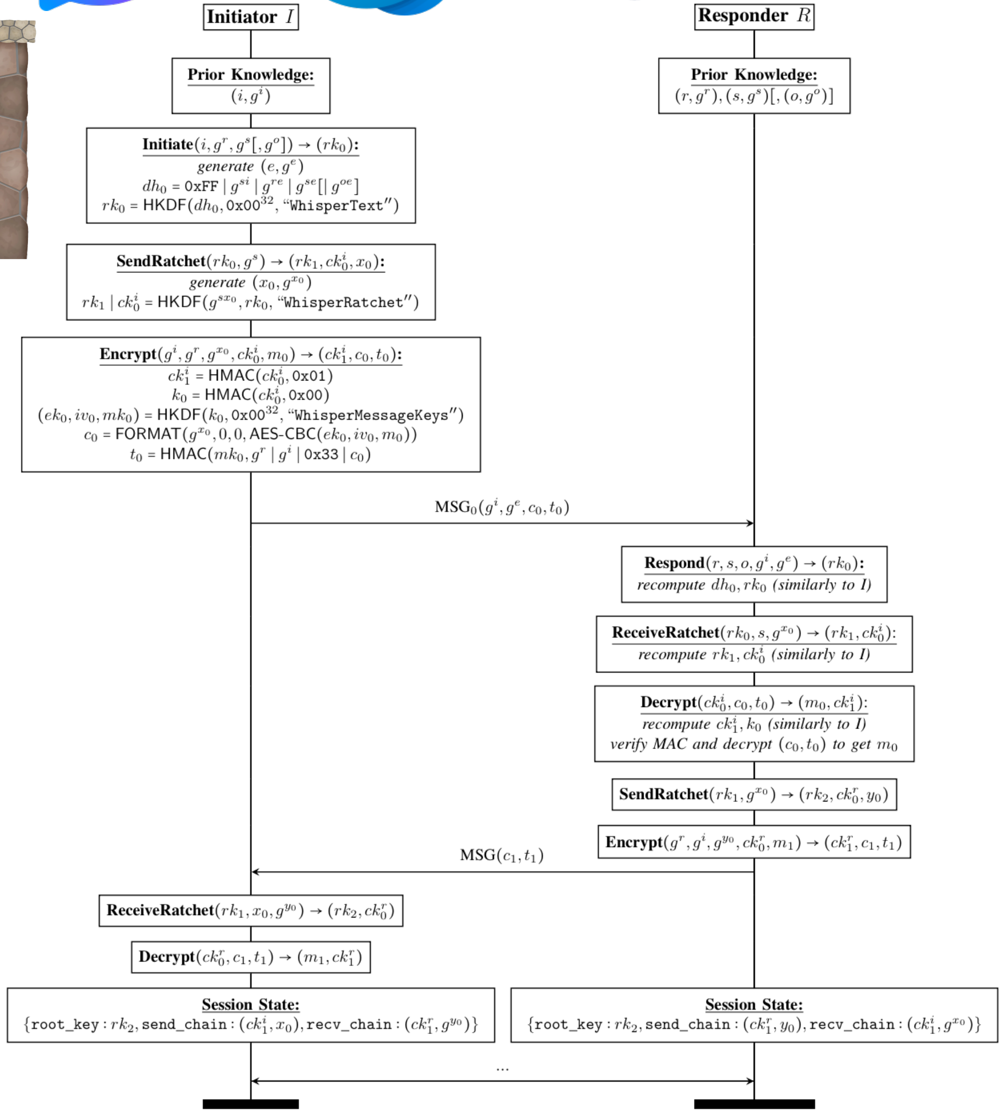
- Signal Messaging Protocol

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

- 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!