Flexible Authenticated and Confidential Channel Establishment (fACCE):
Analyzing the Noise Protocol Framework

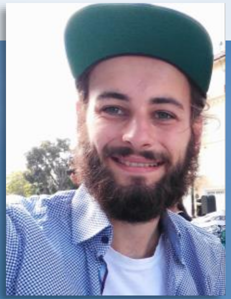
IACR PKC 2020

2020-06-01

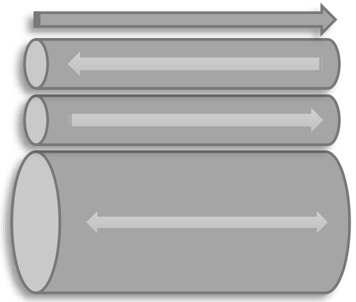
Chair for Network and Data Security
Horst Görtz Institute for IT Security
Ruhr University Bochum

Applied Cryptography Group
Institute of Information Security
ETH Zürich

Benjamin Dowling, **Paul Rösler**, Jörg Schwenk

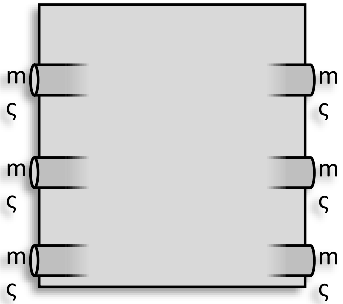




Agenda



Introduction to Noise Framework

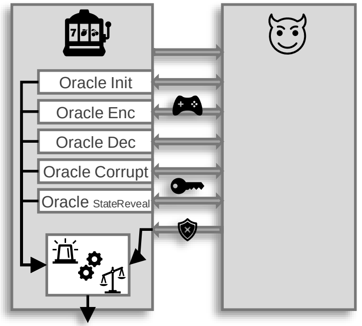
Security Model for Channel Establishment



	au^i	au^r	fs	rp^i	rp^r	kc^i	kc^r	eck	rl^i	rl^r
N^*	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
X^*	1	∞	∞	∞	∞	∞	∞	1	1	∞
K	1	∞	∞	∞	∞	∞	∞	1	1	∞
NN^*	∞	∞	2	2	0	∞	∞	∞	∞	∞
NK^*	∞	2	2	2	2	∞	2	∞	1	∞
NX^*	∞	2	2	2	0	∞	2	∞	2	∞
XN^*	3	∞	2	2	0	3	∞	∞	∞	3
XK^*	3	2	2	2	2	3	2	∞	1	3
XX^*	3	2	2	2	0	3	2	∞	2	3
KN	3	∞	2	2	0	3	∞	∞	∞	2
KK	1	2	2	2	2	3	2	1	1	2
KX	3	2	2	2	0	3	2	∞	2	2
IN	3	∞	2	2	0	3	∞	∞	∞	2
IK	1	2	2	2	2	3	2	1	1	2
IX	3	2	2	2	0	3	2	∞	2	2

Analysis Results

Discussion of Security Model



Noise Protocol Framework

Framework for establishment of confidential (and authenticated) two-party channels

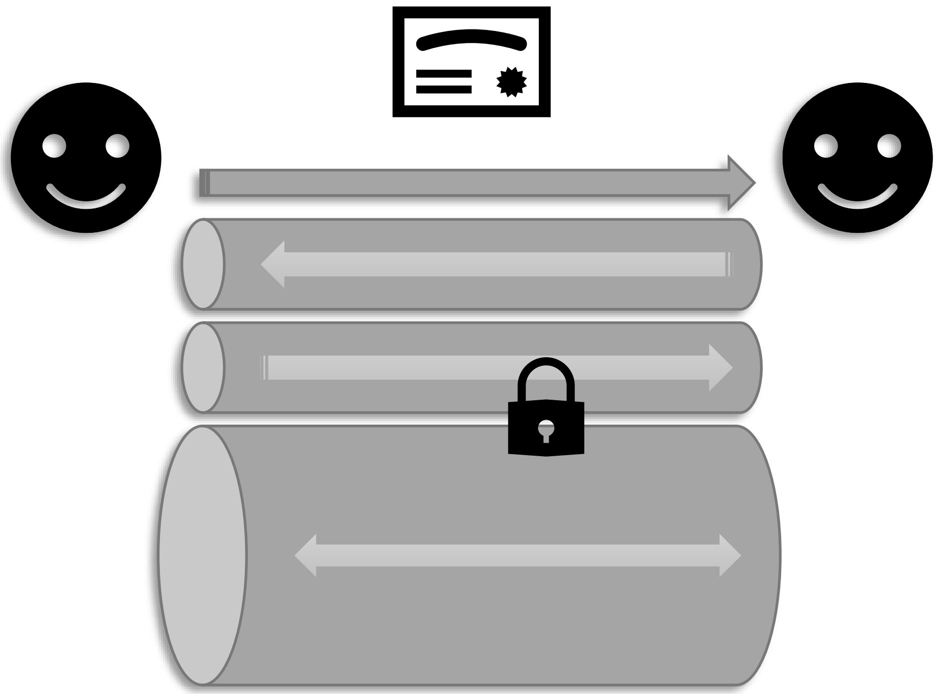
- By Trevor Perrin since 2014
- Used by WhatsApp, Wireguard, Slack, Amazon, …

- Homogenous networks (no parameter negotiation)
- Modular, lightweight
- 15 base patterns + extensions

- Previous Analyses:

  Symbolic model:
  - Kobeissi et al. EuroS&P 2019: All* patterns

  Computational model:
  - Dowling and Paterson ACNS 2017: Wireguard manually
  - Lipp et al. EuroS&P 2019: Wireguard automatically



Noise Protocol Framework

Example:

- N pattern
  - Unauthenticated
  - Unidirectional

Initiator **A** Responder **B**

Handshake

$$g^a, c_0 = \mathrm{aead}_{\mathrm{kdf}(\boxed{g^{aB}})}(g^a, \boxed{m_0})$$

Channel

$$C = \mathrm{aead}_{\mathrm{kdf}(\boxed{g^{aB}})}(\boxed{c_0}, M)$$

(Simplified for clarity)

Noise Protocol Framework

Example:

- N pattern
  - Unauthenticated
  - Unidirectional
- NK pattern
  - B authenticates
  - Bidirectional

(Simplified for clarity)

Initiator **A** Responder **B**

Handshake

$$g^a, c_0 = \mathrm{aead}_{\mathrm{kdf}(g^{aB})}(g^a, m_0) \longrightarrow$$

$$\longleftarrow g^b, c_1 = \mathrm{aead}_{\mathrm{kdf}(g^{aB}, g^{ab})}(c_0 | g^b, m_1)$$

Channel

$$C = \mathrm{aead}_{\mathrm{kdf}(g^{aB}, g^{ab})}(c_1, M) \longleftrightarrow$$

RUHR UNIVERSITÄT BOCHUM RUB
ETH zürich

Noise Protocol Framework

Example:

- N pattern
  - Unauthenticated
  - Unidirectional
- NK pattern
  - B authenticates
  - Bidirectional
- XK pattern
  - A and B authenticate
  - A's authentication key distributed ad-hoc

(Simplified for clarity)

Initiator $\mathbf{A}$ Responder $\mathbf{B}$

Handshake

$$g^a, c_0 = \mathrm{aead}_{\mathrm{kdf}(g^{aB})}(g^a, m_0)$$

$$g^b, c_1 = \mathrm{aead}_{\mathrm{kdf}(g^{aB}, g^{ab})}(c_0 | g^b, m_1)$$

$$c_2 = \mathrm{aead}_{\mathrm{kdf}(g^{aB}, g^{ab})}(c_1, \boxed{g^A})$$

$$c_3 = \mathrm{aead}_{\mathrm{kdf}(g^{aB}, g^{ab}, g^{Ab})}(c_2, m_3)$$

Channel

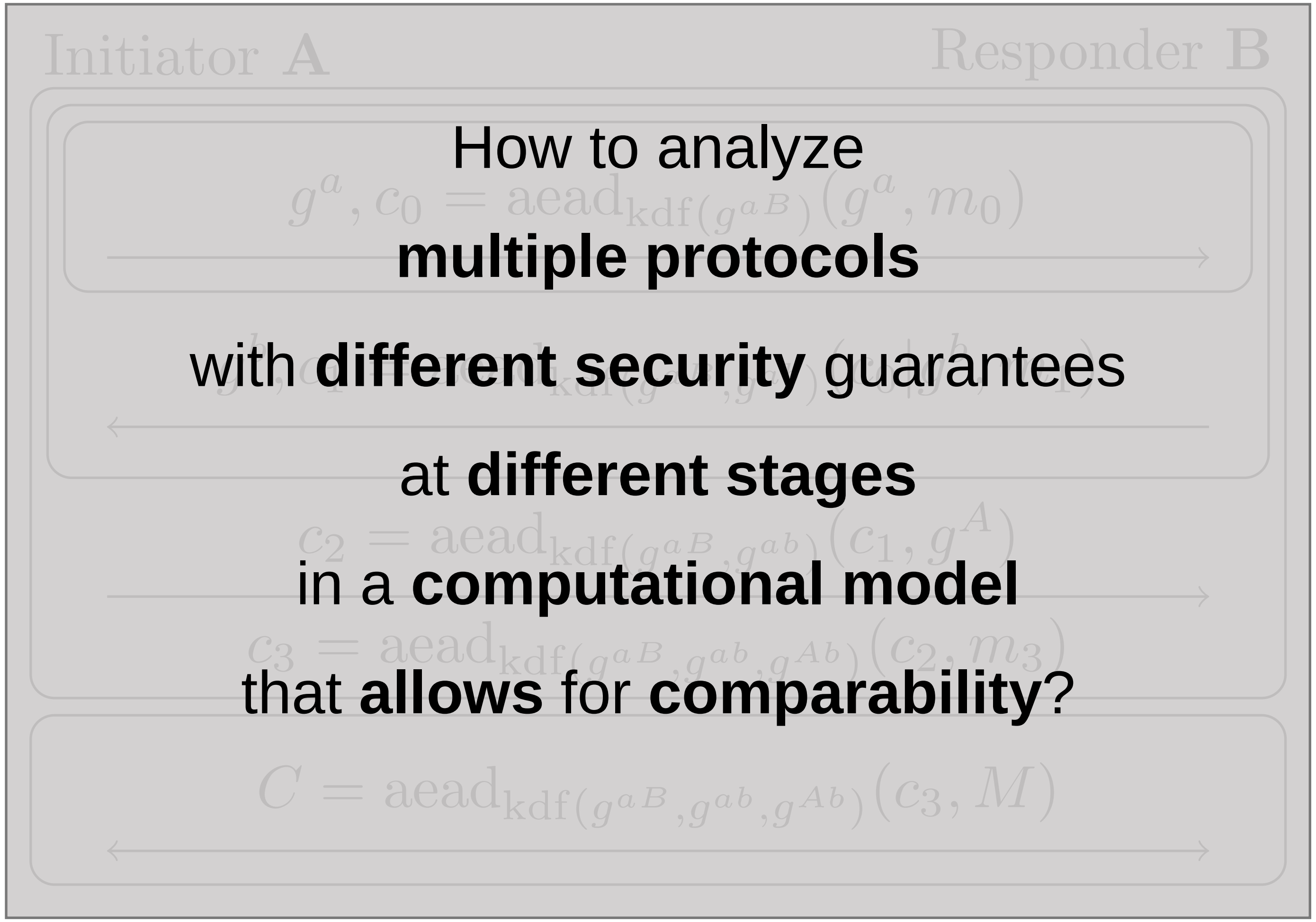
$$C = \mathrm{aead}_{\mathrm{kdf}(g^{aB}, g^{ab}, \boxed{g^{Ab}})}(\boxed{c_3}, M)$$

Noise Protocol Framework

Example:

- N pattern
  - Unauthenticated
  - Unidirectional
- NK pattern
  - B authenticates
  - Bidirectional
- XK pattern
  - A and B authenticate
  - A's authentication key distributed ad-hoc

(Simplified for clarity)



How to analyze

multiple protocols

with **different security** guarantees

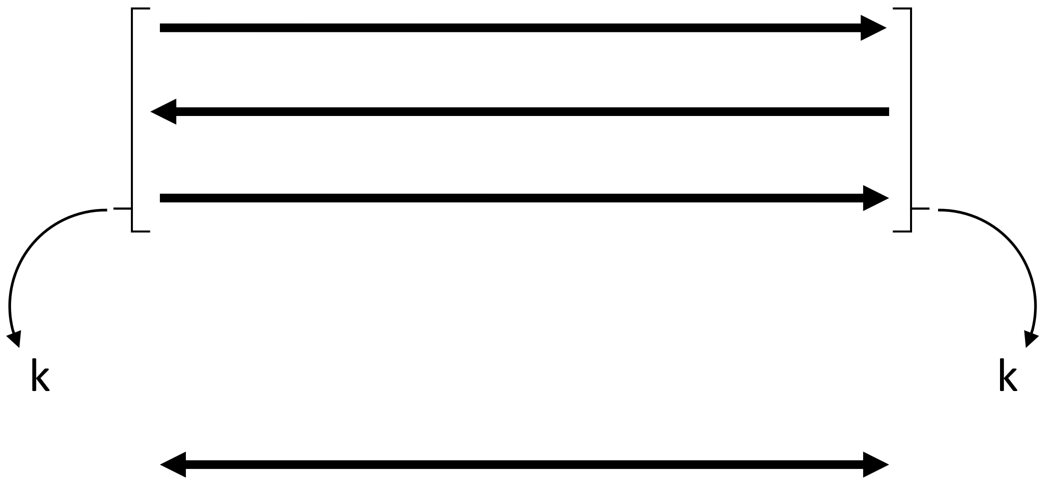
at **different stages**

in a **computational model**

that **allows** for **comparability**?

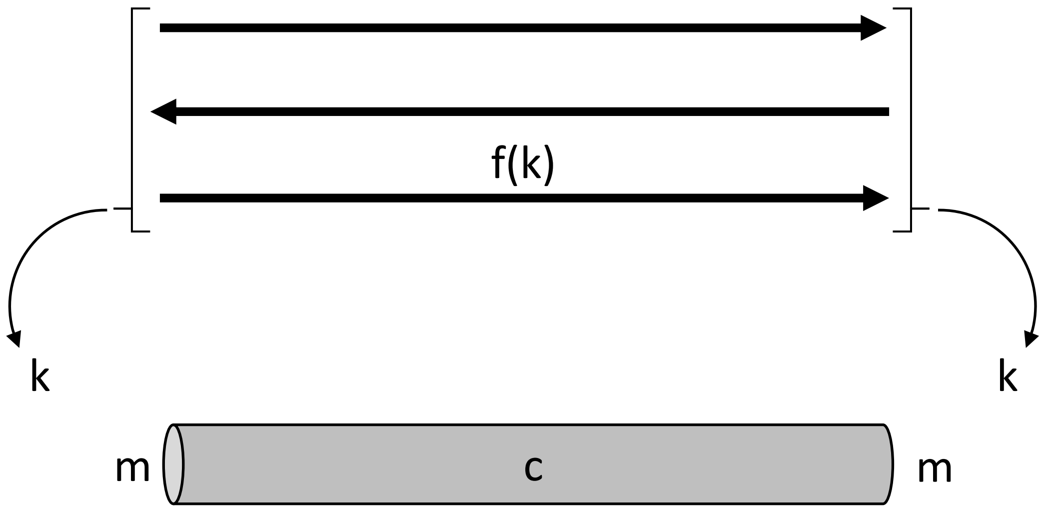
Model for Channel Establishment

- Key exchange then symmetric protocol
  - *Brzuska et al.: Composability of Bellare-Rogaway Key Exchange Protocols CCS11*



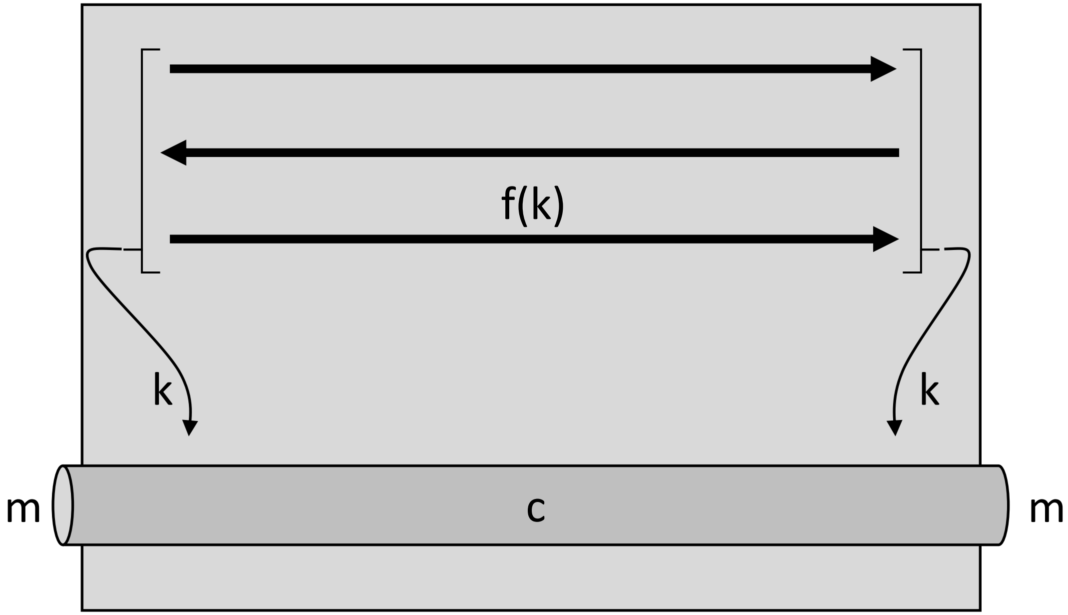
Model for Channel Establishment

- Key exchange then symmetric protocol
  - *Brzuska et al.: Composability of Bellare-Rogaway Key Exchange Protocols CCS11*
- Channel establishment
  - *Jager et al.: On the Security of TLS-DHE in the Standard Model C12*



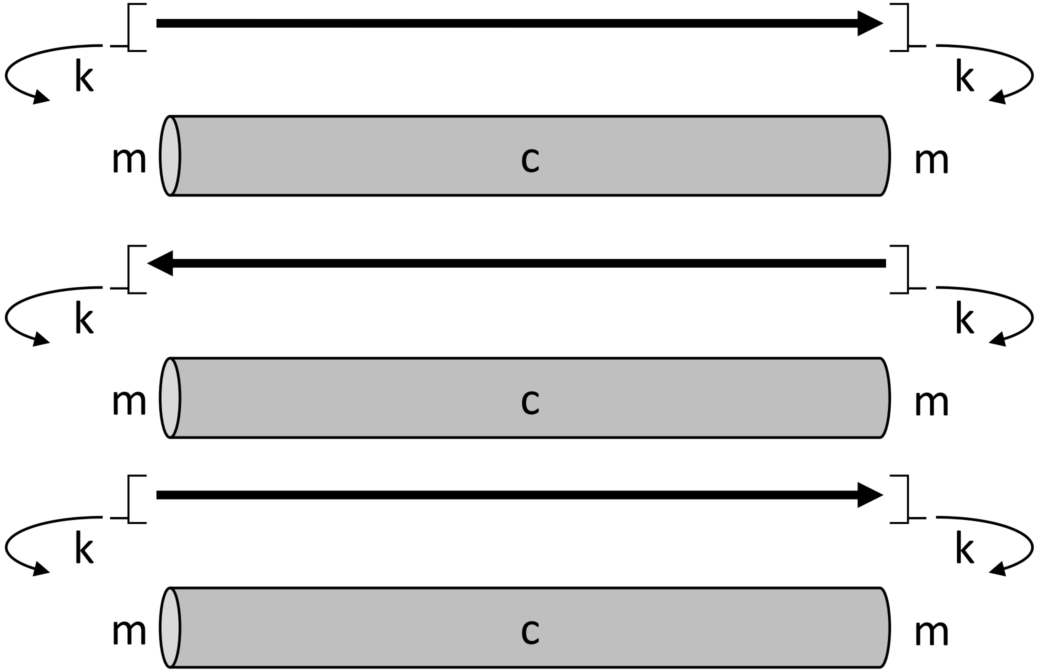
Model for Channel Establishment

- Key exchange then symmetric protocol
  - *Brzuska et al.: Composability of Bellare-Rogaway Key Exchange Protocols CCS11*
- Channel establishment
  - *Jager et al.: On the Security of TLS-DHE in the Standard Model C12*



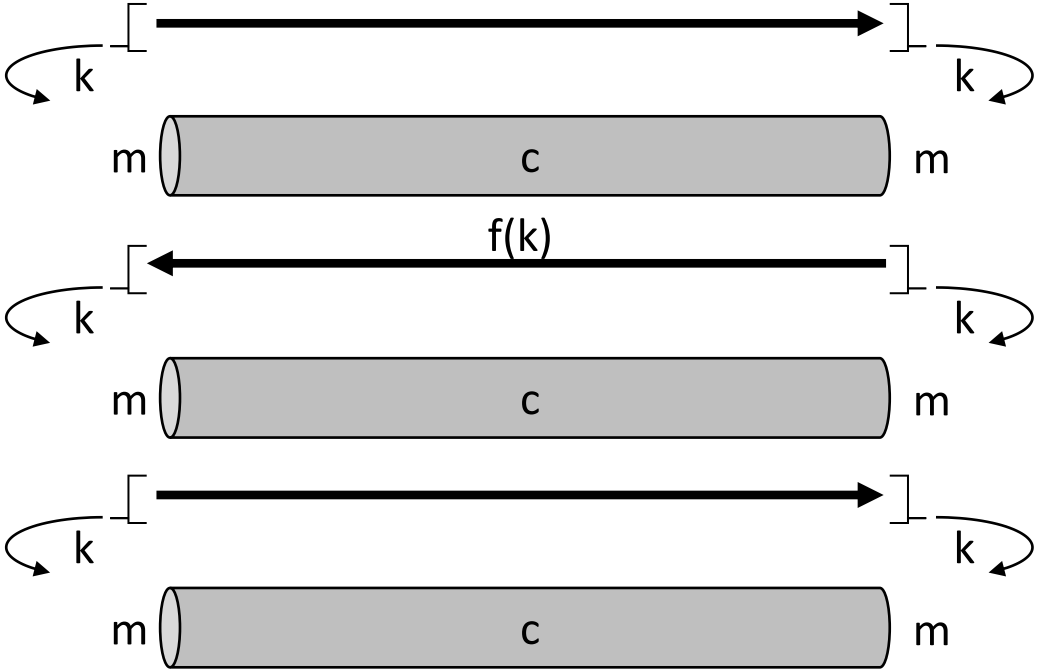
Model for Channel Establishment

- Key exchange then symmetric protocol
  - *Brzuska et al.: Composability of Bellare-Rogaway Key Exchange Protocols CCS11*
- Channel establishment
  - *Jager et al.: On the Security of TLS-DHE in the Standard Model C12*
- Key exchange and symmetric protocol
  - *Fischlin, Günther: Multi-Stage Key Exchange and the Case of Google's QUIC Protocol CCS14*



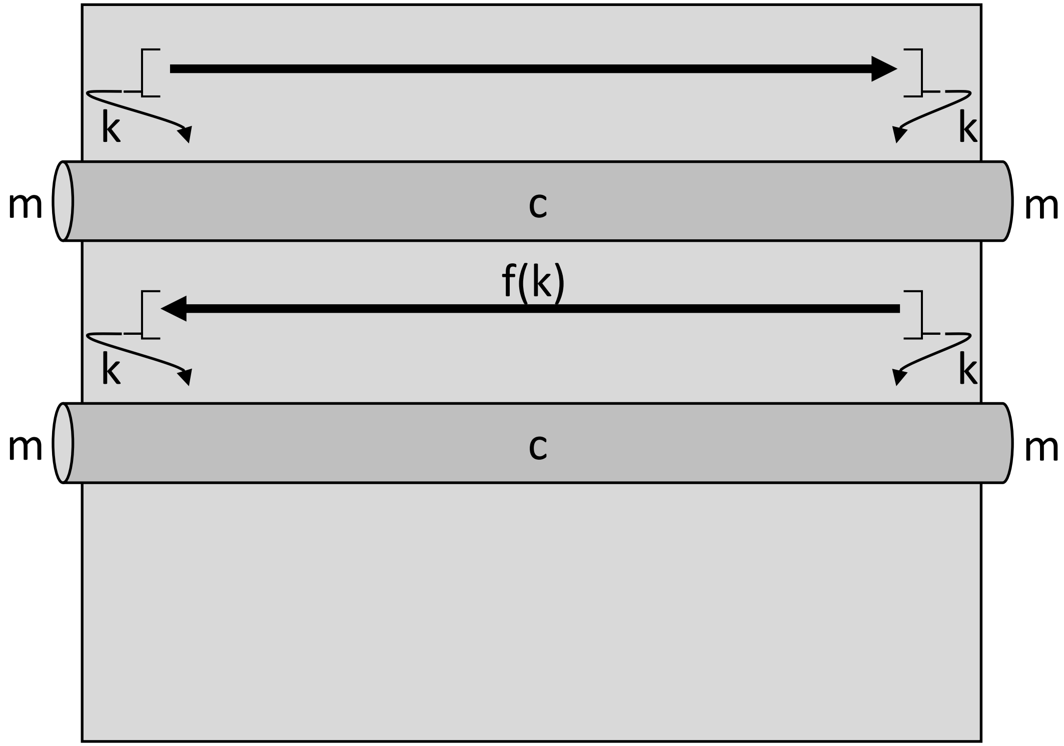
Model for Channel Establishment

- Key exchange then symmetric protocol
  - *Brzuska et al.: Composability of Bellare-Rogaway Key Exchange Protocols CCS11*
- Channel establishment
  - *Jager et al.: On the Security of TLS-DHE in the Standard Model C12*
- Key exchange and symmetric protocol
  - *Fischlin, Günther: Multi-Stage Key Exchange and the Case of Google's QUIC Protocol CCS14*



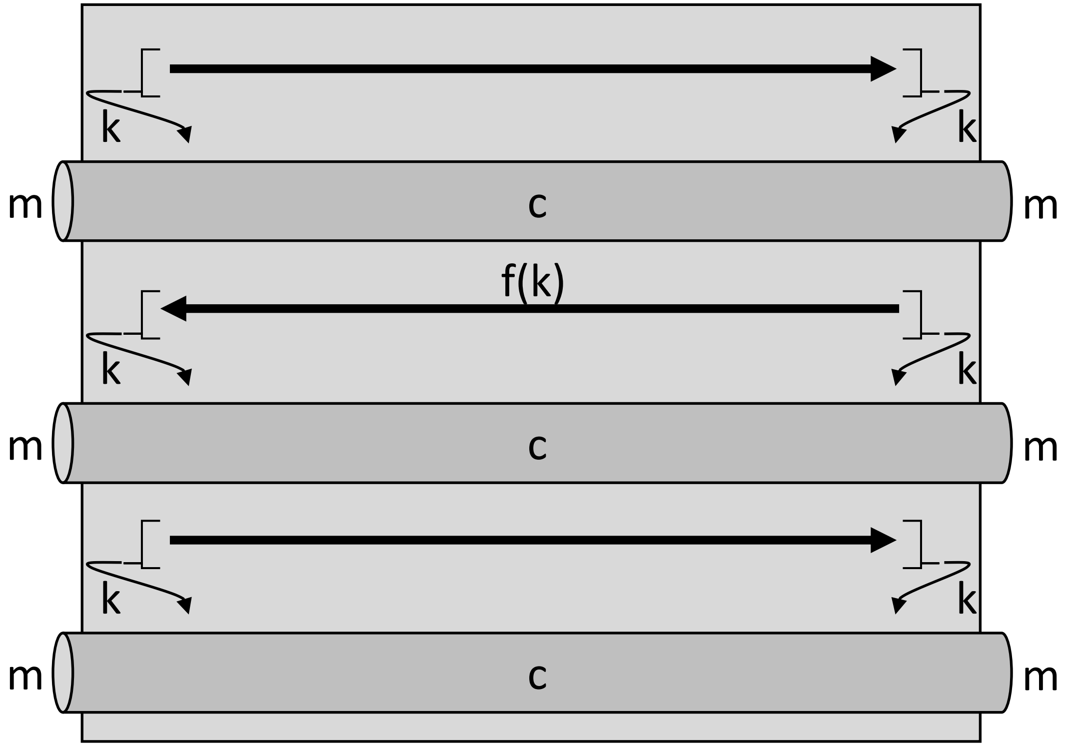
Model for Channel Establishment

- Key exchange then symmetric protocol
  - *Brzuska et al.: Composability of Bellare-Rogaway Key Exchange Protocols CCS11*
- Channel establishment
  - *Jager et al.: On the Security of TLS-DHE in the Standard Model C12*
- Key exchange and symmetric protocol
  - *Fischlin, Günther: Multi-Stage Key Exchange and the Case of Google's QUIC Protocol CCS14*
- Two stage channel establishment
  - *Lychev et al.: How Secure and Quick is QUIC? Provable Security and Performance Analyses S&P15*



Model for Channel Establishment

- Key exchange then symmetric protocol
  - *Brzuska et al.: Composability of Bellare-Rogaway Key Exchange Protocols CCS11*
- Channel establishment
  - *Jager et al.: On the Security of TLS-DHE in the Standard Model C12*
- Key exchange and symmetric protocol
  - *Fischlin, Günther: Multi-Stage Key Exchange and the Case of Google's QUIC Protocol CCS14*
- Two stage channel establishment
  - *Lychev et al.: How Secure and Quick is QUIC? Provable Security and Performance Analyses S&P15*
- …

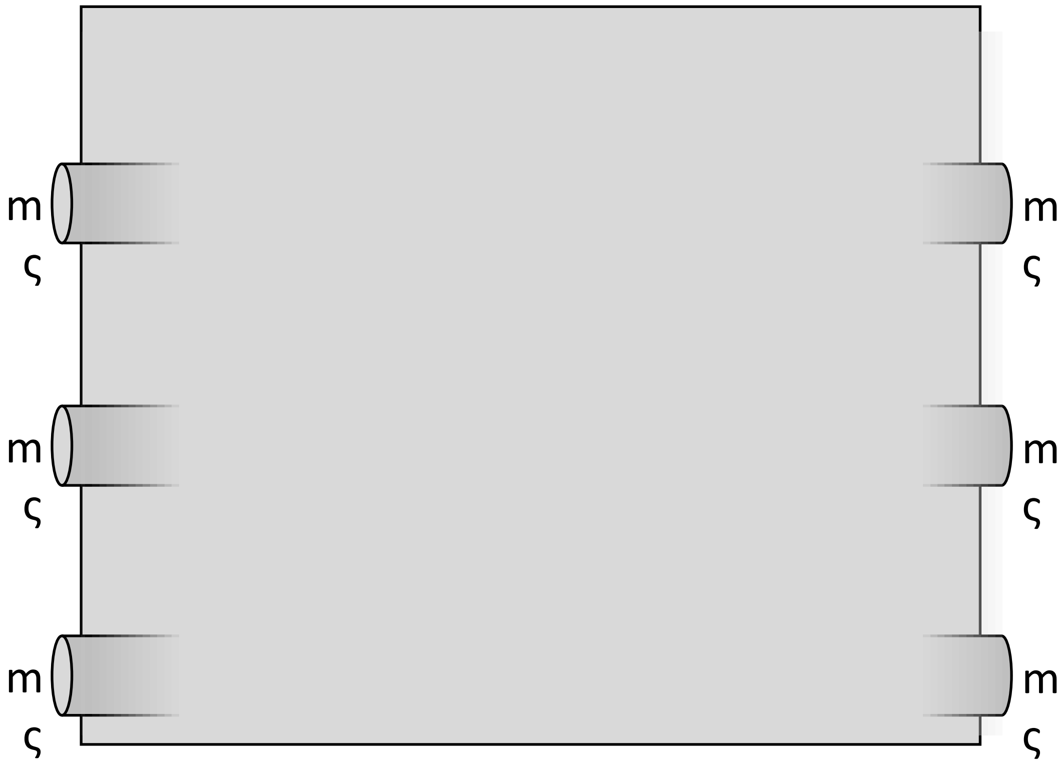


Model for Channel Establishment

- Disregard internal key establishment
- Focus on functionality (channel)

Model for Channel Establishment

- Disregard internal key establishment
- Focus on functionality (channel)
- Additional stage output:
  signals current security level



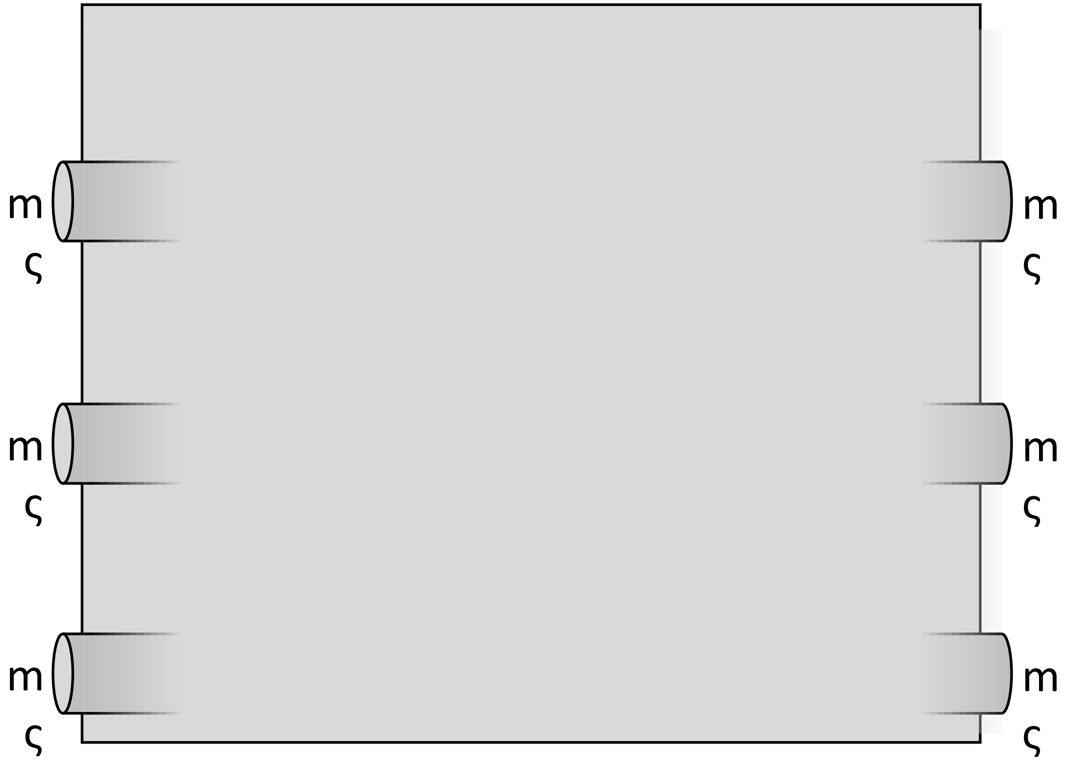
$$\mathrm{KGen} \rightarrow_{\$} (sk, pk) \qquad \mathrm{Enc}(sk, st, m) \rightarrow_{\$} (st, c, \varsigma)$$
$$\mathrm{Init}(sk, pk, \rho, ad) \rightarrow_{\$} st \qquad \mathrm{Dec}(sk, st, c) \rightarrow (st, m, \varsigma)$$

Model for Channel Establishment

- Disregard internal key establishment
- Focus on functionality (channel)
- Additional stage output:
  signals current security level

- Security definition parameterized
  - (au^i,au^r,fs,rp^i,rp^r)

  Example:
  - If $\varsigma > au^i$ then initiator must be authenticated
  - If $\varsigma >$ fs then forward-secrecy must be reached
  - …



$$\mathrm{KGen} \rightarrow_{\$} (sk, pk) \qquad \mathrm{Enc}(sk, st, m) \rightarrow_{\$} (st, c, \varsigma)$$
$$\mathrm{Init}(sk, pk, \rho, ad) \rightarrow_{\$} st \qquad \mathrm{Dec}(sk, st, c) \rightarrow (st, m, \varsigma)$$

Analysis of Noise

- 8 out of 15 patterns analyzed
  - Conjectures for remaining patterns
- Fine grained security properties
  - Authentication (per party)
  - Forward-secrecy
  - Replay attack resistance (per party)
  - More in extended version
- Clean & modular proof structure

Initiator **A** Responder **B**

$g^a, c_0 = \mathrm{aead}_{\mathrm{kdf}(g^{aB})}(g^a, m_0)$ →

$g^b, c_1 = \mathrm{aead}_{\mathrm{kdf}(g^{aB}, g^{ab})}(c_0|g^b, m_1)$ ←

$c_2 = \mathrm{aead}_{\mathrm{kdf}(g^{aB}, g^{ab})}(c_1, g^A)$ →

$c_3 = \mathrm{aead}_{\mathrm{kdf}(g^{aB}, g^{ab}, g^{Ab})}(c_2, m_3)$

$C = \mathrm{aead}_{\mathrm{kdf}(g^{aB}, g^{ab}, g^{Ab})}(c_3, M)$ ↔

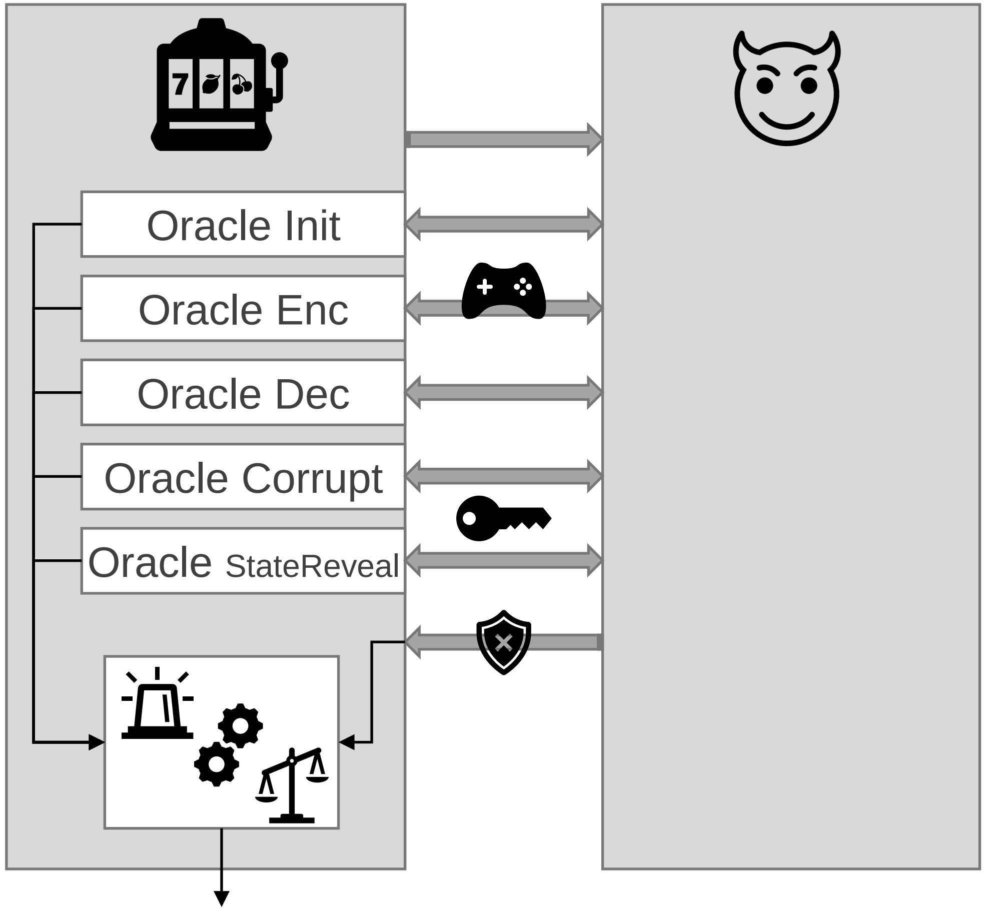
	au^i	au^r	fs	rp^i	rp^r	kc^i	kc^r	eck	rl^i	rl^r
N*	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
X*	1	∞	∞	∞	∞	∞	∞	1	1	∞
K	1	∞	∞	∞	∞	∞	∞	1	1	∞
NN*	∞	∞	2	2	0	∞	∞	∞	∞	∞
NK*	∞	2	2	2	2	∞	2	∞	1	∞
NX*	∞	2	2	2	0	∞	2	∞	2	∞
XN*	3	∞	2	2	0	3	∞	∞	∞	3
XK*	3	2	2	2	2	3	2	∞	1	3
XX*	3	2	2	2	0	3	2	∞	2	3
KN	3	∞	2	2	0	3	∞	∞	∞	2
KK	1	2	2	2	2	3	2	1	1	2
KX	3	2	2	2	0	3	2	∞	2	2
IN	3	∞	2	2	0	3	∞	∞	∞	2
IK	1	2	2	2	2	3	2	1	1	2
IX	3	2	2	2	0	3	2	∞	2	2

Model Discussion

- Control over algorithm invocations
  - Create own (realistic) target
- Access to (independent) secrets
  - Demonstrate independence and reflect realistic attacks
- Definition of security goal
  - Here: confidentiality and authenticity
- Exclude unpreventable attacks
  - Necessary for satisfiable security definition
- Exclude preventable attacks
  - Allows for efficient constructions
  - Controlled by our model parameters

- Soft security goals:
  - Forward-secrecy, replay-attack resistance, …
  - Preventable attack treatment

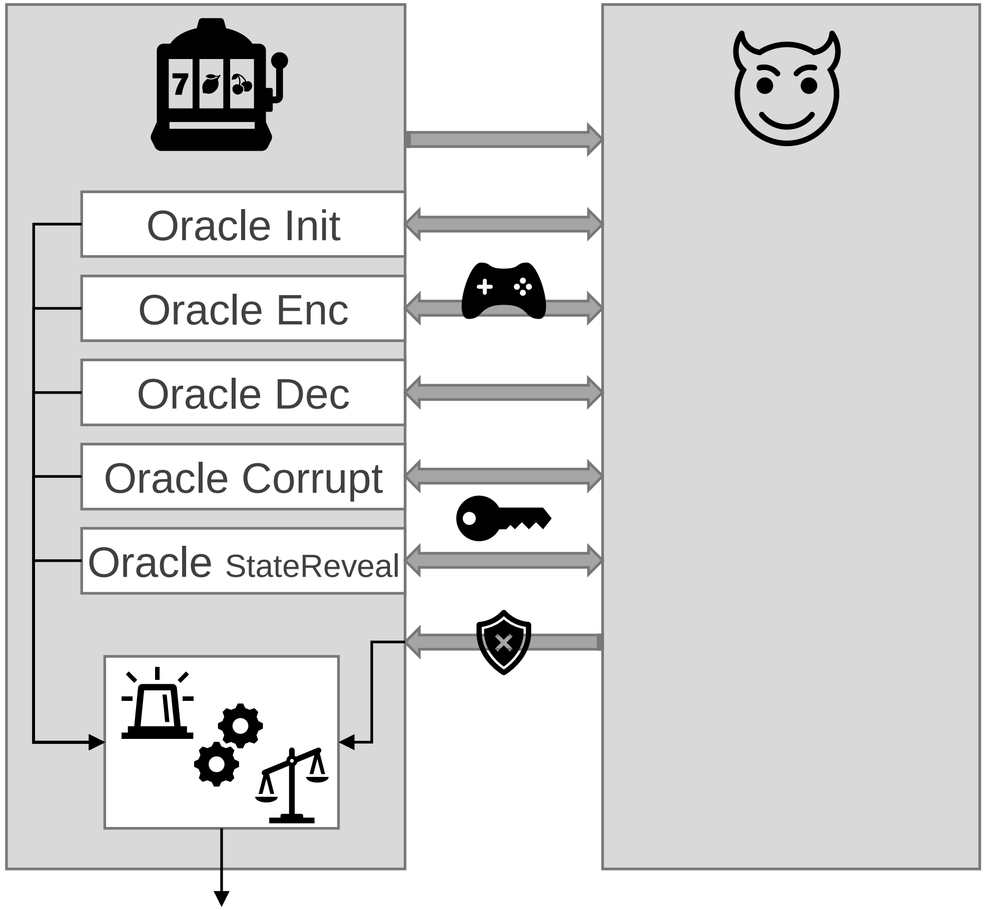
  → Only "derivative" security goals



Model Discussion

State reveal ↔ Replay attack-resistance

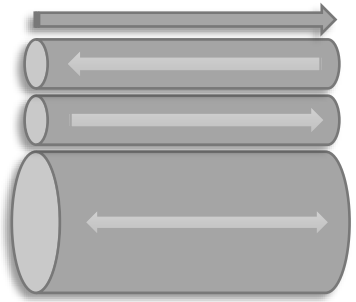
- State reveal:
  - Practically relevant, e.g. long-term (IoT) sessions
  - Demonstrates that two different states are independent
- Replay attacks:
  - “Break authenticity”
  - Unpreventable for static long-term keys for “0-RTT”
  - Deliver same message multiple times
- Relation:
  - Replay attacks establish dependent secrets multiple times
  - Replay-attack resistant: make *different* states *independent*
  - State reveal allowed meaningful “Replay-attack resistant”



Agenda

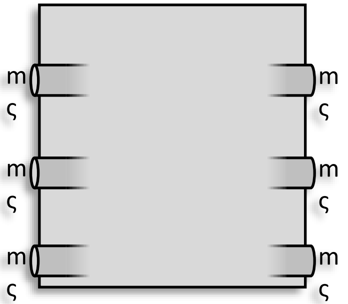
RUHR UNIVERSITÄT BOCHUM RUB

ETH zürich



Modular framework for secure channels

Introduction to Noise Framework → Security Model for Channel Establishment



Understand primitive via its functionality (not via its constructions)

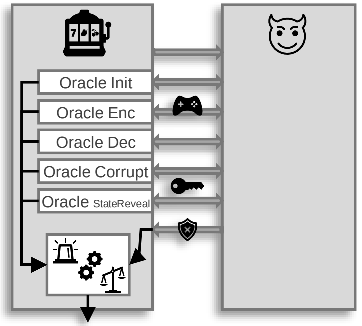
	au^i	au^r	fs	rp^i	rp^r	kc^i	kc^r	eck	rl^i	rl^r
N^*	∞	∞	∞	∞	∞	∞	∞	∞	1	∞
X^*	1	∞	∞	∞	∞	∞	∞	1	1	∞
K	1	∞	∞	∞	∞	∞	∞	1	1	∞
NN^*	∞	∞	2	2	0	∞	∞	∞	∞	∞
NK^*	∞	2	2	2	2	∞	2	∞	1	∞
NX^*	∞	2	2	2	0	∞	2	∞	2	∞
XN^*	3	∞	2	2	0	3	∞	∞	∞	3
XK^*	3	2	2	2	2	3	2	∞	1	3
XX^*	3	2	2	2	0	3	2	∞	2	3
KN	3	∞	2	2	0	3	∞	∞	∞	2
KK	1	2	2	2	2	3	2	1	1	2
KX	3	2	2	2	0	3	2	∞	2	2
IN	3	∞	2	2	0	3	∞	∞	∞	2
IK	1	2	2	2	2	3	2	1	1	2
IX	3	2	2	2	0	3	2	∞	2	2

Precise security proofs for 8/15 patterns

Analysis Results → Discussion of Security Model

@roeslpa

ia.cr/2019/436



Soft goals via preventable attacks are not independent