The strongSwan Project

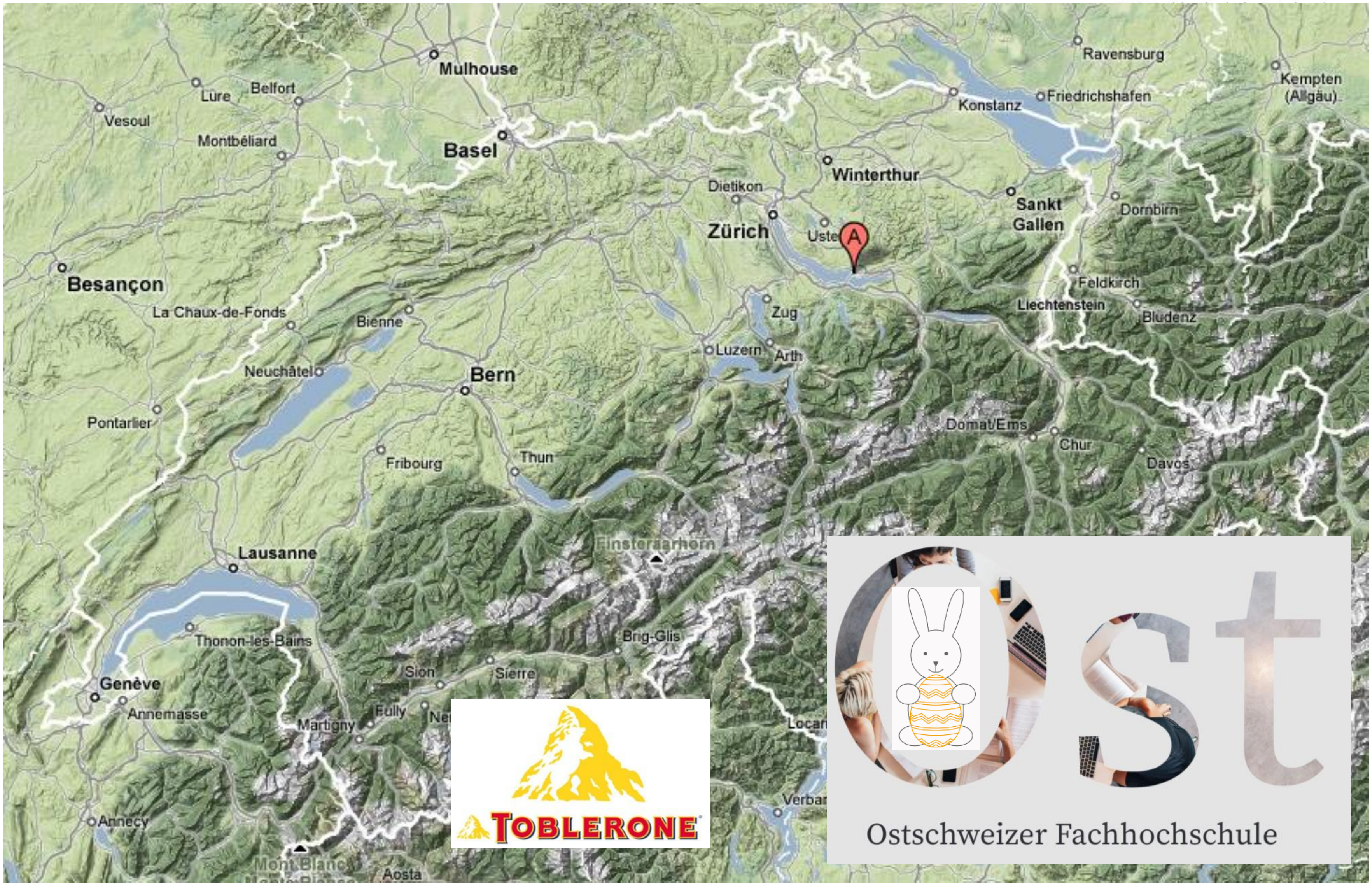
IPsec Workshop Prague, March 18-20 2019

Tobias Brunner & Andreas Steffen
Institute for Networked Solutions
HSR University of Applied Sciences Rapperswil

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Where the heck is Rapperswil?



HSR - Hochschule für Technik Rapperswil

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

- University of Applied Sciences with about 1500 students
- Faculty of Information Technology (300-400 students)
- Bachelor Course (3 years), Master Course (+1.5 years)

The strongSwan Project

IPsec Workshop Prague, March 18-20 2019

Quantum-Save Key Exchange for IKEv2

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

strongSwan

Previous Post-Quantum Crypto Work

PQC Algorithm	IKEv2	strongSwan	Date
NTRUEncrypt (IEEE 1363.1)	KE	5.1.2	Mar 2014
BLISS Signature	AUTH	5.2.2	Jan 2015
NewHope (Exp. Chrome Browser)	KE	5.5.1	Oct 2016

- All three PQC algorithms listed above are lattice-based.
- NTRUEncrypt and NewHope with increased security strength caused IP fragmentation of IKE_SA_INIT messages!

Our Assumptions

- We think that when the NIST PQC finalists are going to be chosen in a 2022-2024 timeframe, we will have sufficient confidence in the selected algorithms that multiple IKEv2 Quantum-Safe Key Exchanges (QSKE) will not be needed.
- Currently we don’t have multiple IKEv2 Diffie-Hellman Key Exchanges (KE) either, just because we don’t trust either the American NIST or the German Brainpool curves!

strongSwan QSKE Prototype (July 2018)

Quick summary of our prototype implementation:

- Based on the IKEv2 AUX (INTERMEDIATE) message defined by draft-smyslov-ipsecme-ikev2-aux-00 (January 2018)
- We define a new IKEv2 QSKE_MECHANISM transform type
- We define a new IKEv2 QSKE payload
- The QSKE payload is initially transported via the AUX message but can also be embedded into the CREATE_CHILD_SA message during rekeying or when negotiating multiple CHILD_SAs.
- We define a new INVALID_QSKE_PAYLOAD notify [error] message
- For quantum-safe crypto we use the liboqs library which is a wrapper around a selection of NIST PCQ Round 1 candidates: https://github.com/open-quantum-safe/liboqs/tree/nist-branch

New QSKE_MECHANISM Transform Type

Description	Abbreviation	Type
Encryption Algorithm	ENCR	1
Pseudorandom Function	PRF	2
Integrity Algorithm	INTEG	3
Diffie-Hellman Group	D-H	4
Extended Sequence Numbers	ESN	5
Quantum-Safe Key Exchange Mechanism	QSKE_MECHANISM	255

QSKE_MECHANISM Transform IDs

Transform ID	Type
QSKE_NEWHOPE	1
QSKE_NEWHOPE_L1	2
QSKE_NEWHOPE_L5	3
QSKE_FRODO_AES_L1	4
QSKE_FRODO_AES_L3	5
QSKE_FRODO_SHAKE_L1	6
QSKE_FRODO_SHAKE_L3	7
QSKE_KYBER_L1	8
QSKE_KYBER_L3	9
QSKE_KYBER_L5	10
QSKE_BIKE1_L1	11
QSKE_BIKE1_L3	12
QSKE_BIKE1_L5	13
QSKE_BIKE2_L1	14
QSKE_BIKE2_L3	15

Transform ID	Type
QSKE_BIKE2_L5	16
QSKE_BIKE3_L1	17
QSKE_BIKE3_L3	18
QSKE_BIKE3_L5	19
QSKE_SIKE_L1	20
QSKE_SIKE_L3	21
QSKE_SABER_L1	22
QSKE_SABER_L3	23
QSKE_SABER_L5	24
QSKE_LIMA_2P_L3	25
QSKE_LIMA_2P_L5	26
QSKE_LIMA_SP_L1	27
QSKE_LIMA_SP_L2	28
QSKE_LIMA_SP_L3	29
QSKE_LIMA_SP_L5	30

QSKE_MECHANISM Transform Attributes

```
 1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Last Substruc |   RESERVED      |        Transform Length       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Transform Type |   RESERVED      |          Transform ID         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                      Transform Attributes                     ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Currently no Transform Attributes
- Security strengths L1, L3, L5 might be encoded

QSKE Payload

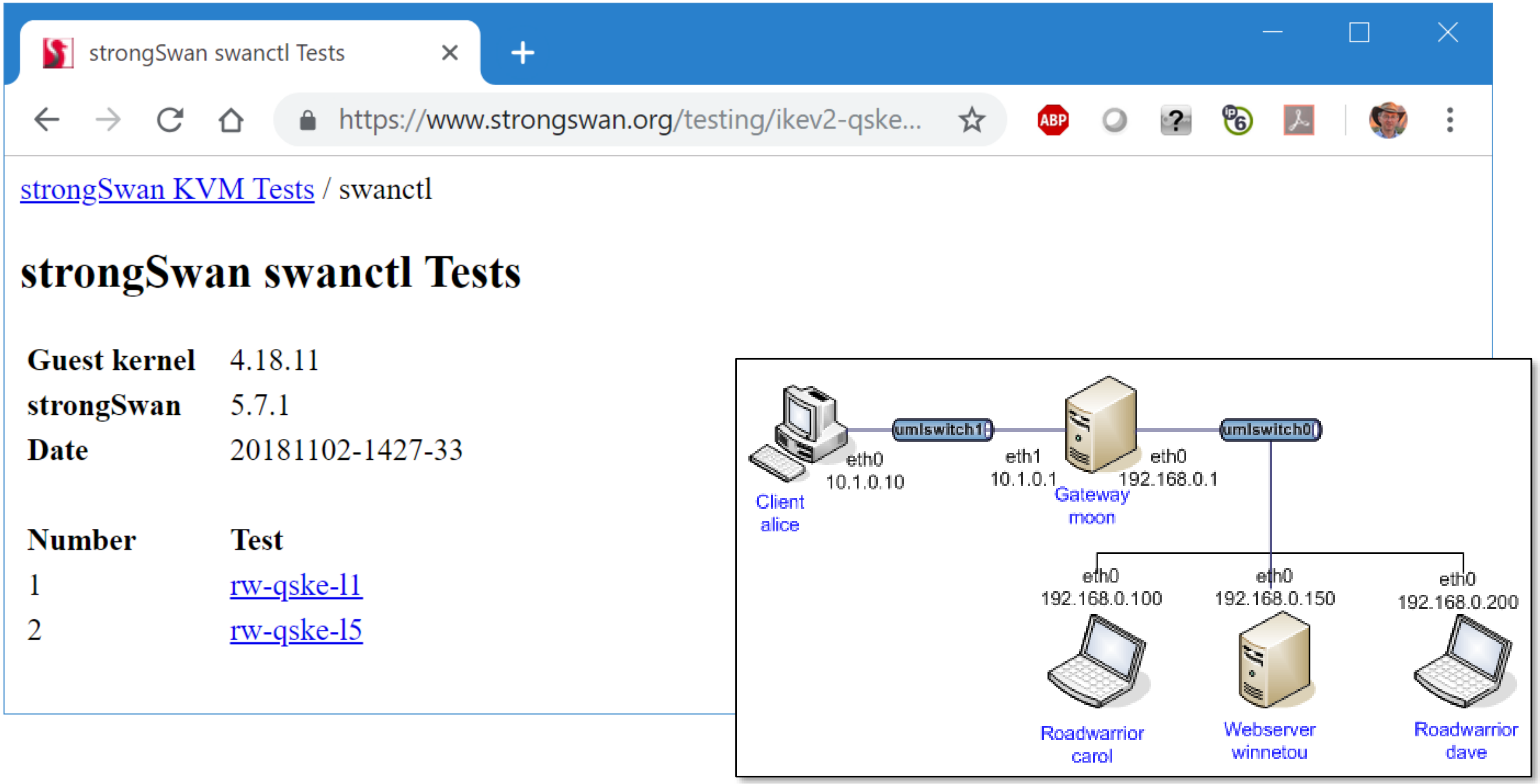
Payload Type	Notation	Type
Key Exchange	KE	34
Quantum-Safe Key Exchange	QSKE	129

```
 1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Payload  |C|  RESERVED   |         Payload Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     QSKE Mechanism Num        |           RESERVED            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~               Quantum-Safe Key Exchange Data                  ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

INVALID_QSKE_PAYLOAD Notify Message

Notify Messages – Error Type	Type
INVALID_KE_PAYLOAD	17
INVALID_QSKE_PAYLOAD	8193

strongSwan IKEv2 QSKE Test Scenarios



[strongSwan KVM Tests](https://www.strongswan.org/testing/) / swanctl

strongSwan swanctl Tests

Guest kernel	4.18.11
strongSwan	5.7.1
Date	20181102-1427-33

Number	**Test**
1	rw-qske-l1
2	rw-qske-l5

- https://www.strongswan.org/testing/ikev2-qske/swanctl
- Based on virtual KVM Debian 9 hosts

Test Scenario rw-qske-l1

The roadwarriors **carol** and **dave** set up a connection each to gateway **moon.**

The IKEv2 hybrid key exchange is using the traditional Diffie-Hellman groups CURVE_25519 and ECP_256_BP, respectively, with the KE payloads exchanged via IKE_SA_INIT, followed by a Quantum-Save Key Exchange proposing the lattice-based QSKE_NEWHOPE_L1 and isogeny-based QSKE_SIKE_L1 mechanisms, respectively, with the QSKE payloads exchanged via IKE_AUX.

The first CHILD_SA net1 is for the remote subnet 10.1.0.0/28.

A second CHILD_SA net2 for the remote subnet 10.1.0.16/28 is established using the QSKE mechanisms QSKE_KYBER_L1 and QSKE_FRODO_AES_L1 by **carol** and **dave**, respectively.

For the second CHILD_SA **dave** proposes QSKE_SABER_L1 as the preferred QSKE mechanism and includes a corresponding QSKE payload in the CREATE_CHILD_SA request.

moon replies with an INVALID_QSKE_PAYLOAD notification proposing QSKE_FRODO_AES_L1 instead.

Configuration of Roadwarrior **dave**

```
connections {
   home {
      remote_addrs = 192.168.0.1
      local {
         auth = pubkey
         certs = daveCert.pem
         id = dave@strongswan.org
      }
      remote {
         auth = pubkey
         id = moon.strongswan.org
      }
      children {
         net1 {
            remote_ts = 10.1.0.0/28
            esp_proposals = aes256gcm128-ecp256bp-qskesike1
         }
         net2 {
            remote_ts = 10.1.0.16/28
            esp_proposals = aes256gcm128-ecp256bp-qskesaber1-qskefrodoa1
         }
      }
      version = 2
      proposals = aes256-sha256-ecp256bp-qskesike1
   }
}
```

Configuration of Gateway **moon**

```
connections {
   rw {
      local_addrs  = 192.168.0.1
      local {
         auth = pubkey
         certs = moonCert.pem
         id = moon.strongswan.org
      }
      remote {
         auth = pubkey
      }
      children {
         net1 {
            local_ts  = 10.1.0.0/28
            esp_proposals = aes256gcm128-x25519-ecp256bp-qskenewhope1-qskesike1
         }
         net2 {
            local_ts  = 10.1.0.16/28
            esp_proposals = aes256gcm128-x25519-ecp256bp-qskekyber1-qskefrodoa1
         }
      }
      version = 2
      proposals = aes256-sha256-x25519-ecp256bp-qskenewhope1-qskesike1
   }
}
```

dave as Initiator – First CHILD_SA

- IKE_SA_INIT request 0

```
SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) V
```

- IKE_SA_INIT response 0

```
SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(FRAG_SUP) N(HASH_ALG) V
```

- IKE_AUX request 1 # no fragments (SIKE QSKE)

```
QSKE
```

- IKE_AUX response 1 # no fragments (SIKE QSKE)

```
QSKE
```

- IKE_AUTH request 2 # 2 fragments (CERT)

```
IDi CERT CERTREQ IDr AUTH SA TSi TSr
```

- IKE_AUTH response 2 # 2 fragments (CERT)

```
IDr CERT AUTH SA TSi TSr
```

dave as Initiator – Second CHILD_SA

- CREATE_CHILD_SA request 3 # no fragments (SABER QSKE)

```
SA No KE TSi TSr QSKE
```

- CREATE_CHILD_SA response 3 # INVALID_QSKE_PAYLOAD

```
N(INVAL_QSKE)
```

- CREATE_CHILD_SA request 4 # 8 fragments (FRODO_AES QSKE)

```
SA No KE TSi TSr QSKE
```

- CREATE_CHILD_SA response 4 # 8 fragments (FRODO_AES QSKE)

```
SA No KE TSi TSr QSKE
```

Thank you for your attention!

Questions?

www.strongswan.org