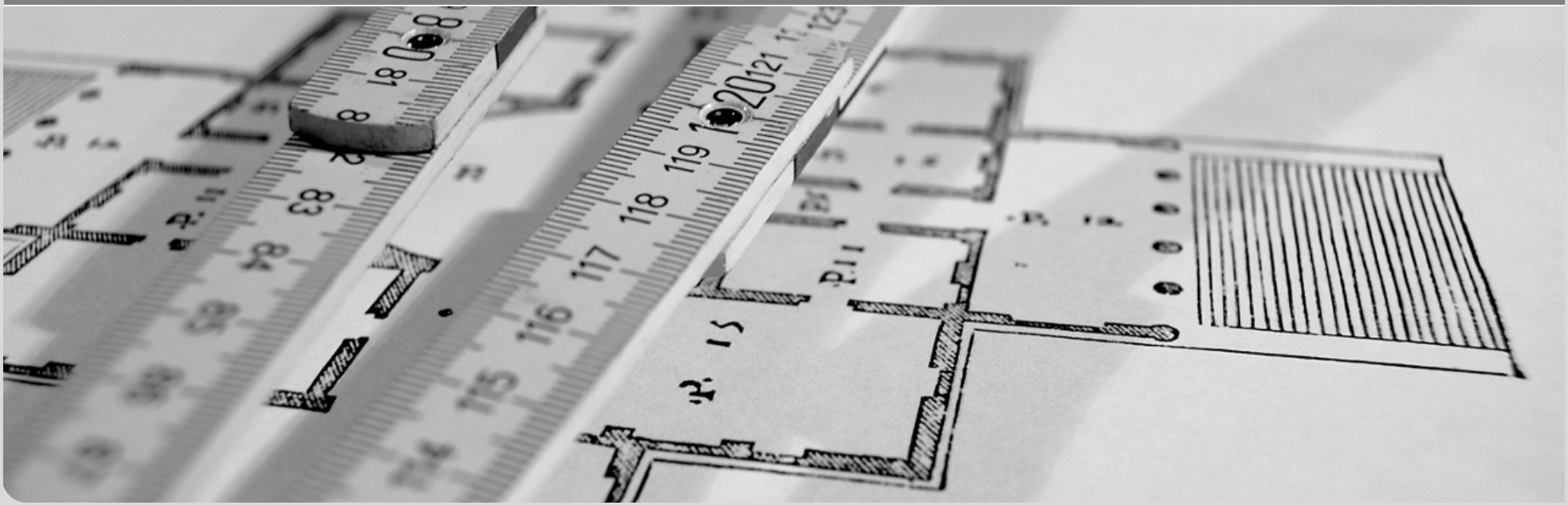
Karlsruhe Institute of Technology

Synchronous Universally Composable Computer Networks

Dirk Achenbach, Jörn Müller-Quade, Jochen Rill | September 4, 2015

INSTITUTE FOR CRYPTOGRAPHY AND SECURITY



Context of this Work

Provable security exists for cryptographic protocols, encryption algorithms, cryptographic hash functions, . . .

. . . but for real computer networks?

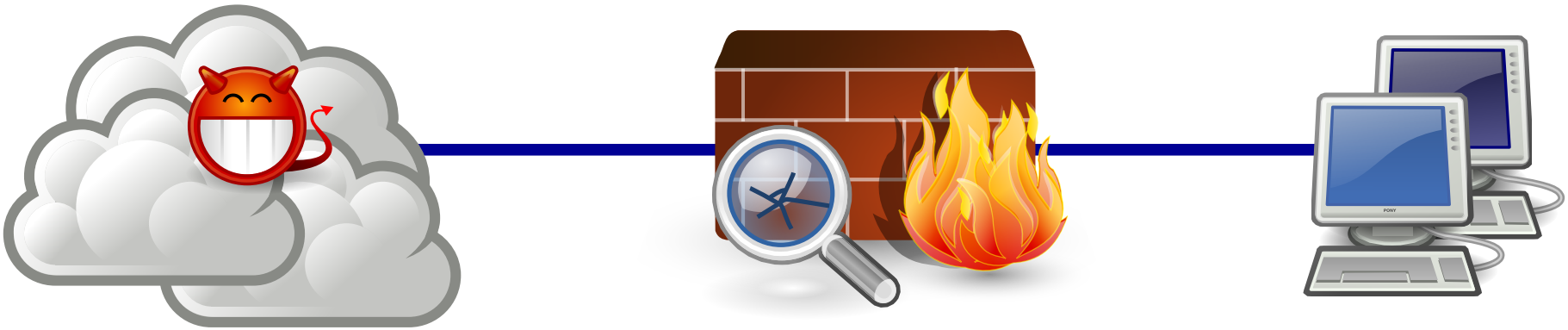
Context of this Work

Real networks are always built using ad-hoc security guarantees. We need a cryptographic model to give mathematically founded security guarantees.

Previously . . .

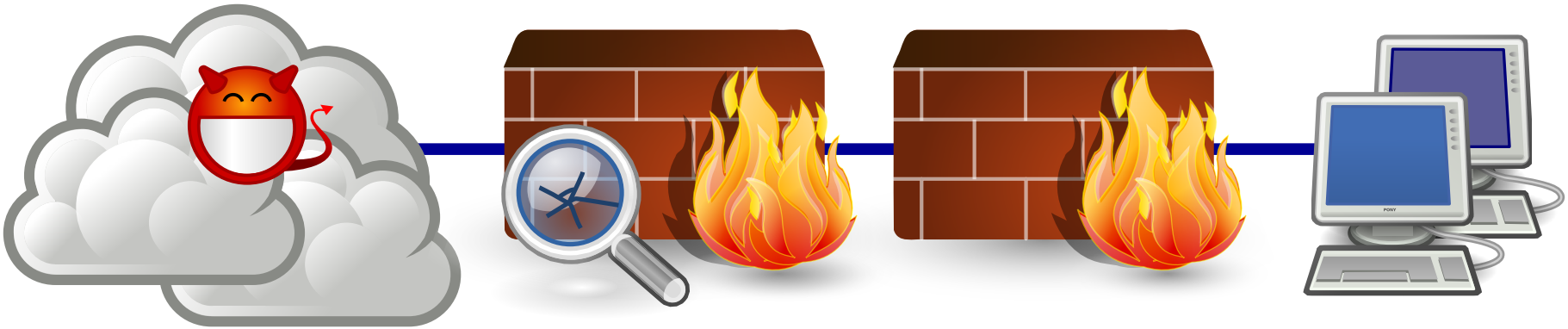
Universally Composable Firewall Architectures using Trusted Hardware (Achenbach et al. [1]).

Previously . . .



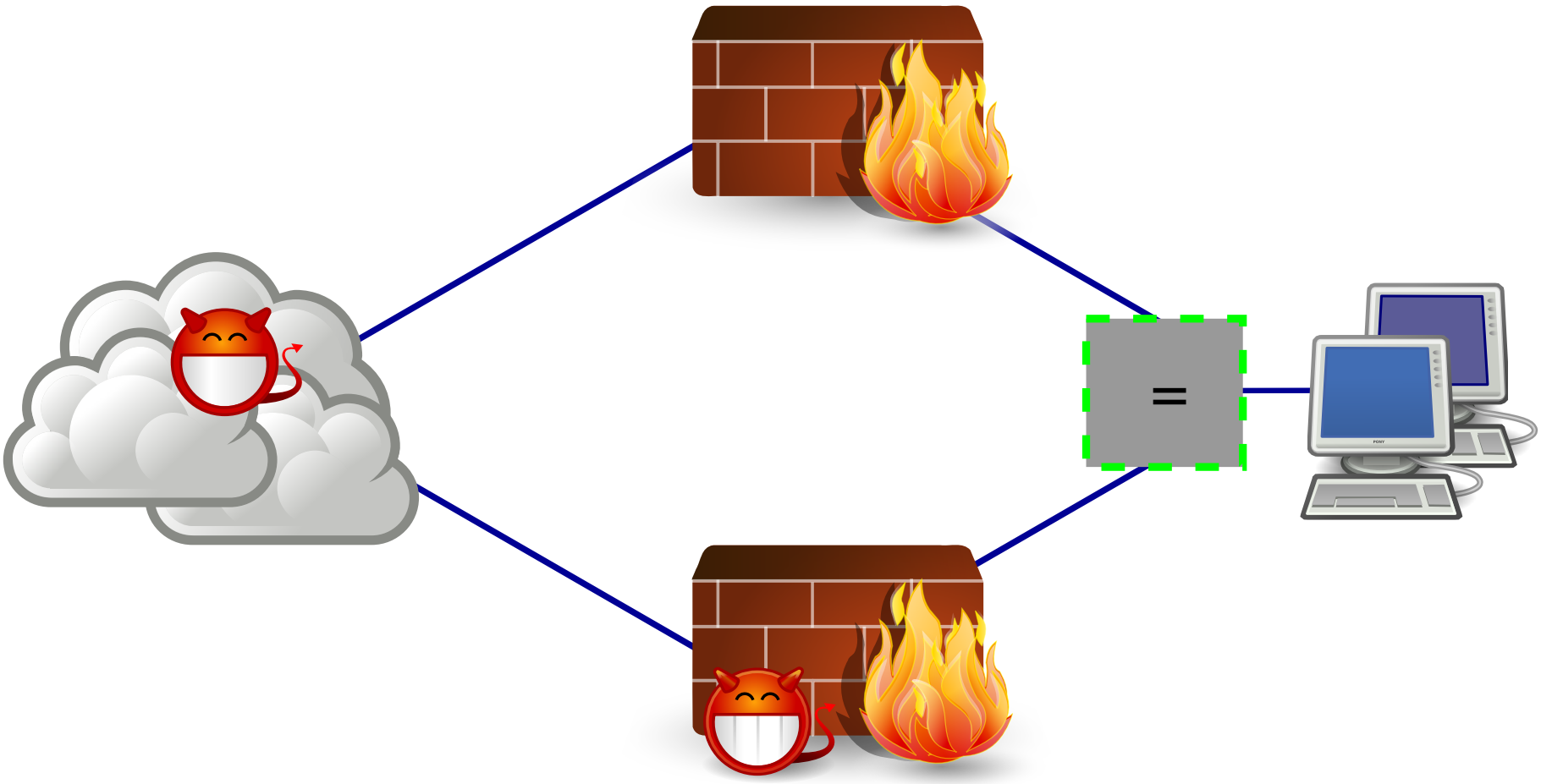
What if you don’t trust your firewall?

Previously . . .



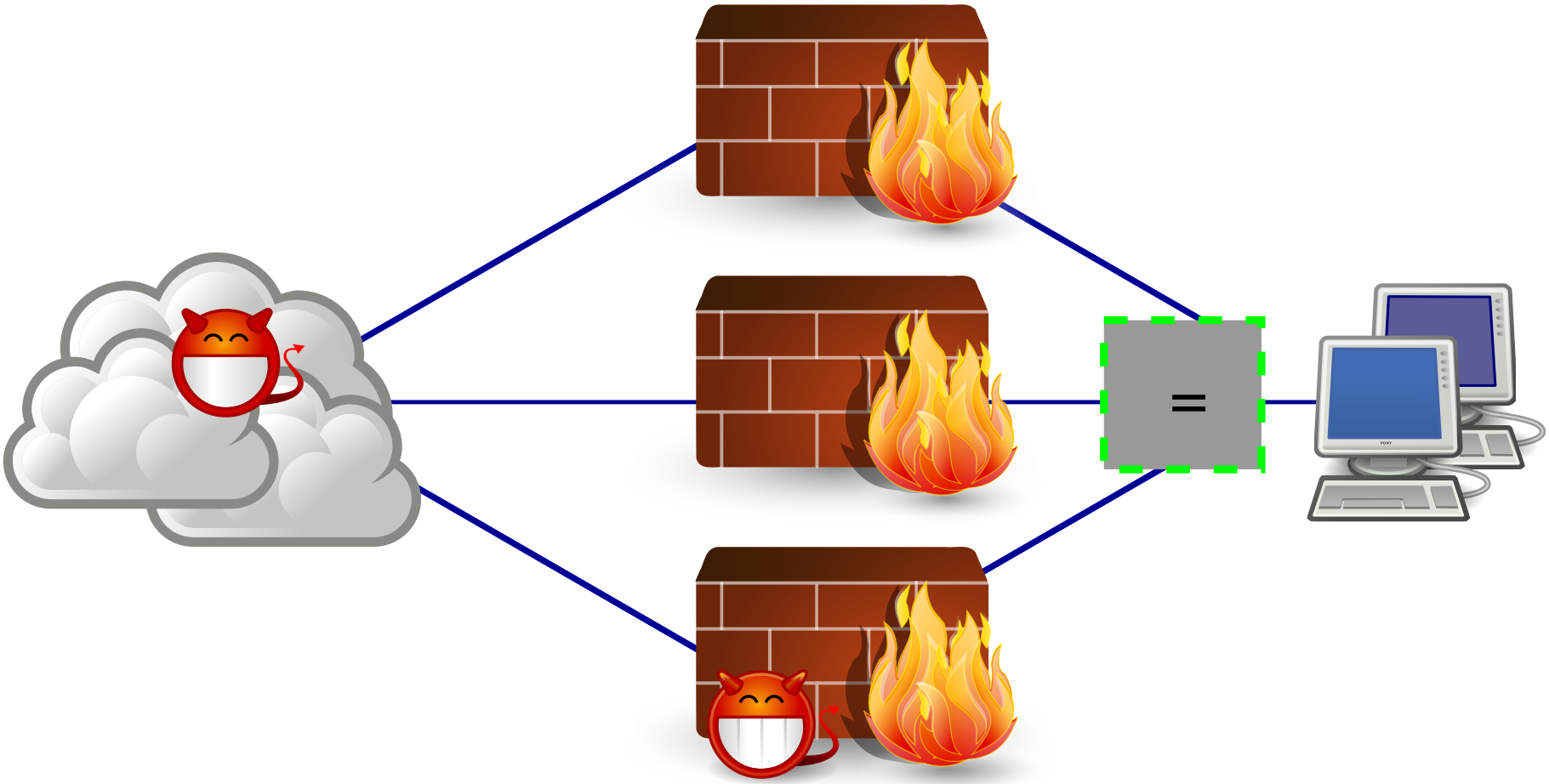
Use two?

Previously . . .



Or this way?

Previously . . .



Or use three?

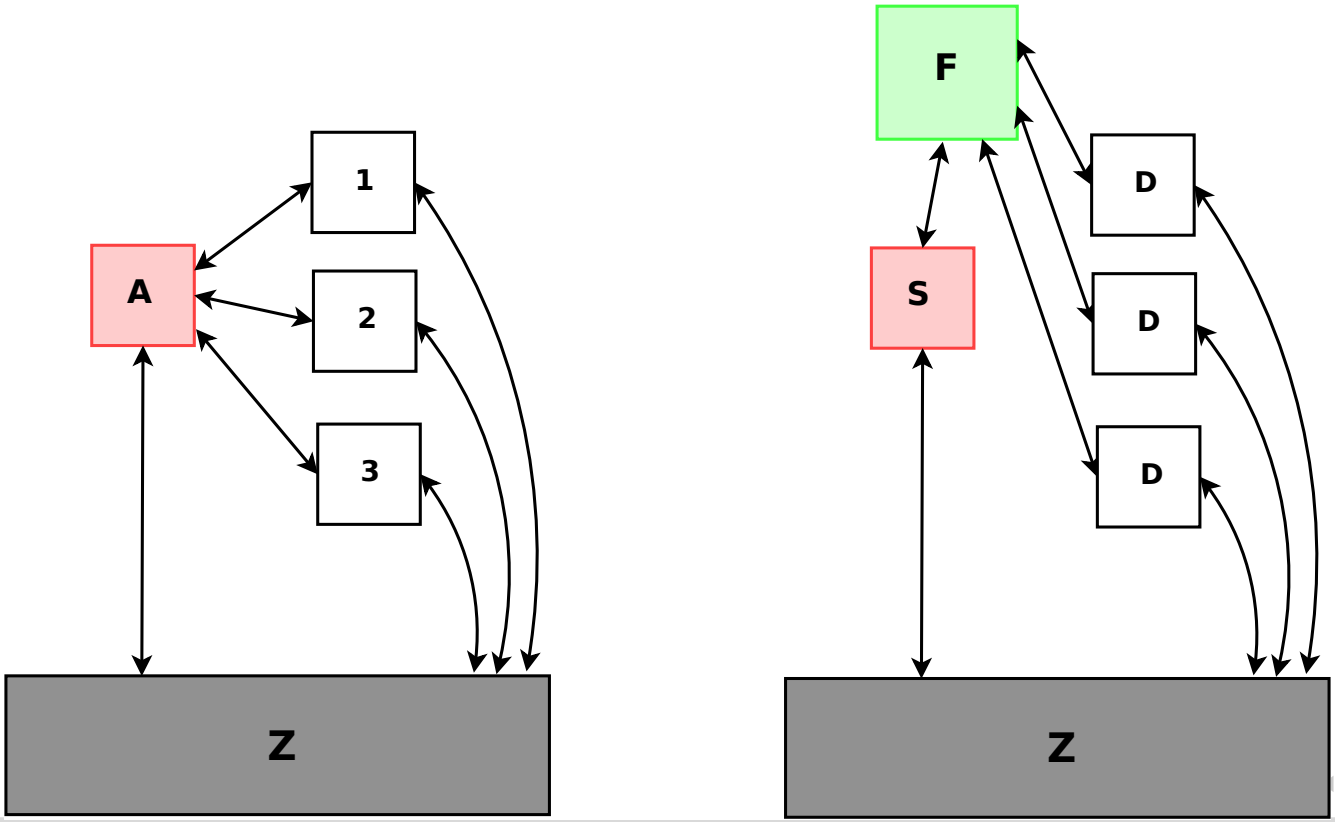
Previously . . .

How can we investigate this in a formal cryptographic model?

The Universal Composability Framework (Canetti [2])

A protocol π securely realises an ideal functionality $\mathcal{F}$ iff

$$\forall \mathcal{A} \exists \mathcal{S} \forall \mathcal{Z} : \text{REAL}_{\pi,\mathcal{A},\mathcal{Z}} \approx \text{IDEAL}_{\mathcal{F},\mathcal{S},\mathcal{Z}}$$



Why UC?

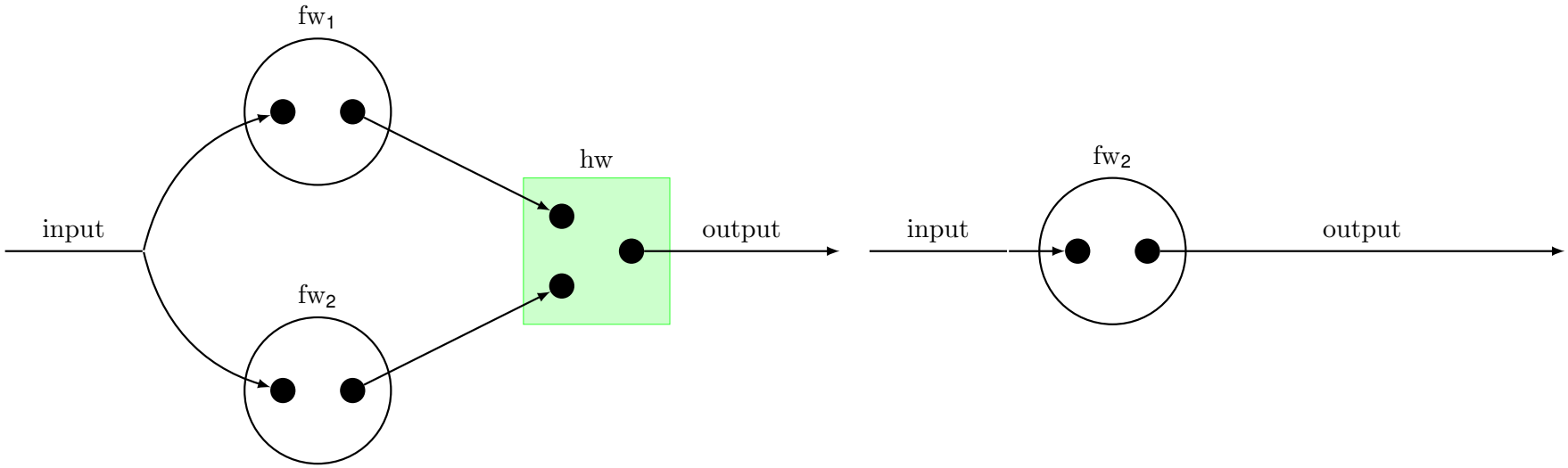
It provides a Composition Theorem which makes it possible to construct secure networks from smaller components:

Theorem (Composition Theorem [2])

Let ρ, ϕ, π be protocols such that ρ uses ϕ as subroutine and π UC-emulates ϕ. Then protocol $\rho^{\phi \to \pi}$ UC-emulates ρ.

Why UC?

It should be easy to judge the security properties of a protocol based on its ideal functionality.



The Universal Composability Framework (Canetti [2])

Using UC, we can formally prove that one firewall solution is more secure than another . . .

. . . but we do not get any statements about availability.

Synchronous Composability (Katz et al. [3])

We get

- A global clock functionality $\mathcal{F}_{\text{clock}}$.
- A model for channels with bounded delay $\mathcal{F}^{\delta}$.

This suffices to model synchronous communication ([3]) and therefore availability!

Synchronous Composability (Katz et al. [3])

This extension makes the UC framework even more difficult to use however.

- The environment now schedules the protocol execution (makes the description of the protocol difficult).
- Parties can base their computation on the number of times they have been activated (make the description of protocols difficult).
- The number of activations is also important for the ideal model (make the description of ideal functionalities difficult).
- Also the underlying network has to be modeled using $\mathcal{F}^{\delta}$ which has to memorize the delay for each available channel.

Our contribution

- We give a structured methodology to model computer networks using UC and Katz's extension (5-phase paradigm).
- We give a generic ideal network functionality $\mathcal{F}_{\text{net}}^{G,\delta}$ for networks, which instantiates $\mathcal{F}^{\delta}$ from the graph G of the network.
- We give a wrapping functionality $\mathcal{F}_{\text{wrap}}$ which acts as a wrapper around the ideal functionality and hides artifacts of the model which are difficult to handle.
- We extend the result of Achenbach et al. with availability guarantees.

Specifically: 5-phase Paradigm

Goal: Facilitate the description of the network protocol

Each party will require exactly 5 activation before it finishes its round.

1. “input phase”: party will accept input by the environment.
2. “fetch phase”: party will fetch messages from the network channel.
3. “send phase”: party will compute a response and send it to other parties using a single call.
4. “output phase”: party can produce output to the environment.
5. “RoundOK phase”: party will notify $\mathcal{F}_{\text{clock}}$ that it is finished with this round.

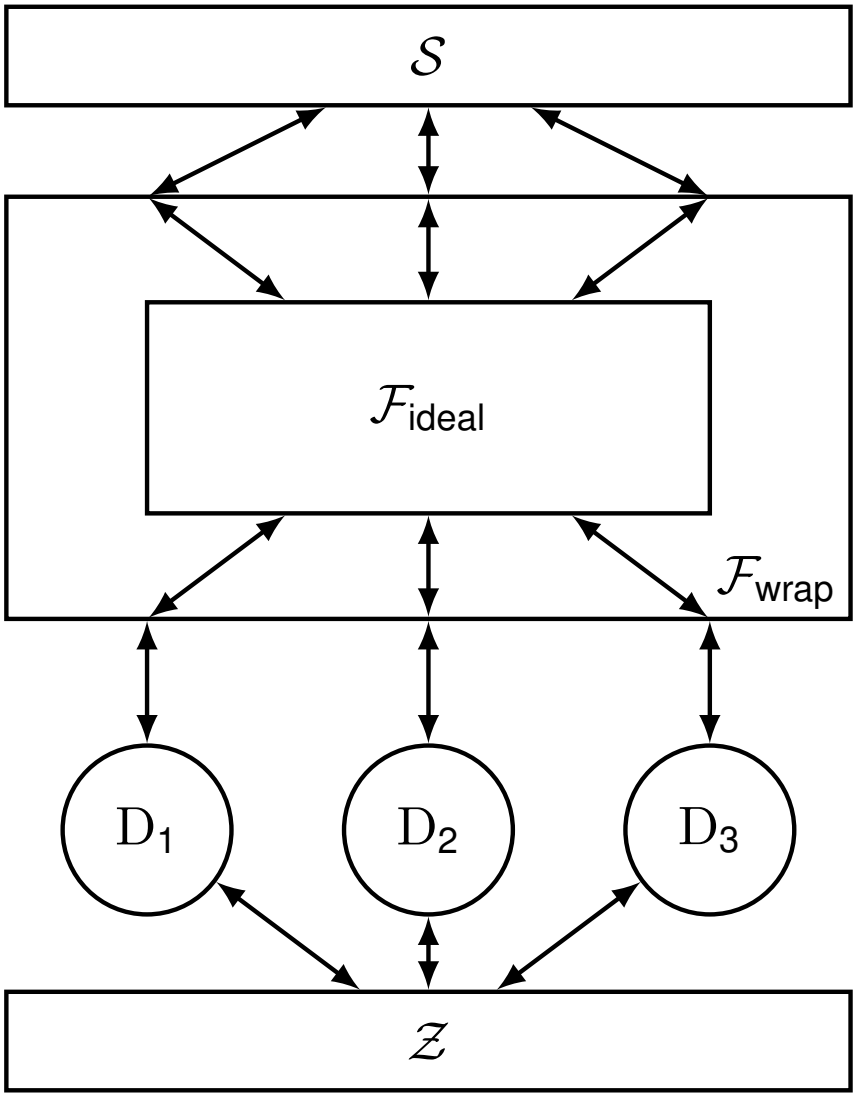
Specifically: $\mathcal{F}_{\text{wrap}}$

Goal: Facilitate the description of the ideal functionality.

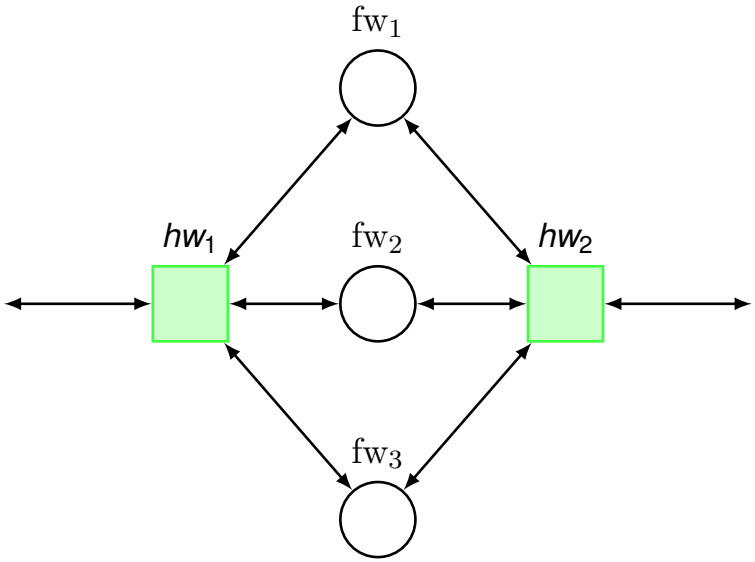
Maintain an activation counter c_p for each of the honest dummy parties. Relay all communication from $\mathcal{F}_{\text{ideal}}$ directly to the environment. Upon activation by the environment, i.e. upon receiving input m through a dummy party p:

- If $c_p < 5$ increase the activation counter of the party.
- If $c_p = 1$ send message (input, m, p) to $\mathcal{F}_{\text{ideal}}$.
- If $c_p = 2$ or $c_p = 3$, send message $(\text{activated}, \text{p})$ to the adversary.
- If $c_p = 4$ send message (output, p) to $\mathcal{F}_{\text{ideal}}$.
- If $\forall p' : c_{p'} = 5$ reset all activation counters and send (RoundComplete) to $\mathcal{F}_{\text{ideal}}$.

Specifically: $\mathcal{F}_{\text{wrap}}$



Specifically: $\mathcal{F}_{\text{net}}^{G}$



$\mathcal{F}_{\text{net}}^{G}$: $G = (V, E)$ with $V = \{hw_1, hw_2, fw_1, fw_2, fw_3\}$ and $E' = \{(hw_1, fw_1), (hw_1, fw_2), (hw_1, fw_3), (hw_2, fw_1), (hw_2, fw_2), (hw_2, fw_3)\}$, $E = E' \cup \{(v, u) \mid (u, v) \in E'\}$.

Future Work

- Extend the model to adaptive corruption
- We need even an even simpler model for investigating the security of networks (it should imply the security in the UC model however)

Bibliography I

Dirk Achenbach, Jörn Müller-Quade, and Jochen Rill. “Universally Composable Firewall Architectures Using Trusted Hardware”. English. In: *Cryptography and Information Security in the Balkans*. Ed. by Berna Ors and Bart Preneel. Vol. 9024. Lecture Notes in Computer Science. Springer International Publishing, 2015, pp. 57–74. ISBN: 978-3-319-21355-2. DOI: 10.1007/978-3-319-21356-9_5. URL: http://dx.doi.org/10.1007/978-3-319-21356-9_5.

Ran Canetti. “Universally composable security: a new paradigm for cryptographic protocols”. In: *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*. Oct. 2001.

Bibliography II

Jonathan Katz et al. “Universally Composable Synchronous Computation”. In: *Theory of Cryptography*. Ed. by Amit Sahai. Vol. 7785. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 477–498. ISBN: 978-3-642-36593-5. DOI: 10.1007/978-3-642-36594-2_27. URL: http://dx.doi.org/10.1007/978-3-642-36594-2_27.