Part III
TLS 1.3 and other Protocols

TECHNISCHE UNIVERSITÄT DARMSTADT

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

8th BIU Winter School on Key Exchange, 2018

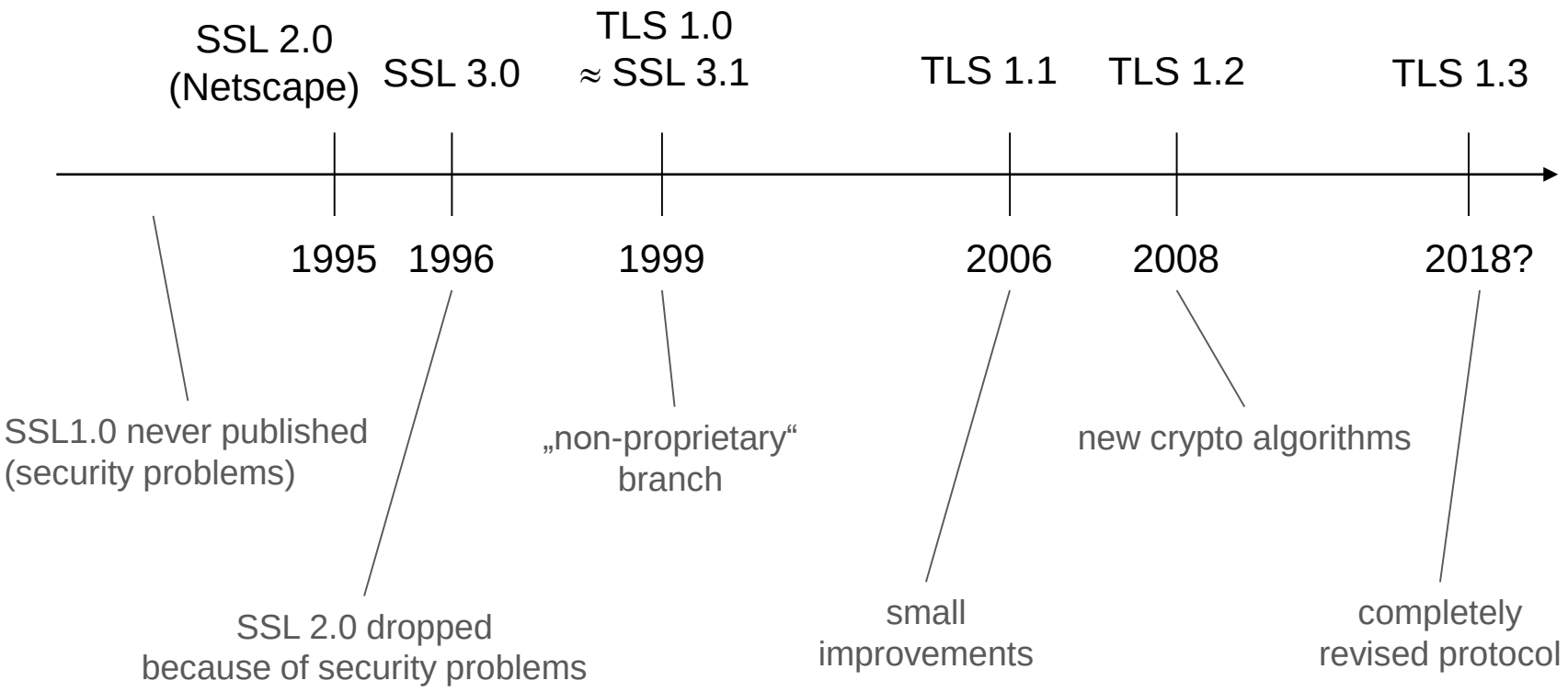
Marc Fischlin

TLS 1.3

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

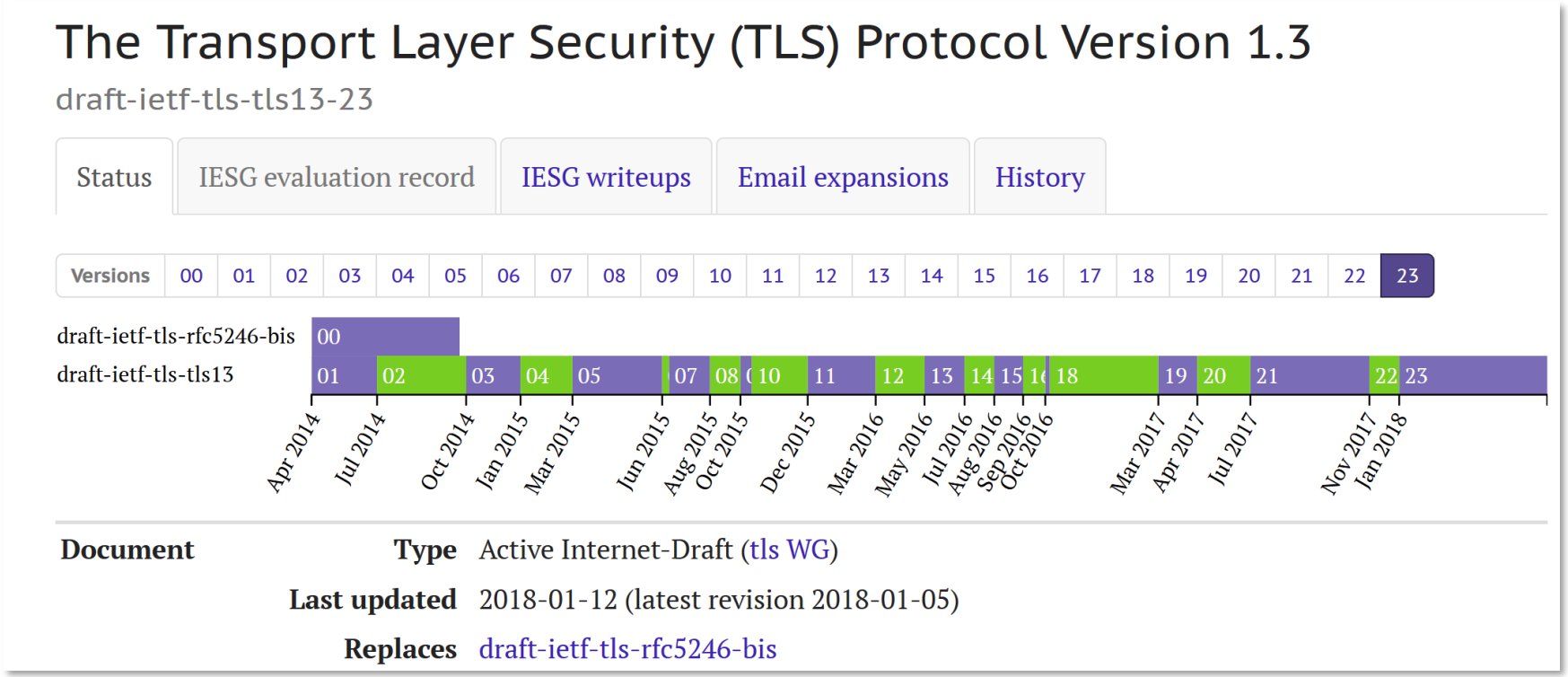
Development of SSL/TLS

SSL=Secure Socket Layer
TLS=Transport Layer Security



TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

The Path to TLS 1.3

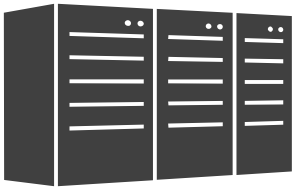


https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity

TLS 1.3: (EC)DHE-Handshake Overview

ClientHello
ClientKeyShare



ServerHello
ServerKeyShare

handshake key

handshake key

{ServerConfiguration*}
{ServerCertificate*}
{ServerCertificateVerify*}
{ServerFinished}

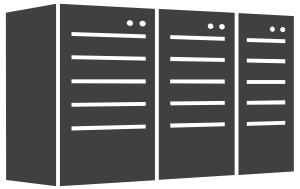
{ClientCertificate*}
{ClientCertificateVerify*}
{ClientFinished}

channel key

channel key

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

TLS 1.3: (EC)DHE-Handshake (Crypto Details)



CH
CKS
$r_c \leftarrow \{0,1\}^{256}$
g^x

$r_s \leftarrow \{0,1\}^{256}$
g^y
SH
SKS

handshake key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{SKS})$

handshake key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{SKS})$

{SConf*}
pk_S, cert_S {SCert*}
s {SCertV*}
t {SF}

$s \leftarrow \mathrm{Sign}(\mathrm{sk}_s, \mathtt{CH} \ldots \mathtt{SCert})$
$t \leftarrow \mathrm{MAC}(\mathrm{k}_{\mathrm{SF}}, \mathtt{CH} \ldots \mathtt{SCert})$

derived from handshake key

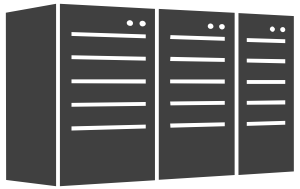
{CCert*}
{CCertV*}
{CF}

channel key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{CF})$

channel key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{CF})$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

TLS 1.3: (EC)DHE-Handshake (Crypto Details)



CH
CKS

SH
SKS

handshake key
- client hs traffic key
- server hs traffic key
- client MAC key
- server MAC key

{SConf*}
{SCert*}
{SCertV*}
{SF}

{CCert*}
{CCertV*}
{CF}

- exporter EMS
- resumption RMS
- client app traffic key
- server app traffic key

channel key (master secret)

handshake key
- client hs traffic key
- server hs traffic key
- client MAC key
- server MAC key

- exporter EMS
- resumption RMS
- client app traffic key
- server app traffic key

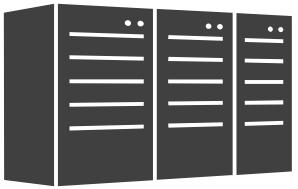
channel key (master secret)

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity

Pre-Shared Key (PSK) Variant

PSK

```
ClientHello
ClientKeyShare*
early_data
psk_key_exchange_modes
pre_shared_key
```



PSK

externally or from **RMS**

```
ServerHello
ServerKeyShare*
pre_shared_key
{EncryptedExtensions}
{ServerFinished}
```


TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

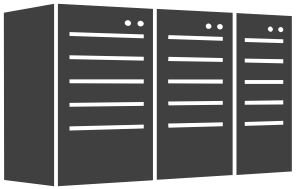
Analysis of Unilateral DH Case

Dowling, Fischlin, Günther, Stebila:
A Cryptographic Analysis of the TLS 1.3 Handshake Protocol Candidates, CCS 2015 (eprint)

$r_c,\ g^x$

$r_s,\ g^y$

$\mathrm{pk}_S,\ \mathrm{cert}_S,\ s$



$s \leftarrow \mathrm{Sign}(\mathrm{sk}_s, \texttt{CH}\ldots\texttt{SCert})$

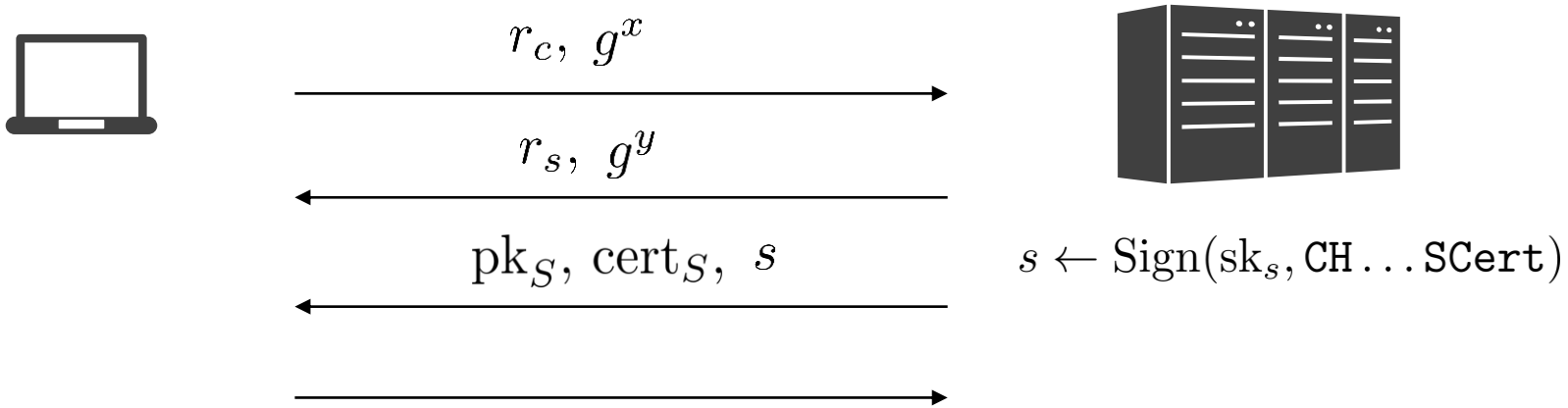
$\mathrm{pid} = \mathrm{cert}_S \qquad \mathrm{sid} = (r_c, g^x, r_s, g^y, \mathrm{pk}_S, \mathrm{cert}_S)$

simplification here: no encryption in handshake and ignore finished MACs

(Warning: full analysis much more complicated and needs PRF-ODH assumption)

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Analysis of Unilateral DH Case: Strategy



$\mathrm{pid} = \mathrm{cert}_S \qquad \mathrm{sid} = (r_c, g^x, r_s, g^y, \mathrm{pk}_S, \mathrm{cert}_S)$

Analysis according to case distinction:

1. Adversary tests client session without partner
2. Adversary tests server session without partner
3. Adversary tests session with partner

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Analysis of Unilateral DH Case: Case 1

client w/o partner

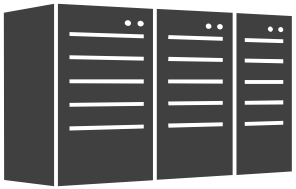
TEST session

$r_c,\ g^x$ →

← $r_s,\ g^y$

← $\mathrm{pk}_S,\ \mathrm{cert}_S,\ s$

$s \leftarrow \mathrm{Sign}(\mathrm{sk}_s, \texttt{CH}\ldots\texttt{SCert})$



$\mathrm{pid} = \mathrm{cert}_S \qquad \mathrm{sid} = (r_c, g^x, r_s, g^y, \mathrm{pk}_S, \mathrm{cert}_S)$

no partner session by assumption → **S has never signed sid**

+

authenticated partner S must not be corrupt

→ **adversary must have forged signature for S to make client accept**

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Analysis of Unilateral DH Case: Case 2

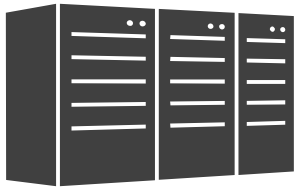
server w/o partner

TEST session

$r_c,\ g^x$

$r_s,\ g^y$

$\mathrm{pk}_S,\ \mathrm{cert}_S,\ s$



$s \leftarrow \mathrm{Sign}(\mathrm{sk}_s, \texttt{CH}\ldots\texttt{SCert})$

$\mathrm{pid} = \mathrm{cert}_S \qquad \mathrm{sid} = (r_c, g^x, r_s, g^y, \mathrm{pk}_S, \mathrm{cert}_S)$

not allowed by definition of unilaterally authenticated protocols

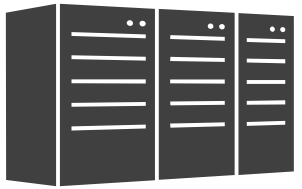
TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Analysis of Unilateral DH Case: Case 3

test with partner

TEST session

TEST session



$r_c,\ g^x$

$r_s,\ g^y$

$\mathrm{pk}_S,\ \mathrm{cert}_S,\ s$

$s \leftarrow \mathrm{Sign}(\mathrm{sk}_s, \texttt{CH}\ldots\texttt{SCert})$

$\mathrm{pid} = \mathrm{cert}_S \qquad \mathrm{sid} = (r_c, g^x, r_s, g^y, \mathrm{pk}_S, \mathrm{cert}_S)$

two honest parties have chosen g^x resp. g^y in test session

adversary must compute g^{xy} from g^x and g^y

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Other Security Properties (and Other Protocols)

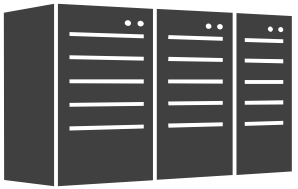
TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

How to (not) Authenticate Anonymous Protocols

g^x

g^y

Unauthenticated Key Exchange



$\mathrm{Sig}(\mathrm{sk}_S, g^x, g^y), \mathrm{cert}_S$

$\mathrm{Sig}(\mathrm{sk}_C, g^x, g^y), \mathrm{cert}_C$

Authentication

$K = \mathrm{KDF}(g^{xy}, g^x, g^y)$

$\mathrm{sid} = (g^x, g^y)$

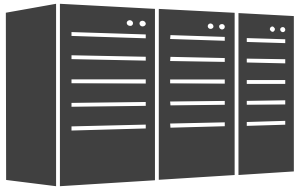
pid =certificate

$K = \mathrm{KDF}(g^{xy}, g^x, g^y)$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Key Secrecy

TEST session



g^x

g^y

Unauthenticated Key Exchange

partner C must not be corrupt

$\mathrm{Sig}(\mathrm{sk}_S, g^x, g^y), \mathrm{cert}_S$

$\mathrm{Sig}(\mathrm{sk}_C, g^x, g^y), \mathrm{cert}_C$

Authentication

Sig scheme secure ⇒ can only have been created by C for its g^x and my g^y

⇒Adversary cannot compute g^{xy}

$K = \mathrm{KDF}(g^{xy}, g^x, g^y)$

$\mathrm{sid} = (g^x, g^y)$

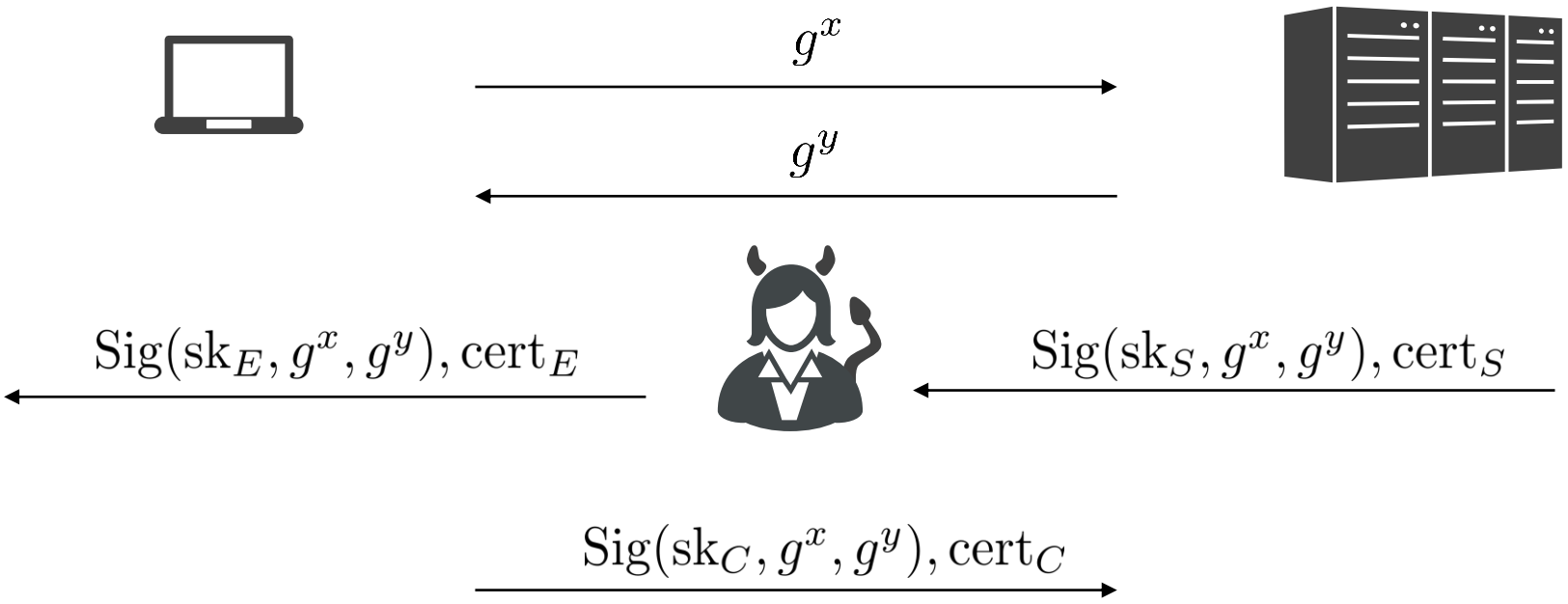
pid =certificate

$K = \mathrm{KDF}(g^{xy}, g^x, g^y)$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Unknown-Key-Share (UKS) Attack

Blake-Wilson, Menezes: Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol, PKC'99



Believes to share key *K* with E

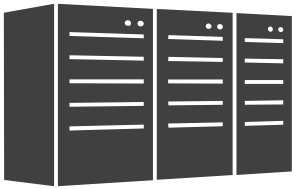
Believes to share key *K* with C

$K = \mathrm{KDF}(g^{xy}, g^x, g^y)$

$K = \mathrm{KDF}(g^{xy}, g^x, g^y)$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Secure and Insecure???



Security guarantees of authenticated key exchange:

At most one other party (≤1) holds the session key (and for authenticated cases, if intended partner is honest then it is that party)

Believes to share key *K* with E

Also true: only S knows key (but not E), and intended partner E is corrupt

Believes to share key *K* with C

Obviously true

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Thwarting UKS Attacks

Bind intended partner identity into authentication

$$\mathrm{Sig}(\mathrm{sk}_C, g^x, g^y, S), \mathrm{cert}_C$$

(or via MACs)

Examples:
ISO/IEC 9798-3 (KE version)
IKEv2 in IPSec
TLS 1.3

Bind intended partner identity into key derivation

$$K = \mathrm{KDF}(g^{xy}, g^x, g^y, s_C, \mathrm{cert}_C, \dots)$$

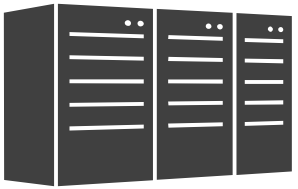
(and sid = entire transcript)

Example:
TLS 1.3

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

ISO/IEC 9798-3 (augmented by KE / SIG-DH)

$$g^x \longrightarrow$$



$$\longleftarrow g^y,\ \mathrm{Sig}(\mathrm{sk}_S, g^x, g^y, C), \mathrm{cert}_S$$

$$\mathrm{Sig}(\mathrm{sk}_C, g^y, g^x, S), \mathrm{cert}_C \longrightarrow$$

$K = \mathrm{KDF}(g^{xy}, g^x, g^y)$

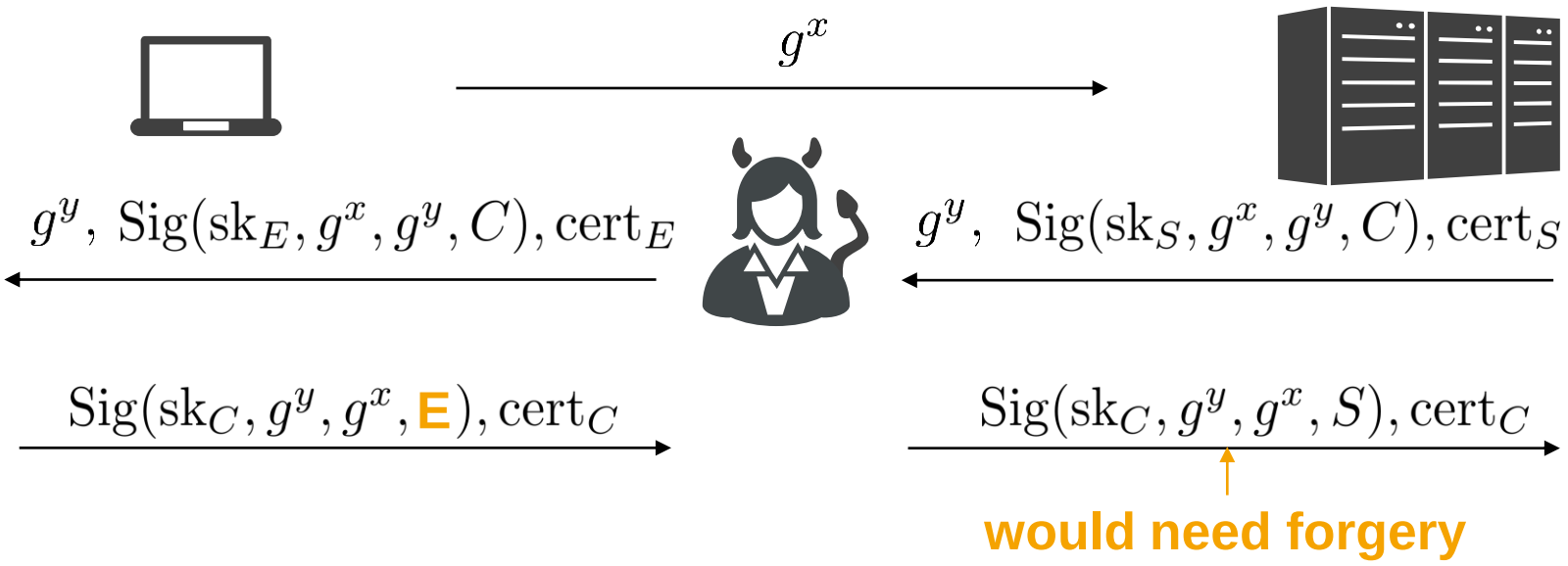
$\mathrm{sid} = (g^x, g^y)$

pid =certificate

$K = \mathrm{KDF}(g^{xy}, g^x, g^y)$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

ISO/IEC 9798-3 Resistance against UKS



$K = \mathrm{KDF}(g^{xy}, g^x, g^y)$

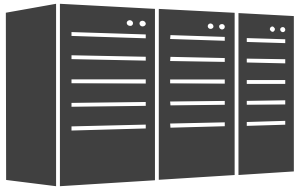
$\mathrm{sid} = (g^x, g^y)$

pid =certificate

$K = \mathrm{KDF}(g^{xy}, g^x, g^y)$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

TLS 1.3 and UKS-Resistance



CH
CKS
$r_c \leftarrow \{0,1\}^{256}$
g^x

$r_s \leftarrow \{0,1\}^{256}$
g^y
SH
SKS

handshake key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{SKS})$

handshake key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{SKS})$

{SConf*}
pk_S, cert_S {SCert*}
s {SCertV*}
t {SF}

$s \leftarrow \mathrm{Sign}(\mathrm{sk}_s, \mathtt{CH} \ldots \mathtt{SCert})$
$t \leftarrow \mathrm{MAC}(\mathrm{k}_{\mathrm{SF}}, \mathtt{CH} \ldots \mathtt{SCert})$

Uses MAC over derived key

{CCert*}
{CCertV*}
{CF}

Uses identities in key derivation

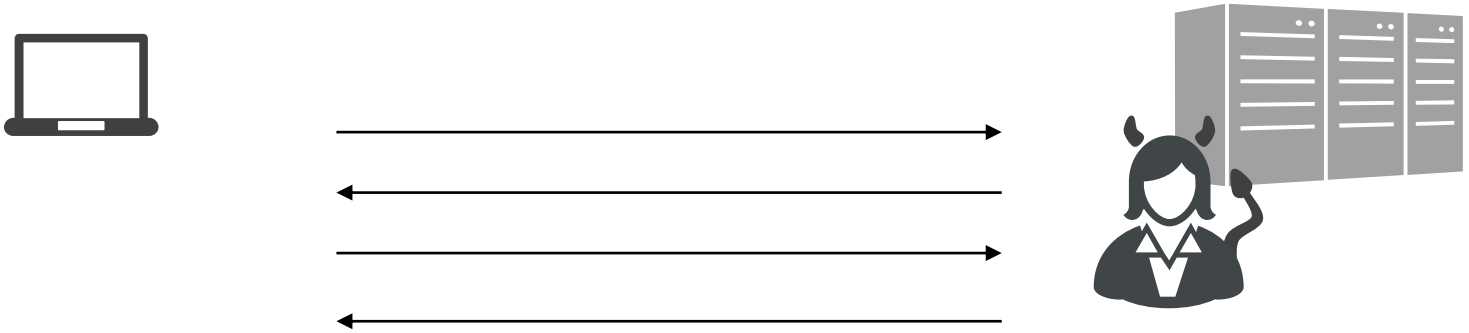
channel key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{CF})$

channel key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{CF})$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

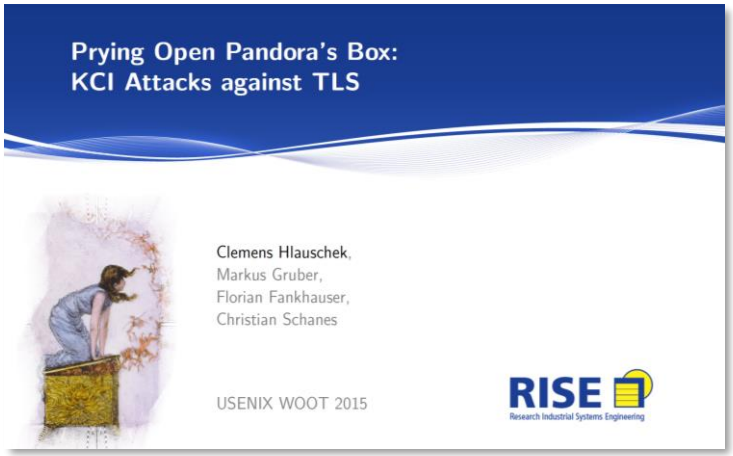
Key Compromise Impersonation (KCI) Attack

Blake-Wilson, Johnson, Menezes: Key Agreement Protocols and Their Security Analysis, IMA'97



1. **Corrupt *client's* long-term secret**

2. **Impersonate towards client as server**



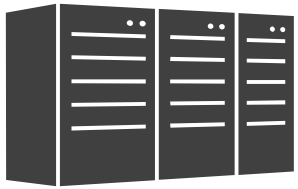
Can be mounted in real life
(here: specific TLS 1.2 sub protocol)

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

TLS 1.2 (static DH) and KCIs

$$g^x \text{ with } \text{cert}_C, r_c \longrightarrow$$

$$\longleftarrow g^y \text{ with } \text{cert}_S, r_s$$



$(K, K_c, K_s) \leftarrow \text{KDF}(g^{xy}, r_c | r_s)$

$(K, K_c, K_s) \leftarrow \text{KDF}(g^{xy}, r_c | r_s)$

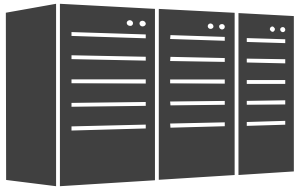
$$\text{MAC}(K_c, g^x, g^y, r_c, r_s) \longrightarrow$$

$$\longleftarrow \text{MAC}(K_s, g^x, g^y, r_c, r_s)$$

Adversary knowing x can compute $(g^y)^x$ from server's public key g^y

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

TLS 1.3 and KCI-Resistance



CH
CKS
$r_c \leftarrow \{0,1\}^{256}$
g^x

$r_s \leftarrow \{0,1\}^{256}$
g^y
SH
SKS

handshake key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{SKS})$

handshake key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{SKS})$

{SConf*}
pk_S, cert_S {SCert*}
s {SCertV*}
t {SF}

$s \leftarrow \mathrm{Sign}(\mathrm{sk}_s, \mathtt{CH} \ldots \mathtt{SCert})$
$t \leftarrow \mathrm{MAC}(\mathrm{k}_{\mathrm{SF}}, \mathtt{CH} \ldots \mathtt{SCert})$

Knowledge of client's signing key does not help to forge server signature

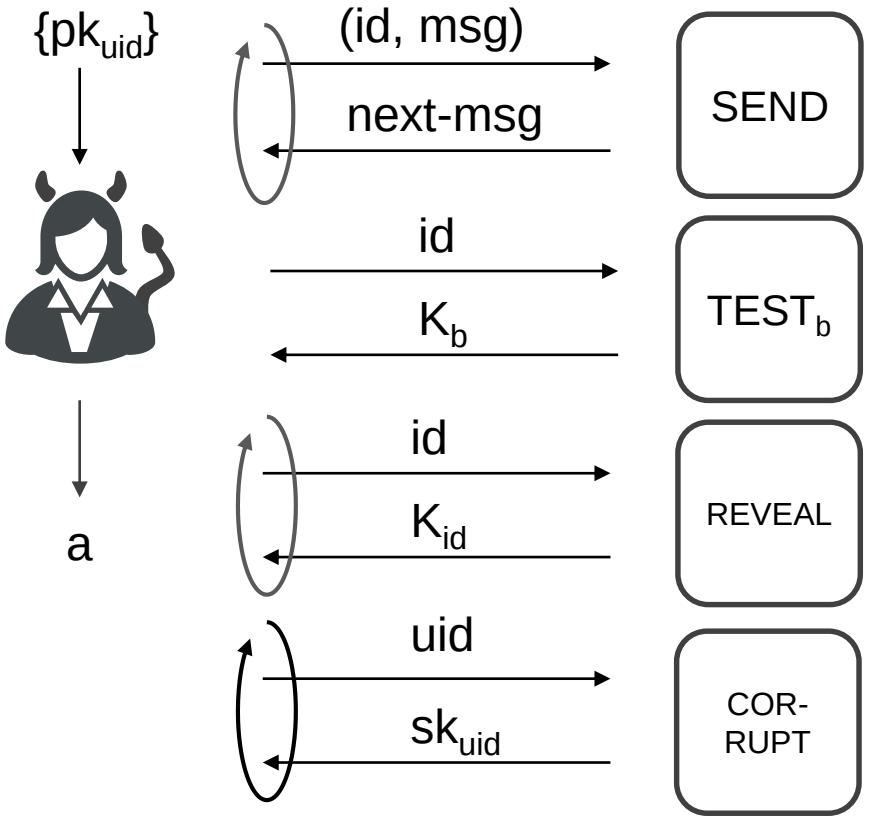
{CCert*}
{CCertV*}
{CF}

channel key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{CF})$

channel key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH} \ldots \mathtt{CF})$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Attacks on the State



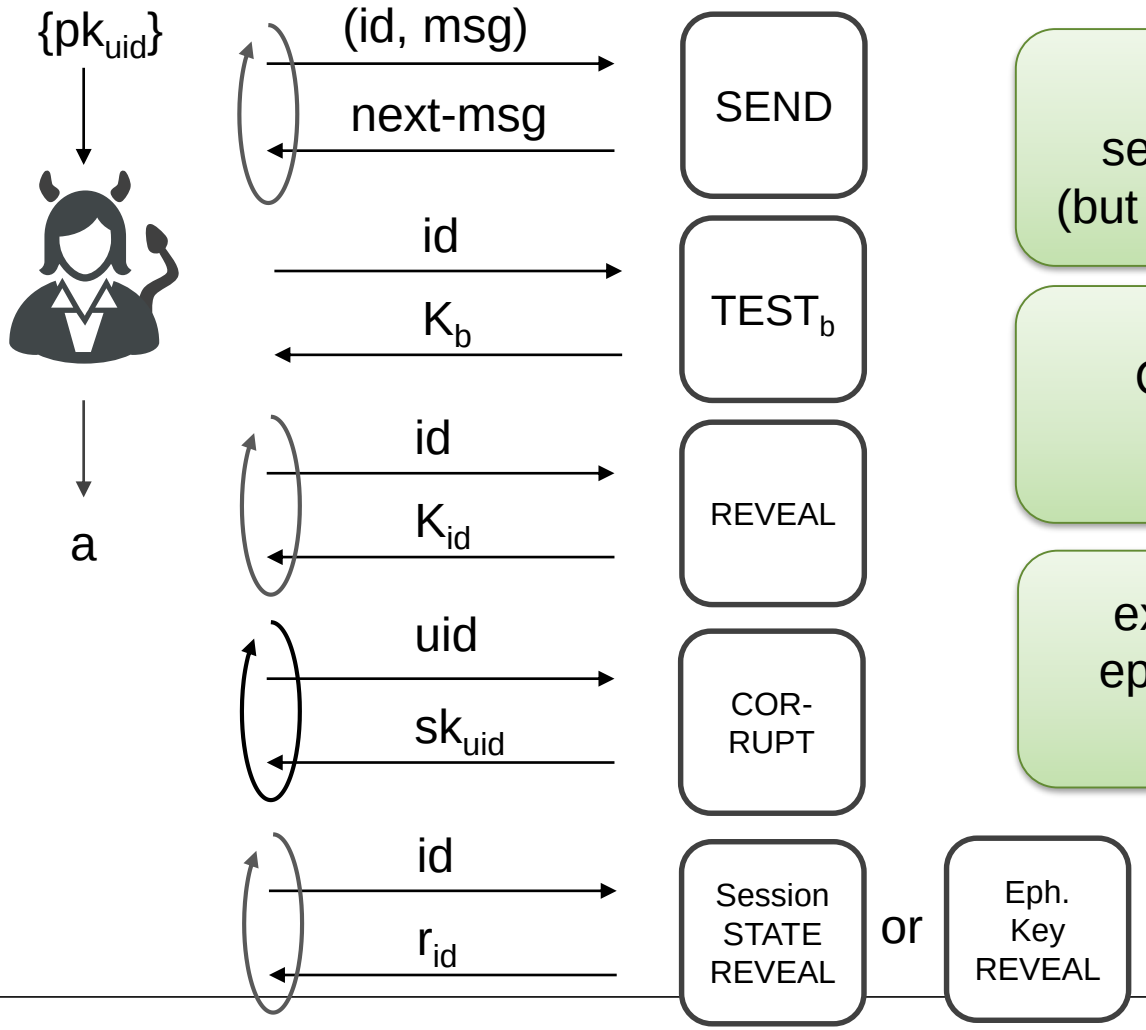
What if adversary breaks into computer and also finds ephemeral keys or randomness?

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Canetti, Krawczyk: Analysis of Key-Exchange Protocols and Their Use for Building …, Eurocrypt 2001

CK and eCK Security

LaMacchia, Lauter, Mityagin: Stronger security of authenticated key exchange. ProvSec 2007



CK model:
session state reveals
(but not in TEST session)

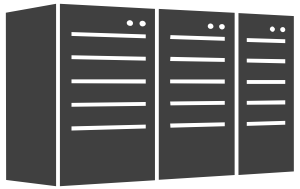
CK/HMQV model:
CK+KCI

extended CK (eCK):
ephemeral key reveal
+KCI

example: NAXOS protocol

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

TLS 1.3 and eCK-Vulnerability



CH
CKS
$r_c \leftarrow \{0,1\}^{256}$
g^x

$r_s \leftarrow \{0,1\}^{256}$
g^y
SH
SKS

handshake key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH}\ldots)$

handshake key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH}\ldots\mathtt{SKS})$

{SConf*}
{SCert*}
{SCertV*}
{SF}

pk_S, cert_S
s
t

$s \leftarrow \mathrm{Sign}(\mathrm{sk}_s, \mathtt{CH}\ldots\mathtt{SCert})$
$t \leftarrow \mathrm{MAC}(\mathrm{k}_{\mathrm{SF}}, \mathtt{CH}\ldots\mathtt{SCert})$

Knowledge of ephemeral key breaks security

{CCert*}
{CCertV*}
{CF}

channel key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH}\ldots\mathtt{CF})$

channel key
$\leftarrow \mathrm{KDF}(g^{xy}, \mathtt{CH}\ldots\mathtt{CF})$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt

Teaser for the Break

Explain why KCI attacks are,

per se,

not covered by BR key secrecy.

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de