(DE-) CONSTRUCTING TLS 1.3

[paper published at indocrypt 2015]

Markulf Kohlweiss	Microsoft Research
Ueli Maurer	ETH Zürich
Cristina Onete	INSA/IRISA Rennes
Björn Tackmann	UC San Diego
Daniele Venturi	Sapienza Univ. of Rome

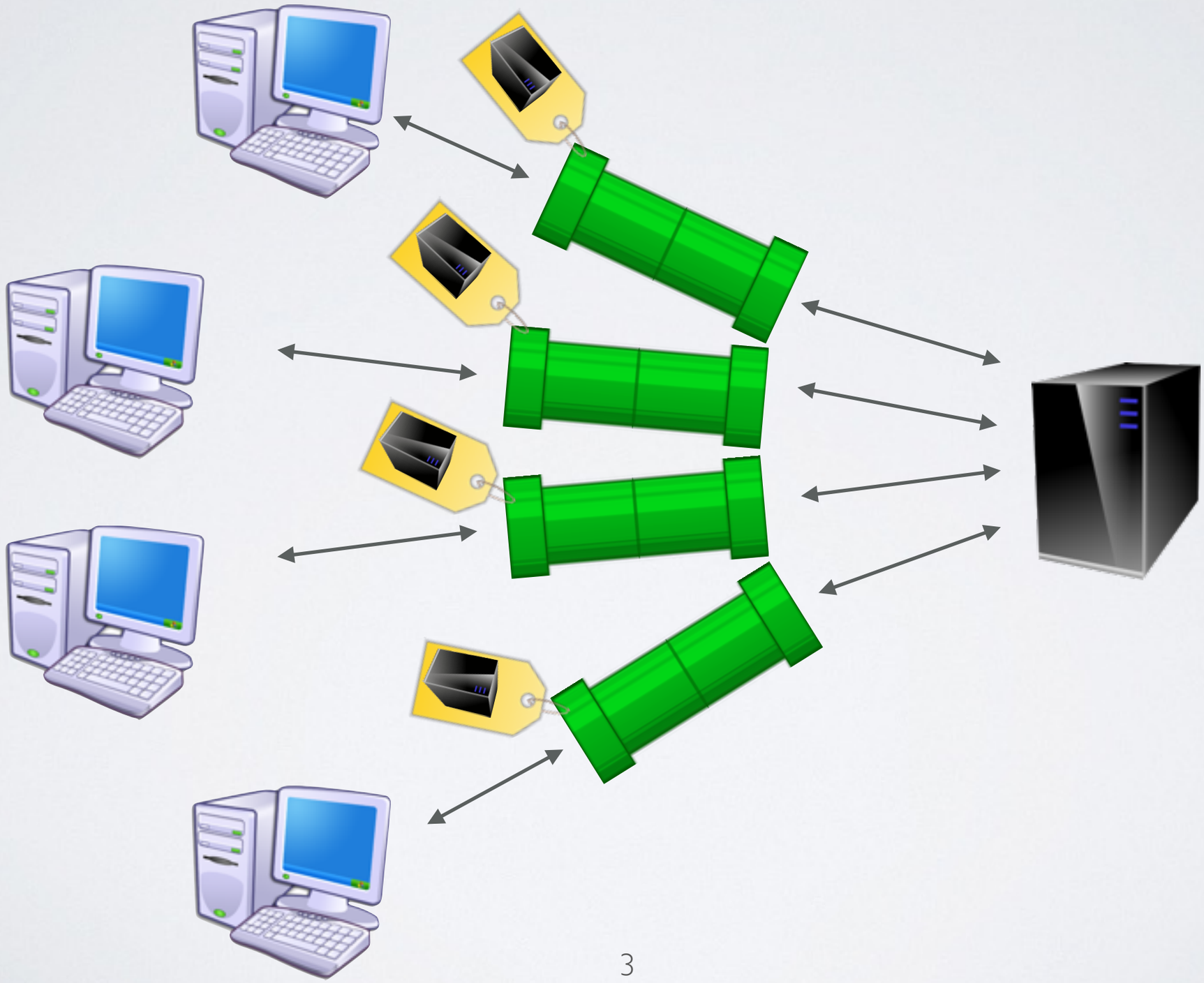
TRON Workshop @NDSS, San Diego, 21 February 2016

TECHNICAL RESULTS

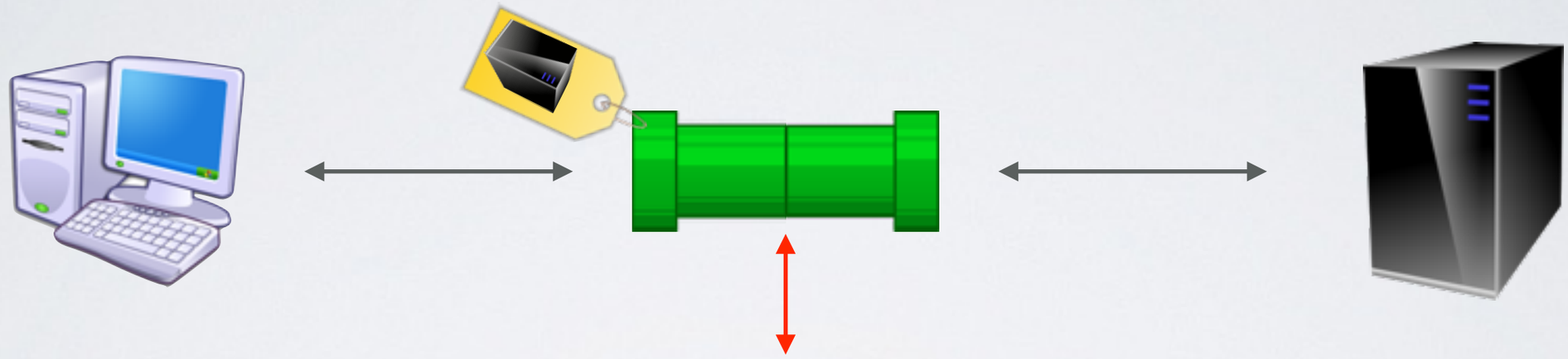
we prove the security of:

- signature-based diffie-hellman mode
- version 9 of the draft, october 2015
- basic security (honest server, no forward secrecy, no client auth, no downgrade analysis)
- caveat: we do **not** encrypt the certificate
- … but we learn more than just the facts during the analysis!

WHAT DOES TLS GIVE US?

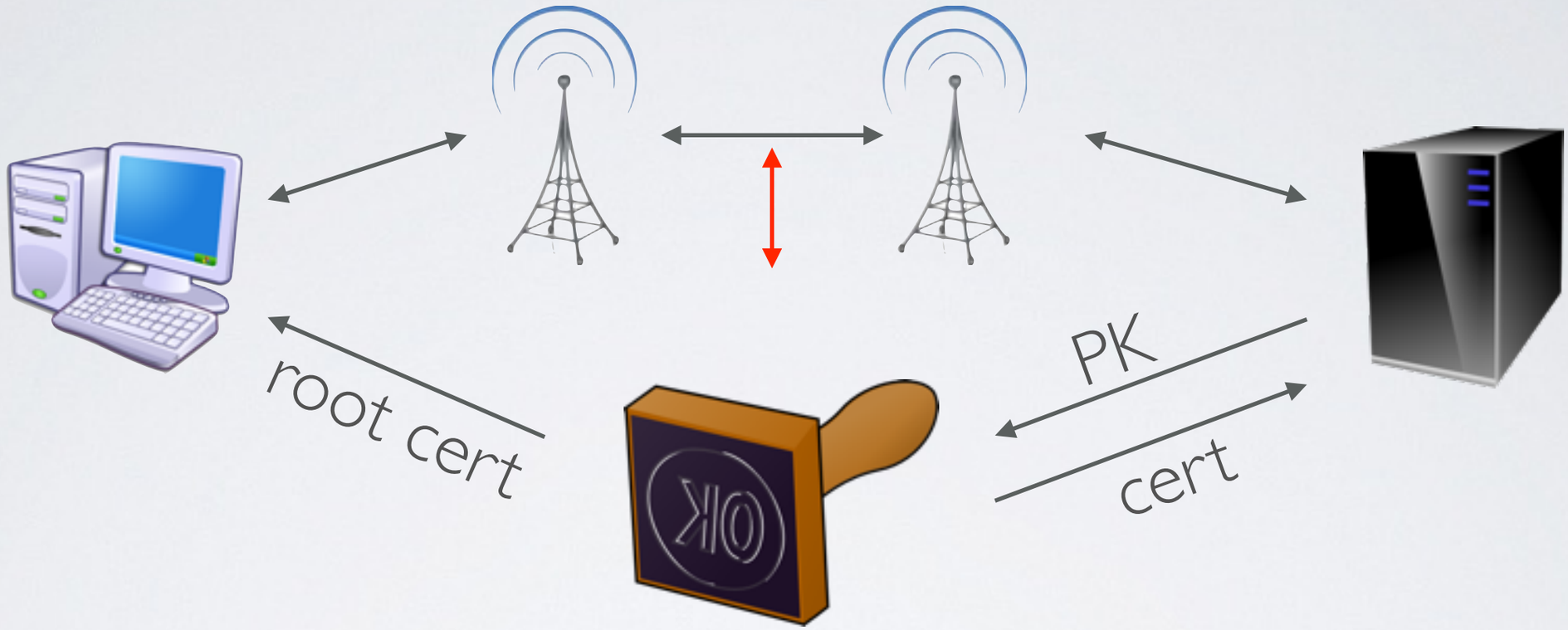


WHAT DOES TLS GIVE US?



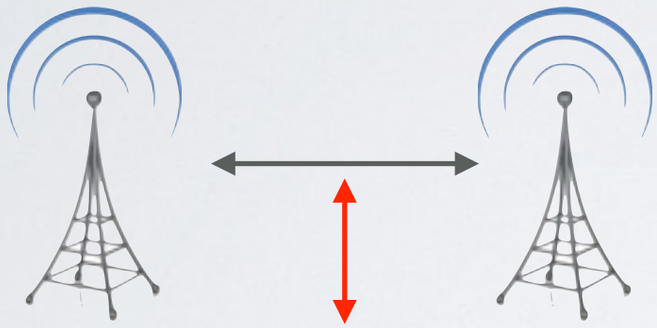
- bidirectional communication
- tls fragments of up to 2^{14} bytes
- attacker may learn message length
- attacker may interrupt the channel between fragments

WHAT DOES TLS ASSUME?

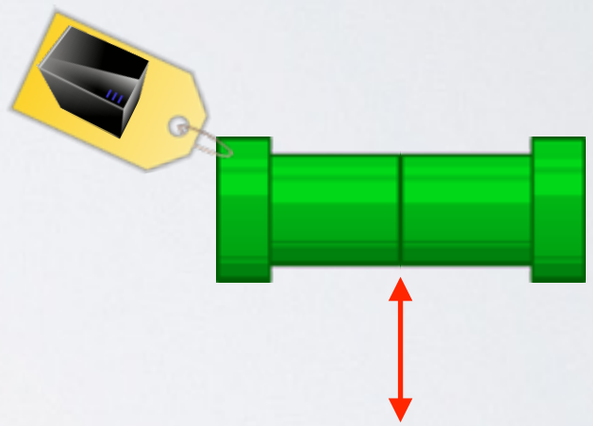


- bidirectional communication
- messages are tls fragments of up to $2^{14}+256$ bytes
- attacker controls communication
- “functional” pki

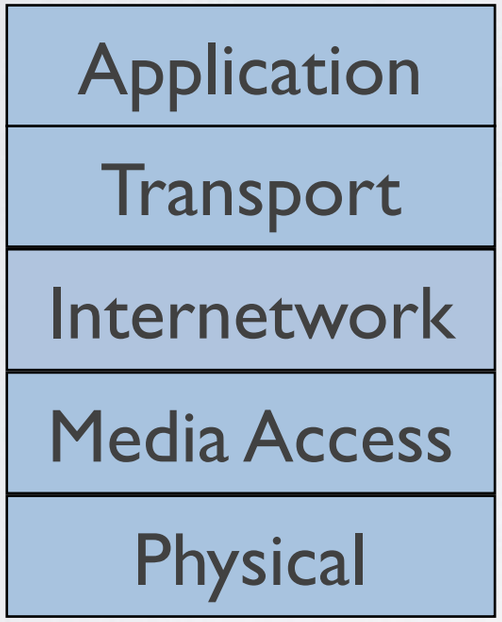
CONSTRUCTIVE SECURITY DEFINITIONS

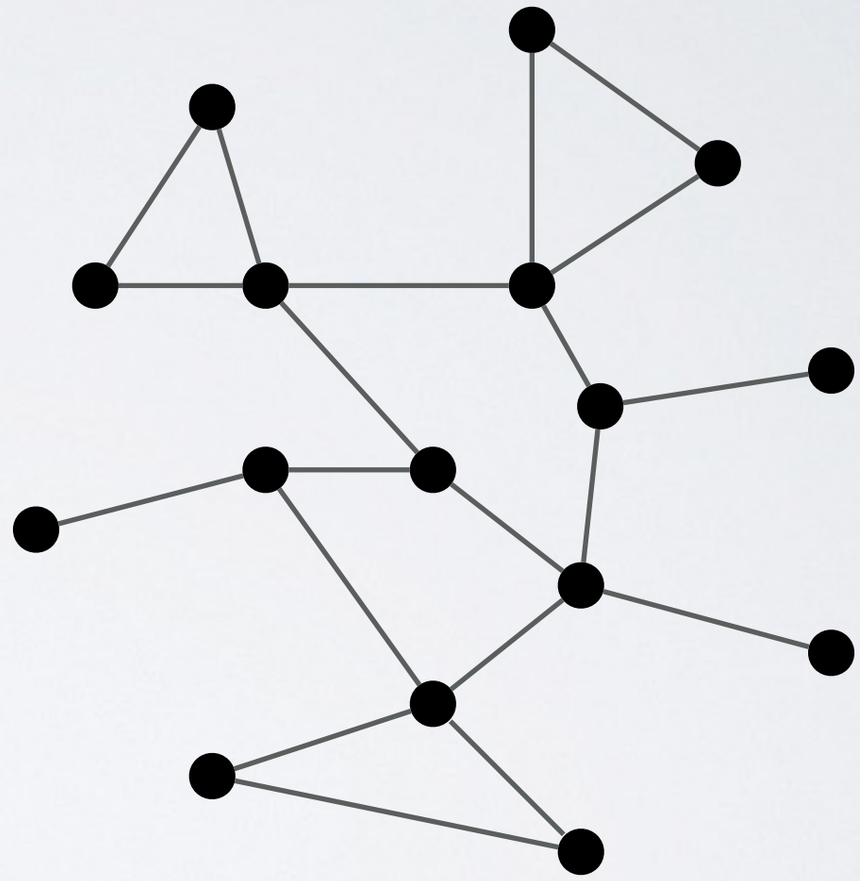


tls

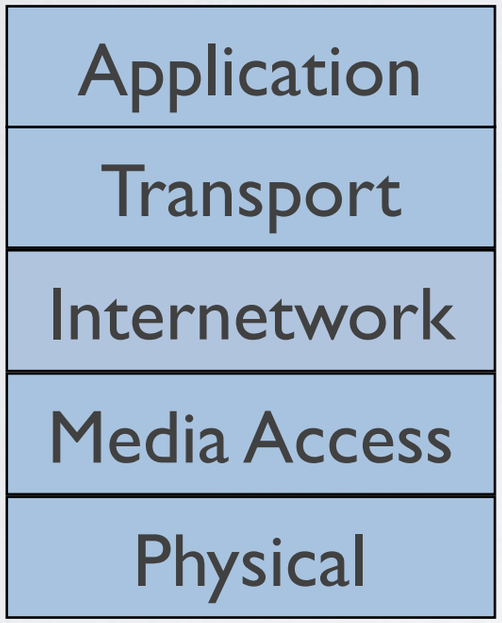


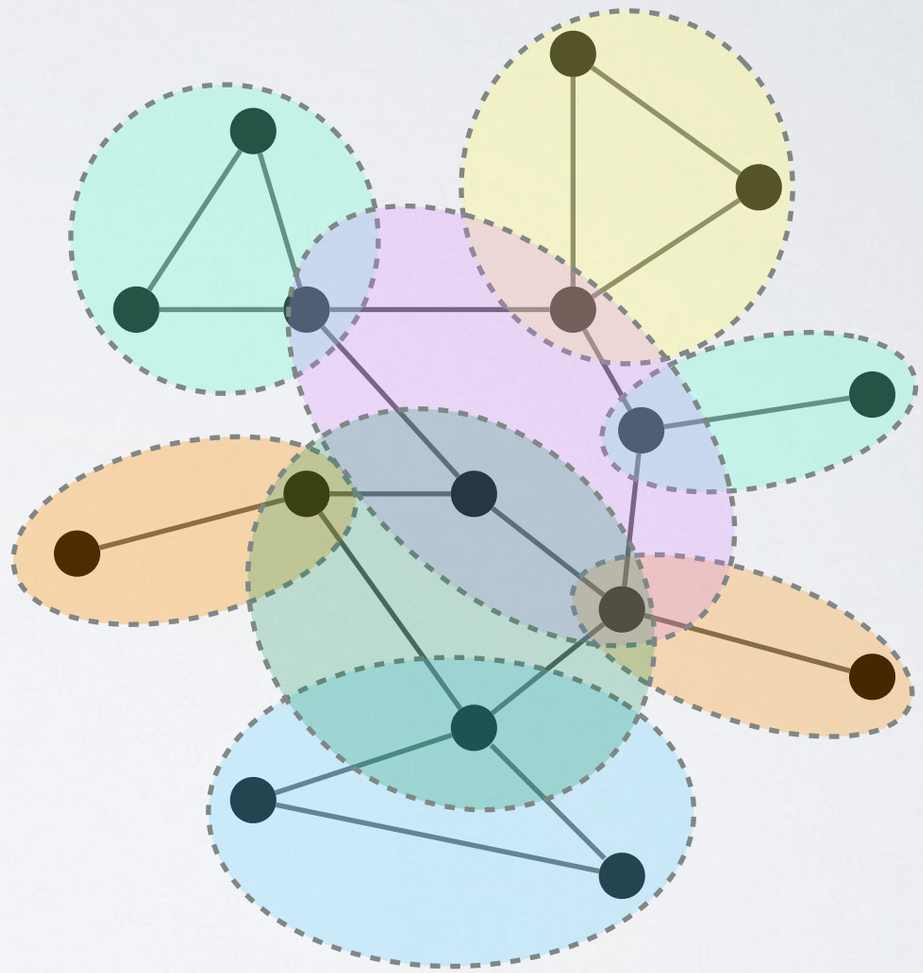
PROTOCOL STACKS



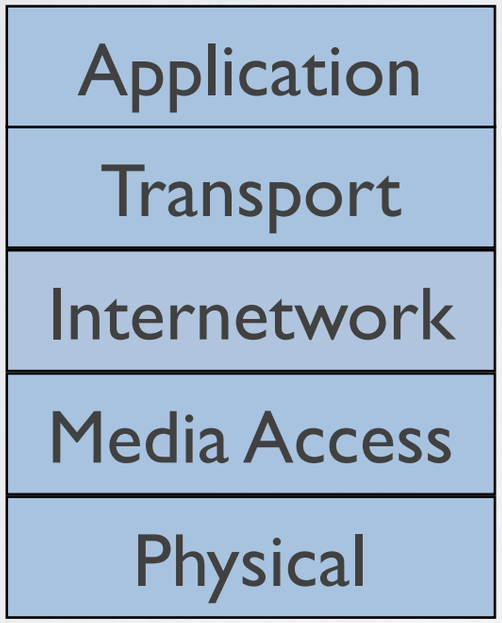


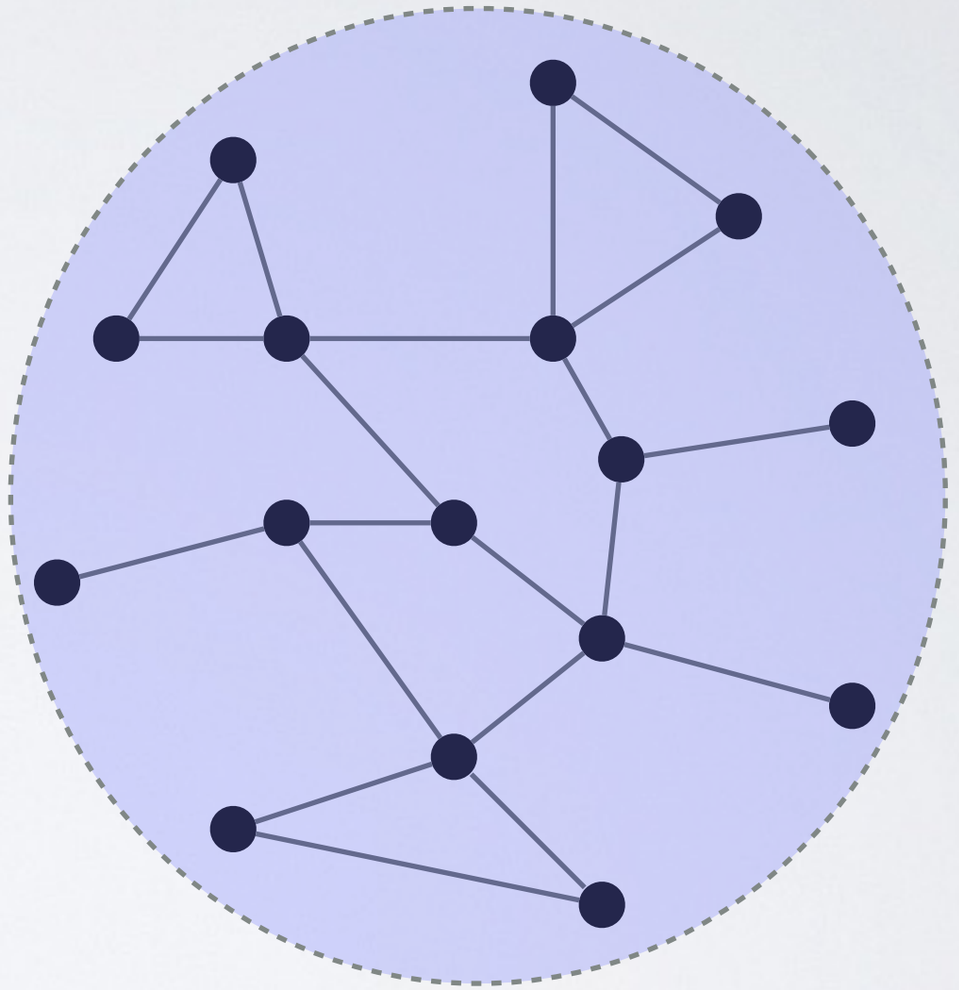
PROTOCOL STACKS



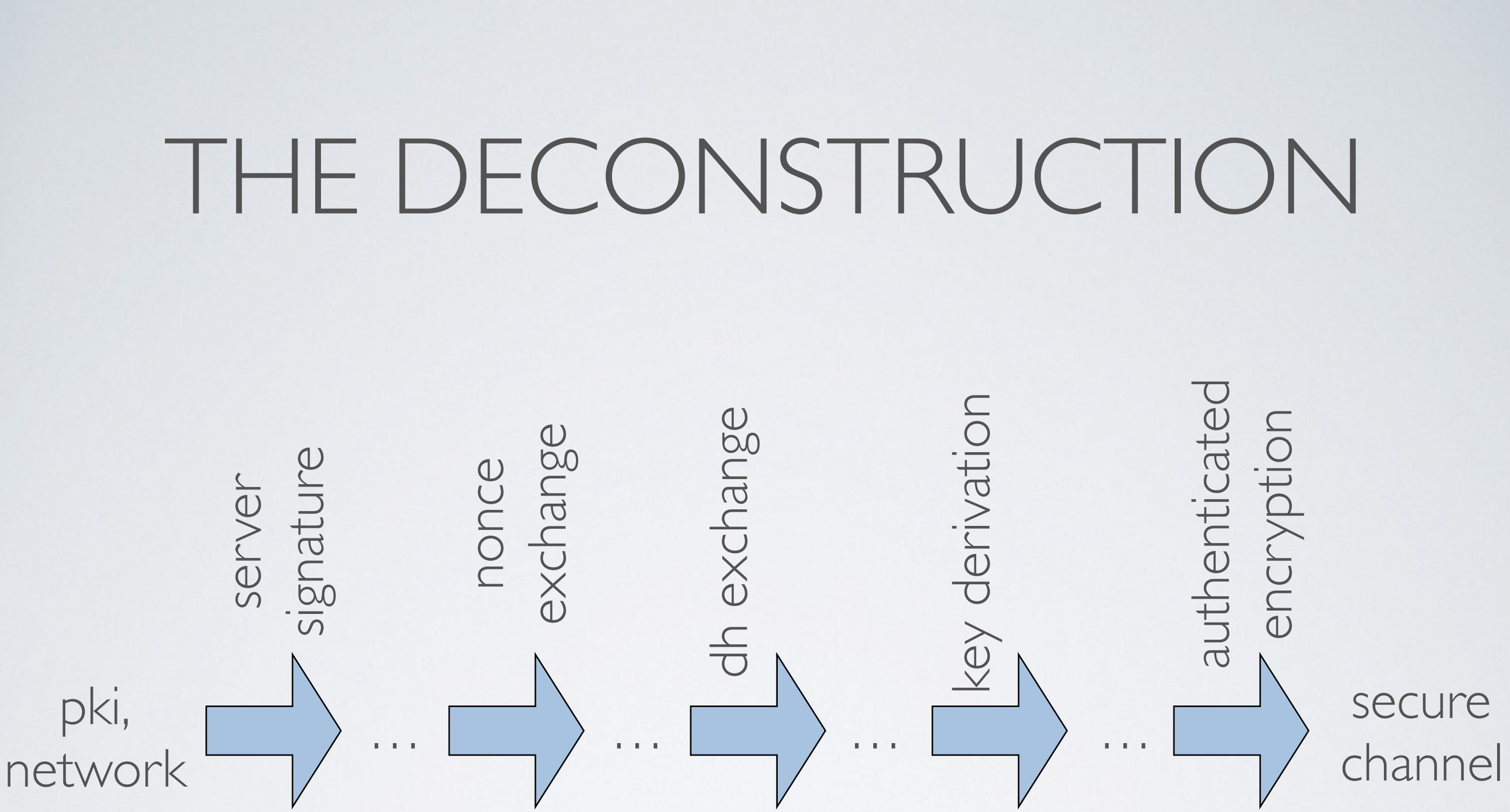


PROTOCOL STACKS

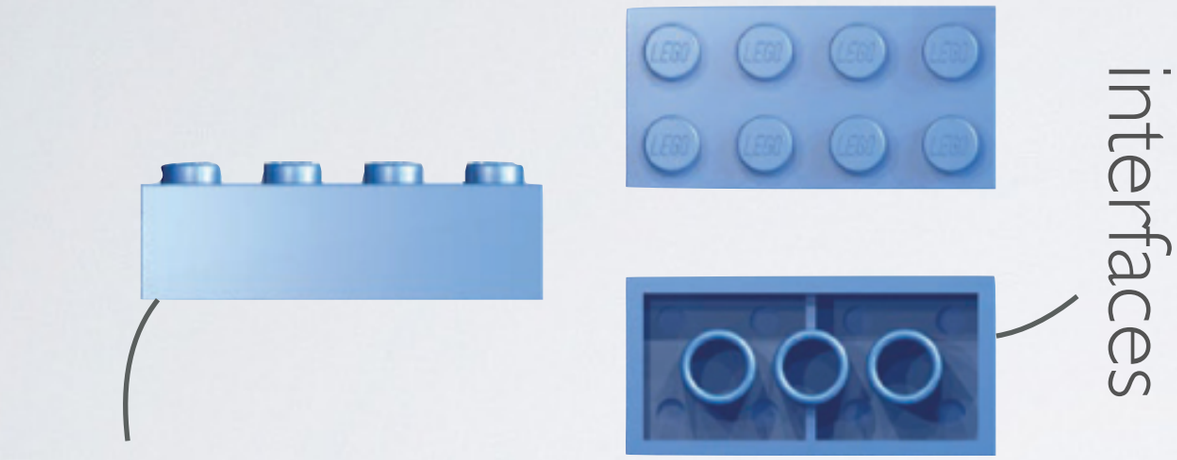




THE DECONSTRUCTION



MODULARITY



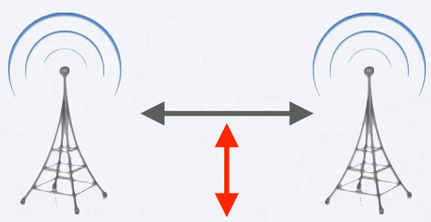
composable analysis
of security mechanisms

simplifies *modular*
design of protocols

SERVER SIGNATURE

=

assumes:

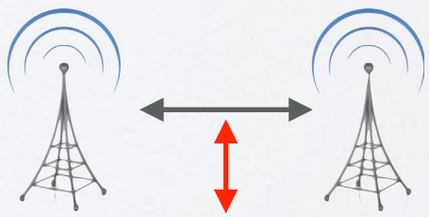


SERVER SIGNATURE

constructs:

server-authenticated message exchange

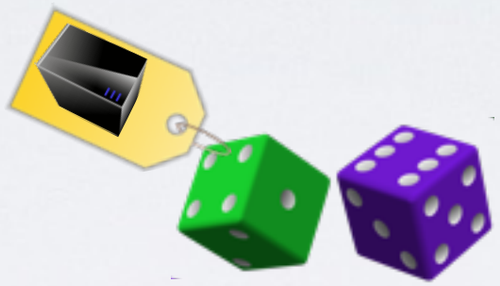
unauthenticated communication
is still available:



NONCE EXCHANGE

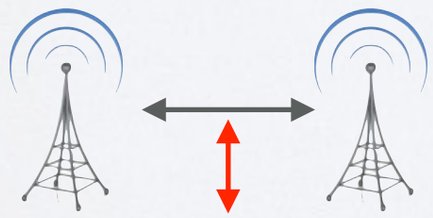
NONCE EXCHANGE

constructs:

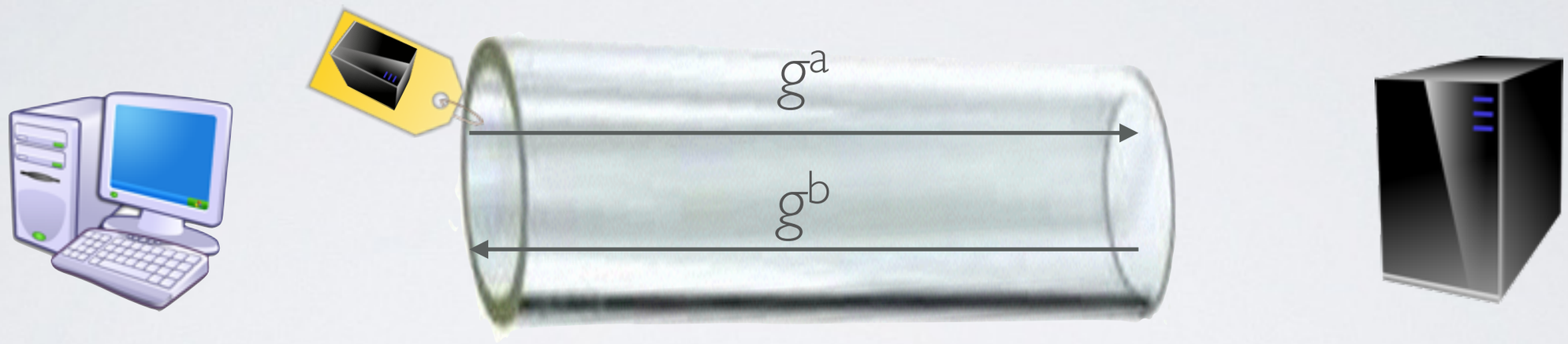


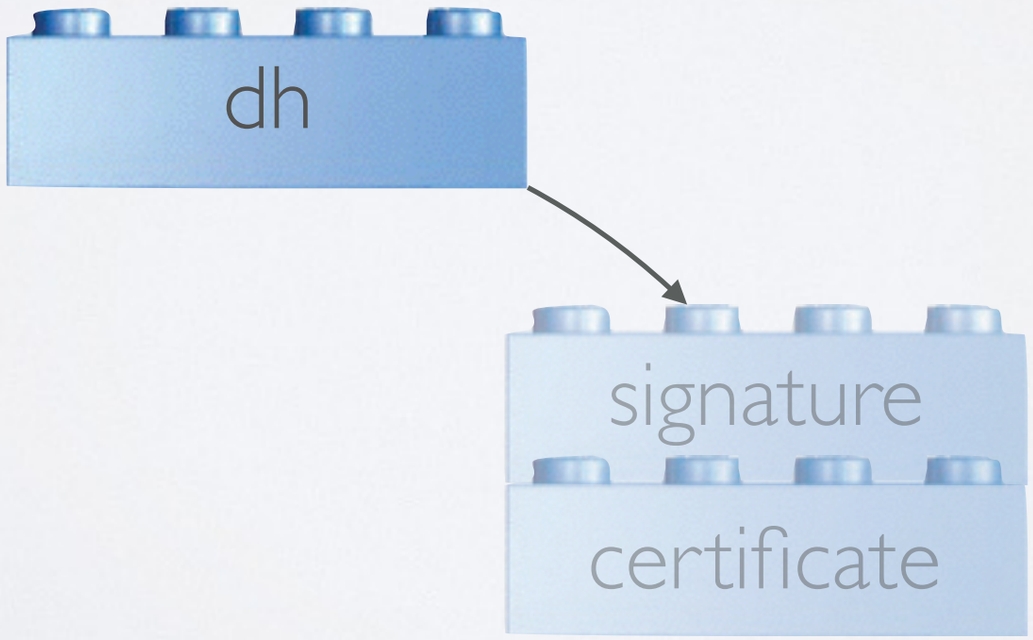
nonces shared between client and server

still available:



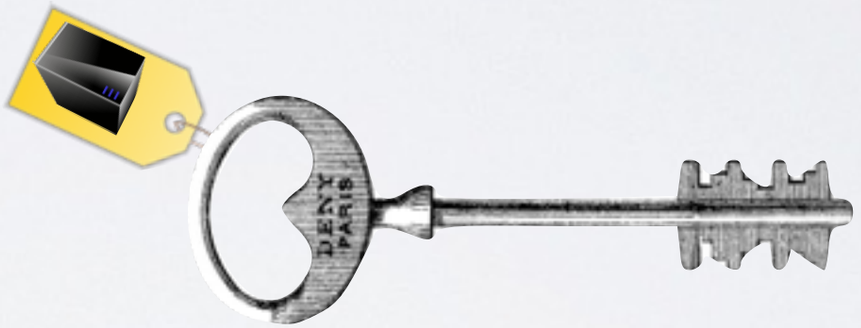
DIFFIE-HELLMAN EXCHANGE





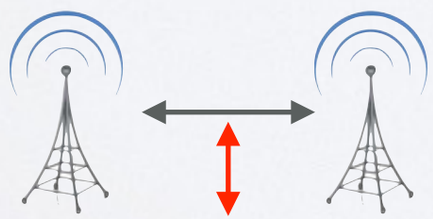
DIFFIE-HELLMAN EXCHANGE

constructs:



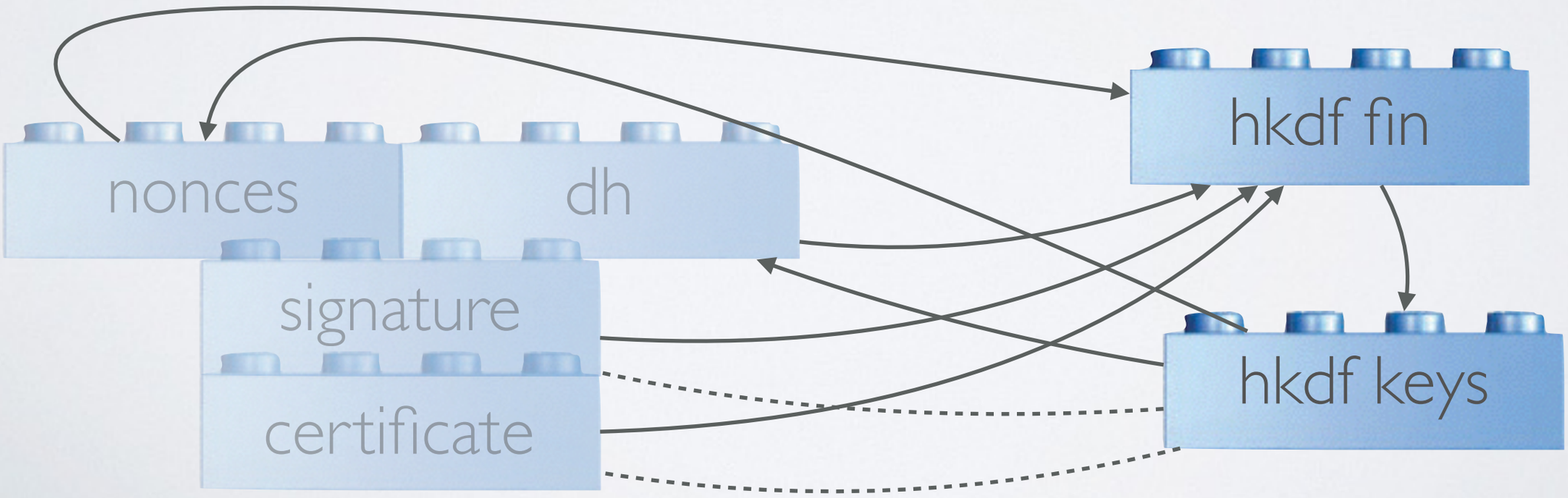
server-authenticated premaster key

still available:



KEY COMPUTATIONS

local computation on



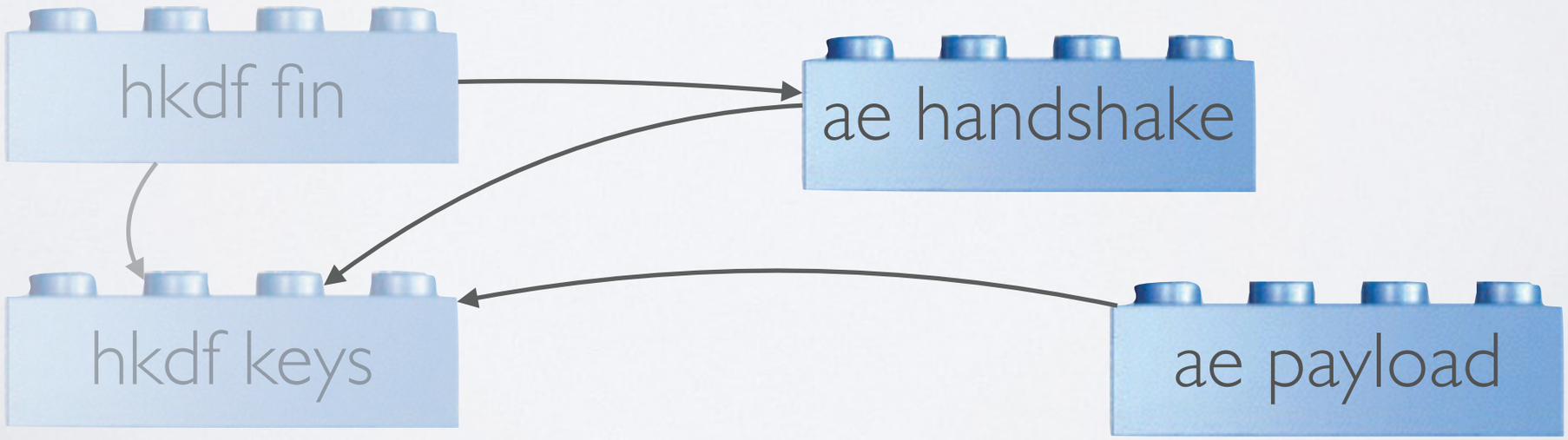
KEY COMPUTATIONS

constructs:

server-authenticated traffic (etc.) keys

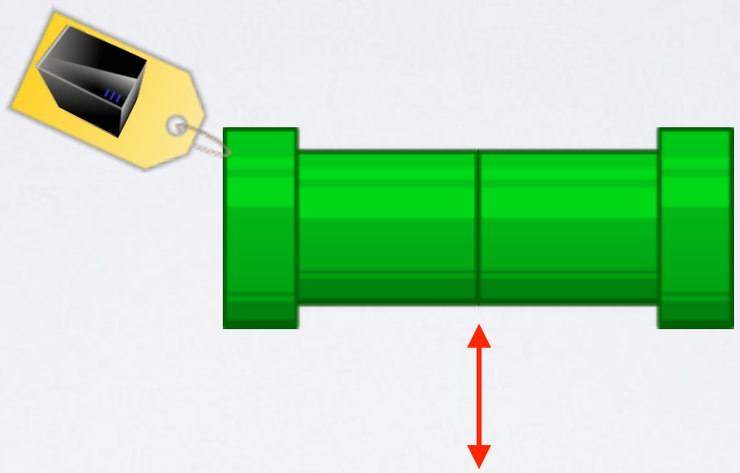
finished messages

PAYLOAD PROTECTION



PAYLOAD PROTECTION

constructs:

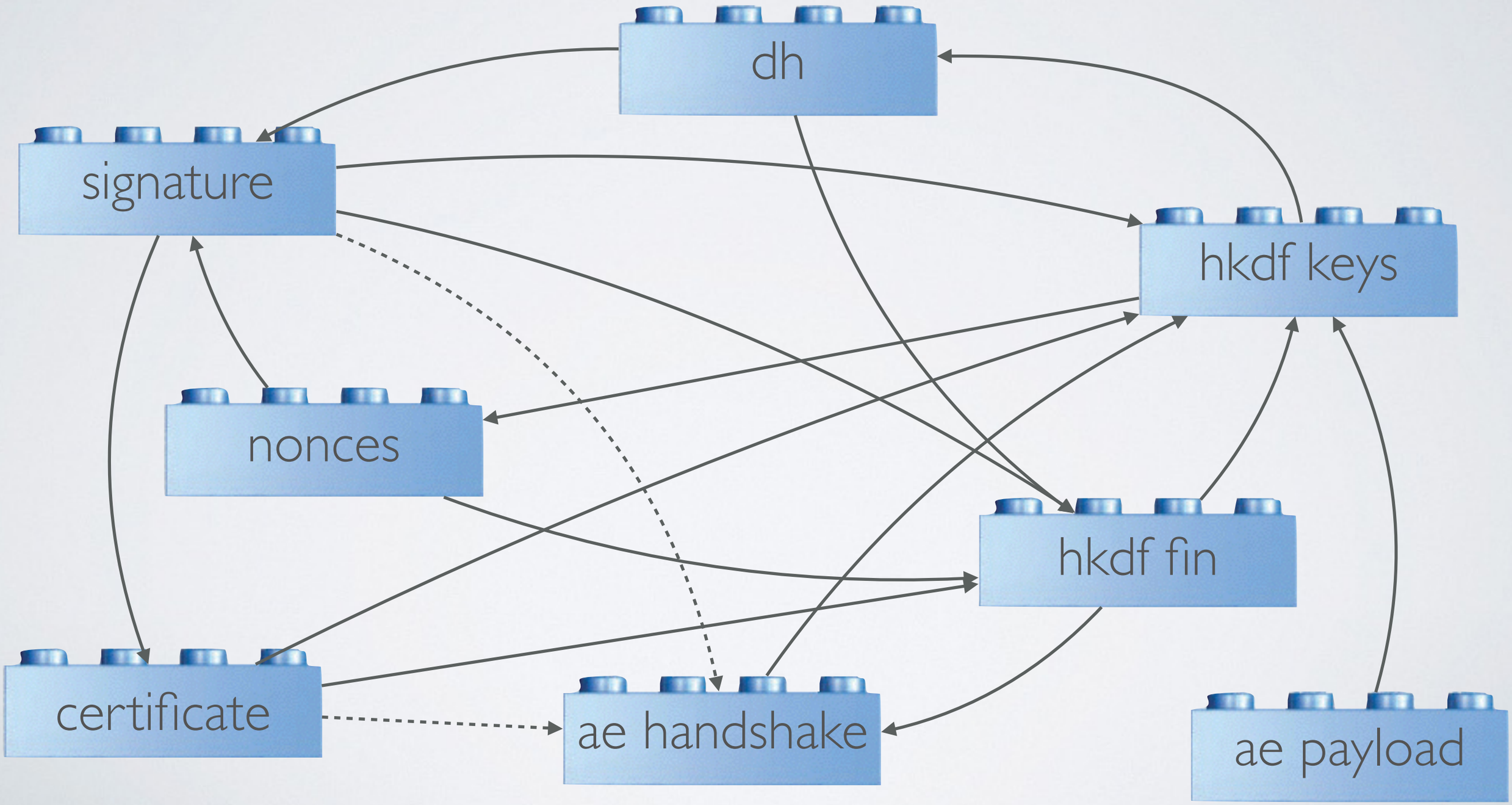


server-authenticated secure channel

[badertscher, matt, maurer, rogaway, t., provsec 2015]

IS TLS 1.3 READY OR NOT?

WHAT ABOUT LEGO?



INSIGHTS FROM ANALYSIS

- we can make the proof work…
- separation of keys simplifies analysis
- "hashing everything" impedes modularization
- mutual dependencies (e.g., certificate/signature/dh exchange) do as well
- usefulness of nonces/finished messages unclear in our analysis