HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

2 Physical Layer Security

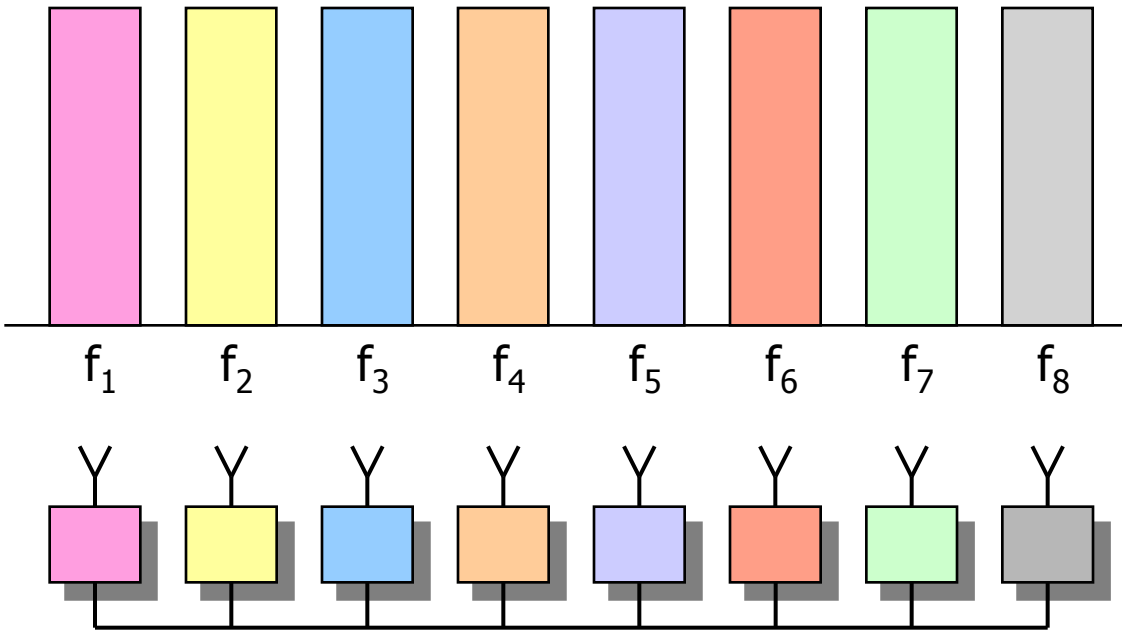
Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)

Security Protocols for the OSI Stack

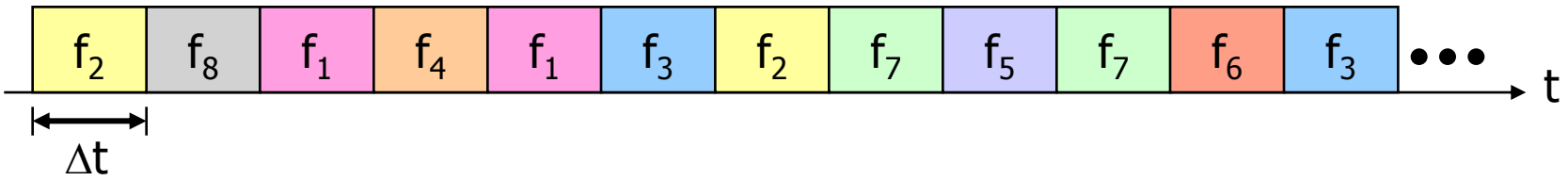
Communication layers	Security protocols
Application layer	Platform Security, Web Application Security, VoIP Security, SW Security
Transport layer	TLS
Network layer	IPsec
Data Link layer	[PPTP, L2TP], IEEE 802.1X, IEEE 802.1AE, IEEE 802.11i (WPA2)
Physical layer	Quantum Cryptography

Layer 1 Security – Frequency Hopping



Frequency band divided into n hopping channels

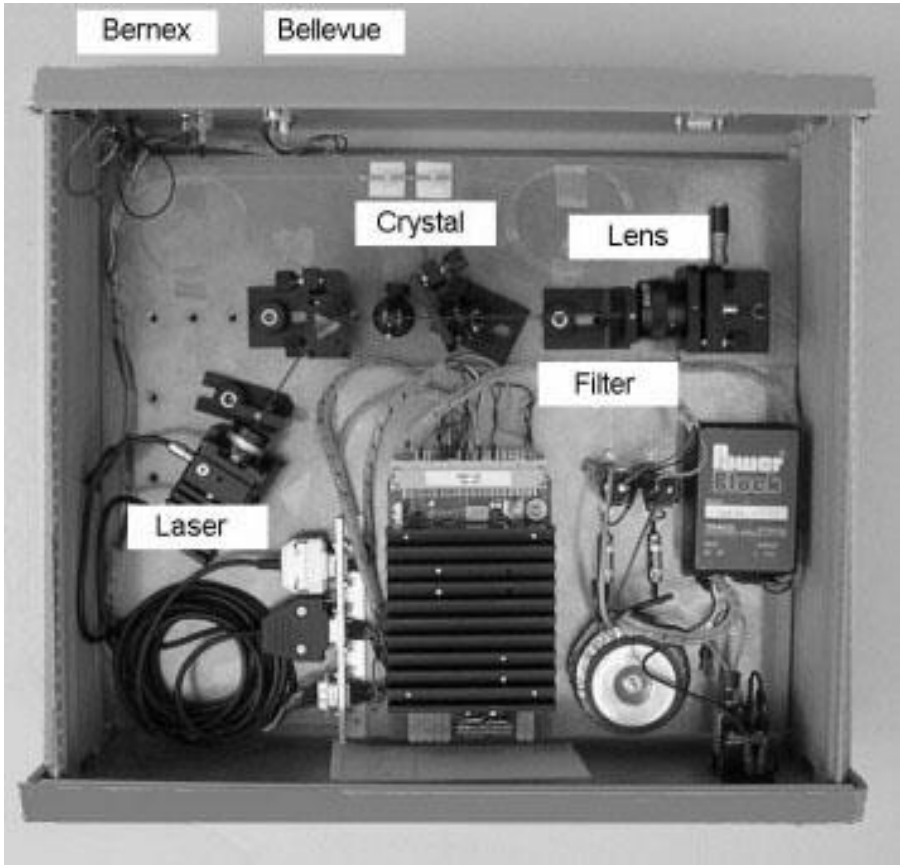
Counter measures: e.g. n parallel receivers

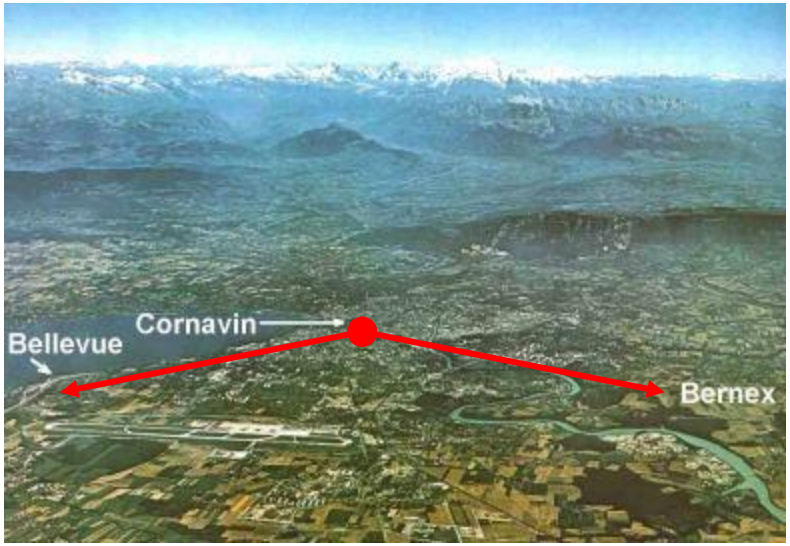


Standardized (public) or secret (military) hopping sequence

2.1 Quantum Cryptography

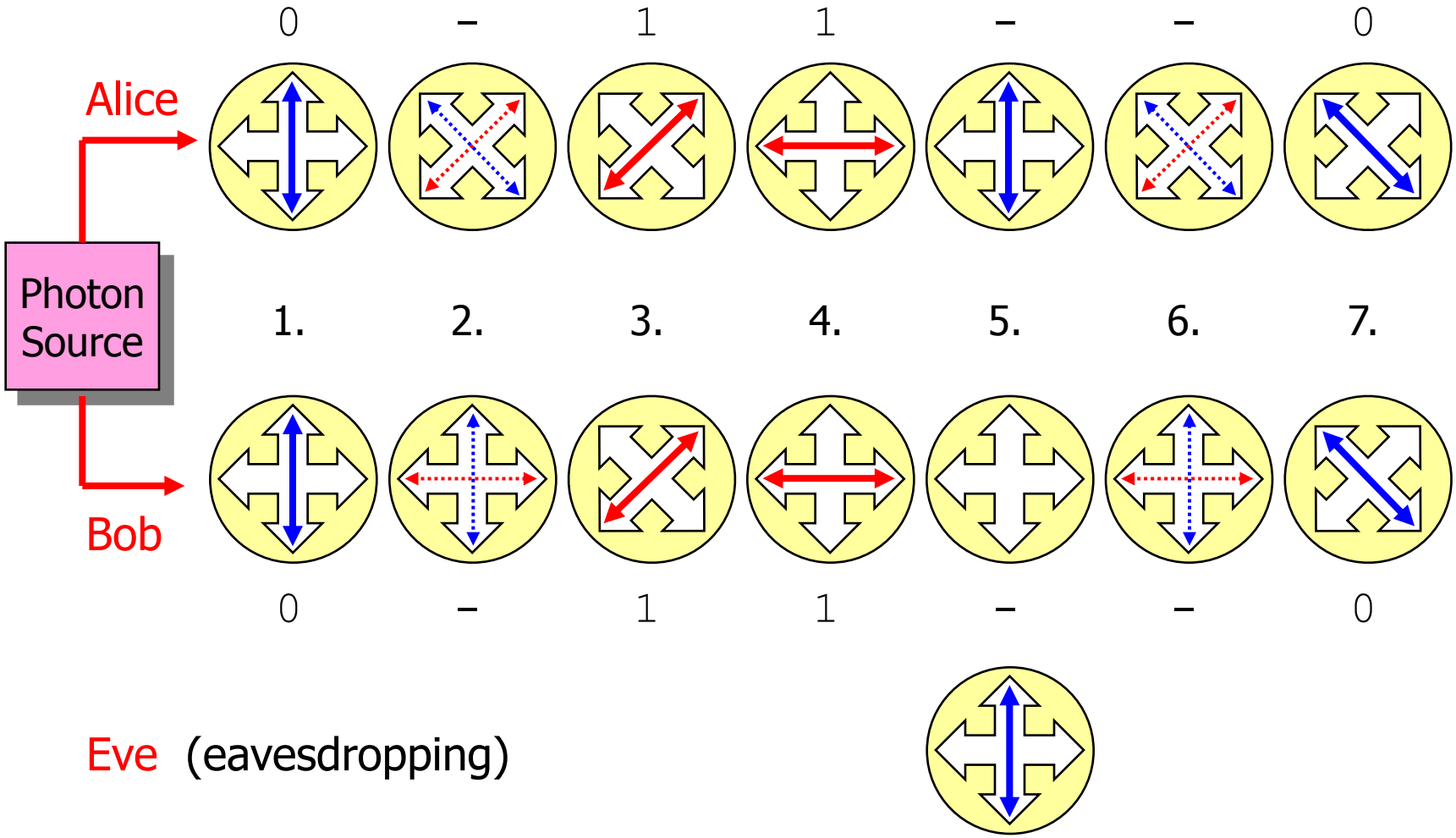
Quantum Cryptography using Entangled Photons





- Nicolas Gisin et al. University of Geneva
- Compact source emitting entangled photon pairs
- Quantum correlation over more than 10 km
- Founding of ID Quantique

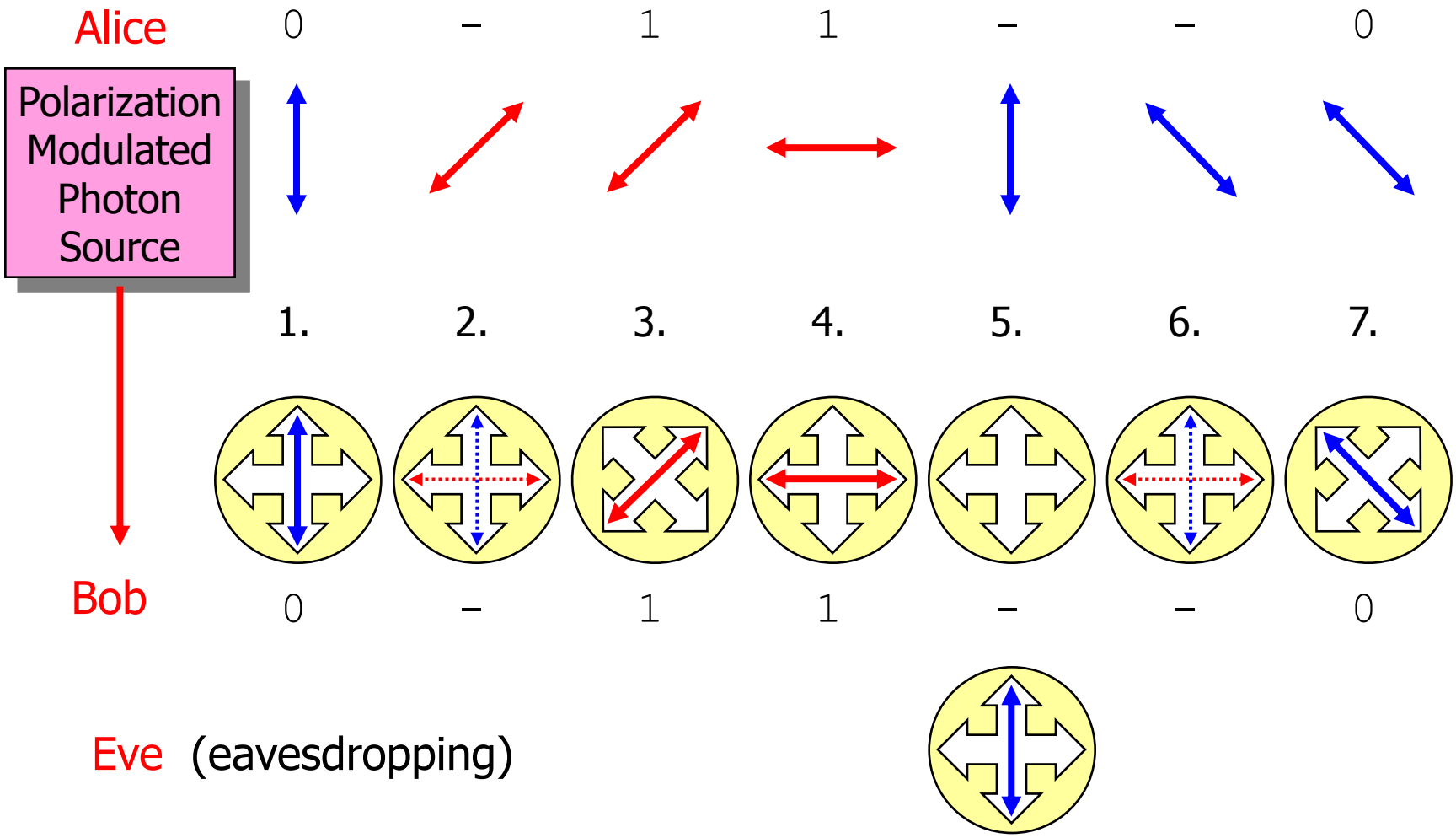
Quantum Key Distribution using Entangled Photons



Eve (eavesdropping)

E91 protocol: Arthur Ekert, 1991

Quantum Key Distribution using the BB84 Protocol



BB84 protocol: Charles Bennett & Gilles Brassard, 1984

Decoy States against Multi-Photon Splitting Attacks

- Single photon lasers are nearly impossible to build.
- The natural Poisson distribution of practical laser sources causes multi-photon pulses to occur which can be split by Eve.
- In order to compensate for the stolen photons, Eve might inject additional photons.
- As a counter measure Alice randomly inserts a certain percentage of decoy states transmitted at a different power level.
- Later Alice reveals to Bob which pulses contained decoy states.
- If Eve was eavesdropping, the yield and bit error rate statistics for the signal and decoy states are modified which can be detected by Alice and Bob.
- The use of decoy states extends the rate of secure key exchange to over 140 km.

Photon Yield versus Power Level

- Poisson distribution of the number of photons in a pulse, measured over 1000 pulses:

	Signal states	Decoy states
Power Level	0.80 photons/pulse	0.12 photons/pulse
0 photons/pulse	449 pulses	887 pulses
1 photon /pulse	360 pulses	106 pulses
2 photons/pulse	144 pulses	7 pulses
3 photons/pulse	38 pulses	0 pulses
4 photons/pulse	8 pulses	0 pulses
5 photons/pulse	1 pulse	0 pulses
Yield	551 of 1000 pulses	113 of 1000 pulses

Photon Yield versus Transmission Distance

- Attenuation in a monomode fiber with λ =1550nm: 0.2 dB/km
  - 50 km: 10dB ⇨ 1 out 10 photons survive
  - 100 km: 20dB ⇨ 1 out of 100 photons survive
  - 150 km: 30dB ⇨ 1 out of 1000 photons survive

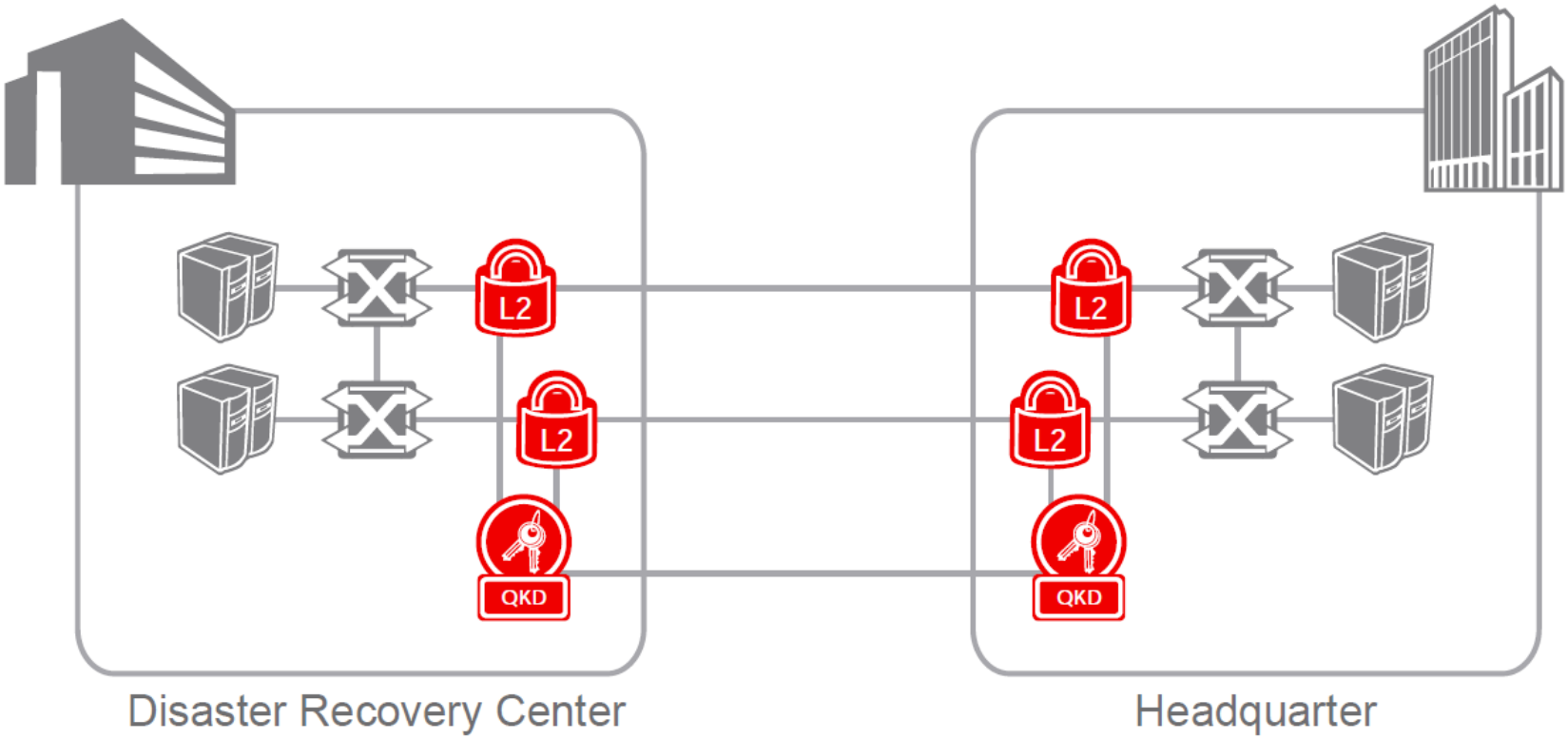
Photon Yield in 50 km (10 dB Attenuation)

- Received pulses containing at least one photon, measured over 1000 pulses:

	Signal states	Decoy states
Power Level	0.80 photons/pulse	0.12 photons/pulse
0 photons/pulse	0 pulses	0 pulses
1 photon /pulse	36 pulses	10 pulses
2 photons/pulse	28 pulses	2 pulses
3 photons/pulse	10 pulses	0 pulses
4 photons/pulse	3 pulses	0 pulses
5 photons/pulse	0 pulses	0 pulses
Yield	77 of 1000 pulses	12 of 1000 pulses

Layer 2 Encryption with Quantum Key Distribution

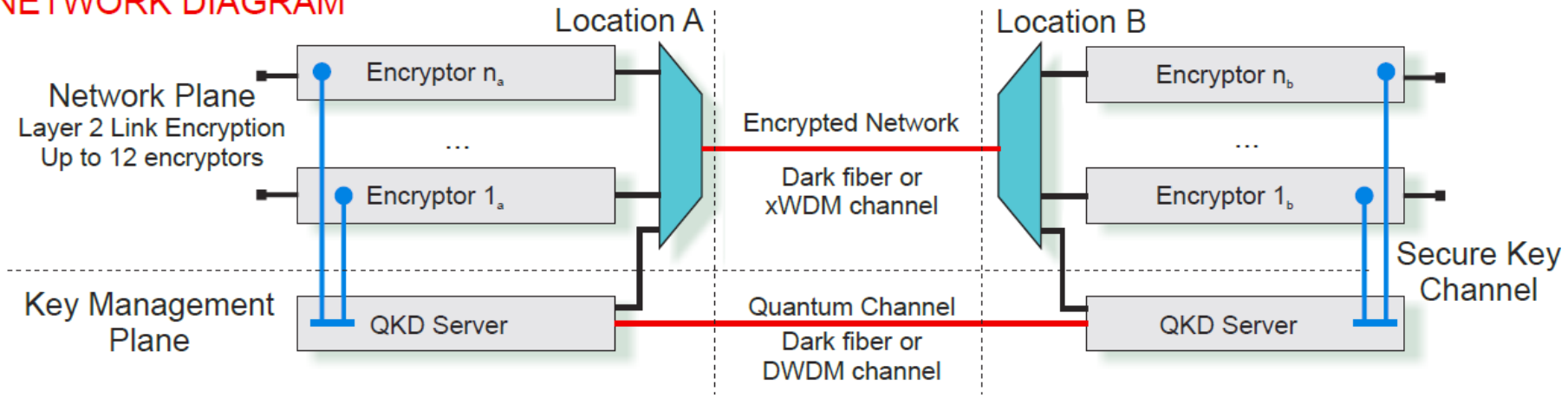
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz



- 10 Gbit/s Ethernet Encryption with AES-256 in Counter Mode
- QKD: RR84 and SARG protocols, up to 50 km (100 km on request)
- Key Management: 1 key/minute up to 12 encryptors

Cerberis QKD Server and Centauris Encryptors

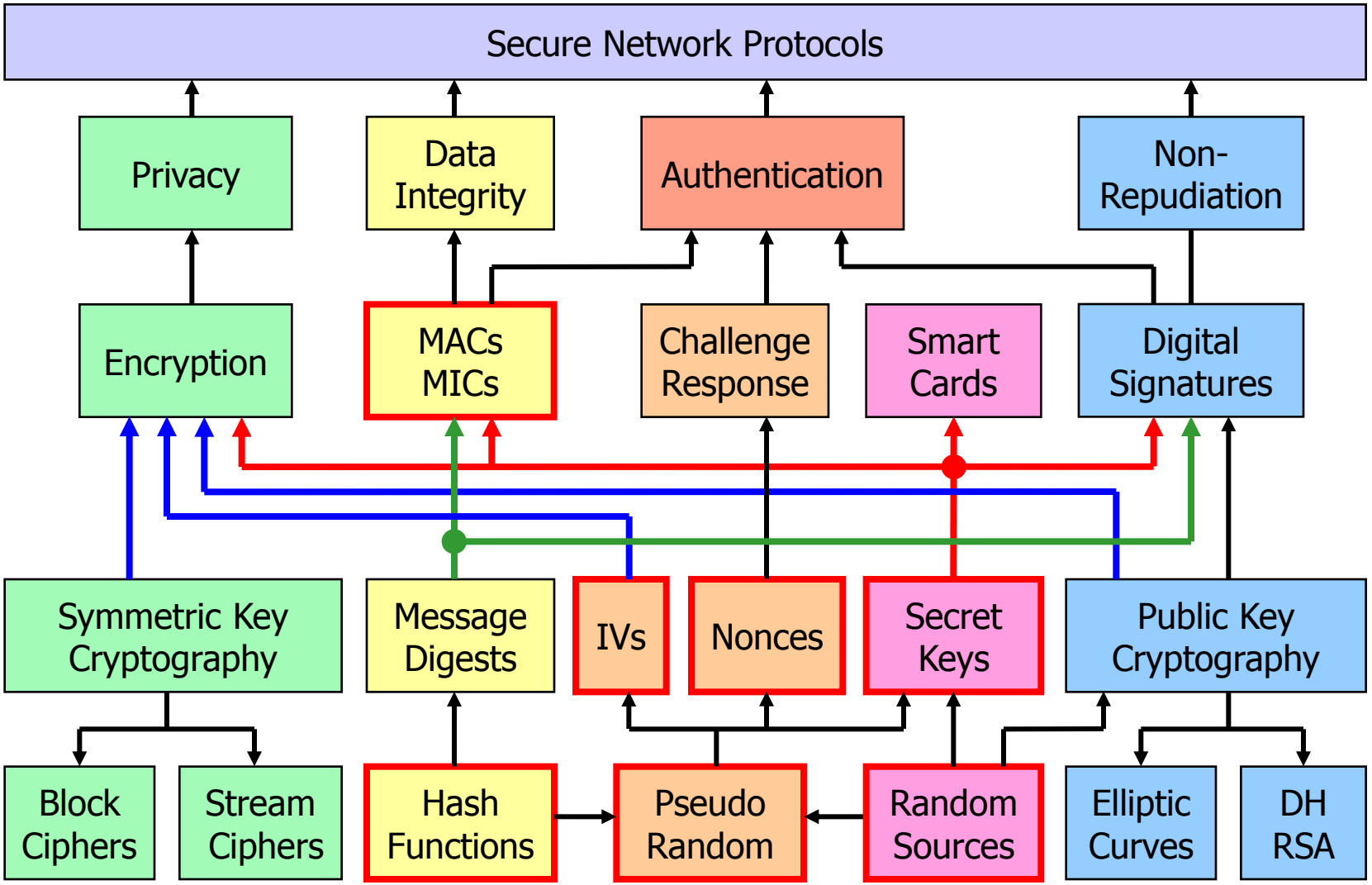
NETWORK DIAGRAM



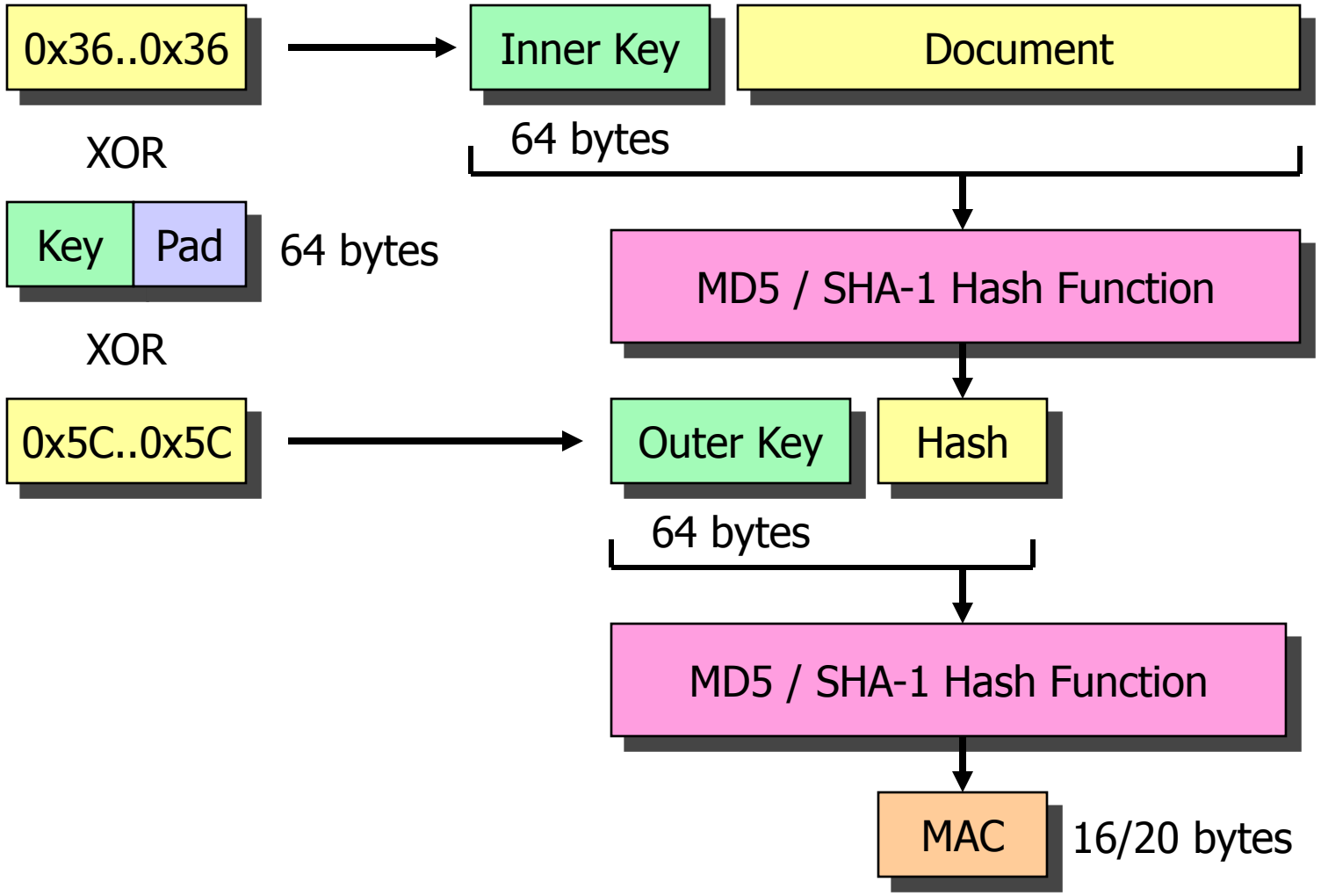
IDQ
FROM VISION TO TECHNOLOGY

2.2 Key Material and Random Numbers

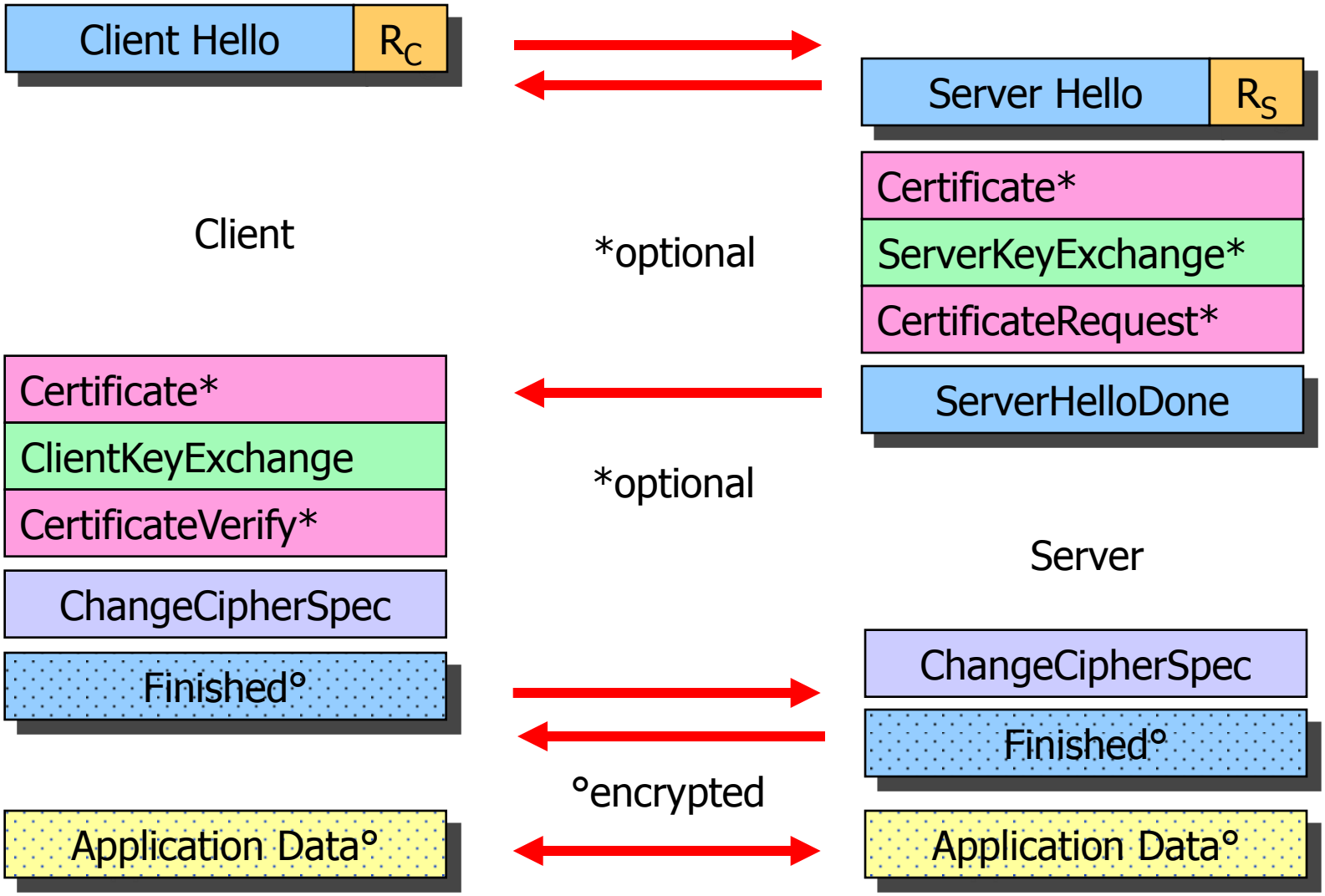
Cryptographical Building Blocks



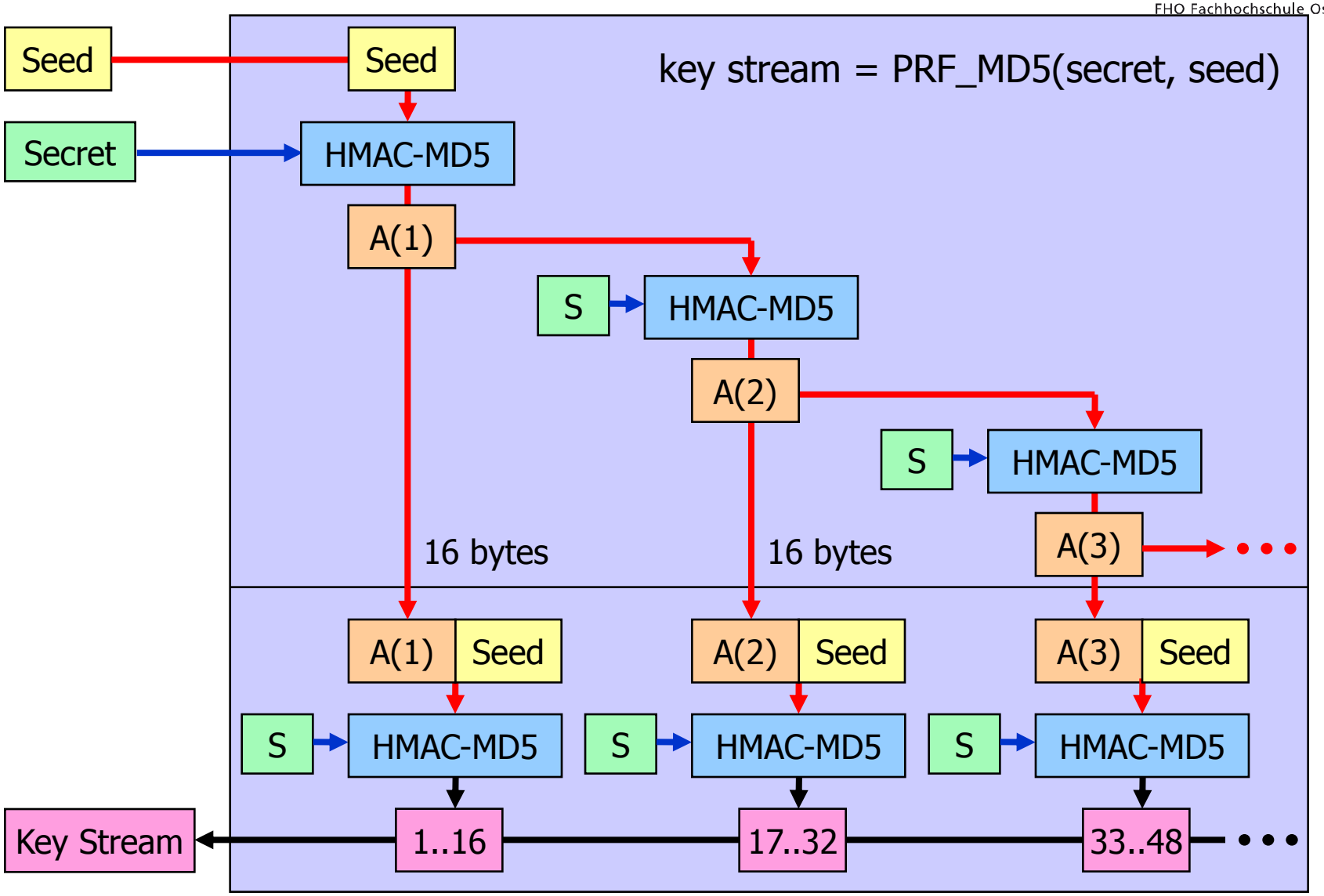
HMAC Function (RFC 2104)



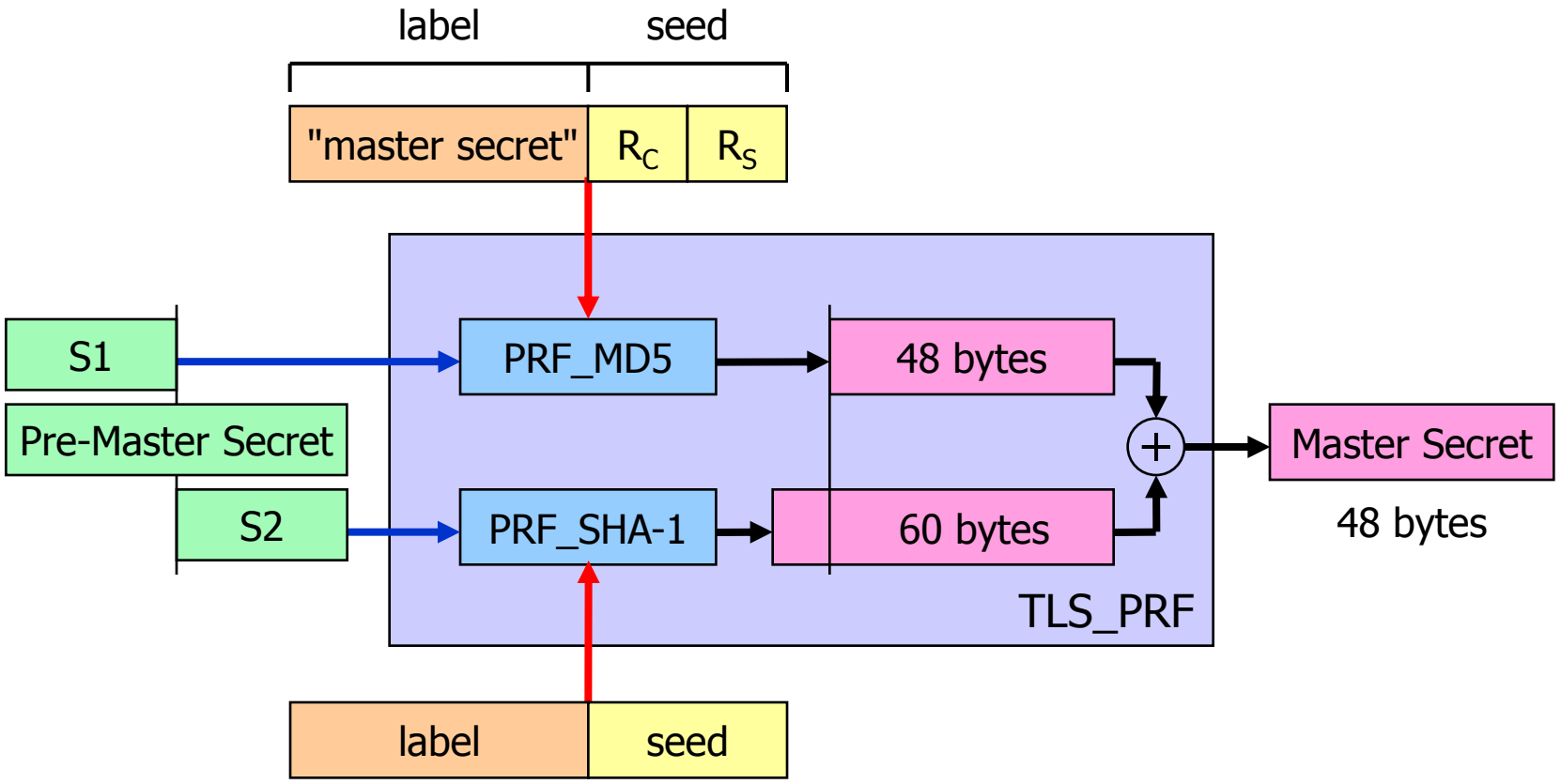
TLS Handshake Protocol



Pseudo Random Function (PRF)

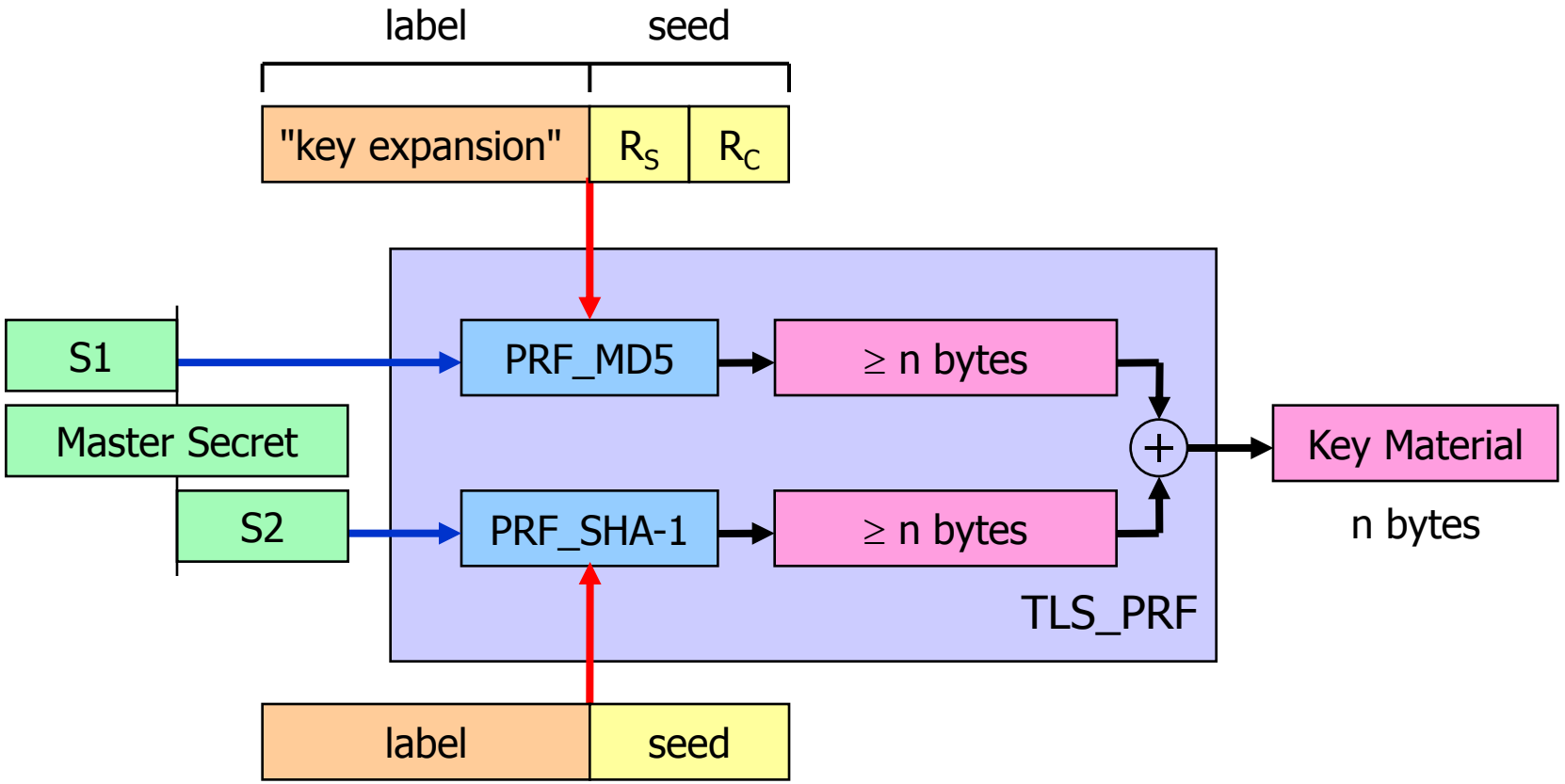


Computing the TLS 1.1 Master Secret



key stream = TLS_PRF(secret, label, seed)

Generating TLS 1.1 Key Material



key stream = TLS_PRF(secret, label, seed)

Generating True Random Numbers (RFC 1750)

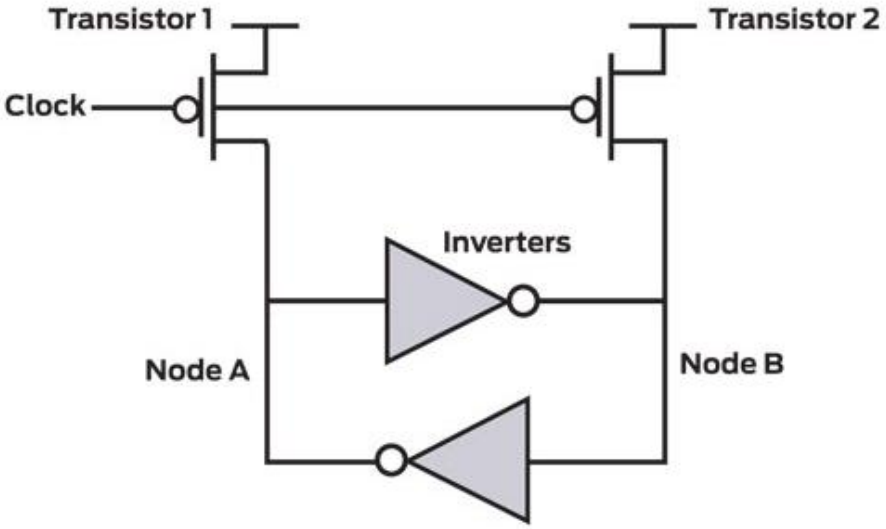
- The security of modern cryptographic protocols relies heavily on the availability of true random key material and nonces.
- On standard computer platforms it is not a trivial task to collect true random material in sufficient quantities:
  - Key Stroke Timing
  - Mouse Movements
  - Sampled Sound Card Input Noise
  - Air Turbulence in Disk Drives
  - RAID Disk Array Controllers
  - Network Packet Arrival Times
  - Computer Clocks
- Best Strategy: Combining various random sources with a strong mixing function (e.g. MD5 or SHA-1 hash) into an entropy pool (e.g. Unix /dev/random) protects against single device failures.

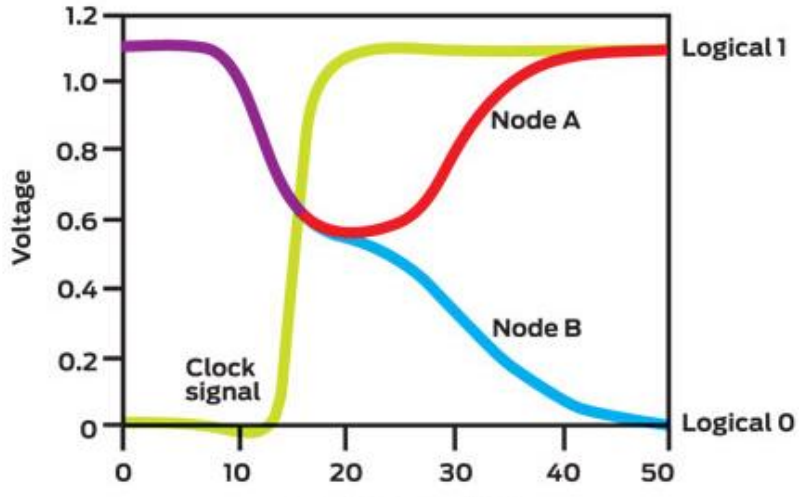
Hardware-based True Random Generators

- Quantum Sources or Radioactive Decay Sources
  - Reliable, high entropy sources, but often bulky and expensive.
- Thermal Noise Sources
  - Noisy diodes or resistors are cheap and compact but level detection usually introduces considerable skew that must be corrected.
- Free Running or Metastable Oscillators
  - The frequency variation of a free running oscillator is a good entropy source if designed and measured properly. Used e.g in smart card crypto co-processors.
  - The Intel Ivy Bridge processor family implements an on-chip metastable digital oscillator.
- Lava Lamps
  - Periodic digital snapshots of a lava lamp exhibit a lot of randomness.

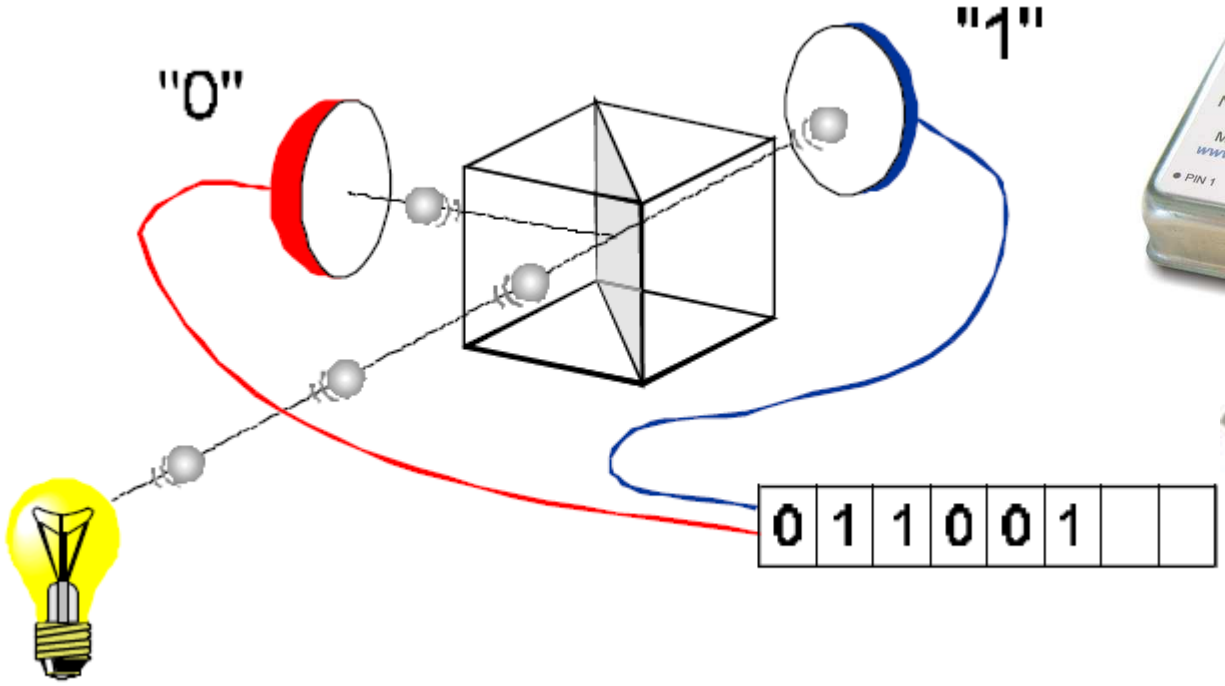
The Intel RDRAND Instruction

- Available with Intel Ivy Bridge Processors (XEON & Core i7)
  - The RDRAND instruction reads a 16, 32 or 64 bit random value
  - Throughput 500+ MB/s random data with 8 concurrent threads
  - The random number generator is compliant with NIST SP800-90, FIPS 140-2, and ANSI X9.82





Quantum Random Number Generator
www.idquantique.com



- Detection of single photons via a semi-transparent mirror
- High throughput: 4 – 16 Mbit/s
- Low cost (990…2230 EUR)

IDQ
FROM VISION TO TECHNOLOGY

Skew Corrections and Tests for Randomness

- Simple Skew Correction (John von Neumann)
  - p(1) = 0.5+e, p(0) = 0.5-e, -0.5 < e < 0.5
  - Example with e = 0.20, i.e. p(1) = 0.7, p(0) = 0.3

```
11011111101011011000100111100111011111101101111111110101
 - 0 - - 1 1 - 0 1 - 1 0 - 1 0 - 0 - - 1 - 0 - - - - 0 0
```

- Strong Mixing using Hash functions
  - Hashing improves statistical properties but does not increase entropy.
- Statistical Tests for Randomness
  - A number of statistical tests are defined in FIPS PUB 140-2 "*Security Requirements for Cryptographic Modules*" : Monobit Test, Poker Test, Runs Test, etc.
- Entropy Measurements
  - The entropy of a random or pseudo-random binary sequence can be measured using Ueli Maurer's *"Universal Statistical Test for Random Bit Generators"*