

A survey and low-level comparison of network based symmetric key distribution architectures

Presentation by
Benjamin Gittins (CTO)
Synaptic Laboratories Limited



A survey and low-level comparison of network based symmetric key distribution architectures

Comparing the features and limitations of several symmetric identity management and cryptographic key management (IdM/CKM) distribution architectures with the objective of identifying those that might be adapted to satisfy NIST's 2009 call for a new cryptographic key management design based solely on symmetric key techniques - not a rip and replacement design, but one that extends the life, availability and functionality of our existing security standards investments

Presentation by
Benjamin Gittins (CTO)
Synaptic Laboratories Limited

Table of Contents



Table of Contents

- ▣➤ **The Objective: Secure private communications over a network**
- ▣➤ **Taxonomy of unencrypted networks**
- ▣➤ **Two party symmetric key security model**
- ▣➤ **Protecting against side-channel attacks**
- ▣➤ **Securing networks**
- ▣➤ **Survey of Symmetric IdM/CKM Protocols**
 - ▣➤ Quantum Key Distribution (Key Distribution Only)
 - ▣➤ Kerberos (Enterprise IdM with CKM)
 - ▣➤ Omnisec Security Architecture (Enterprise Security)
 - ▣➤ Goldkey (Enterprise Security)
 - ▣➤ Diffie-Hellman-Lampport (Enterprise IdM with CKM)
- ▣➤ **Closing Statement**

Seeking to identify:



Seeking to identify:



Orange globe: <http://www.lumaxart.com/>
Background on smart card © Inmage, used with permission.

Seeking to identify:

- Symmetric key techniques to enable secure private communications between any 2 people in the world, with global scalability



Orange globe: <http://www.lumaxart.com/>
Background on smart card © Imagine, used with permission.

Seeking to identify:

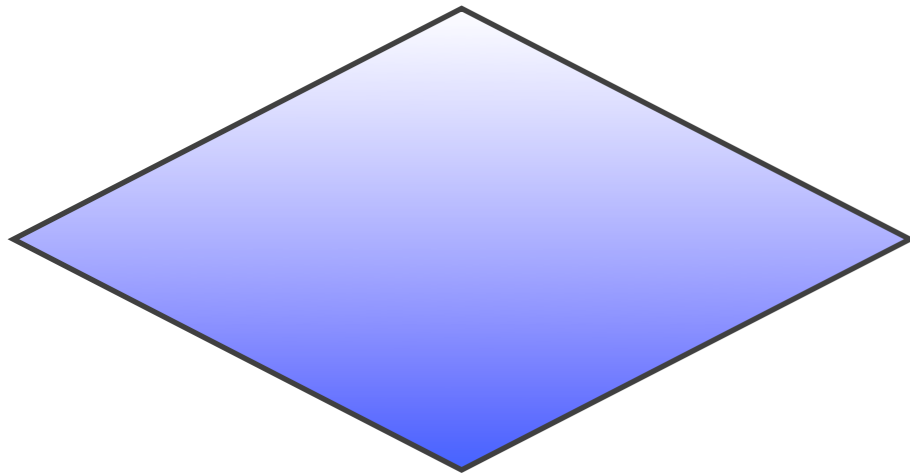
- Symmetric key techniques to enable secure private communications between any 2 people in the world, with global scalability
- Preferably using smart cards (hardware security modules) to manage symmetric key material



Orange globe: <http://www.lumaxart.com/>
Background on smart card © Inmage, used with permission.

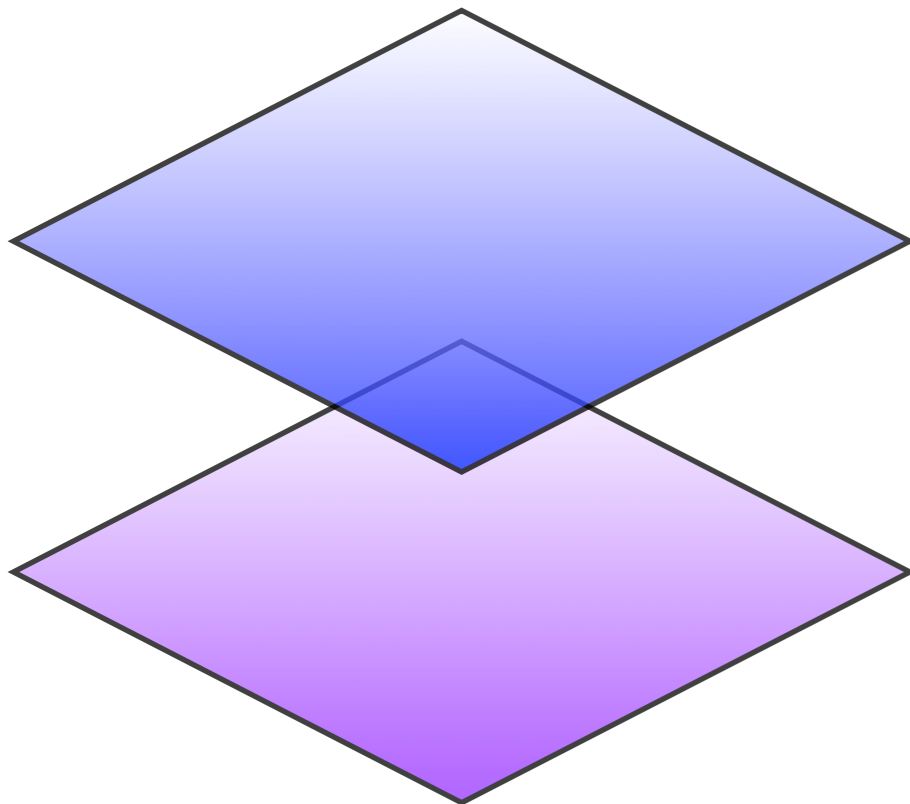
Synaptic is seeking a defense-in-depth solution:

Synaptic is seeking a defense-in-depth solution:



⇐ **Asymmetric** (SSL, IPSEC)
Leverage existing NIST standards
Ready for 2nd generation technologies

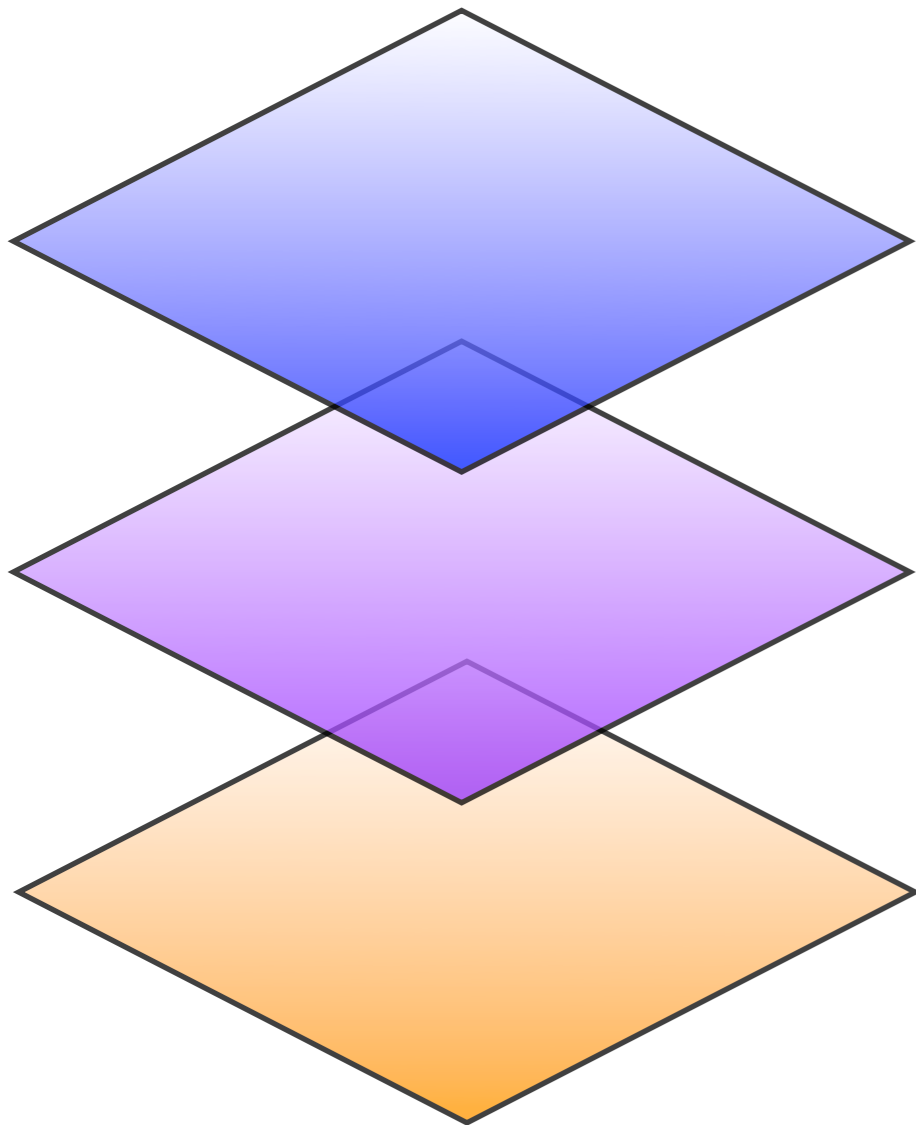
Synaptic is seeking a defense-in-depth solution:



- ⇐ **Asymmetric** (SSL, IPSEC)
Leverage existing NIST standards
Ready for 2nd generation technologies
- ⇐ **Symmetric Systems**
Leverage NIST standards (PQS)
Ensure secure against insider attacks



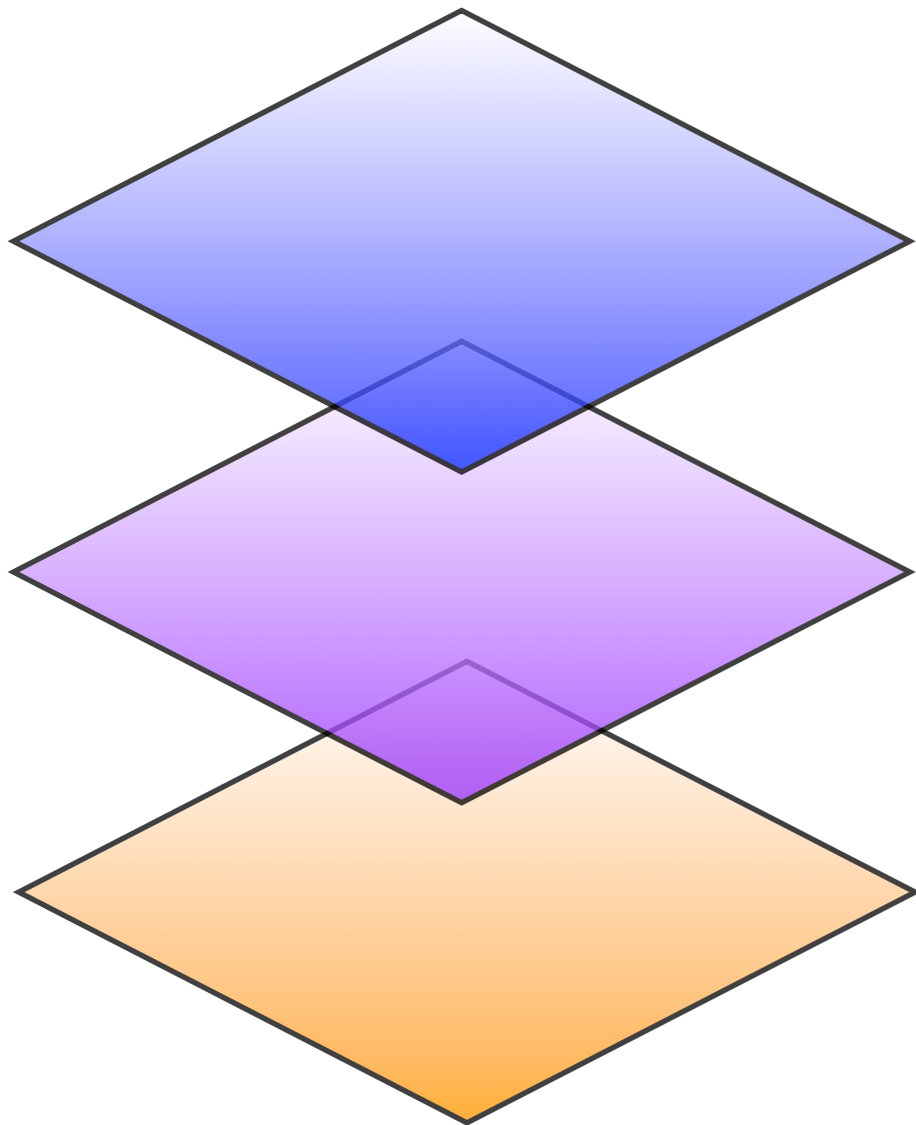
Synaptic is seeking a defense-in-depth solution:



- ⇐ **Asymmetric** (SSL, IPSEC)
Leverage existing NIST standards
Ready for 2nd generation technologies
- ⇐ **Symmetric Systems**
Leverage NIST standards (PQS)
Ensure secure against insider attacks
- ⇐ **Quantum Key Distribution**
Next generation transceivers (robust)
2nd generation network topologies



Synaptic is seeking a defense-in-depth solution:



- ⇐ **Asymmetric** (SSL, IPSEC)
Leverage existing NIST standards
Ready for 2nd generation technologies
- ⇐ **Symmetric Systems**
Leverage NIST standards (PQS)
Ensure secure against insider attacks
- ⇐ **Quantum Key Distribution**
Next generation transceivers (robust)
2nd generation network topologies

➡ Advance 3 classes of cryptography, look for synergistic design strategies



NIST 2009: Cybersecurity requires new CKM designs

NIST 2009: Cybersecurity requires new CKM designs

Some features requested by NIST Management in 2009	X.509 PKI
Fault tolerance (all services)	FAIL
High availability (all services)	FAIL
Secure against destructive attacks (insider attacks)	FAIL
Scalable to billions of users/devices	FAIL
Support accountability, auditing and policy management	FAIL
Interoperable	imperfect
Enable ubiquitous take up of encryption	FAIL
Secure against code-breaking quantum computers	FAIL



Brian SNOW



Peter SHOR





Brian SNOW

"The [*ed.* quantum] **threat to cryptography** is well understood due to work by (Peter) Shor and others

A **symmetric algorithm** like AES or other standard crypto processes is **cut key-size in half**, which is a **dramatic reduction**..."

Brian SNOW

Former Technical Director of the Information Assurance Directorate, US NSA



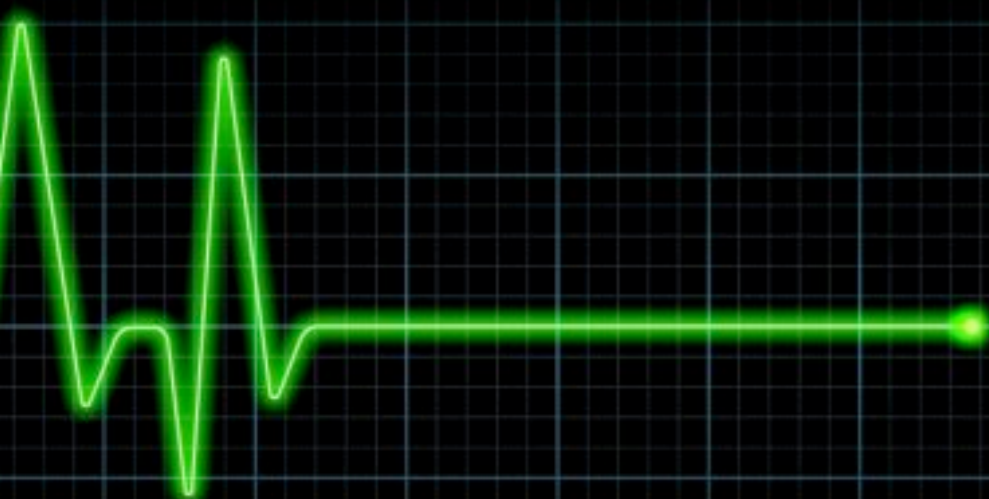
Peter SHOR



Whitfield **DIFFIE**

Martin **HELLMAN**

Brian **SNOW**

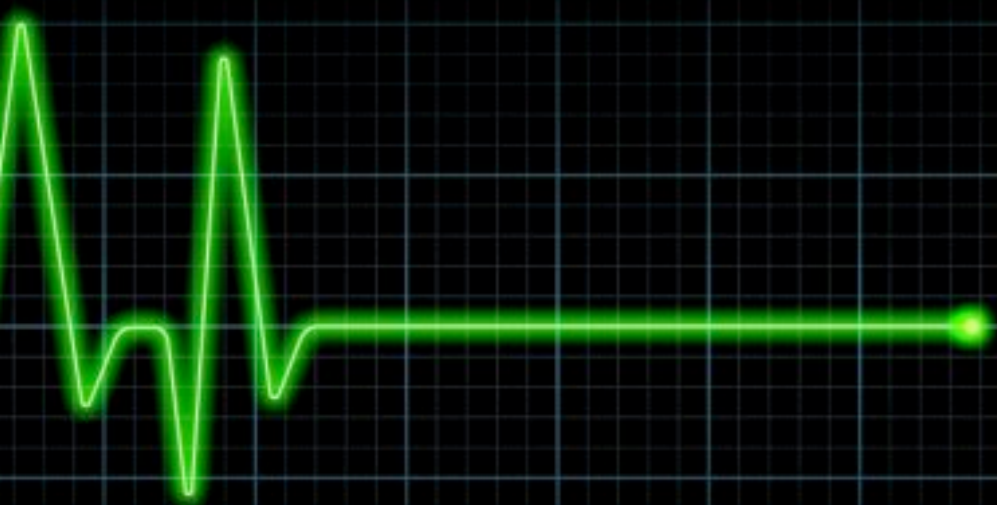




Whitfield **DIFFIE**

Martin **HELLMAN**

Brian **SNOW**



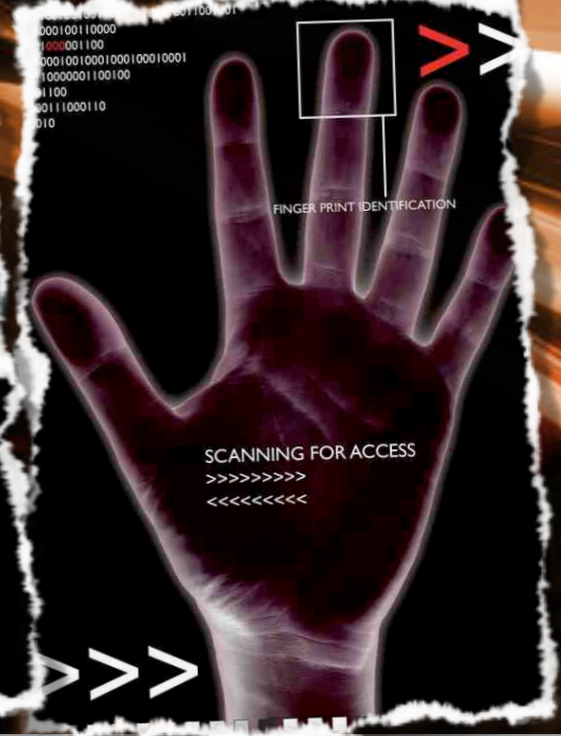
"Now for key management purposes,
against the **RSA** and the **Diffie-Hellman**, they
FLAT-LINE under a quantum computer."

Brian **SNOW**



SYNAPTIC LABORATORIES LTD.

A survey and low-level comparison
of network based symmetric key
distribution architectures





The RSA algorithm has been deployed in
more than one billion applications worldwide

Over One Billion Applications At Risk





PQCrypto 2010

The Third International Workshop on Post-Quantum Cryptography
Darmstadt, Germany, May 25-28, 2010



PQCrypto 2010

The Third International Workshop on Post-Quantum Cryptography
Darmstadt, Germany, May 25-28, 2010

- ➔ The cryptographic community has begun searching for next generation public key solutions (2006, 2008, and now 2010)



PQCrypto 2010

The Third International Workshop on Post-Quantum Cryptography
Darmstadt, Germany, May 25-28, 2010

- The cryptographic community has begun searching for next generation public key solutions (2006, 2008, and now 2010)
- However this initiative has only just begun and meanwhile all PKC protected data can be expected to be decrypted and exploited up until when PKC is post quantum secure



PQCrypto 2010

The Third International Workshop on Post-Quantum Cryptography
Darmstadt, Germany, May 25-28, 2010

- The cryptographic community has begun searching for next generation public key solutions (2006, 2008, and now 2010)
- However this initiative has only just begun and meanwhile all PKC protected data can be expected to be decrypted and exploited up until when PKC is post quantum secure
- A long, difficult challenge, expected to morph with new quantum algorithms being discovered (ARDA Report 2004)



PQCrypto 2010

The Third International Workshop on Post-Quantum Cryptography
Darmstadt, Germany, May 25-28, 2010



PQCrypto 2010

The Third International Workshop on Post-Quantum Cryptography
Darmstadt, Germany, May 25-28, 2010

- ➔ It is conceivable that code-breaking quantum computers will arrive well before a secure 2nd generation PKC solution is found and confidence won



PQCrypto 2010

The Third International Workshop on Post-Quantum Cryptography
Darmstadt, Germany, May 25-28, 2010

- It is conceivable that code-breaking quantum computers will arrive well before a secure 2nd generation PKC solution is found and confidence won
- ARDA Report pointed to the known survivability of certain types of symmetric algorithms (such as NIST AES-256 and SHA-256) against Grover's quantum algorithm as potentially the best way forwards

On the current state of PKI

On the current state of PKI

- ▶ The Electronic Freedom Foundation now advocates the ubiquitous use of SSL/TLS, which uses PKI X.509

On the current state of PKI

- The Electronic Freedom Foundation now advocates the ubiquitous use of SSL/TLS, which uses PKI X.509
- Dr Peter Gutmann in his draft book nearing publication titled “Engineering Security” argues it is impossible to differentiate SSL/TLS security from placebo, due to multiple single points of potential catastrophic failure at the CA level, specification and implementation problems



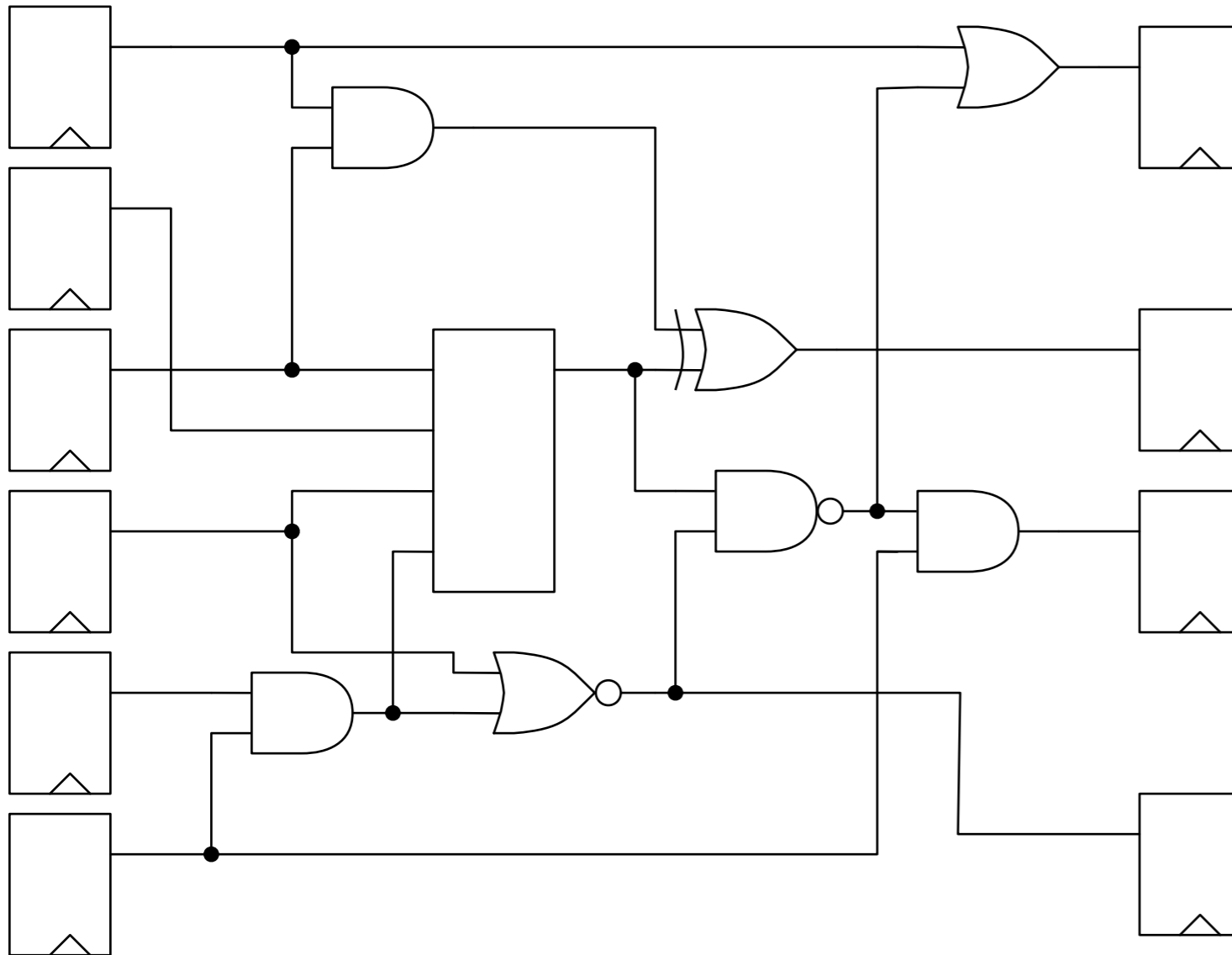
On the current state of PKI

- The Electronic Freedom Foundation now advocates the ubiquitous use of SSL/TLS, which uses PKI X.509
- Dr Peter Gutmann in his draft book nearing publication titled “Engineering Security” argues it is impossible to differentiate SSL/TLS security from placebo, due to multiple single points of potential catastrophic failure at the CA level, specification and implementation problems
- Prof Richard Brooks’ presentation at ORNL CSIR Workshop April 2010 titled “Lies and the Lying Liars that Tell Them - A fair and balanced look at TLS” - came to a similar conclusion

What is a network?

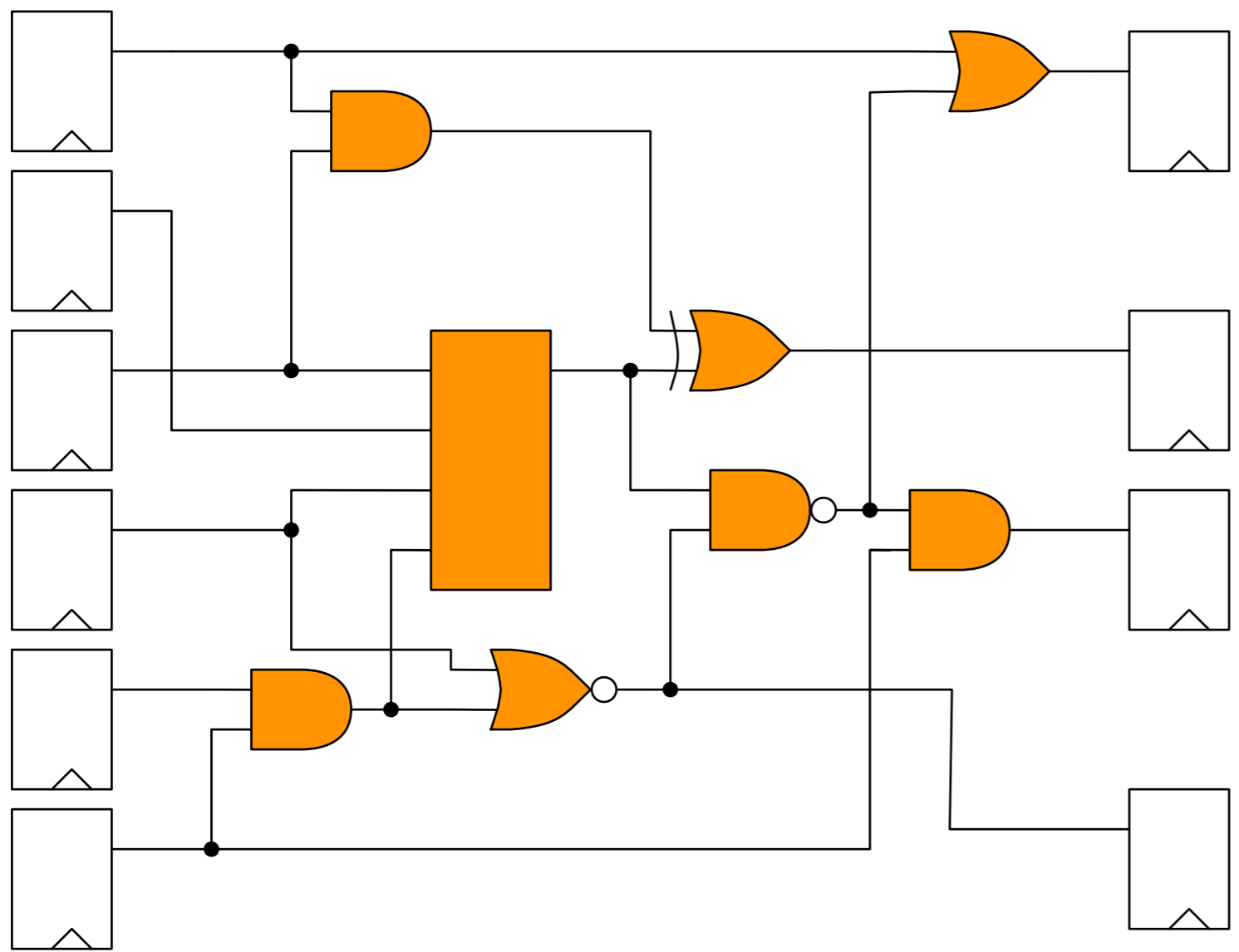
What is a network?

➡ At a very low level of abstraction, every network comprises:



What is a network?

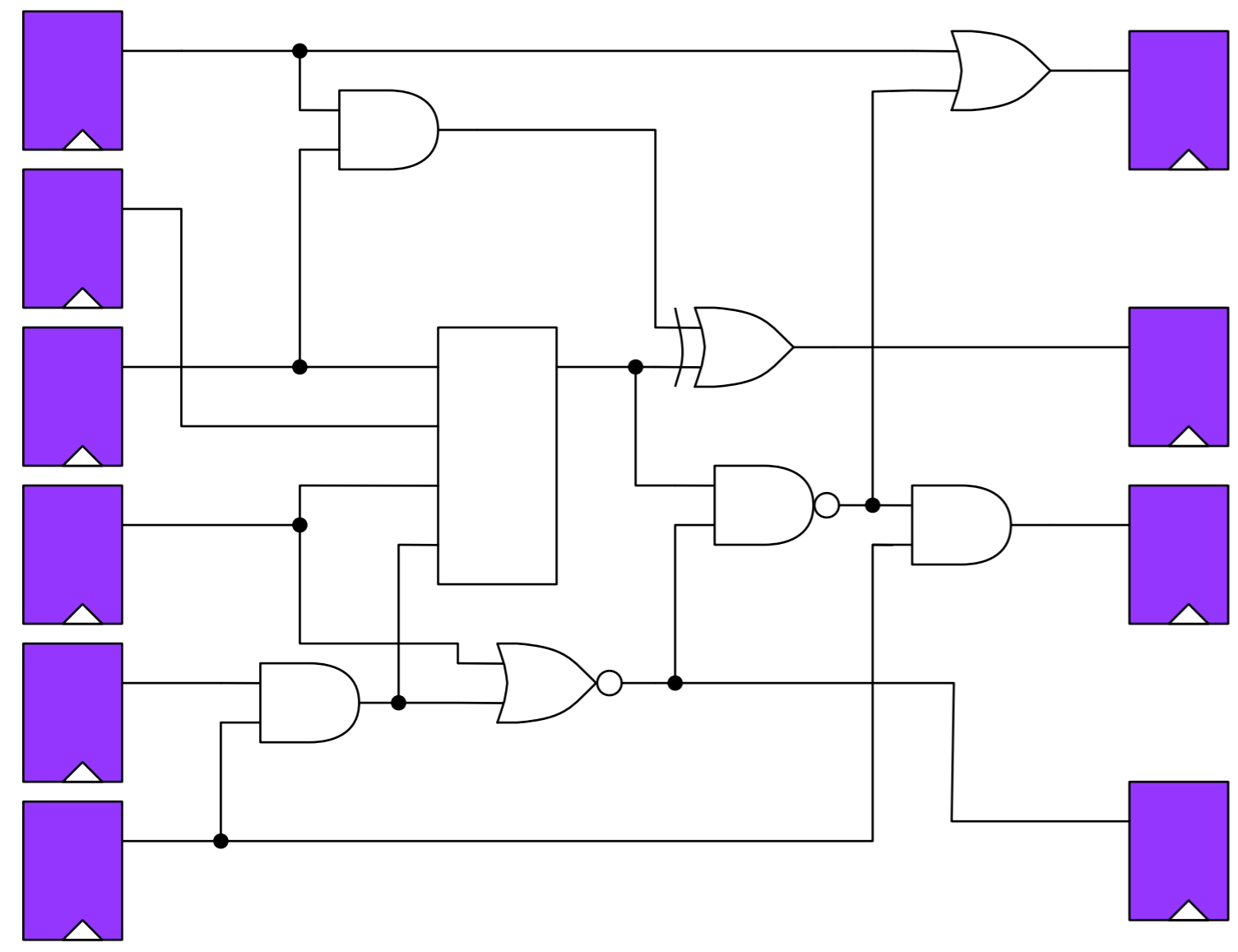
At a very low level of abstraction, every network comprises:



Combinatorial logic

What is a network?

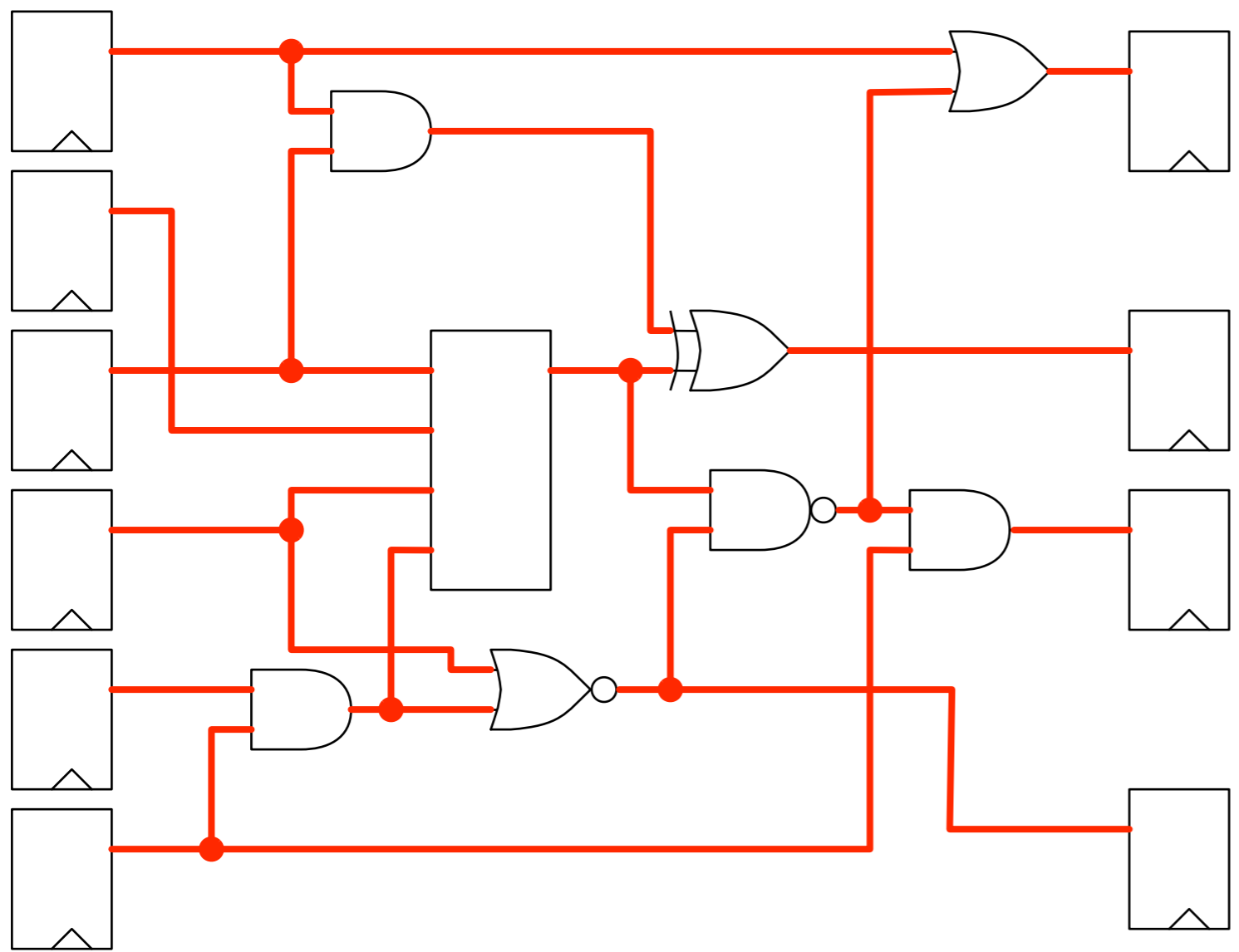
At a very low level of abstraction, every network comprises:






- Combinatorial logic
- Memory / State

What is a network?

At a very low level of abstraction, every network comprises:

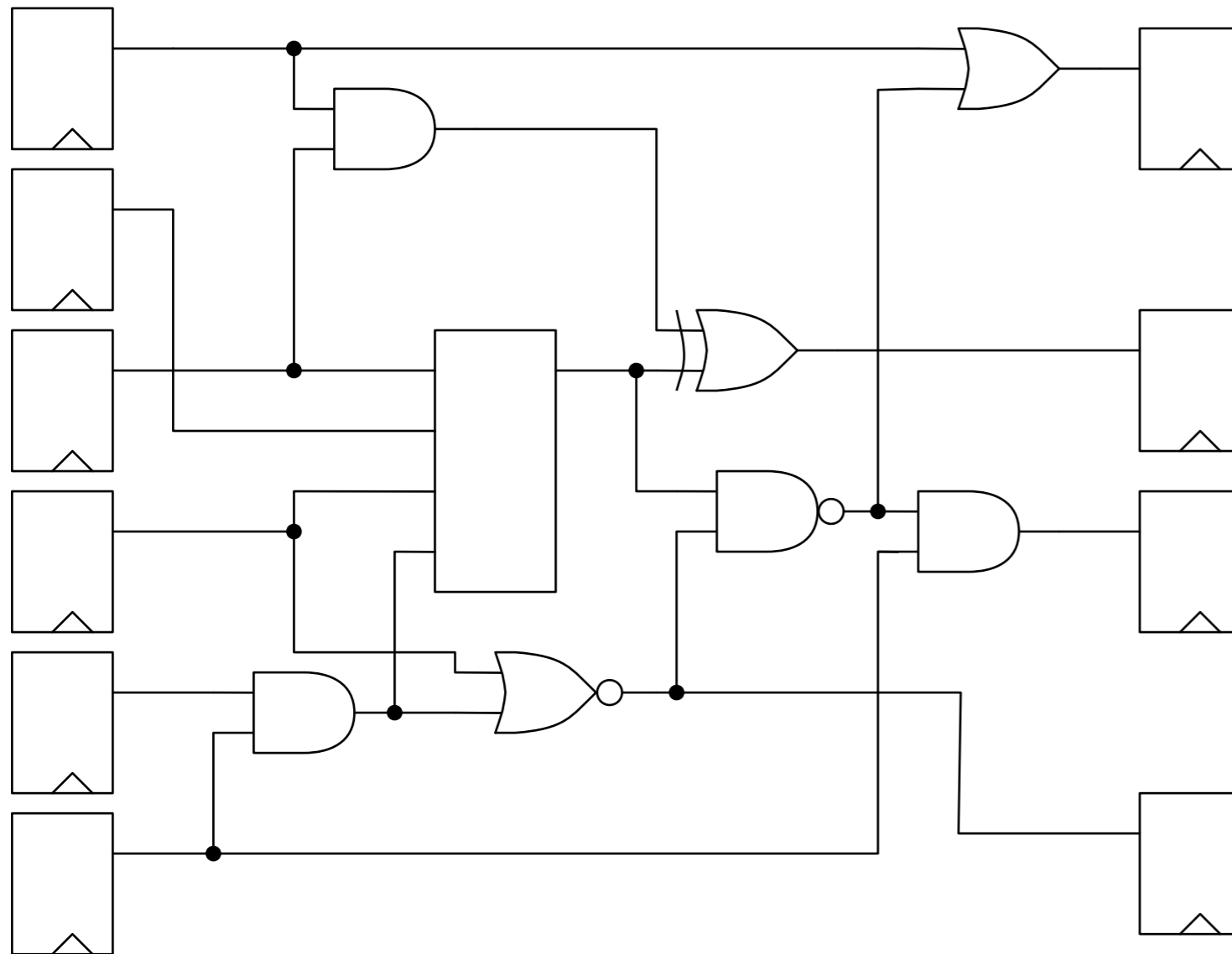


-  Combinatorial logic
-  Memory / State
-  Wires connecting logic and memory together



What is a network?

➡ At a very low level of abstraction, every network comprises:



➡ Combinatorial logic

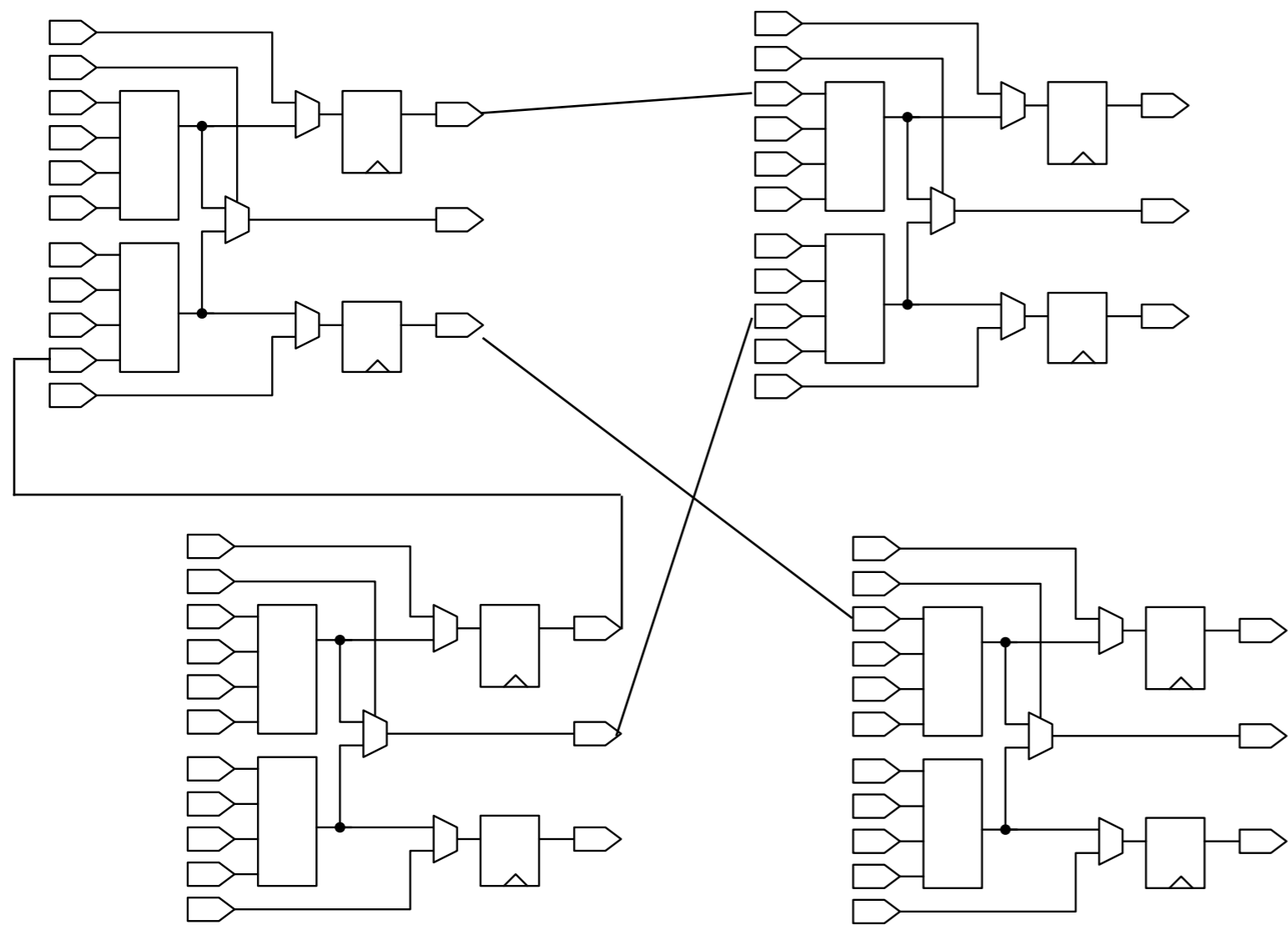
➡ Memory / State

➡ Wires connecting
logic and memory
together

➡ In fact, every analog
and digital circuit is an
electronic network

What is a network?

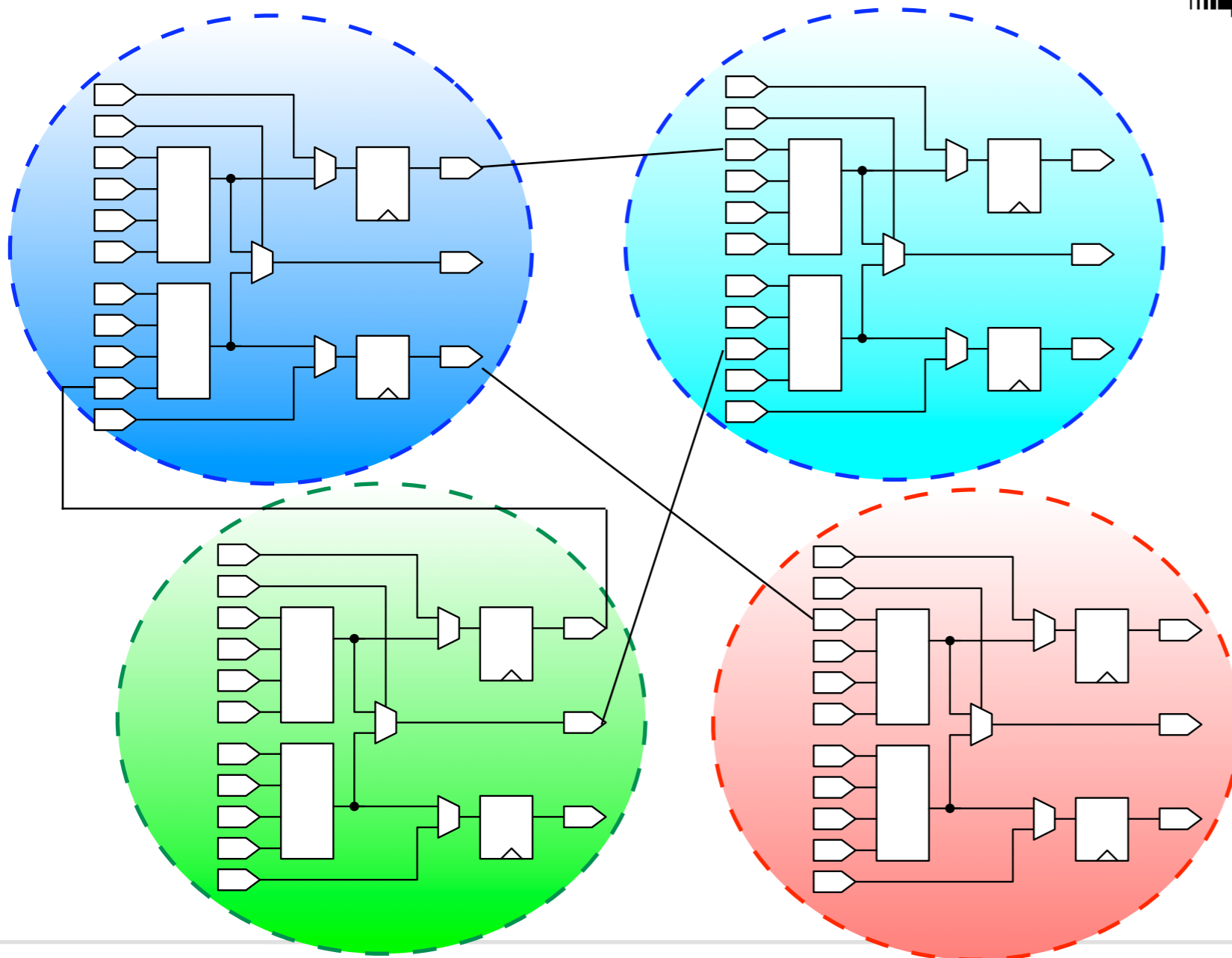
At a very low level of abstraction, **The Internet™** is a monolithic network of processing and storage elements



What is a network?

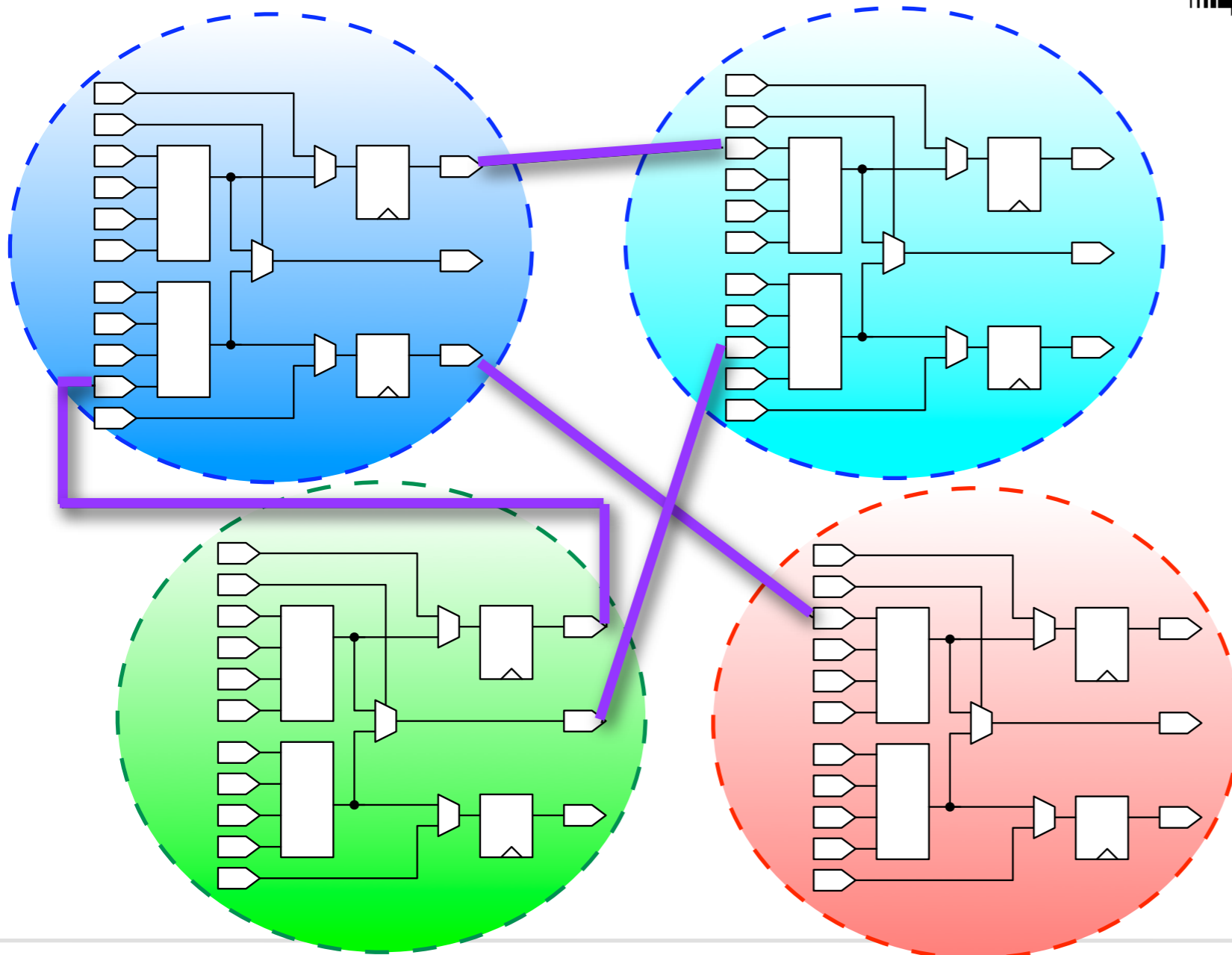
➤ At a very low level of abstraction, **The Internet™** is a monolithic network of processing and storage elements

➤ At a higher level of abstraction, we place somewhat arbitrary boundaries around groups of processing elements, and call them **devices or computers**



What is a network?

➤ At a very low level of abstraction, **The Internet™** is a monolithic network of processing and storage elements



➤ At a higher level of abstraction, we place somewhat arbitrary boundaries around groups of processing elements, and call them **devices** or **computers**

➤ By convention, the act of connecting computers using relatively long “wires” creates a (wireless) computer network



Taxonomy of unencrypted network topologies



Taxonomy of unencrypted network topologies



- ➡ Where 2 parties are communicating within one “device”



Taxonomy of unencrypted network topologies



- Where 2 parties are communicating within one “device”
- Software in isolated address spaces



Taxonomy of unencrypted network topologies



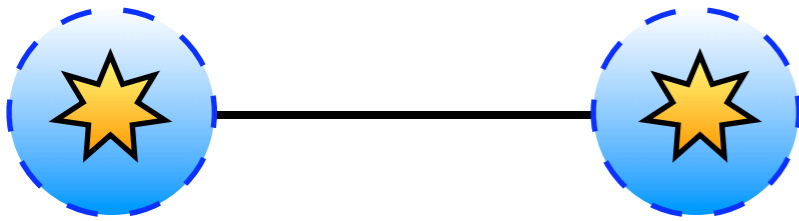
- Where 2 parties are communicating within one “device”
- Software in isolated address spaces
- Between IC (chips) on a motherboard



Taxonomy of unencrypted network topologies



- Where 2 parties are communicating within one “device”
- Software in isolated address spaces
- Between IC (chips) on a motherboard



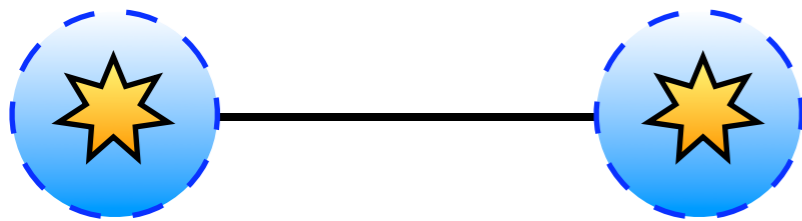
- Where 2 leaf-nodes are communicating over a relatively long network cable, or wireless, without further assistance



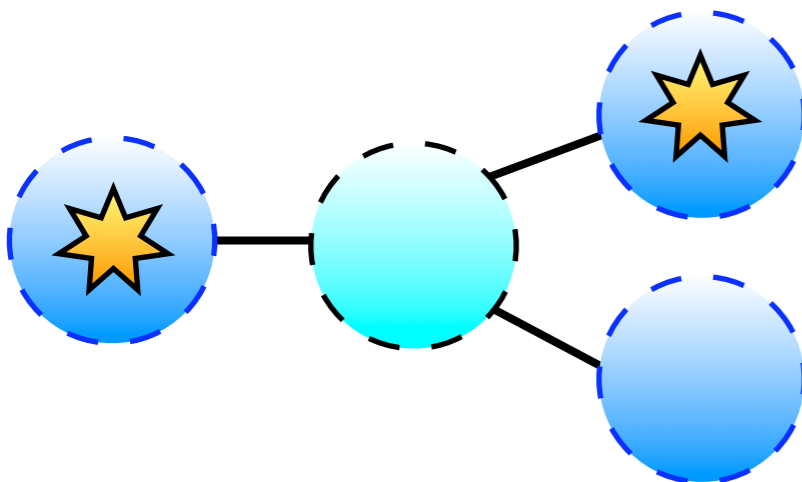
Taxonomy of unencrypted network topologies



- Where 2 parties are communicating within one “device”
- Software in isolated address spaces
- Between IC (chips) on a motherboard



- Where 2 leaf-nodes are communicating over a relatively long network cable, or wireless, without further assistance

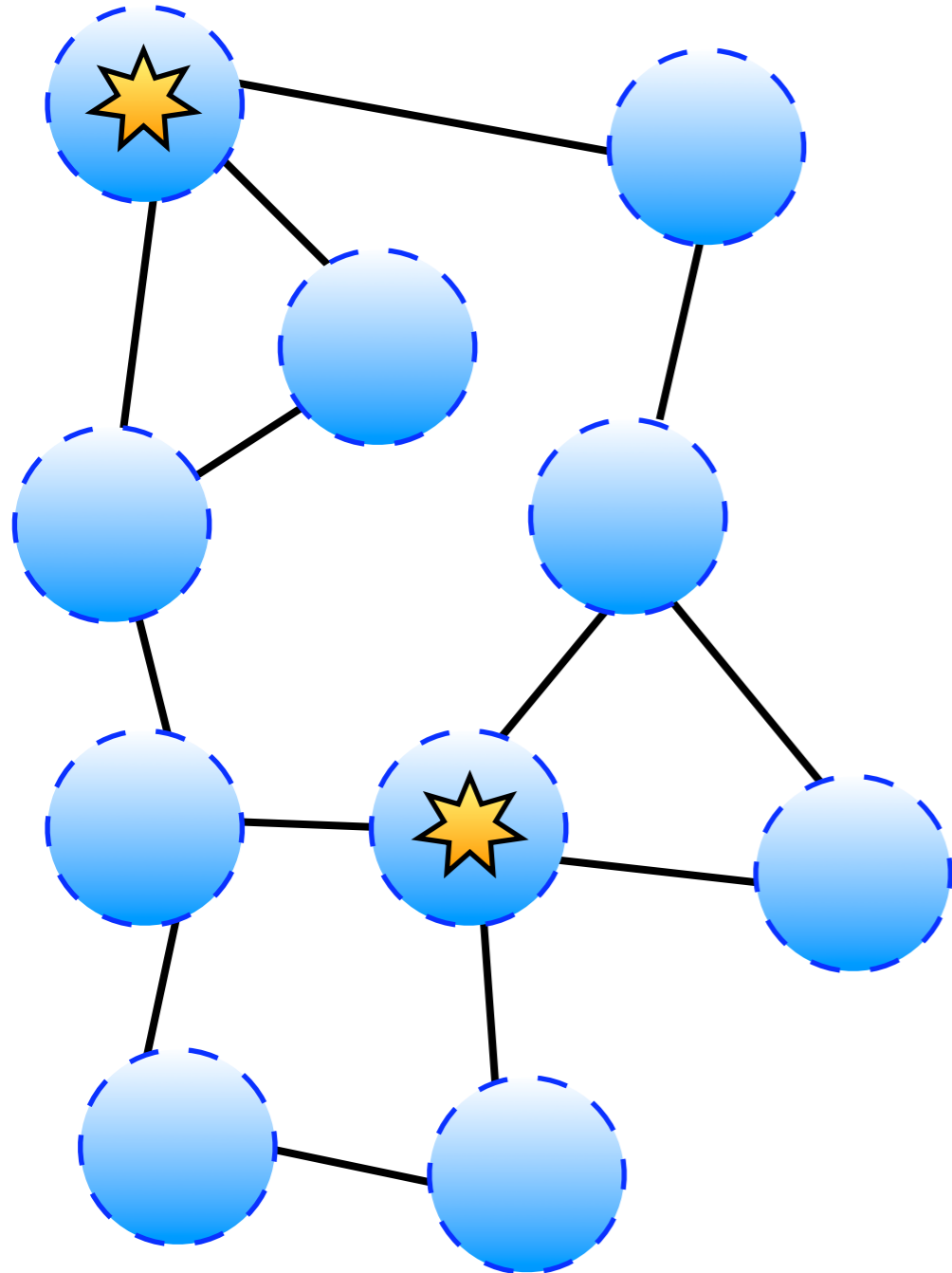


- Where 2 leaf-nodes are communicating over a relatively long distance, with the assistance of 1 or more other internal nodes that may or may not be multi-homed (hub, switch, router...)

Taxonomy of unencrypted networks



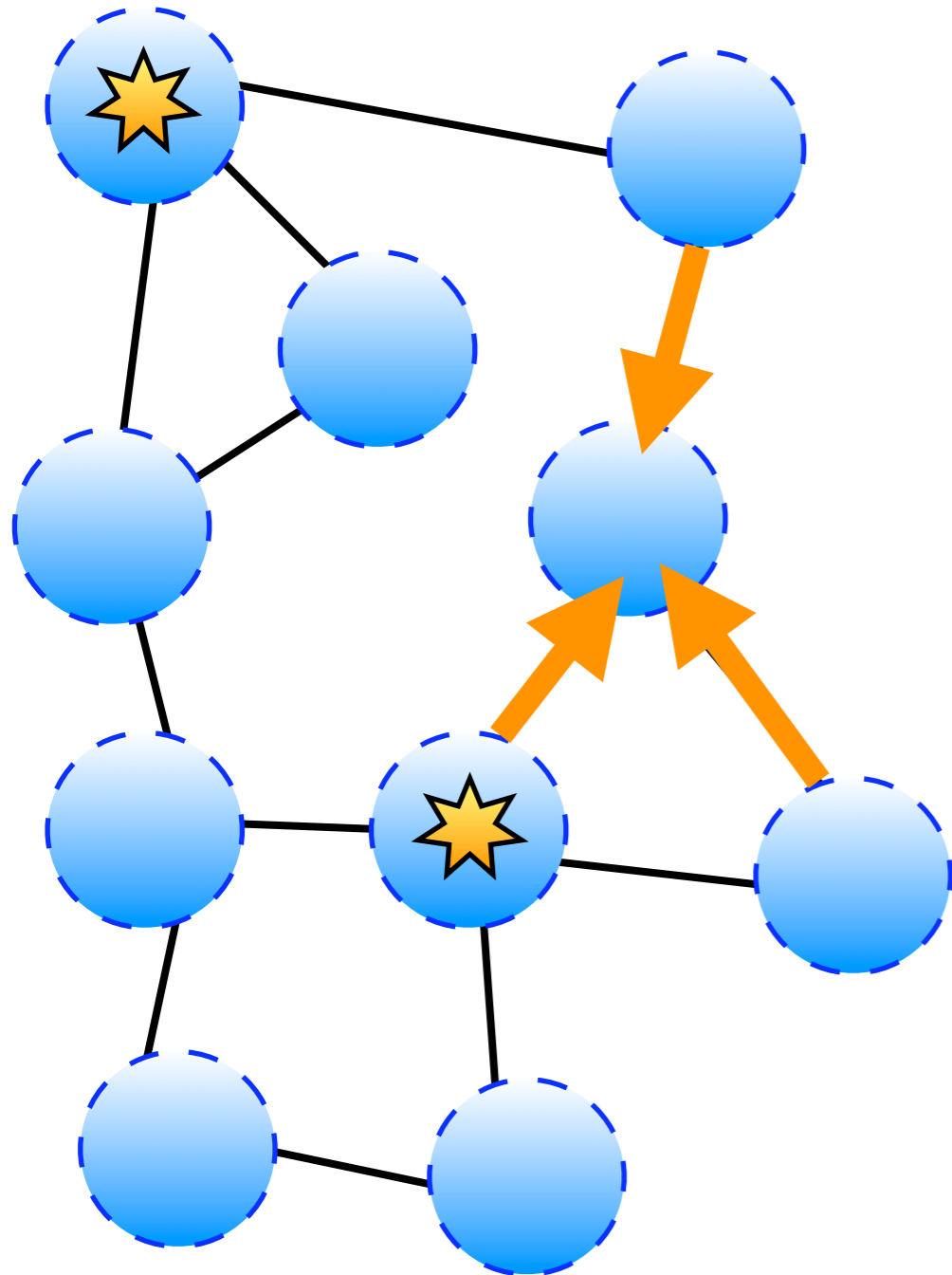
Taxonomy of unencrypted networks



➡ A mesh network topology is where the majority of nodes are:



Taxonomy of unencrypted networks

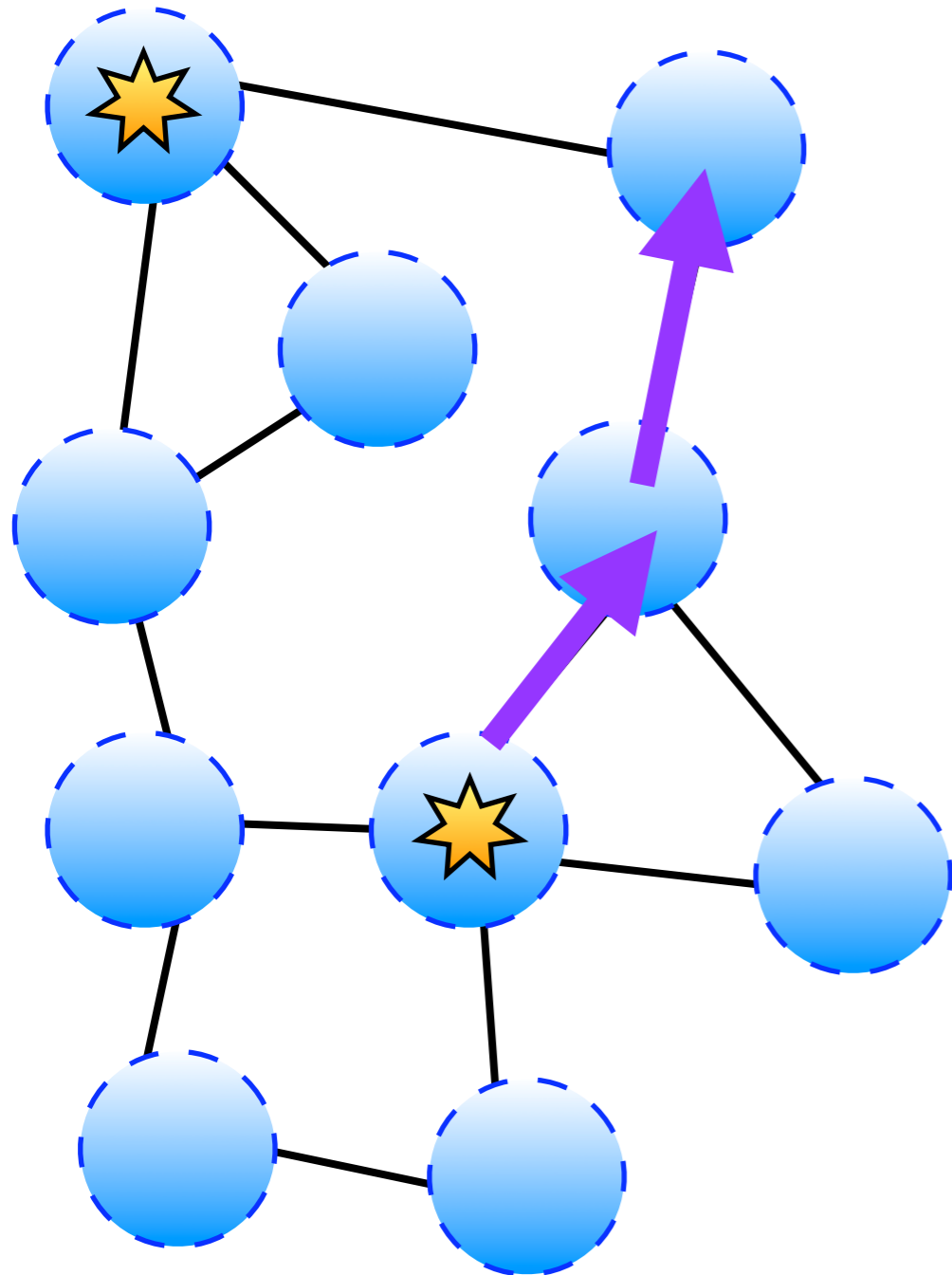


➡ A mesh network topology is where the majority of nodes are:

➡ multi-homed



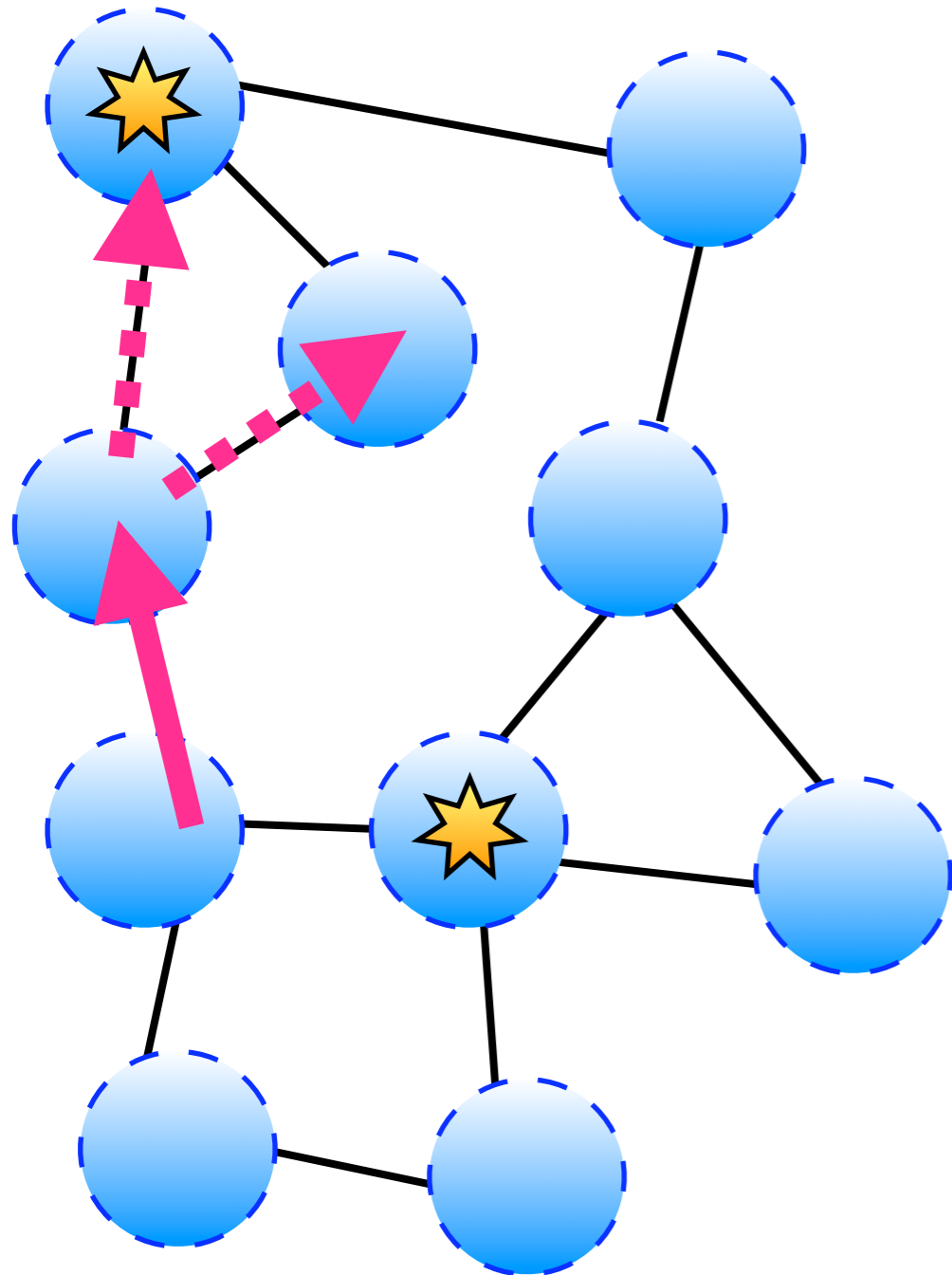
Taxonomy of unencrypted networks



- ➡ A mesh network topology is where the majority of nodes are:
 - ➡ multi-homed
 - ➡ relay traffic with adjacent nodes



Taxonomy of unencrypted networks



➡ A mesh network topology is where the majority of nodes are:

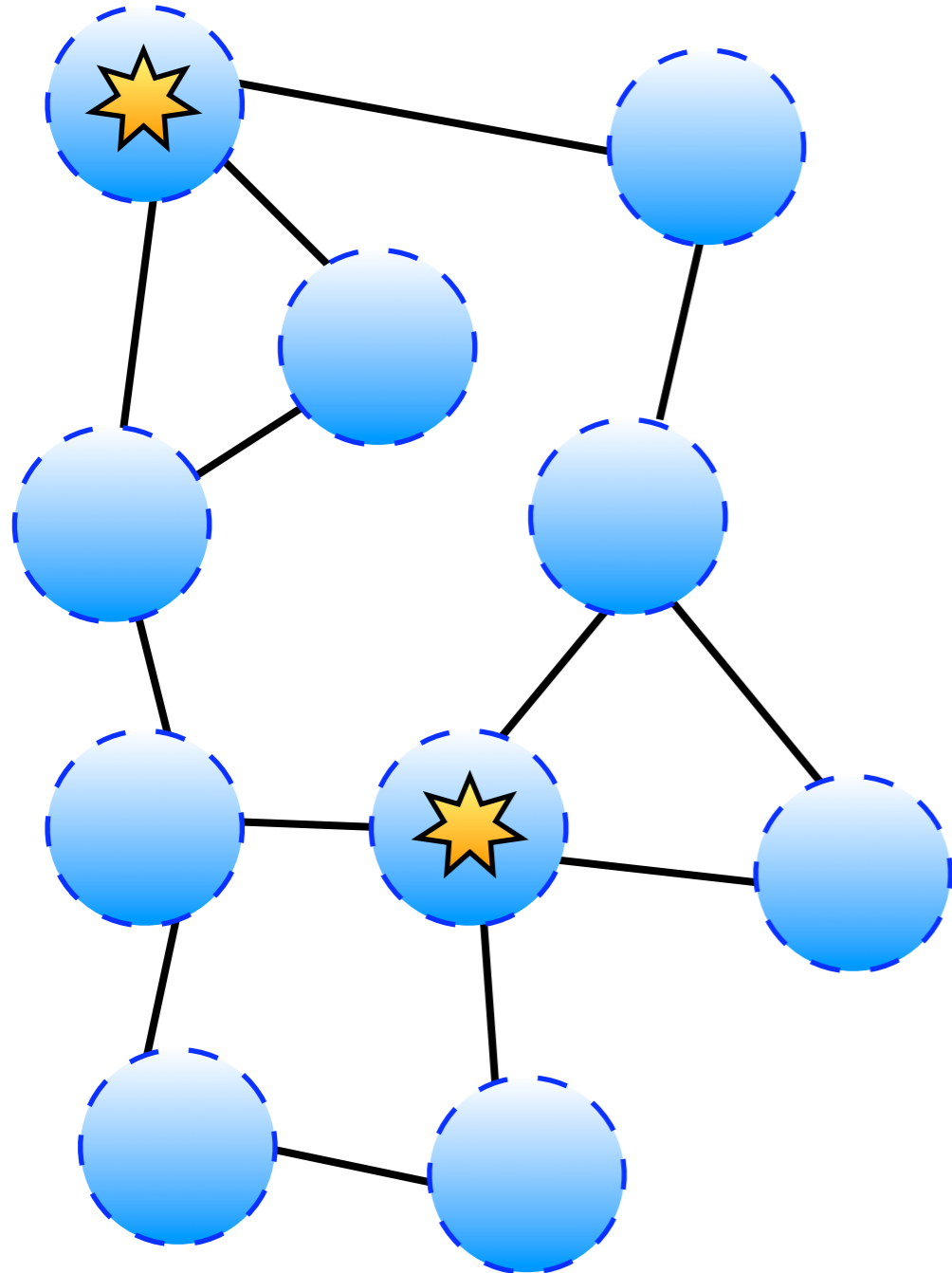
➡ multi-homed

➡ relay traffic with adjacent nodes

➡ may acts as routers



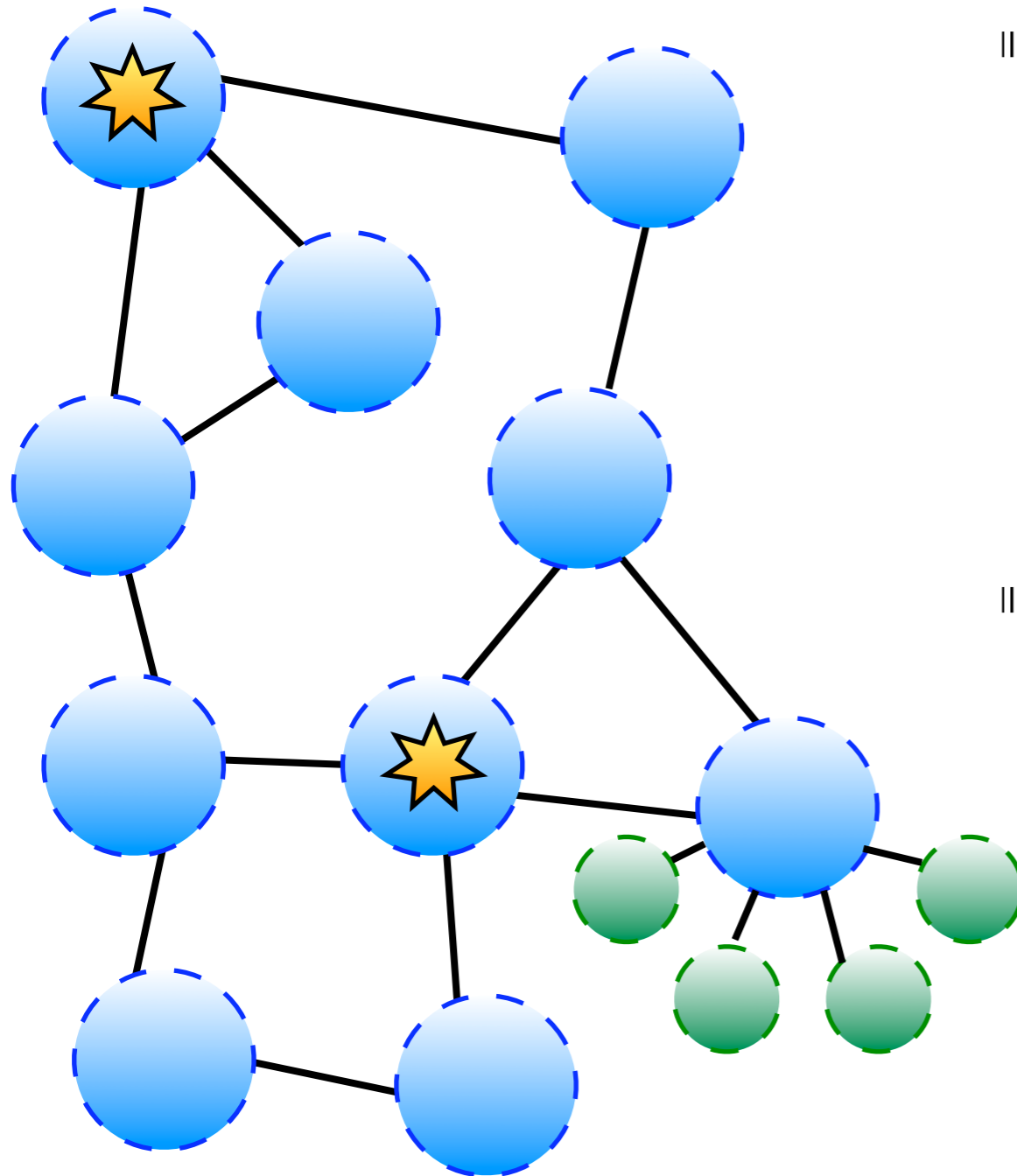
Taxonomy of unencrypted networks



- A mesh network topology is where the majority of nodes are:
 - multi-homed
 - relay traffic with adjacent nodes
 - may acts as routers
- A mesh network may be:
 - The full network itself



Taxonomy of unencrypted networks



- A mesh network topology is where the majority of nodes are:
 - multi-homed
 - relay traffic with adjacent nodes
 - may acts as routers
- A mesh network may be:
 - The full network itself
 - A back-bone for transporting long-distance traffic, where the traffic originates on leaf-nodes that are not multi-homed

Essential Cryptographic Assumptions



Ueli Maurer:

Professor of Computer Science
Information Security and Cryptography
Research Group, ETH Zurich

Essential Cryptographic Assumptions



- All cryptography takes place in a physical universe in which nobody has complete awareness about what is taking place in that universe (No person or computer is all-seeing, all-knowing!)

Ueli Maurer:

Professor of Computer Science
Information Security and Cryptography
Research Group, ETH Zurich

Essential Cryptographic Assumptions



- All cryptography takes place in a physical universe in which nobody has complete awareness about what is taking place in that universe (No person or computer is all-seeing, all-knowing!)
- All cryptographic systems rely on the assumption that random numbers can be generated

Ueli Maurer:

Professor of Computer Science
Information Security and Cryptography
Research Group, ETH Zurich



Essential Cryptographic Assumptions



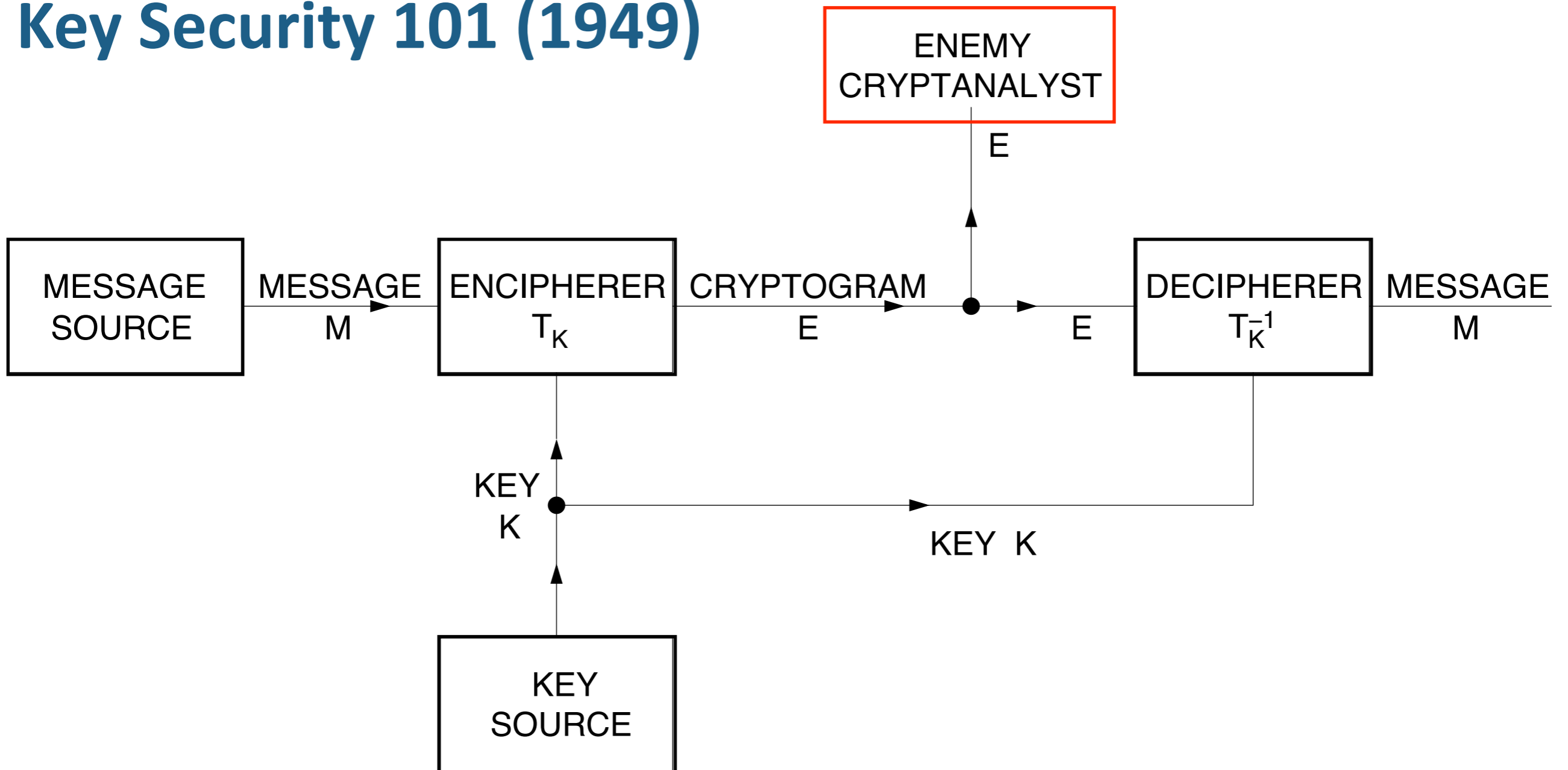
Ueli Maurer:

Professor of Computer Science
Information Security and Cryptography
Research Group, ETH Zurich

- All cryptography takes place in a physical universe in which nobody has complete awareness about what is taking place in that universe (No person or computer is all-seeing, all-knowing!)
- All cryptographic systems rely on the assumption that random numbers can be generated
- An adversary has no idea about the value of the next output of a random number generator

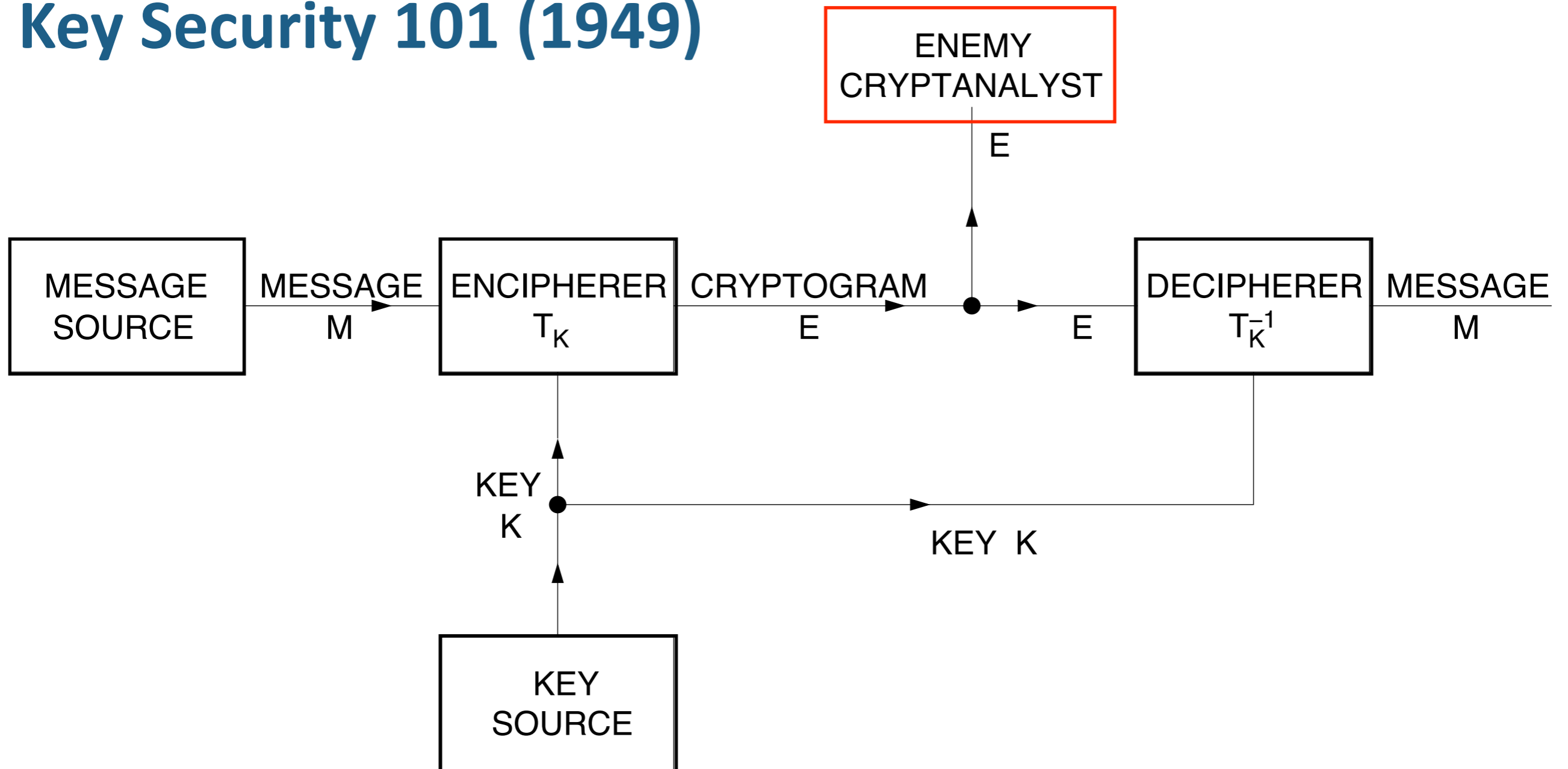


Point-to-Point Symmetric Key Security 101 (1949)





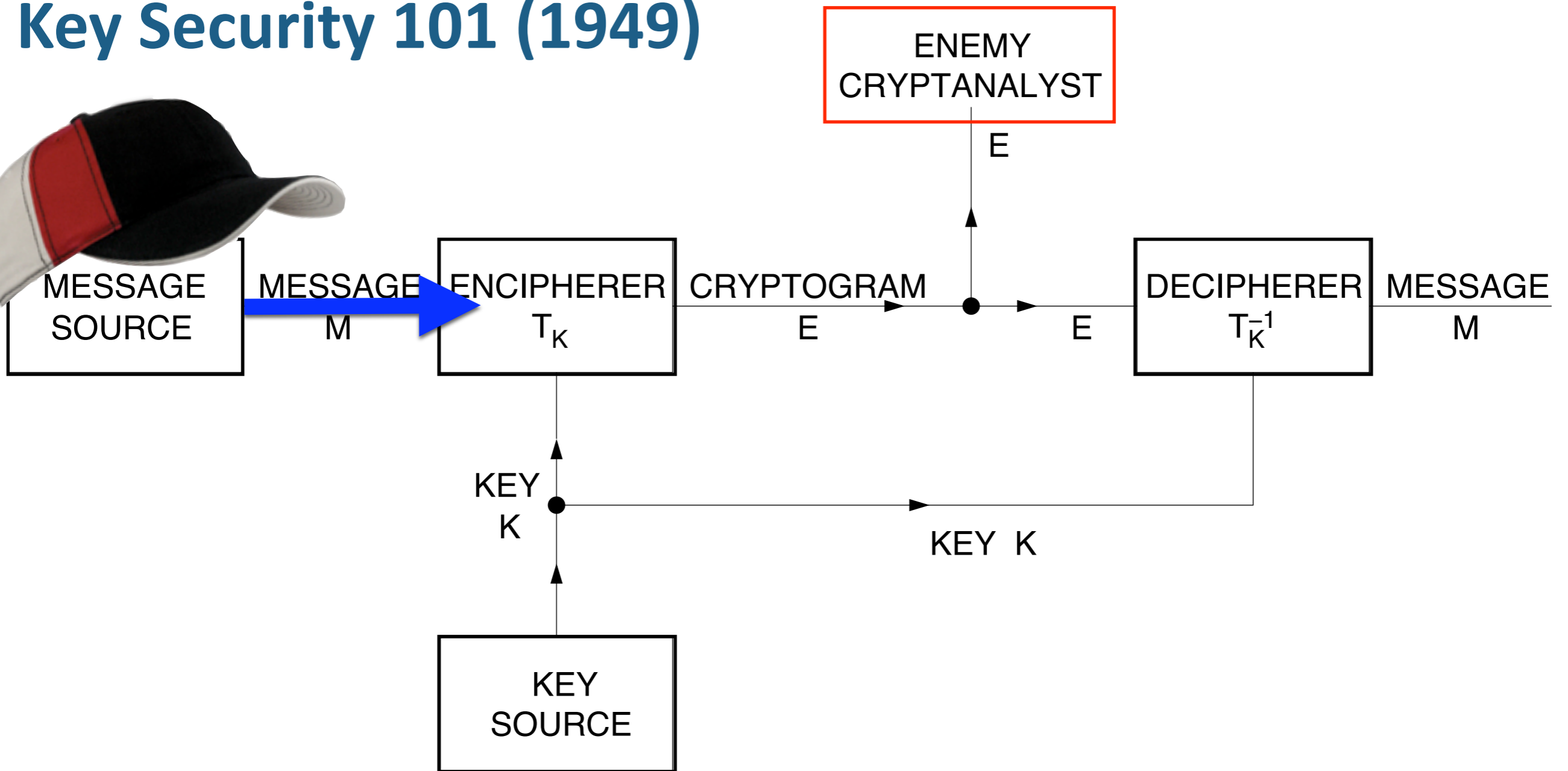
Point-to-Point Symmetric Key Security 101 (1949)



➡ Claude E. Shannon's classical 1949 threat model



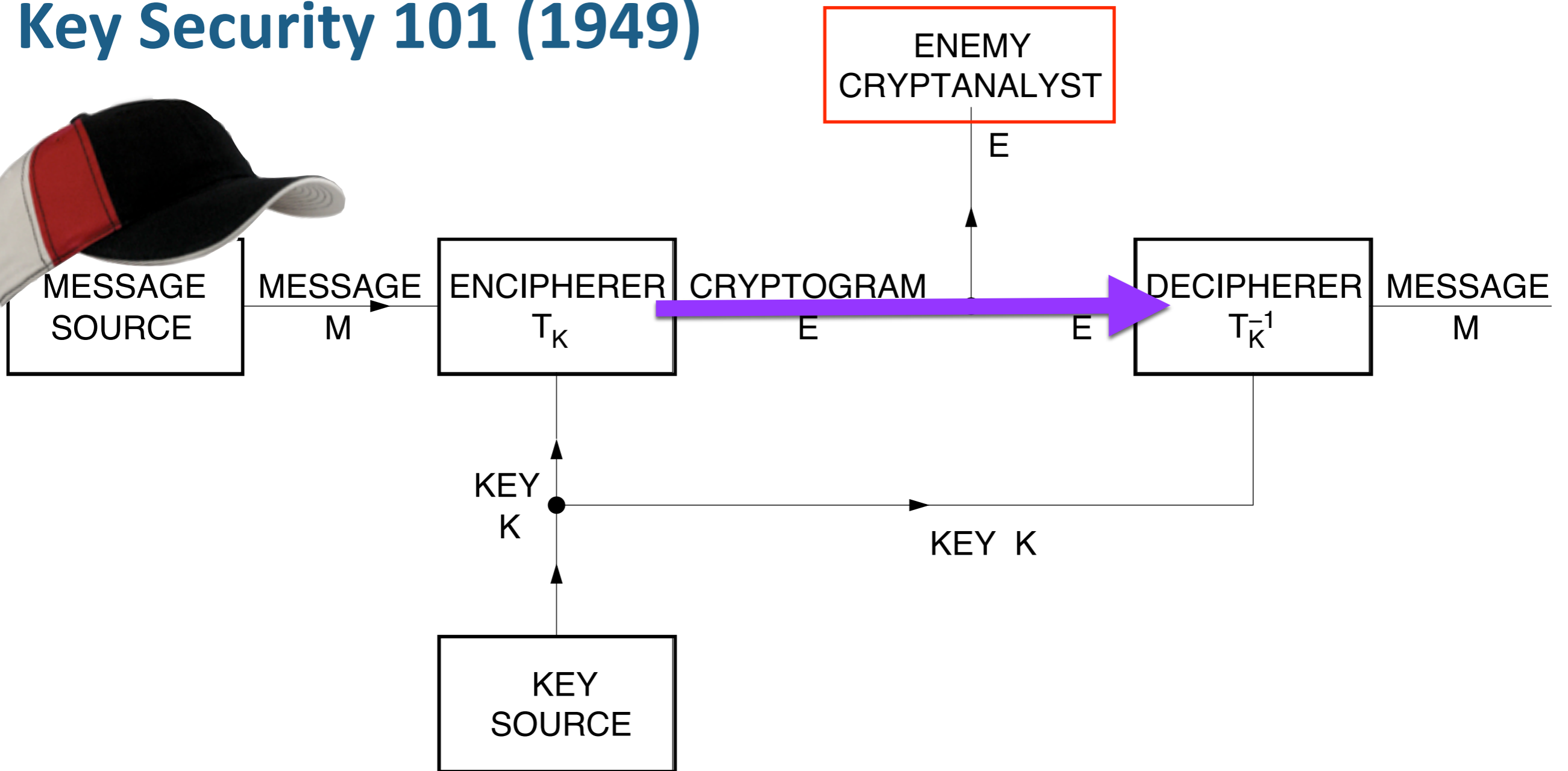
Point-to-Point Symmetric Key Security 101 (1949)



➡ Claude E. Shannon's classical 1949 threat model



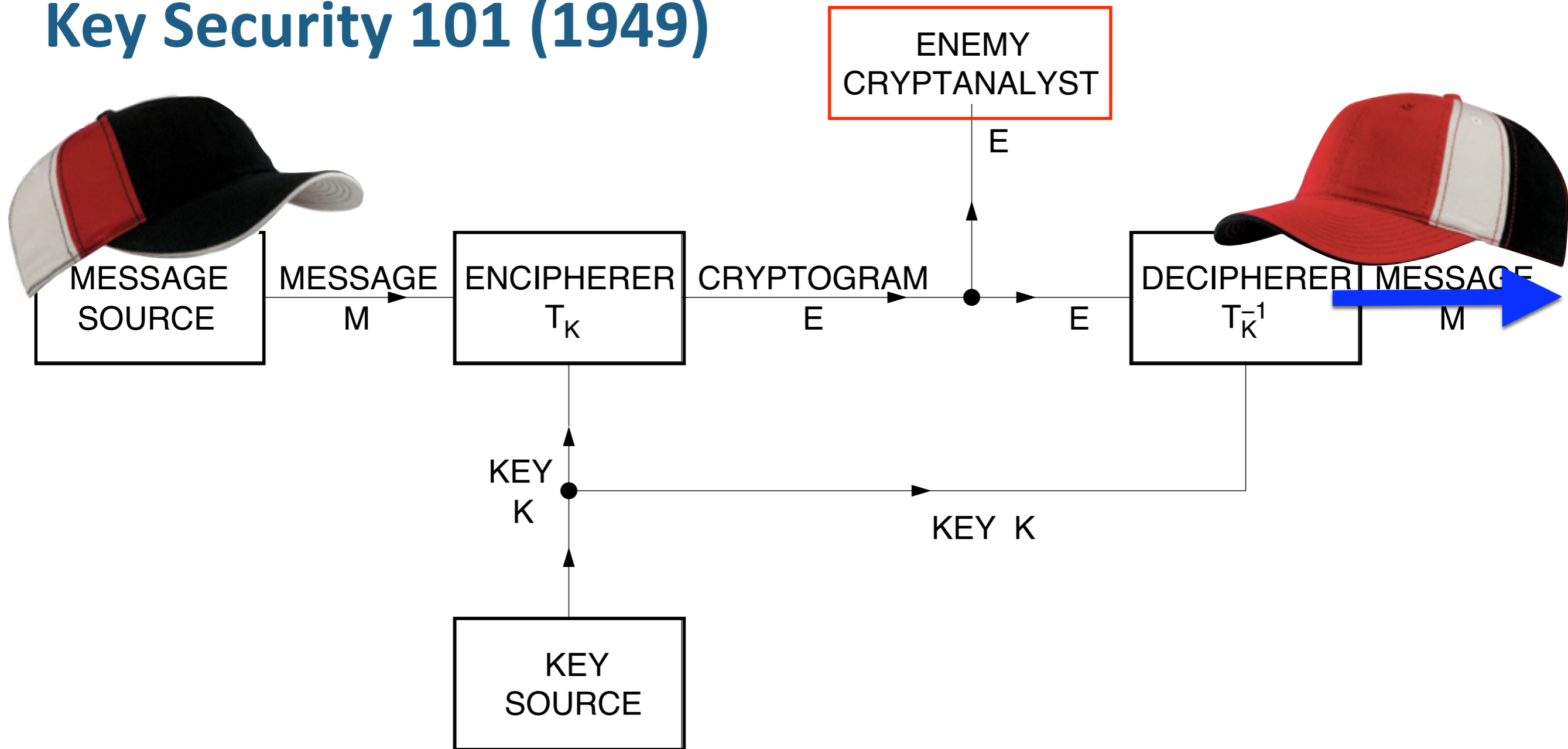
Point-to-Point Symmetric Key Security 101 (1949)



➡ Claude E. Shannon's classical 1949 threat model



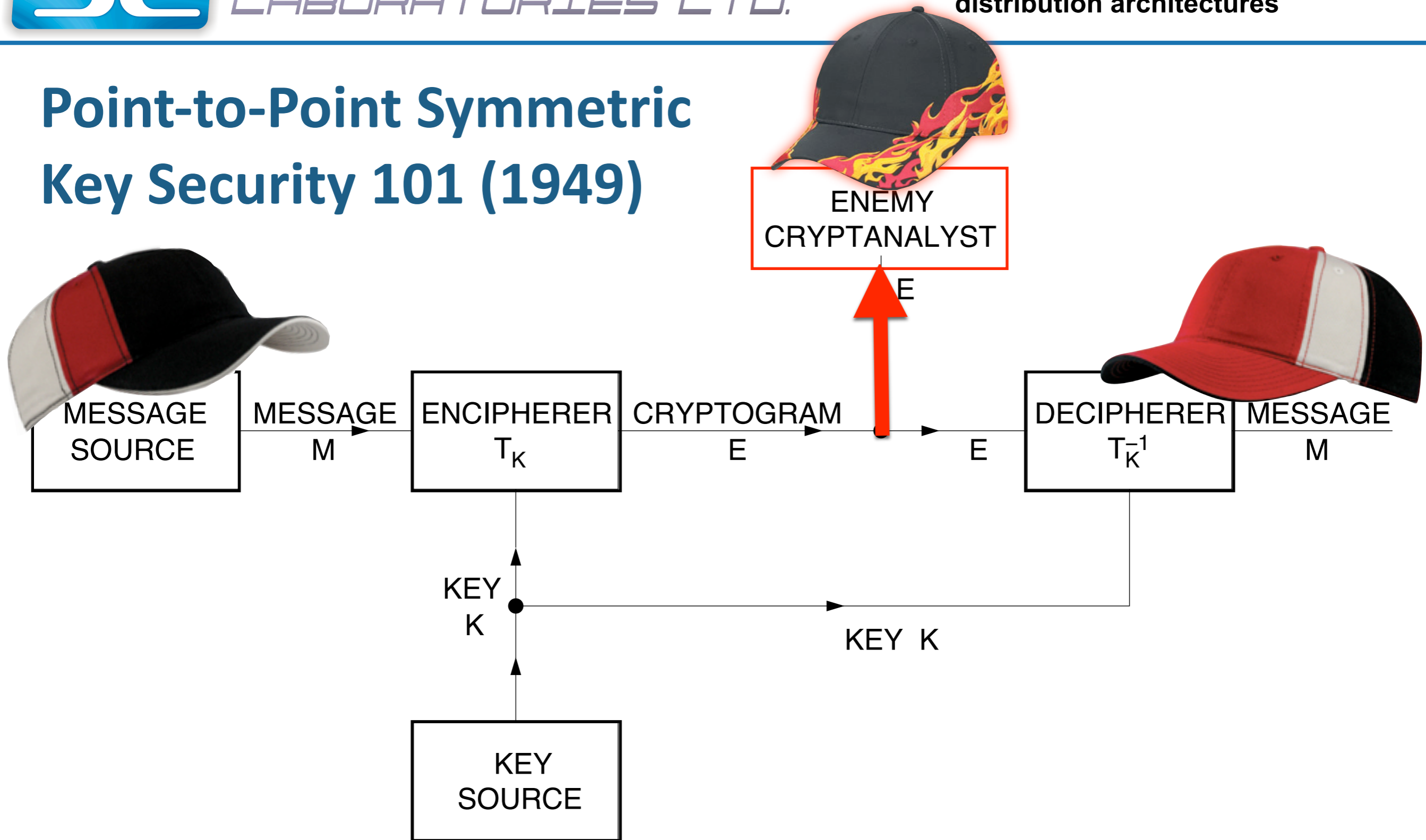
Point-to-Point Symmetric Key Security 101 (1949)



➡ Claude E. Shannon's classical 1949 threat model



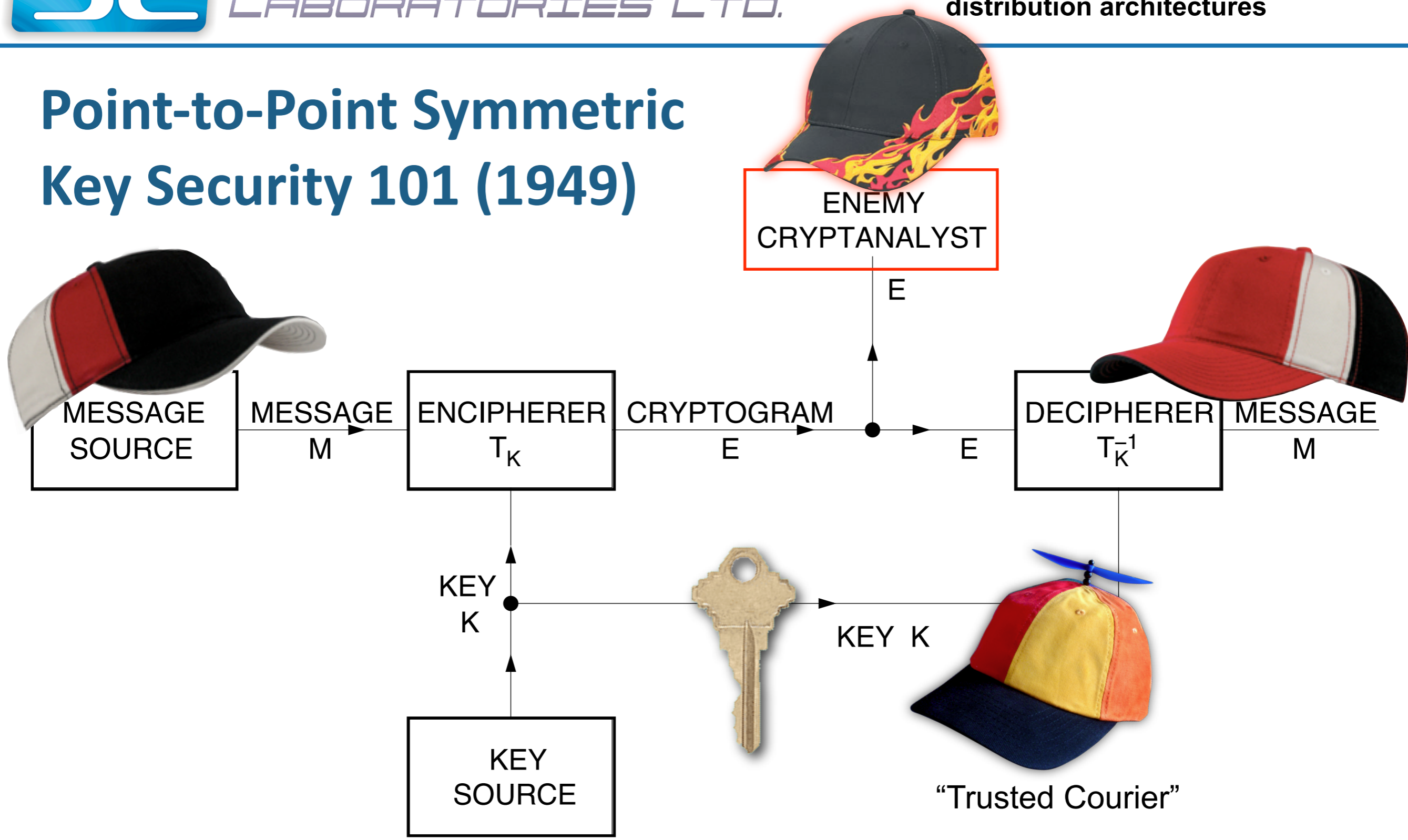
Point-to-Point Symmetric Key Security 101 (1949)



Claude E. Shannon's classical 1949 threat model



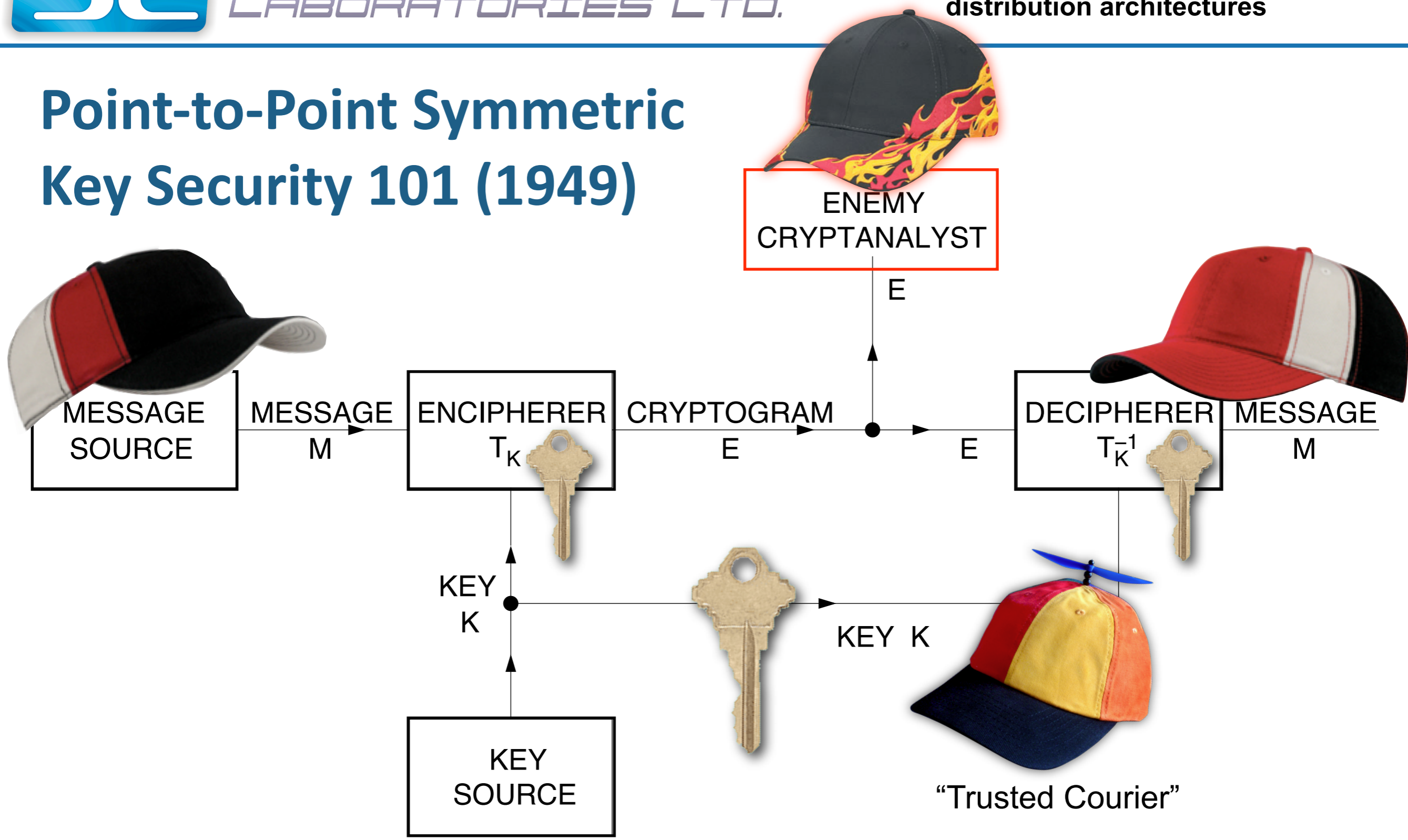
Point-to-Point Symmetric Key Security 101 (1949)



➡ Claude E. Shannon's classical 1949 threat model



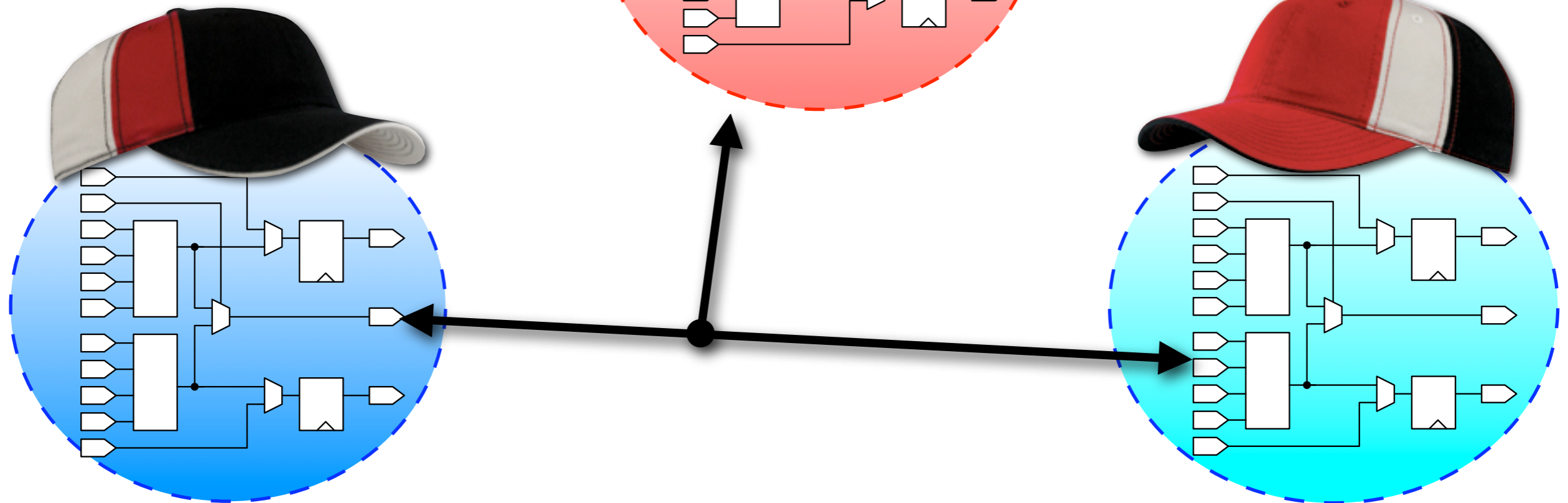
Point-to-Point Symmetric Key Security 101 (1949)



➡ Claude E. Shannon's classical 1949 threat model

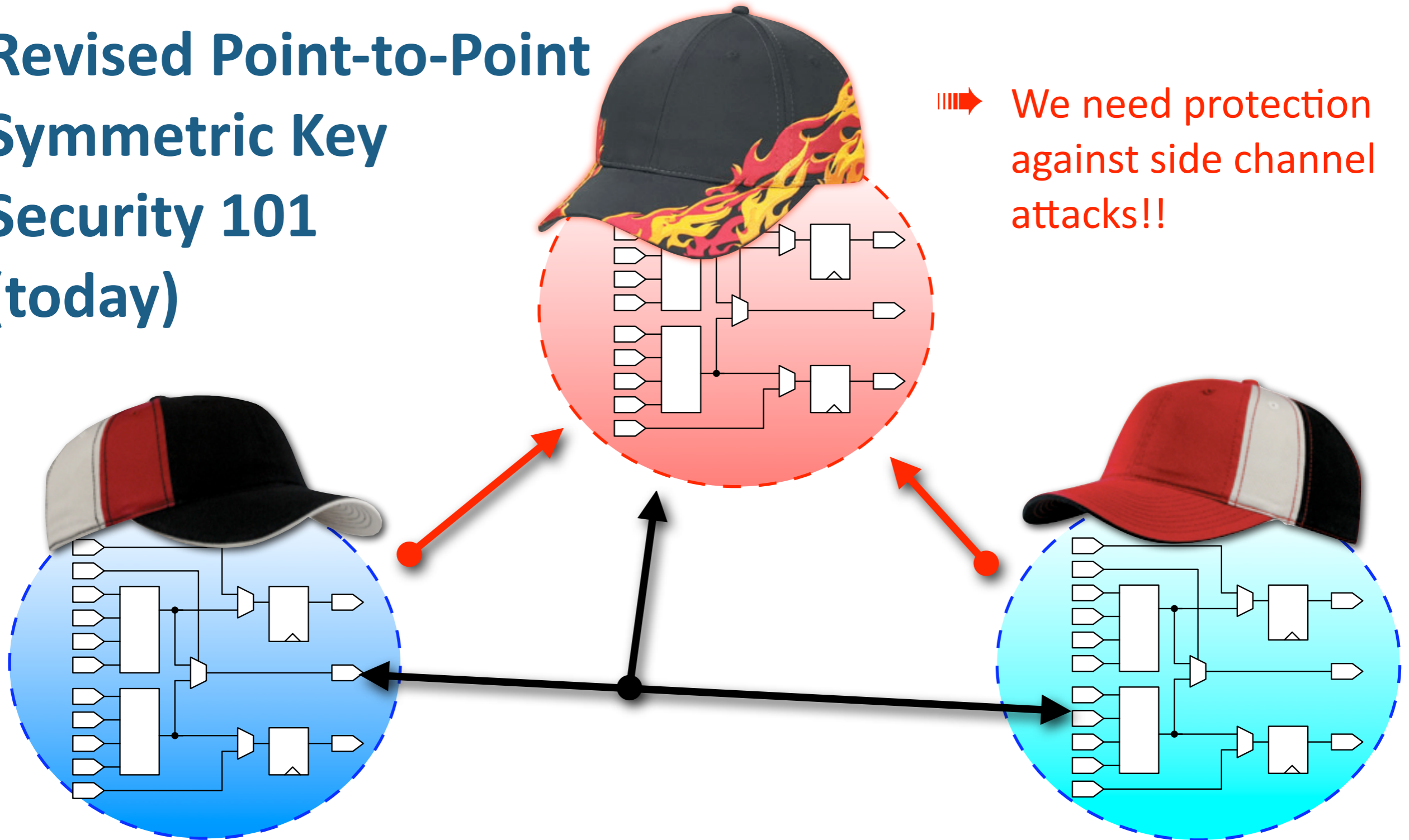


Revised Point-to-Point Symmetric Key Security 101 (today)





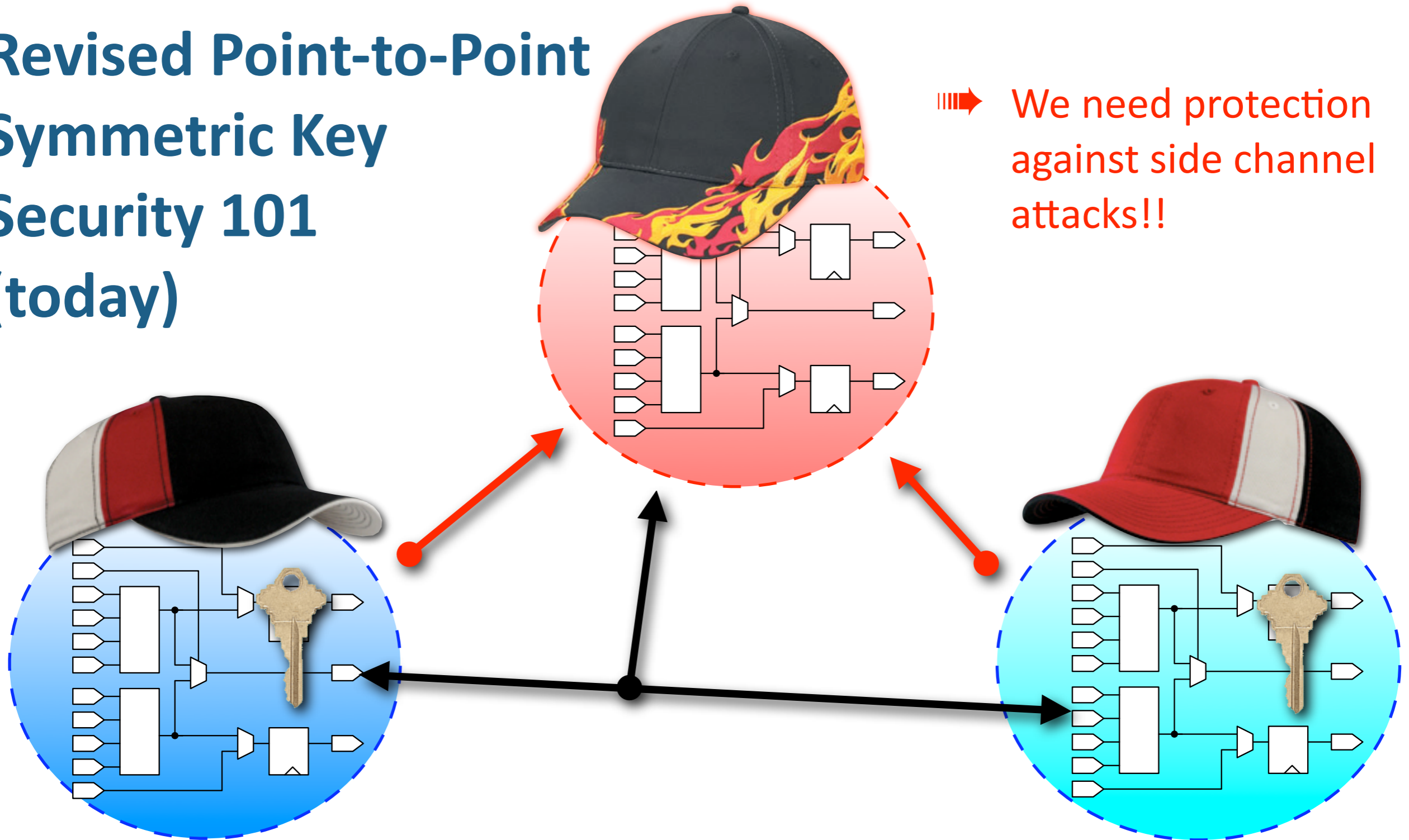
Revised Point-to-Point Symmetric Key Security 101 (today)



➡ We need protection against side channel attacks!!



Revised Point-to-Point Symmetric Key Security 101 (today)





Device boundaries are soft unless hardened



Brian SNOW:

former Technical Director of the
Information **Assurance** Directorate of the
United States National Security Agency



Device boundaries are soft unless hardened



“We Need Assurance!”

Brian SNOW:

former Technical Director of the
Information **Assurance** Directorate of the
United States National Security Agency



Use HSM



“Consider the use of smart cards, smart badges, or other hardware tokens for especially critical functions.

Although more costly than software, when properly implemented **the assurance gain is great.**”

Brian SNOW:

former Technical Director of the Information **Assurance** Directorate of the United States National Security Agency



Hardware Security Modules



Hardware Security Modules



- Hardware security modules are a class of device that deliberately harden the physical boundary around electronic circuits

Hardware Security Modules



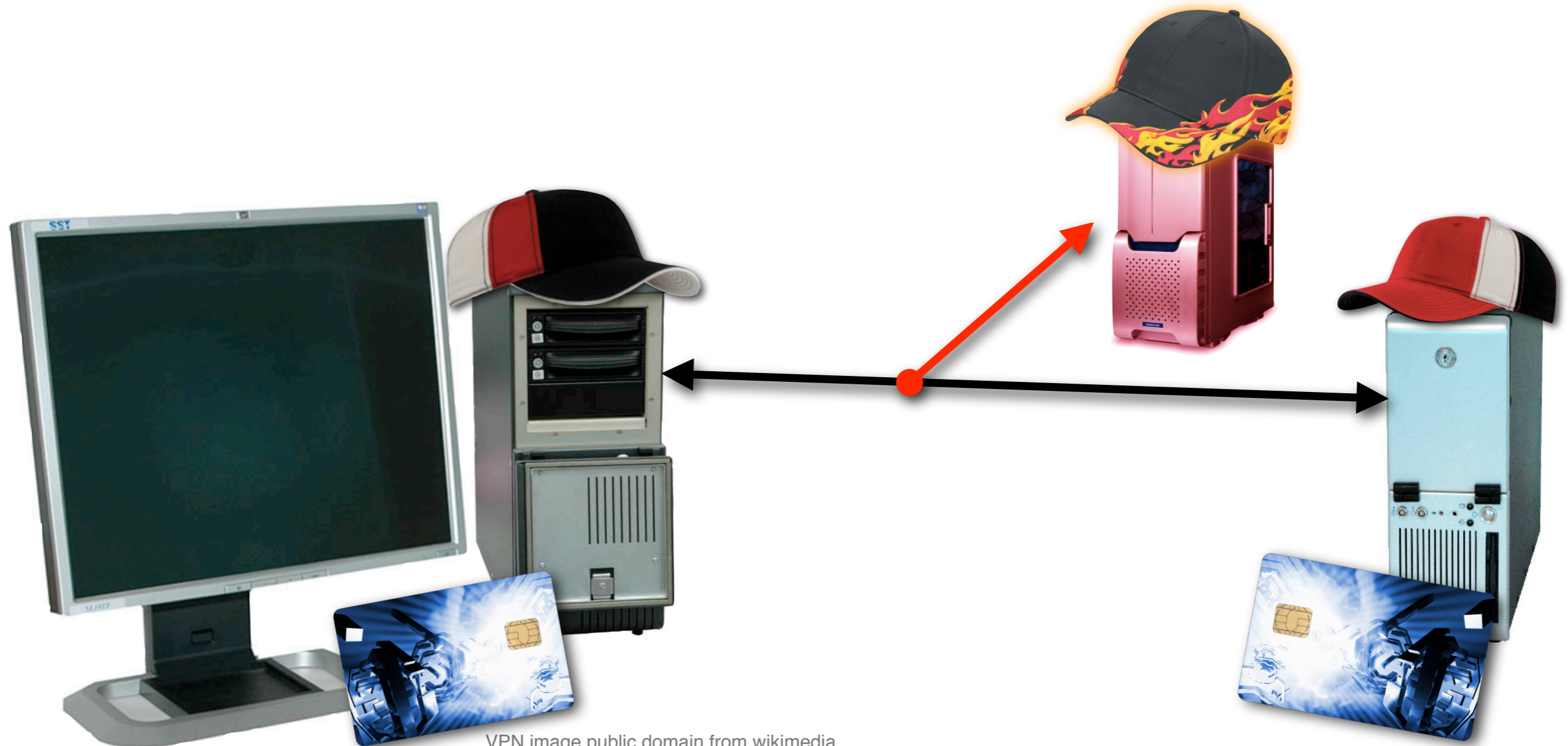
- Hardware security modules are a class of device that deliberately harden the physical boundary around electronic circuits
- Designed to physically isolate the circuit (tamper evidence)
- Sometimes have “memory self-destruct” features on tamper detection
- Varying degrees of protection against side-channel attacks

TEMPEST

- Electromagnetic shielding enclosures (ESE) are another physical method to create hard boundaries between devices, users, organisations
- Designed to mitigate side-channel attacks
- ESE technologies are mature and available commercially



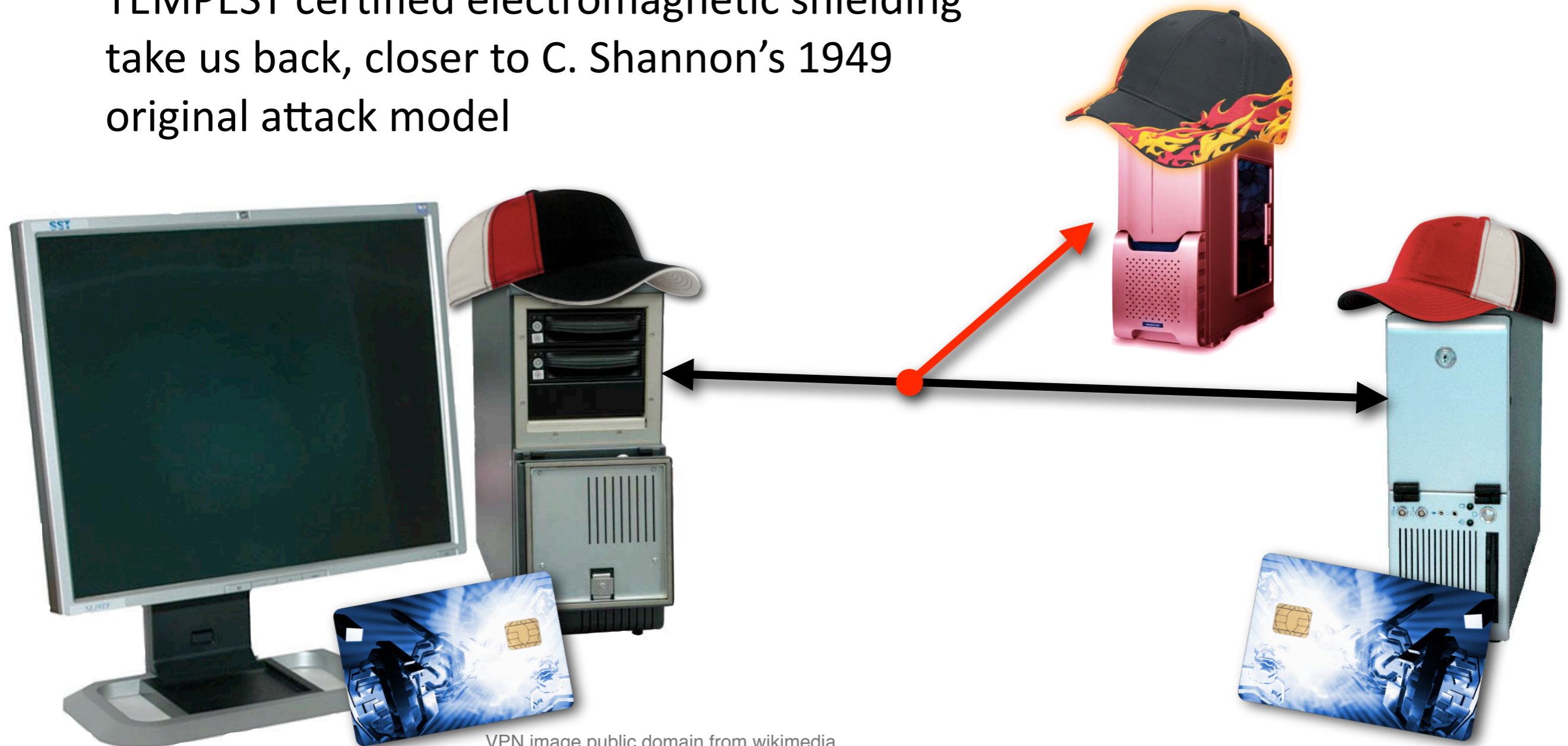
Secured operating environment



VPN image public domain from wikimedia.
Image of Computers © Secure Systems & Technologies Ltd. Used with permission.

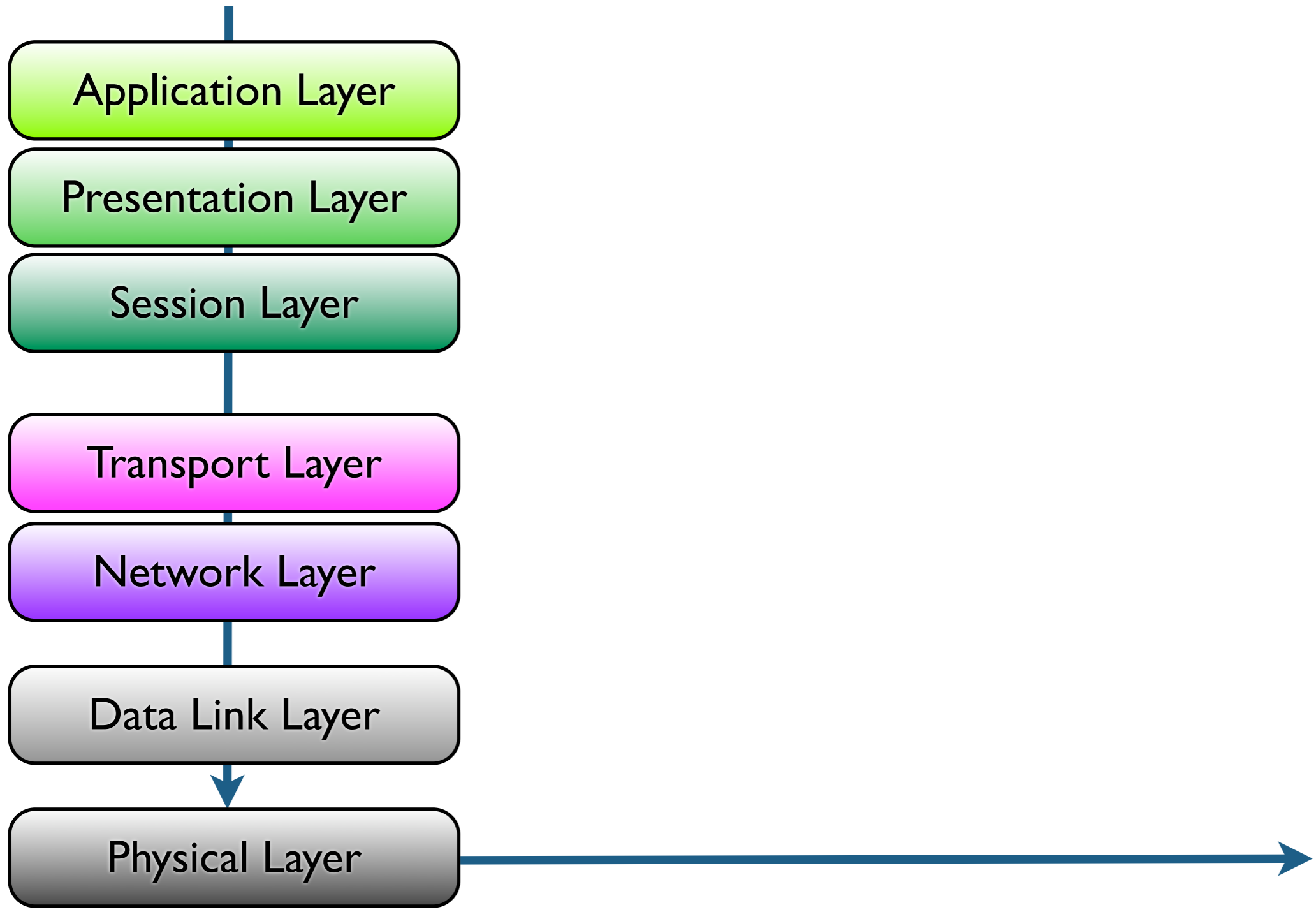
Secured operating environment

- Hardware counter-measures such as HSM and TEMPEST certified electromagnetic shielding take us back, closer to C. Shannon's 1949 original attack model

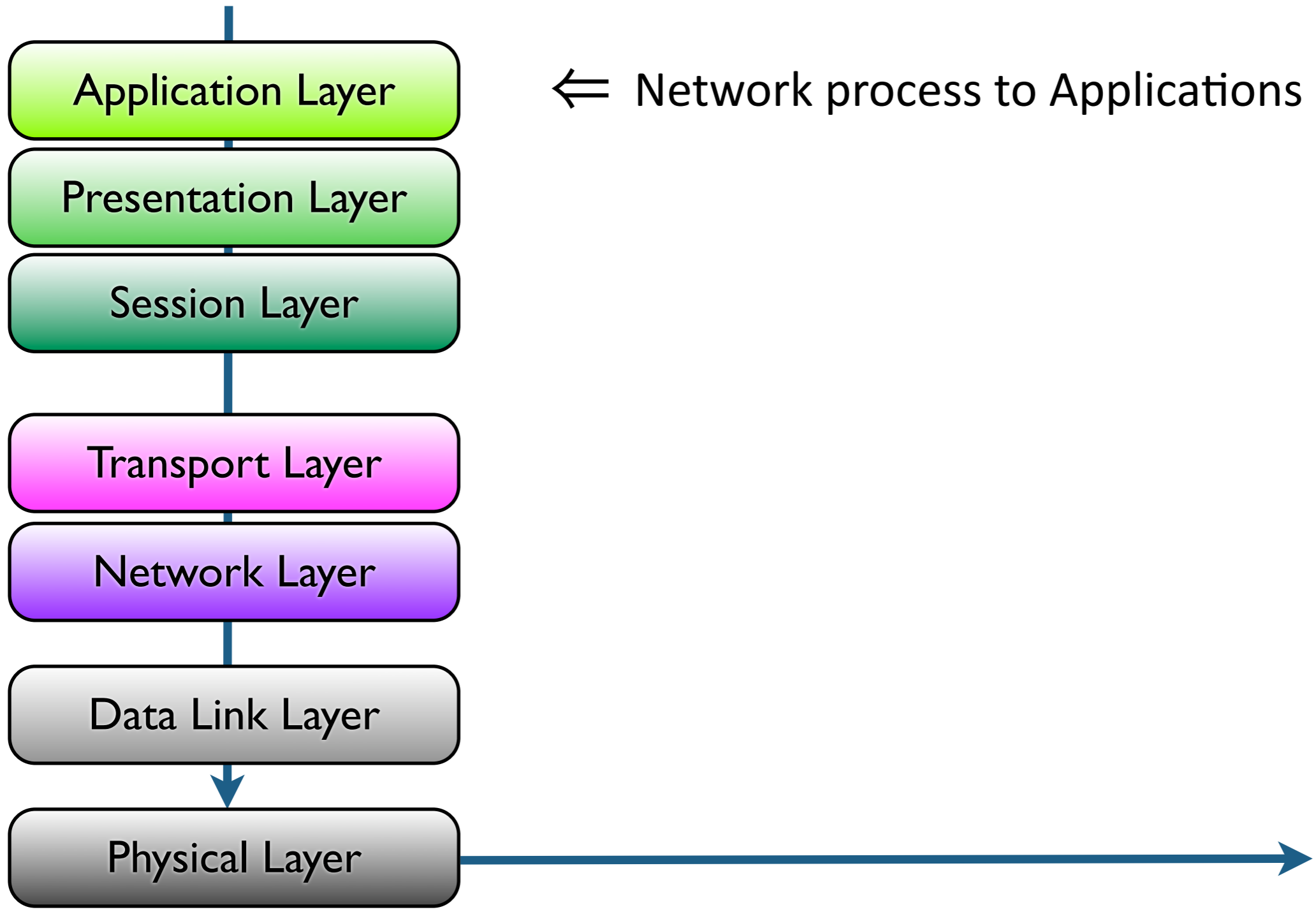


VPN image public domain from wikimedia.
Image of Computers © Secure Systems & Technologies Ltd. Used with permission.

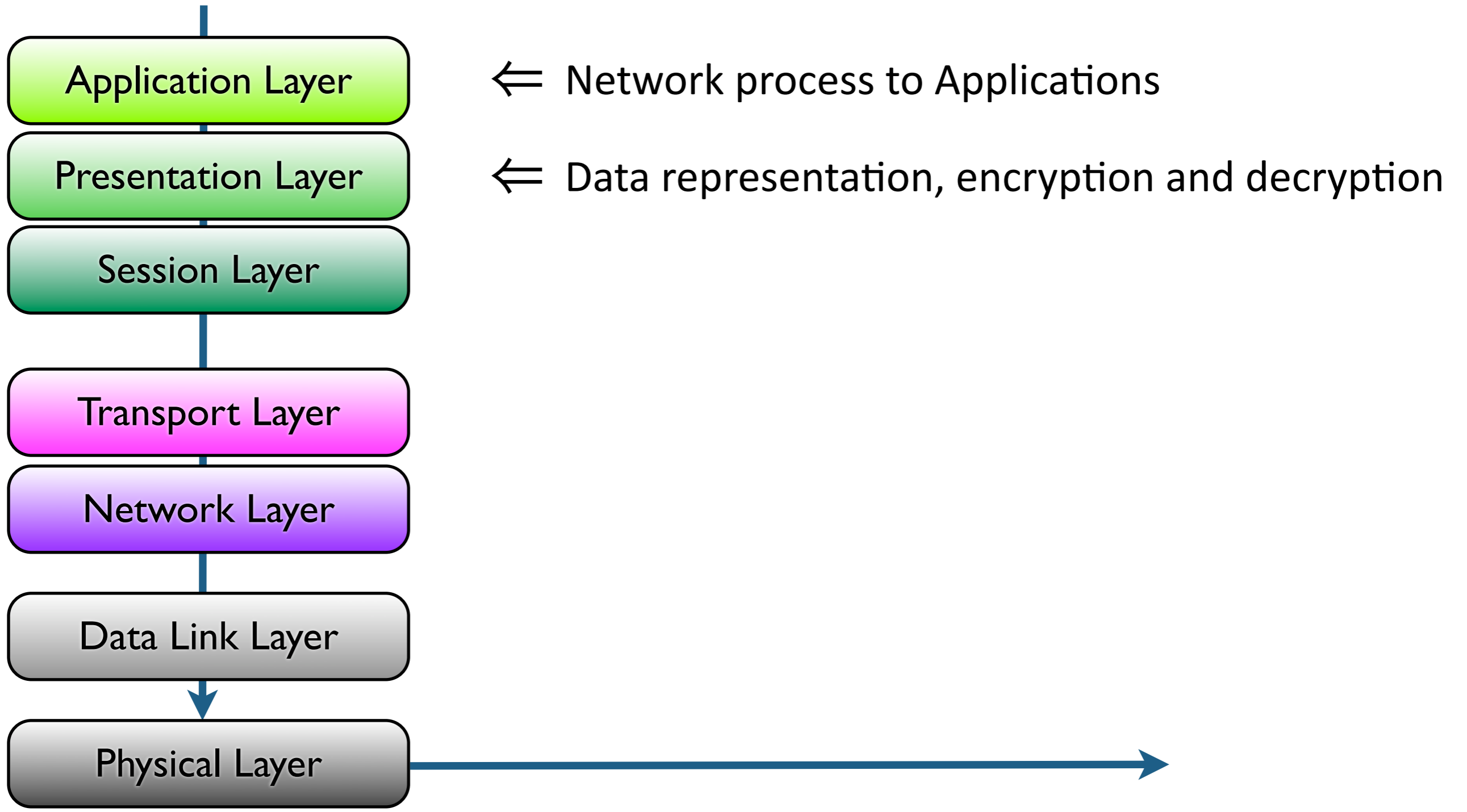
OSI 7 Layer Model



OSI 7 Layer Model

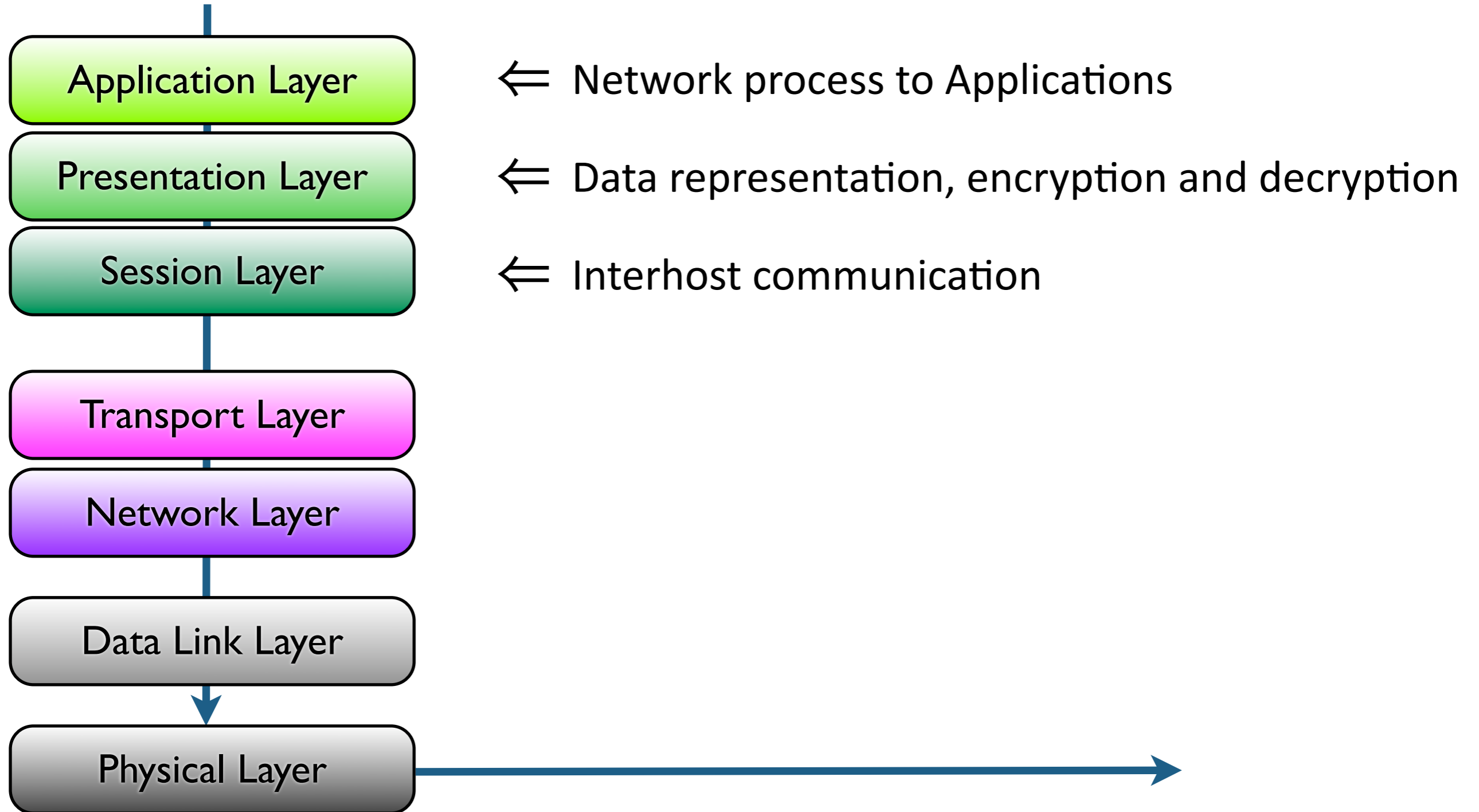


OSI 7 Layer Model



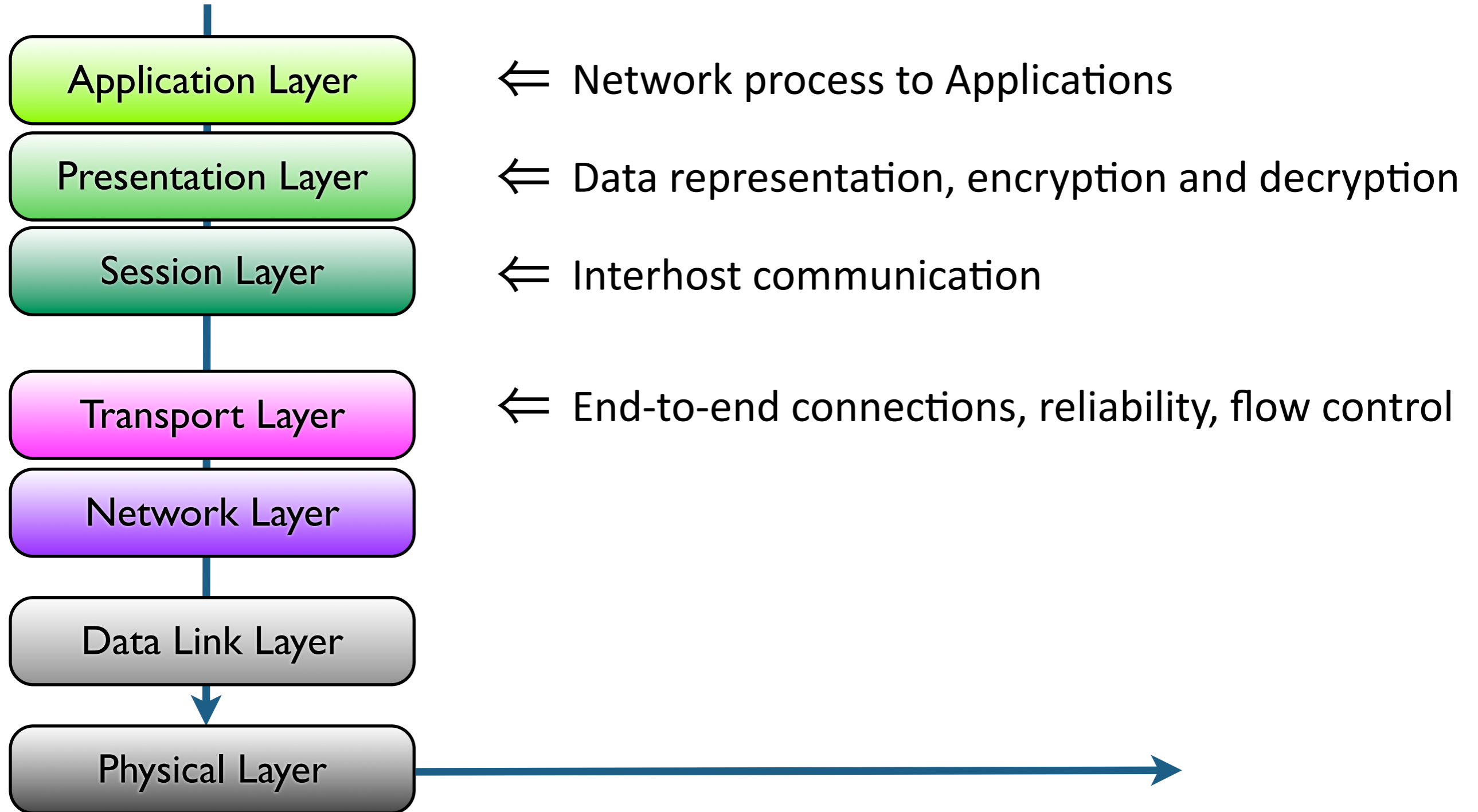


OSI 7 Layer Model



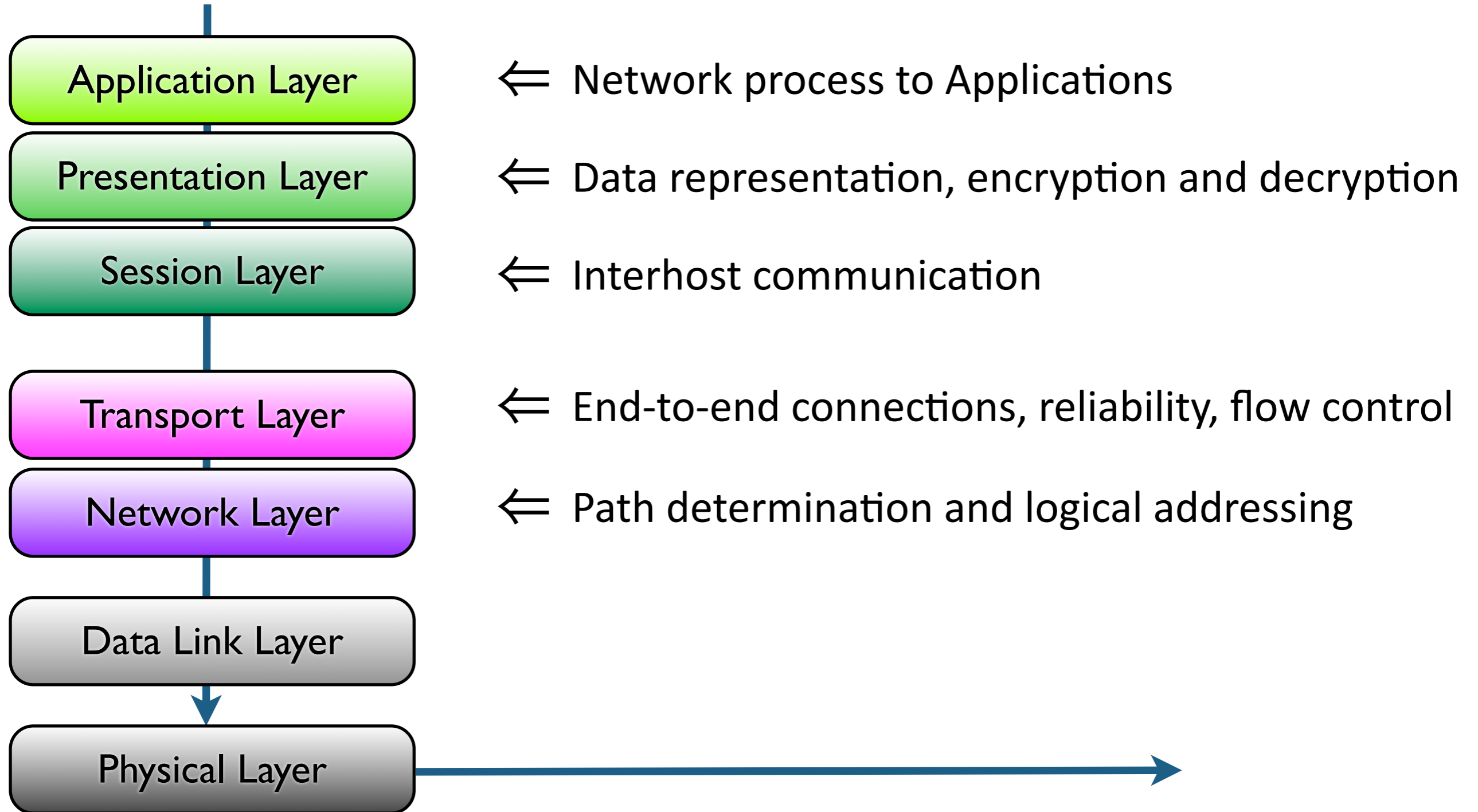


OSI 7 Layer Model



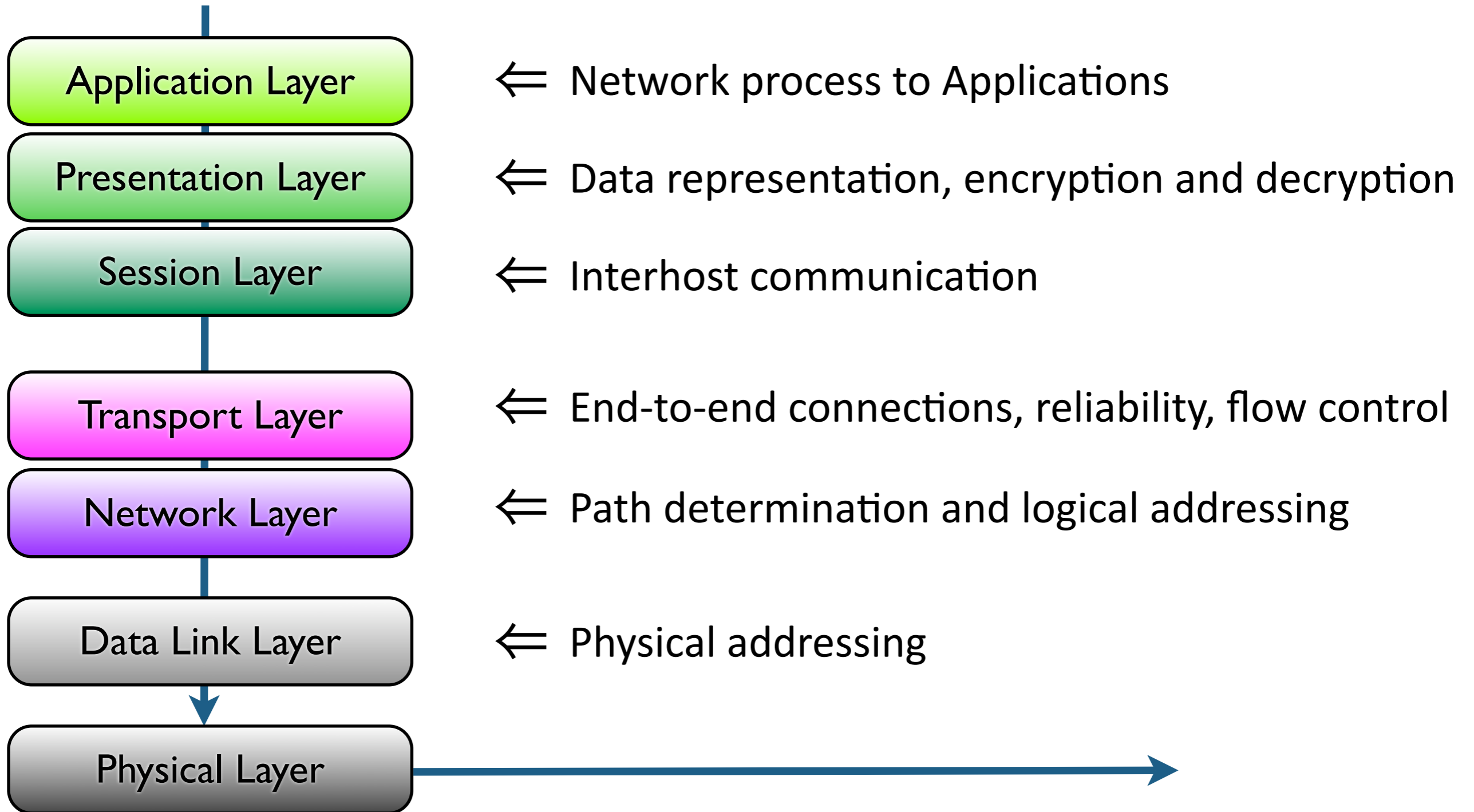


OSI 7 Layer Model

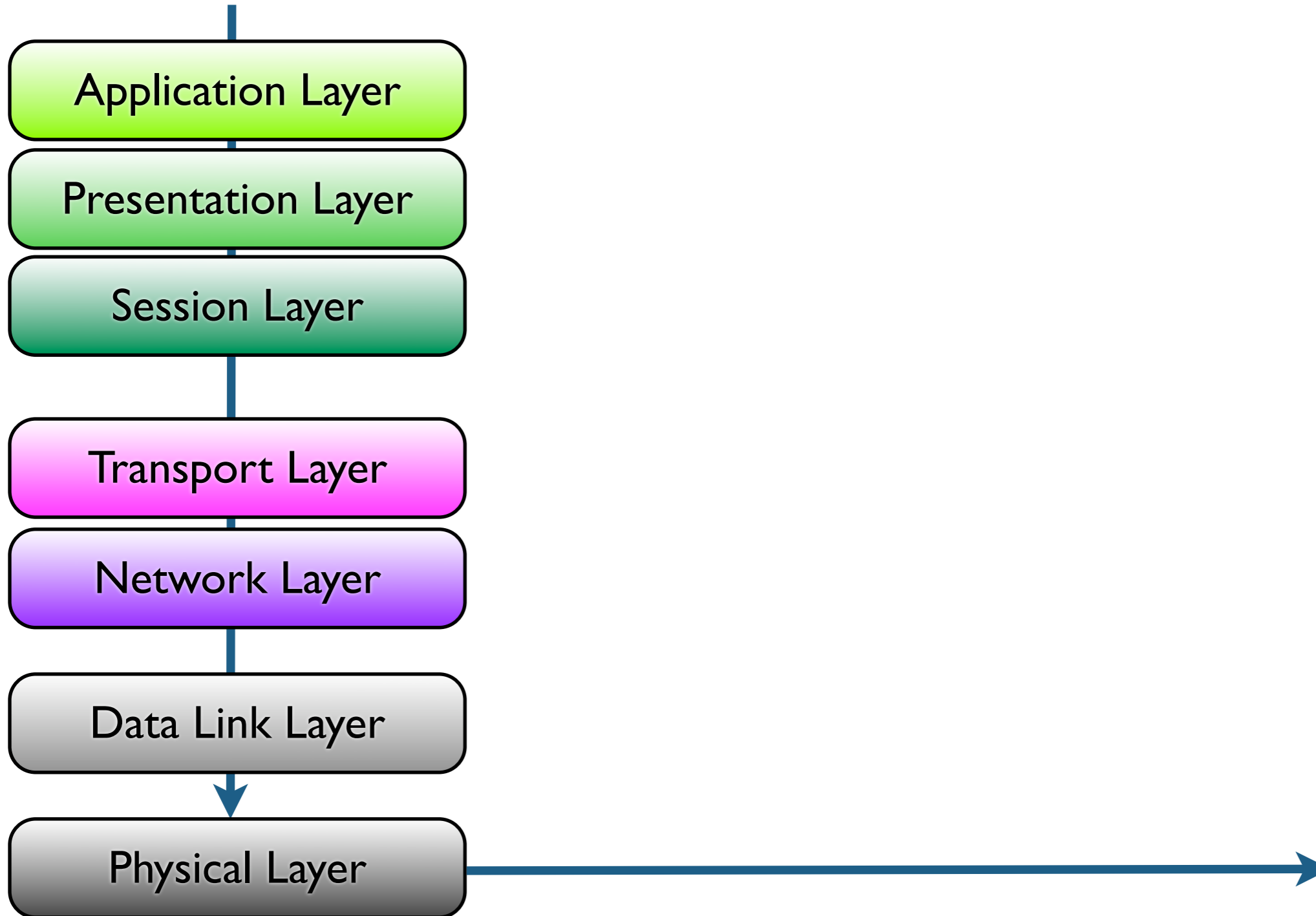




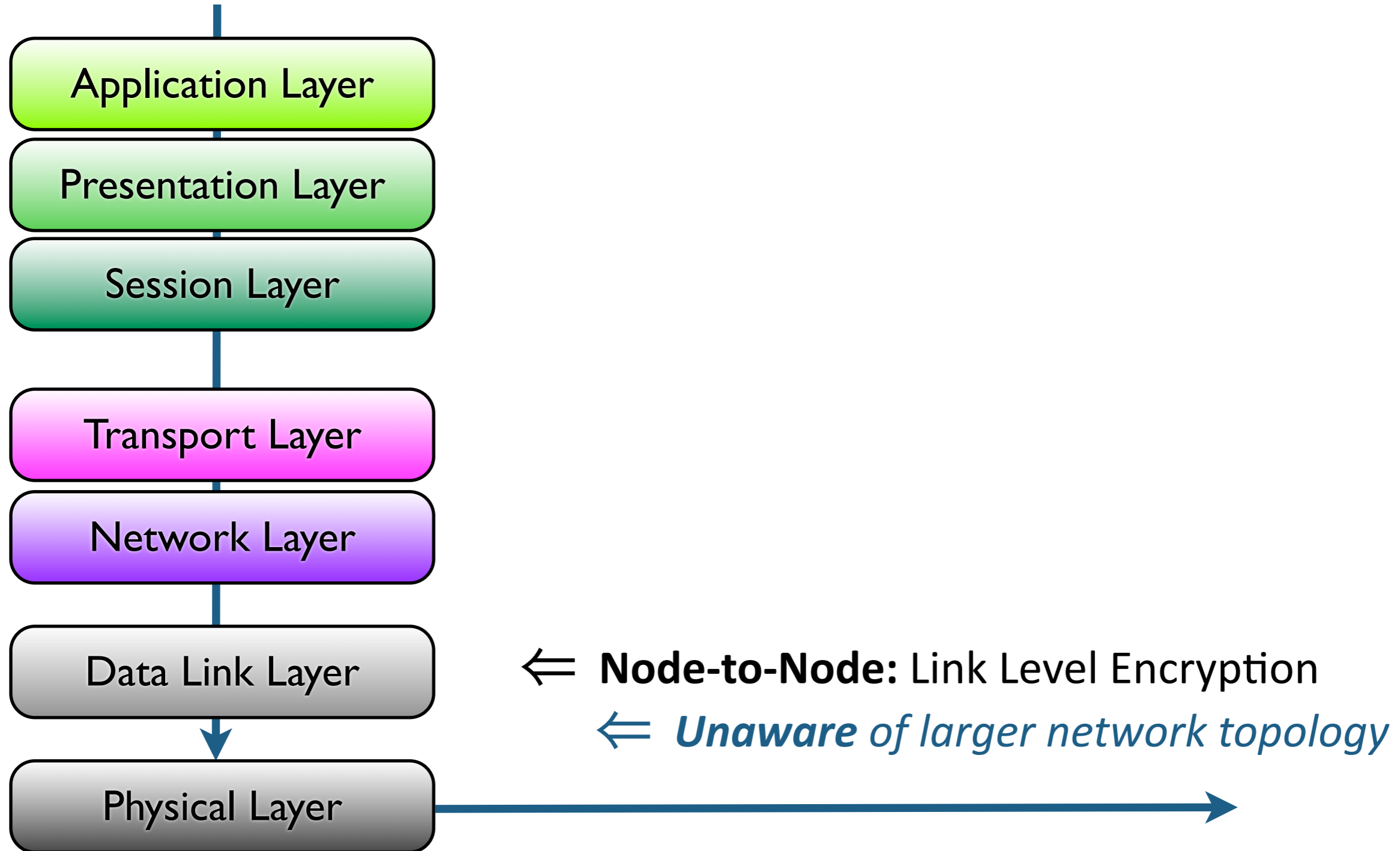
OSI 7 Layer Model



Securing networks: so many layers to choose from

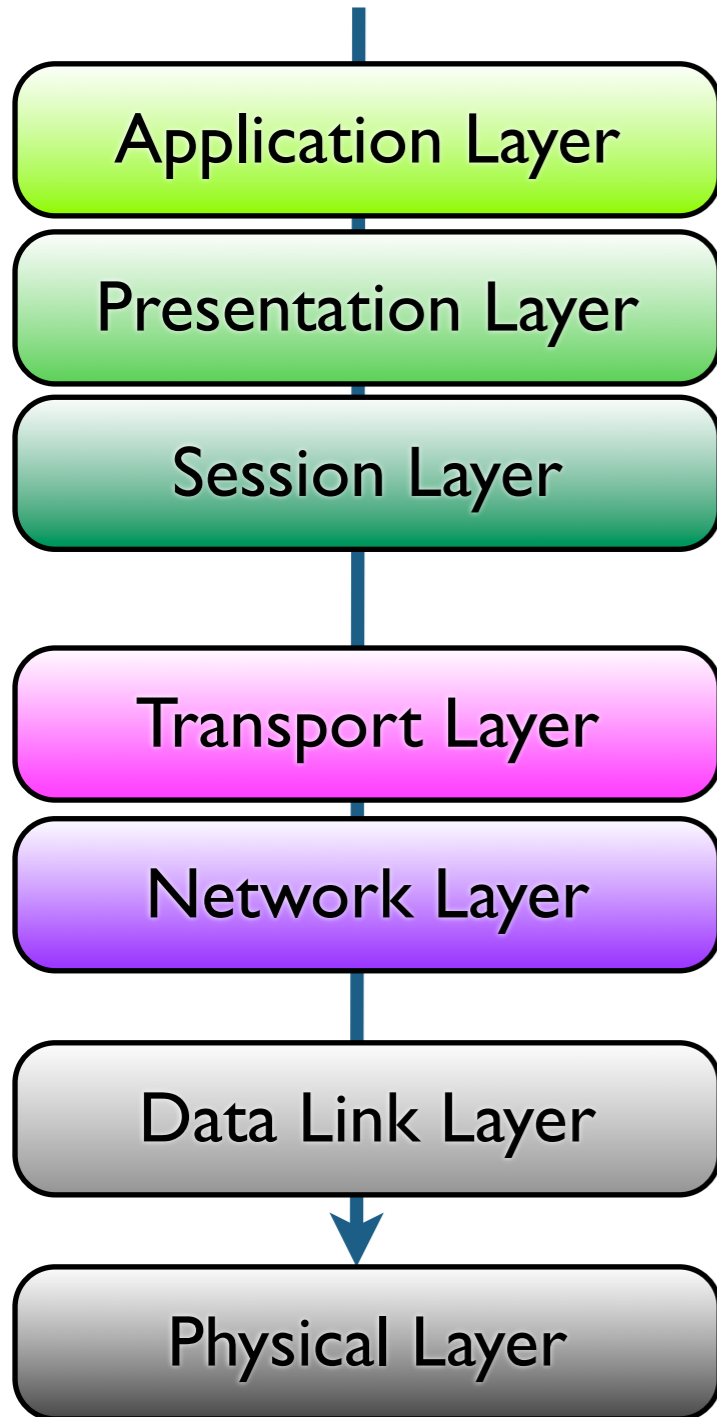


Securing networks: so many layers to choose from





Securing networks: so many layers to choose from



⇐ **End-to-End:** (Application to Application)

⇐ SSL/TLS

⇐ Application specific (Home Brew)

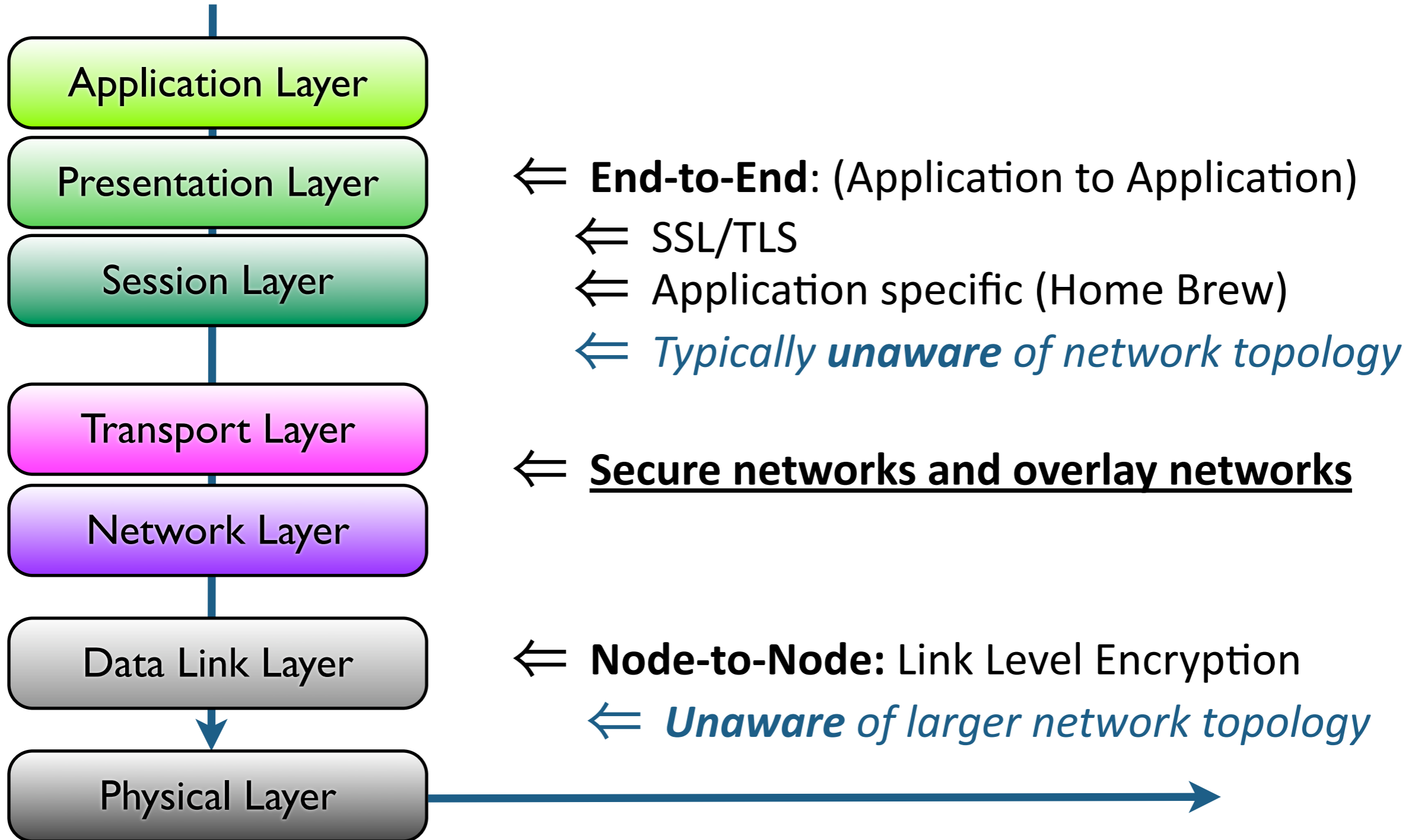
⇐ *Typically unaware of network topology*

⇐ **Node-to-Node:** Link Level Encryption

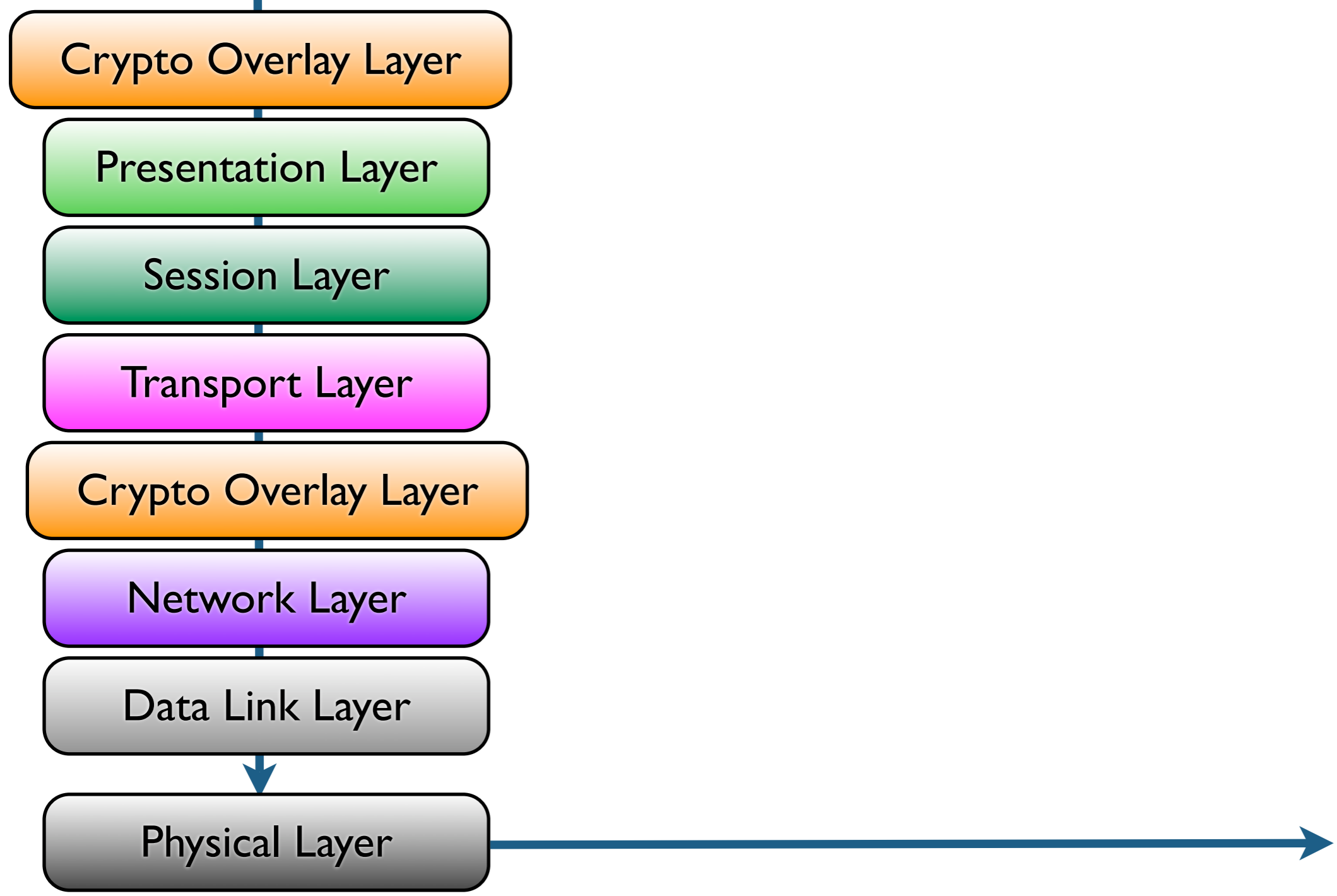
⇐ *Unaware of larger network topology*



Securing networks: so many layers to choose from

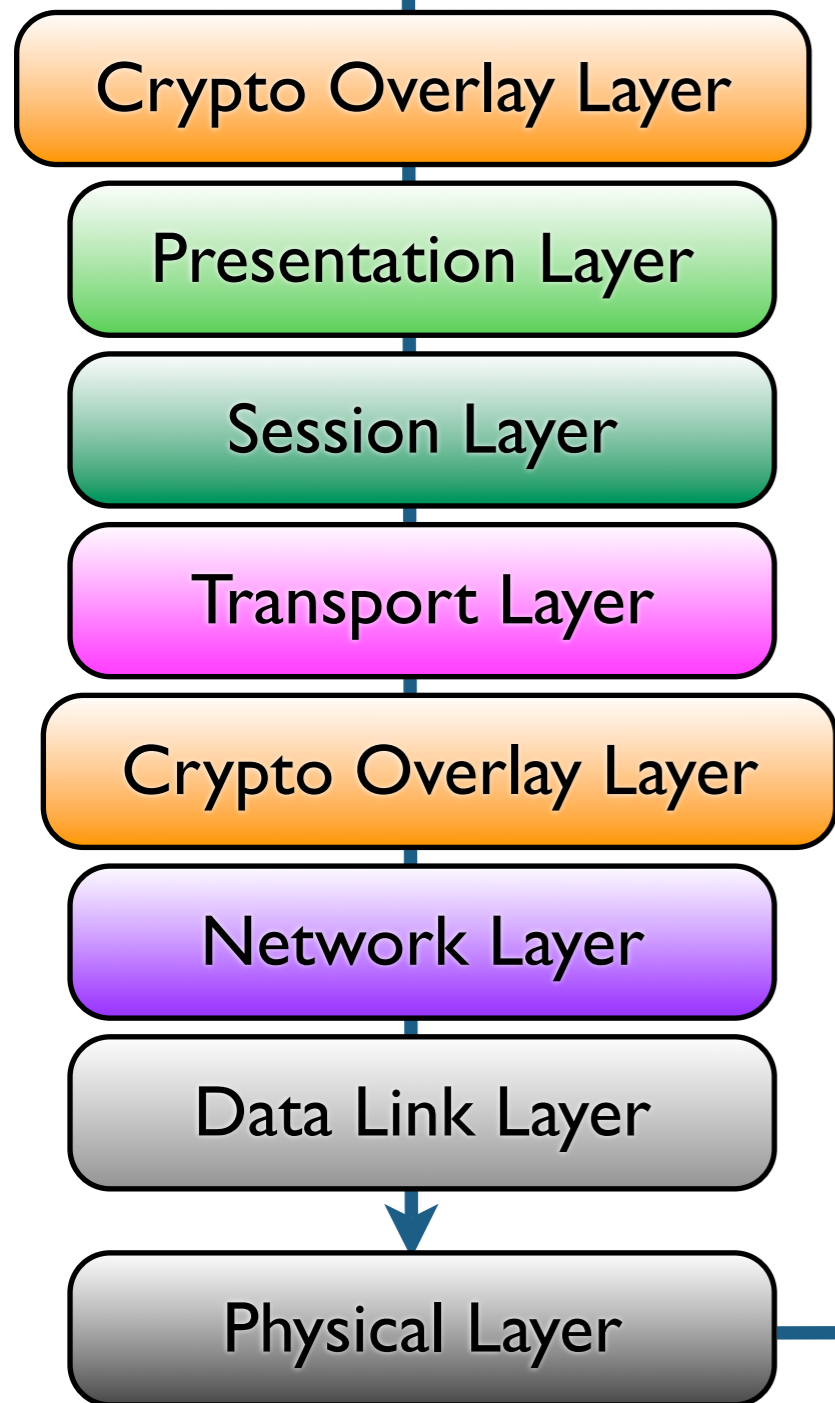


Overlay Networks come in various flavours





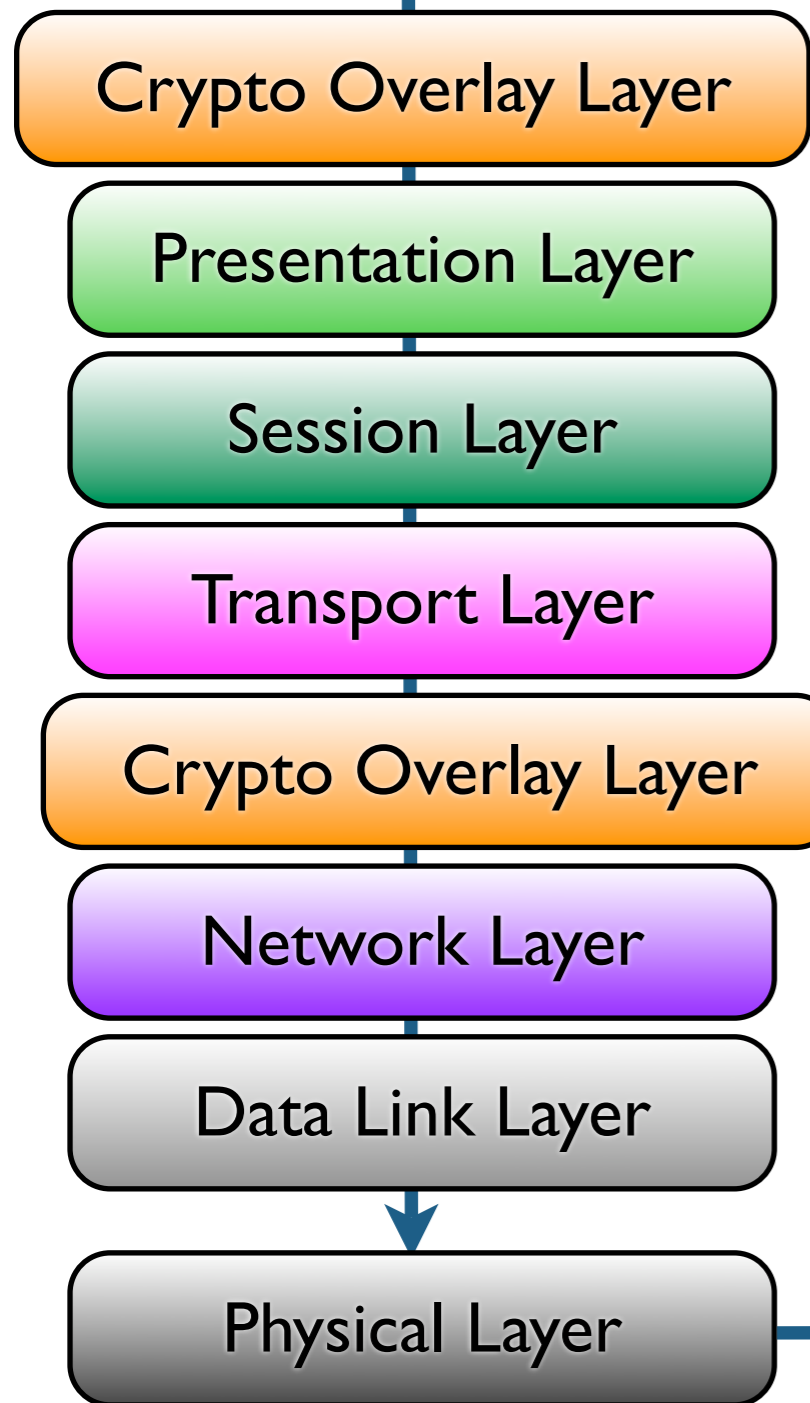
Overlay Networks come in various flavours



- ⇐ *Topology independent of physical network*
- ⇐ *Peer-to-Peer File Sharing*
- ⇐ *The onion router (Anonymity)*
- ⇐ *Key Distribution: Branstad, Diffie-Merkle-Lamport, Kerberos...*



Overlay Networks come in various flavours



- ⇐ *Topology independent of physical network*
 - ⇐ *Peer-to-Peer File Sharing*
 - ⇐ *The onion router (Anonymity)*
 - ⇐ *Key Distribution: Branstad, Diffie-Merkle-Lamport, Kerberos...*

- ⇐ *Topology 1:1 with physical network*
 - ⇐ *Mobile ad-hoc mesh networks*
 - ⇐ *(Military) sensor networks*
 - ⇐ ***Quantum key distribution networks***



QKD Research Agenda

Using Quantum Cryptography to Distribute Keys

PART 1: Point-to-Point

Image: (c) Austrian Research Centers

QKD: Stopping Hackers



Development of a Global Network for Secure
Communication based on Quantum Cryptography



Image: (c) Austrian Research Centers

QKD: Stopping Hackers



Development of a Global Network for Secure
Communication based on Quantum Cryptography



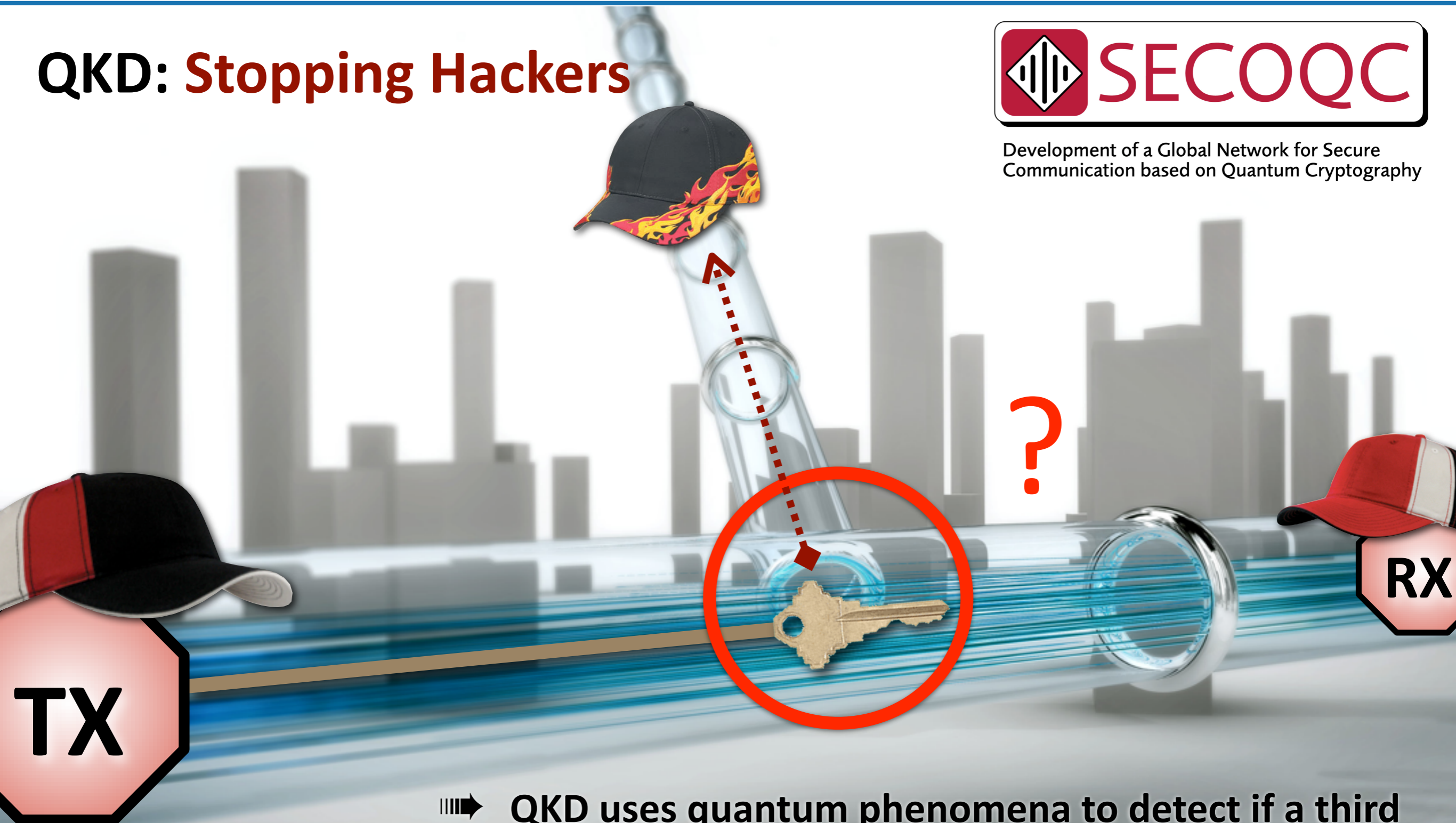
➡ QKD uses quantum phenomena to detect if a third party has intercepted unencrypted key material

Image: (c) Austrian Research Centers

QKD: Stopping Hackers



Development of a Global Network for Secure
Communication based on Quantum Cryptography



- ➡ QKD uses quantum phenomena to detect if a third party has intercepted unencrypted key material

Image: (c) Austrian Research Centers



Image: (c) Austrian Research Centers



Image: (c) Austrian Research Centers



QKD security relies on Pre-Shared Keys!



Image: (c) Austrian Research Centers



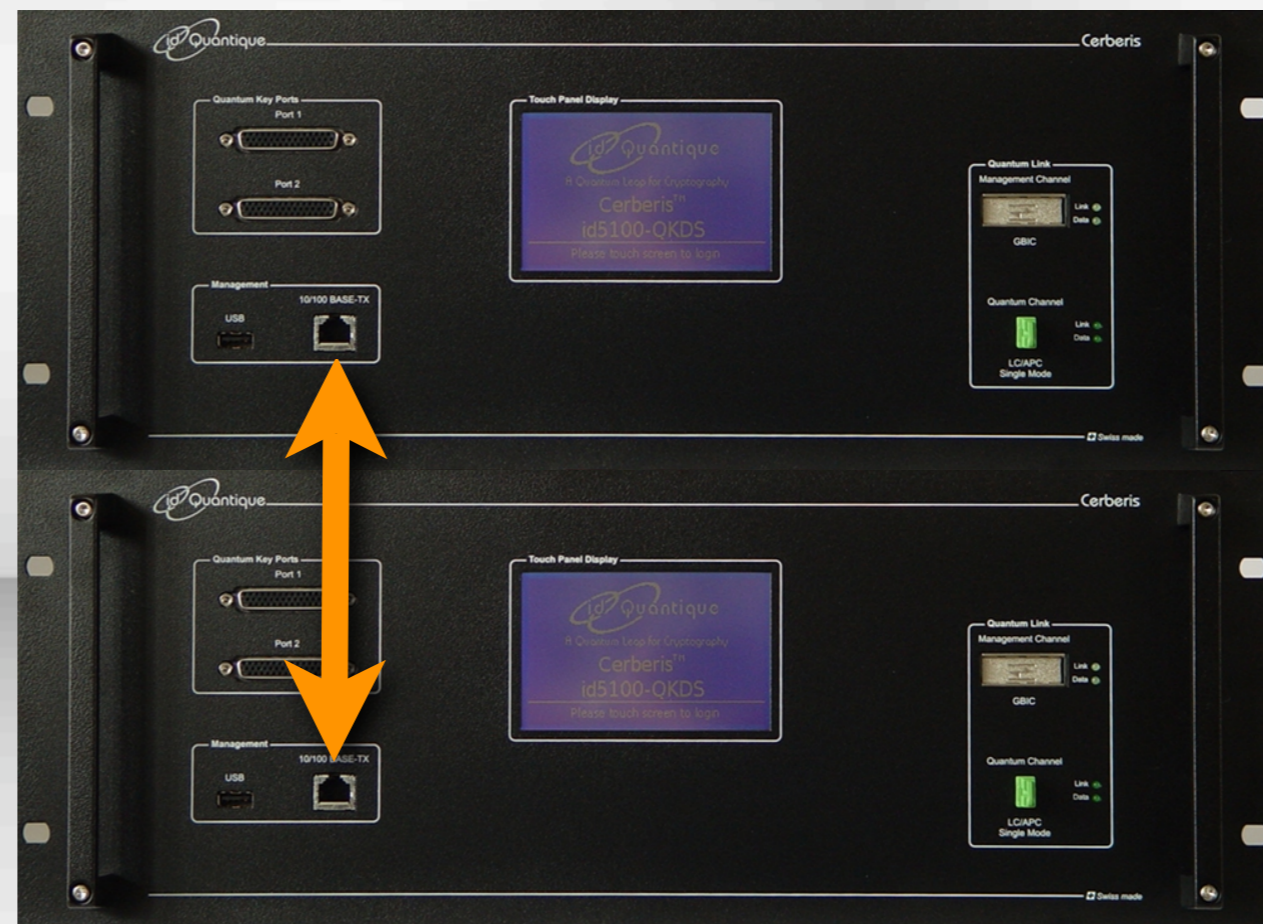
Currently those PSK are exchanged in a closed room



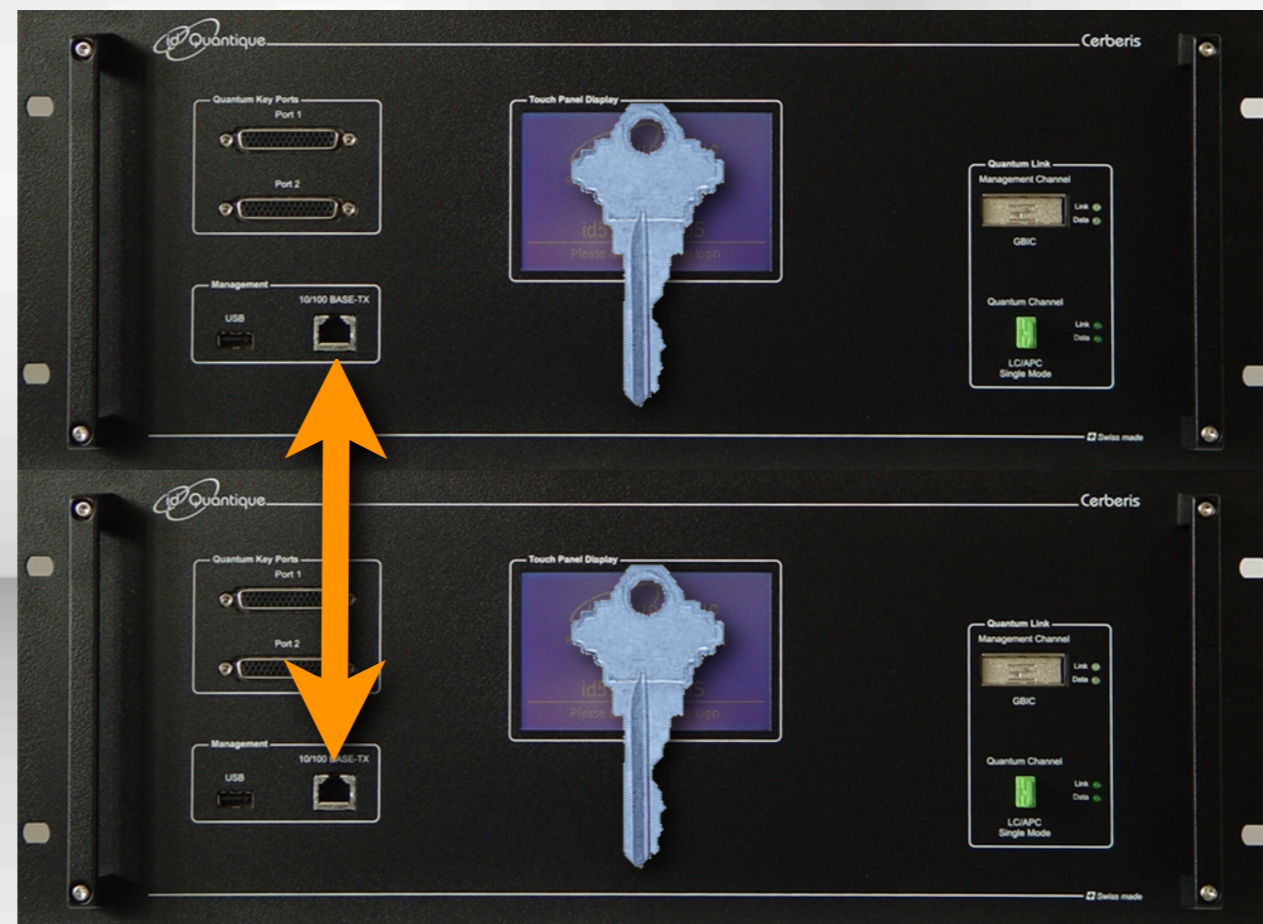
Currently those PSK are exchanged in a closed room



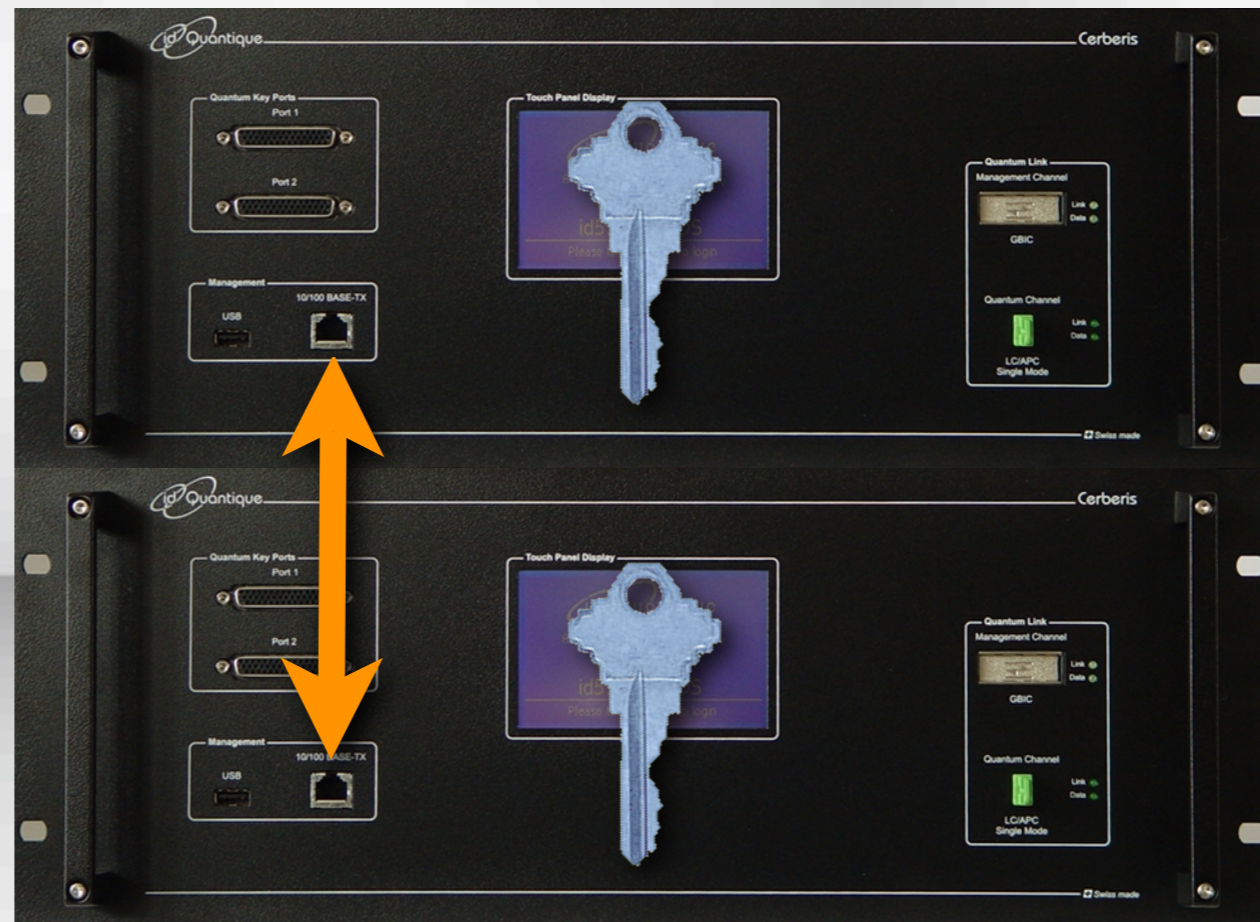
Currently those PSK are exchanged in a closed room



Currently those PSK are exchanged in a closed room

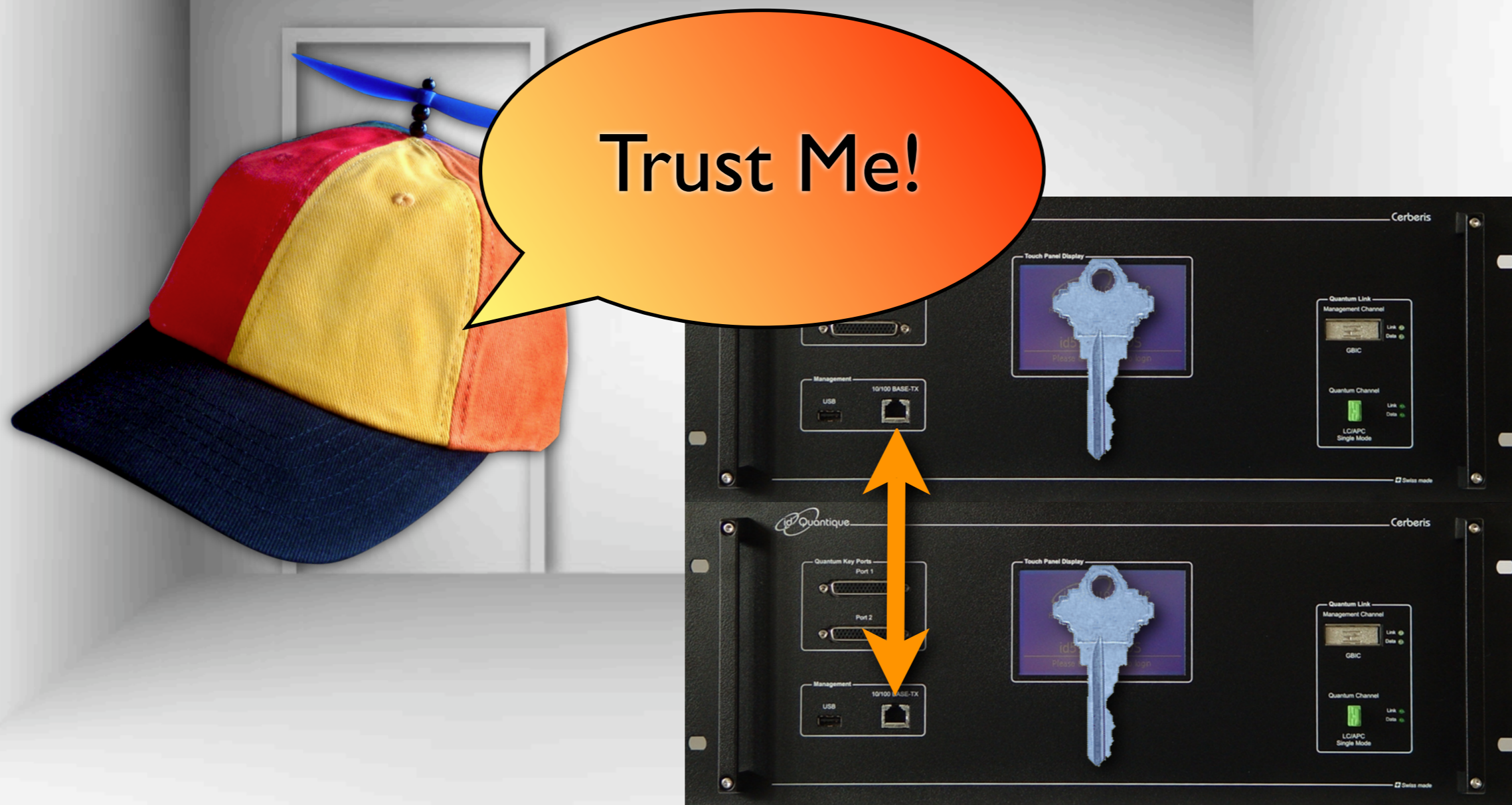


Currently those PSK are exchanged in a closed room



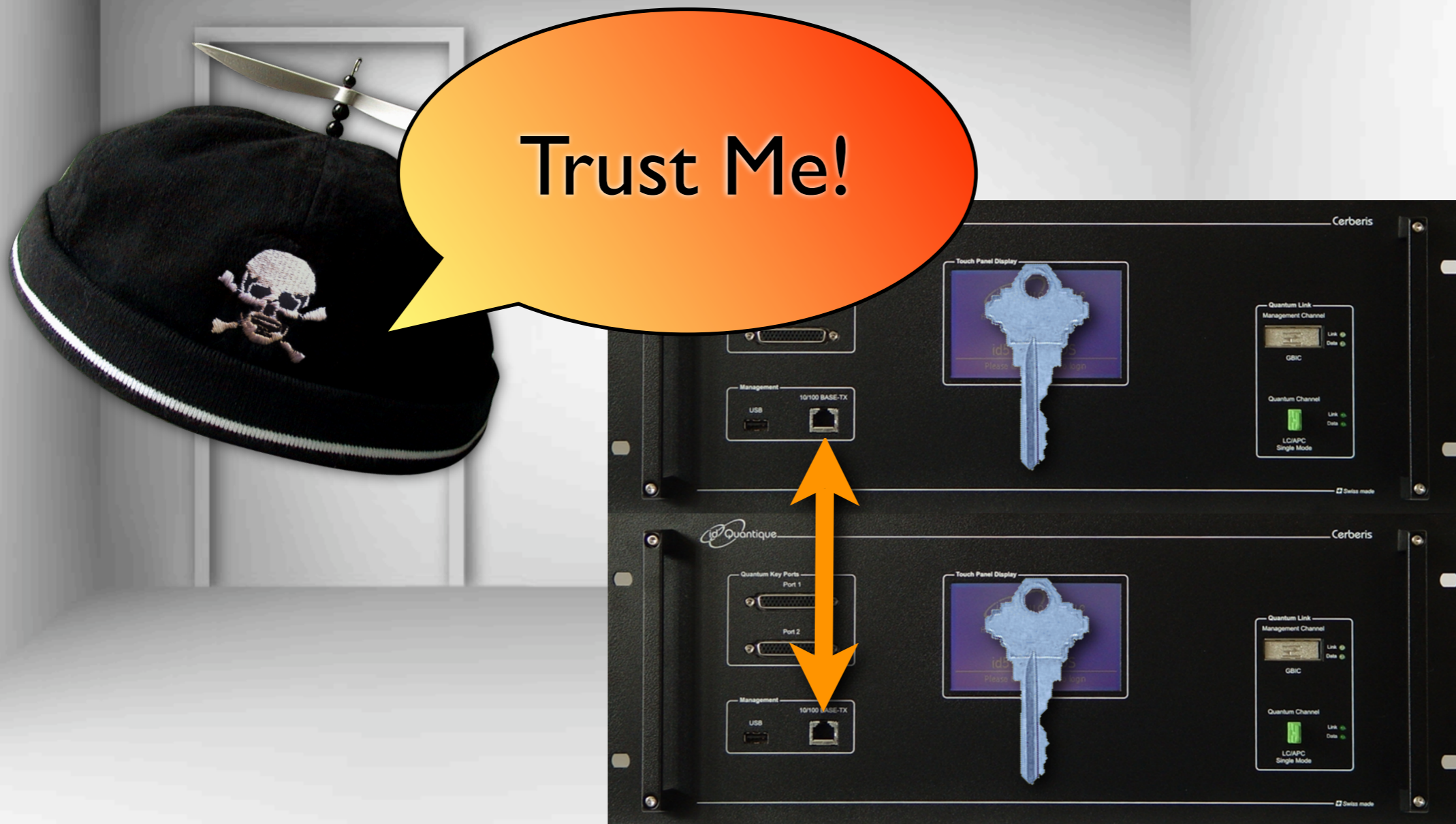


Currently those PSK are exchanged in a closed room





Currently those PSK are exchanged in a closed room



Symmetric Key Cryptography Theory:



Ueli Maurer:

Professor of Computer Science
Information Security and Cryptography
Research Group, ETH Zurich

Symmetric Key Cryptography Theory:



- ➡ All two-party secret key cryptosystems rely on the ability for those two parties to share some partially secret correlated information

Ueli Maurer:

Professor of Computer Science
Information Security and Cryptography
Research Group, ETH Zurich

Symmetric Key Cryptography Theory:



- All two-party secret key cryptosystems rely on the ability for those two parties to share some partially secret correlated information
- In most cases that correlated information is the value of a completely secret random number called a pre-shared key (PSK)

Ueli Maurer:

Professor of Computer Science
Information Security and Cryptography
Research Group, ETH Zurich

Symmetric Key Cryptography Theory:



- All two-party secret key cryptosystems rely on the ability for those two parties to share some partially secret correlated information
- In most cases that correlated information is the value of a completely secret random number called a pre-shared key (PSK)
- In entirely symmetric systems, the shared value of the PSK must be negotiated over a private channel in an...

Ueli Maurer:

Professor of Computer Science
Information Security and Cryptography
Research Group, ETH Zurich



Symmetric Key Cryptography Theory:



Ueli Maurer:

Professor of Computer Science
Information Security and Cryptography
Research Group, ETH Zurich

- All two-party secret key cryptosystems rely on the ability for those two parties to share some partially secret correlated information
- In most cases that correlated information is the value of a completely secret random number called a pre-shared key (PSK)
- In entirely symmetric systems, the shared value of the PSK must be negotiated over a private channel in an...

information-theoretically secure manner
(perfectly secure manner)

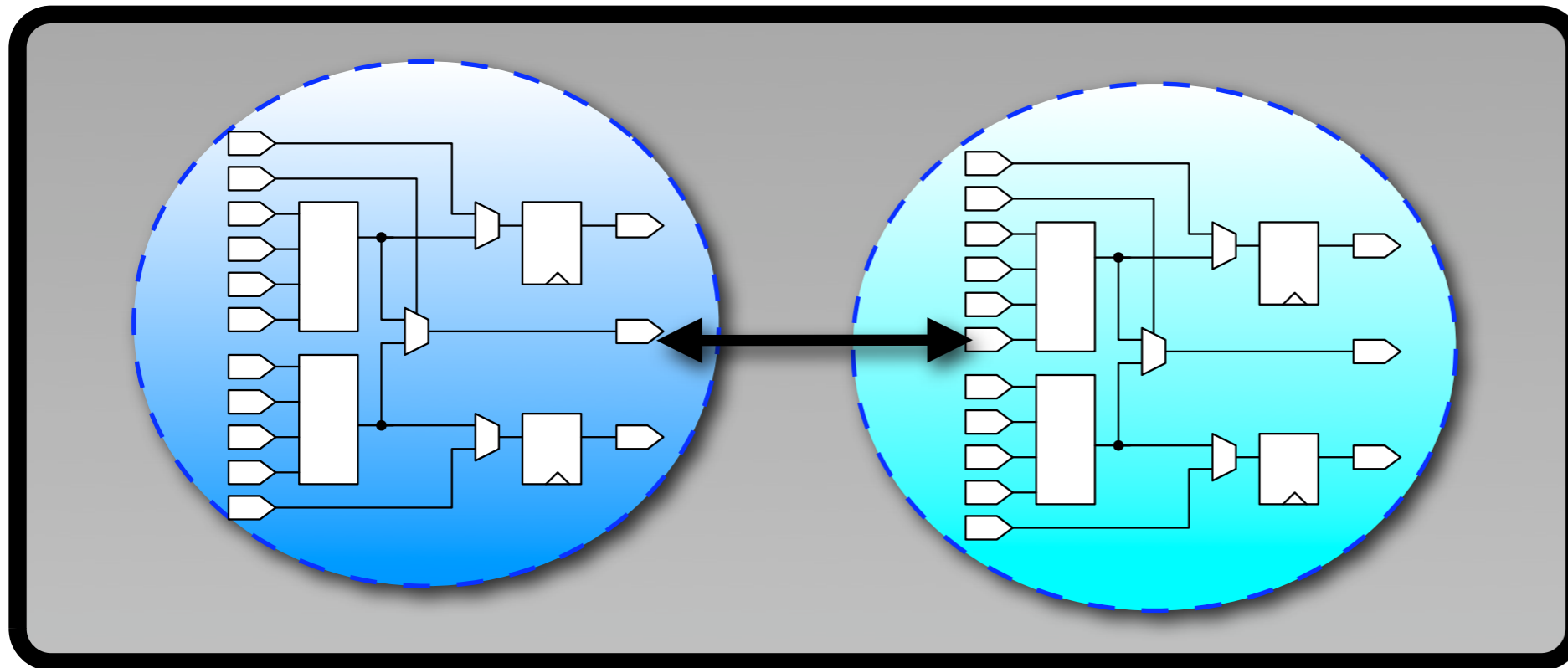




FIX: How to Securely Initialise Pre Shared Keys

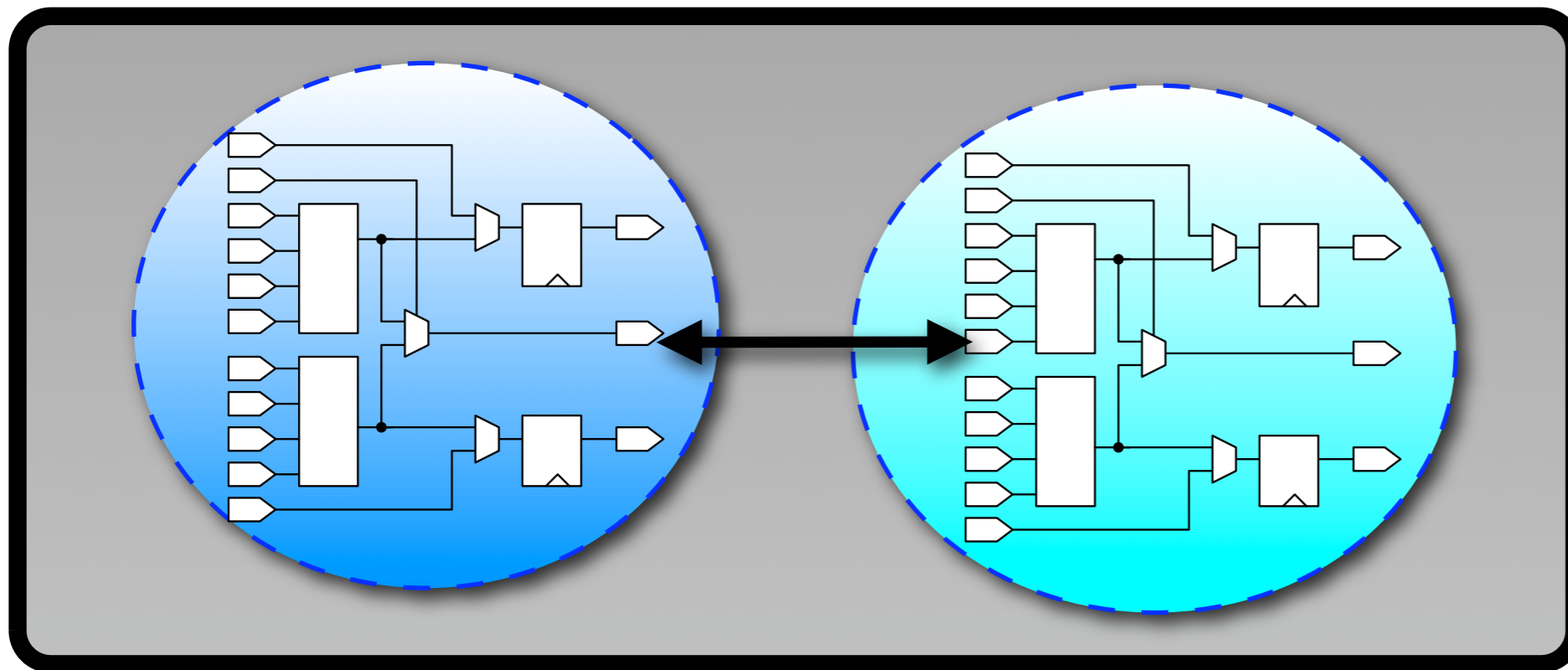


FIX: How to Securely Initialise Pre Shared Keys





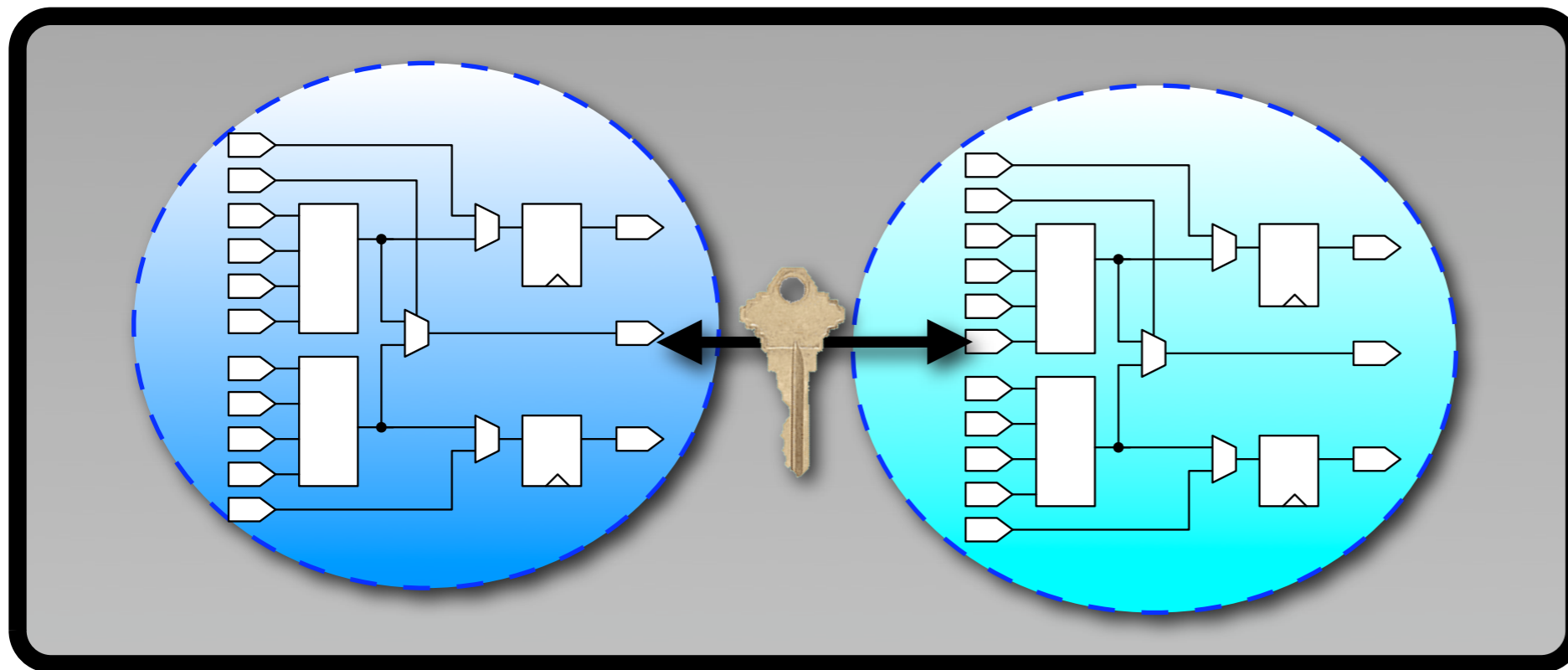
FIX: How to Securely Initialise Pre Shared Keys



Negotiate PSK
within a certified
TEMPEST
Electromagnetic
Shielded Enclosure



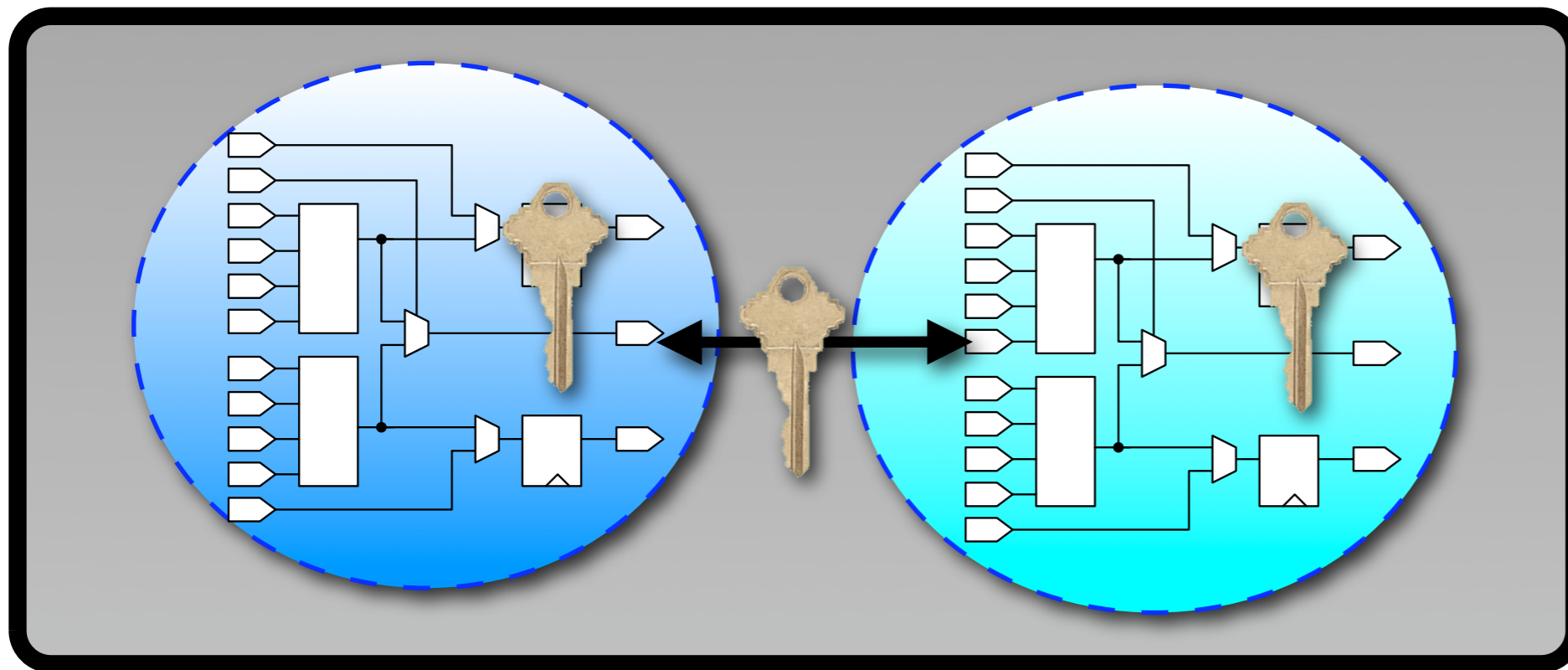
FIX: How to Securely Initialise Pre Shared Keys



Negotiate PSK
within a certified
TEMPEST
Electromagnetic
Shielded Enclosure



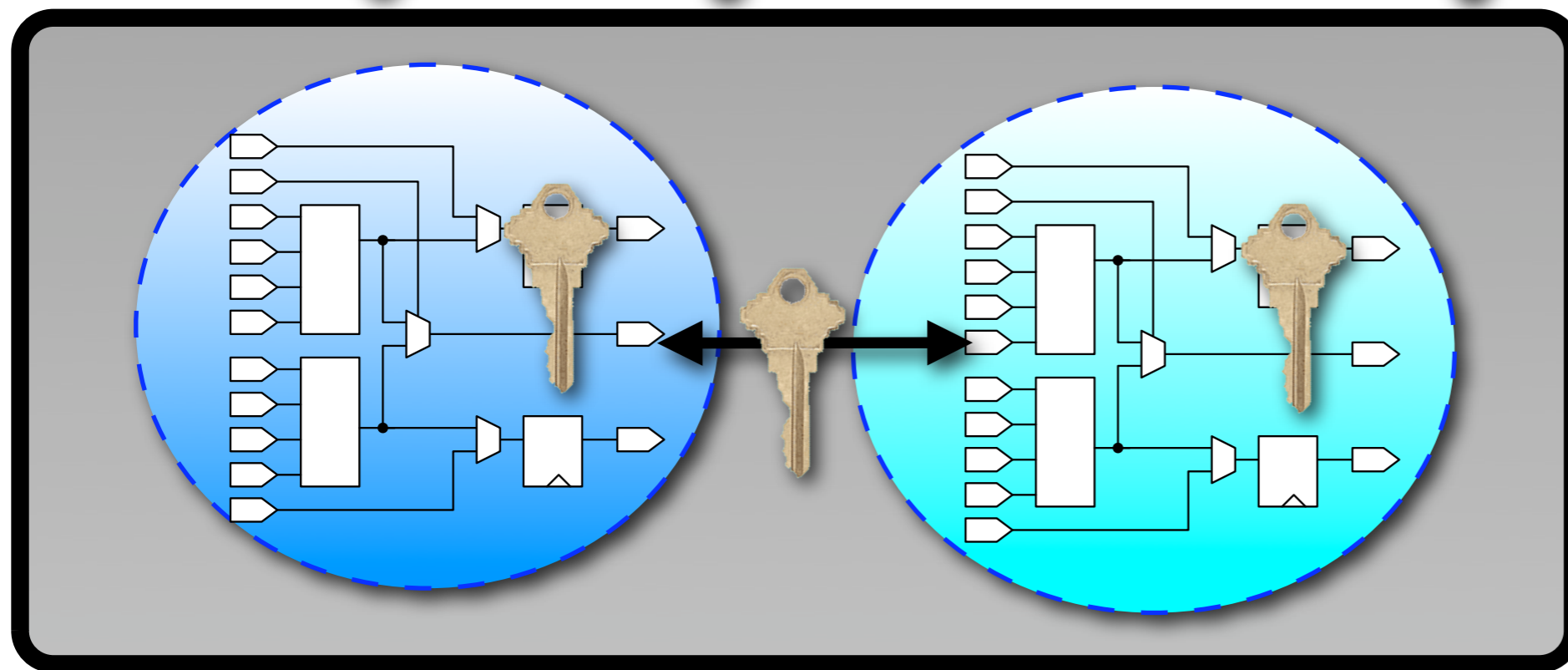
FIX: How to Securely Initialise Pre Shared Keys



Negotiate PSK
within a certified
TEMPEST
Electromagnetic
Shielded Enclosure



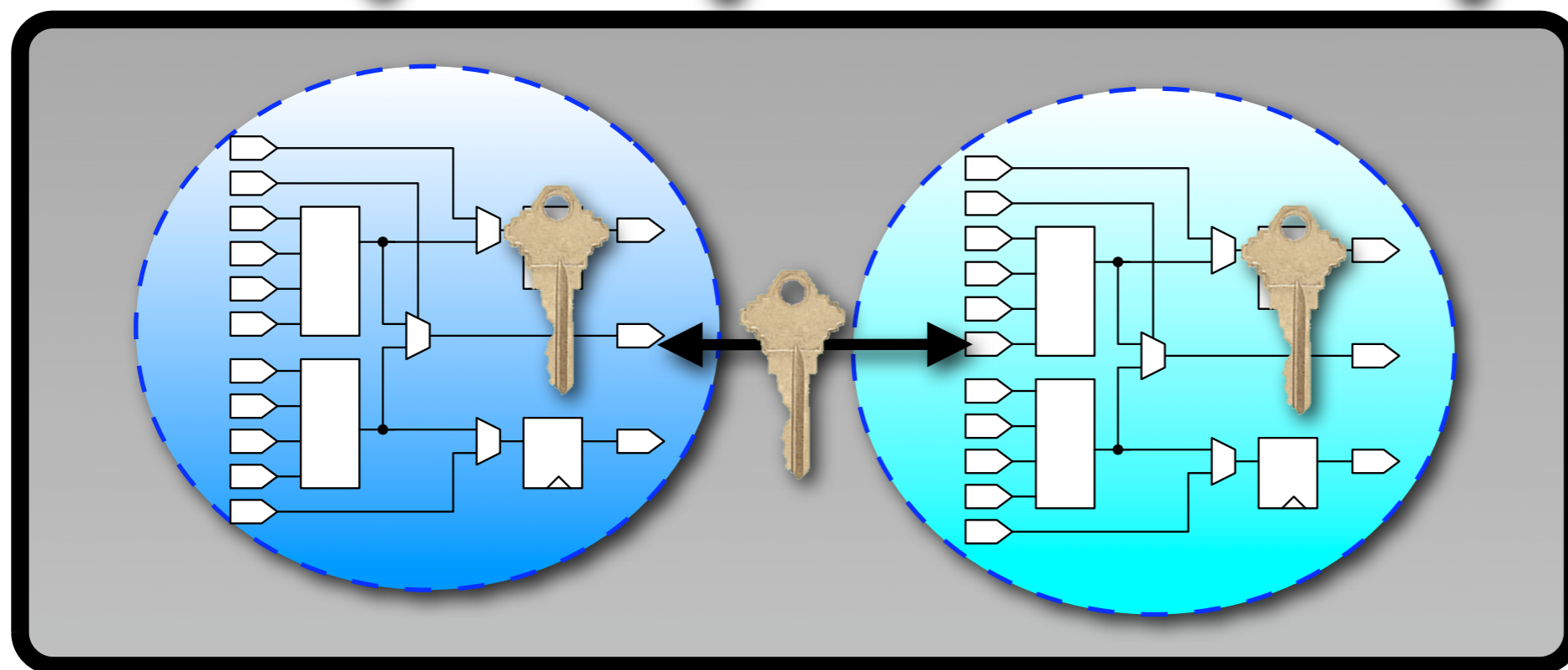
FIX: How to Securely Initialise Pre Shared Keys



Negotiate PSK
within a certified
TEMPEST
Electromagnetic
Shielded Enclosure



FIX: How to Securely Initialise Pre Shared Keys



Negotiate PSK
within a certified
TEMPEST
Electromagnetic
Shielded Enclosure

➡ **First step towards non-repudiation in symmetric key crypto systems**

Regarding 1st Generation Quantum Key Distribution implementations



Brian SNOW:

former Technical Director of the
Information **Assurance** Directorate of the
United States National Security Agency

Regarding 1st Generation Quantum Key Distribution implementations



“On quantum cryptography, yes,
in theory, it is absolutely perfect.

Brian SNOW:

former Technical Director of the
Information **Assurance** Directorate of the
United States National Security Agency



Regarding 1st Generation Quantum Key Distribution implementations



“On quantum cryptography, yes,
in theory, it is absolutely perfect.

**I will go after (attack) the
implementation.”**

Brian SNOW:

former Technical Director of the
Information **Assurance** Directorate of the
United States National Security Agency

100% key recovery attack against QKD



Vadim Makarov in Quantum Hacking
Laboratory at NTNU, October 2008

100% key recovery attack against QKD



In 2008-09, a small team of hackers called 'quackers' proved the QKD devices used in the SECOQC quantum network had a serious security flaw

Vadim Makarov in Quantum Hacking
Laboratory at NTNU, October 2008



100% key recovery attack against QKD



In 2008-09, a small team of hackers called 'quackers' proved the QKD devices used in the SECOQC quantum network had a serious security flaw

This is not the first, and unlikely to be the last, successful attack against quantum cryptographic implementations

Vadim Makarov in Quantum Hacking
Laboratory at NTNU, October 2008

100% key recovery attack against QKD



Vadim Makarov in Quantum Hacking
Laboratory at NTNU, October 2008

In 2008-09, a small team of
hackers called 'quackers'
proved the QKD devices used in
the SECOQC quantum network
had a serious security flaw

***This is not the first, and unlikely
to be the last, successful attack
against quantum cryptographic
implementations***

SEE NTNU 2010 ATTACKS



QKD Research Agenda

PART 2: Quantum Key Distribution Networks (1:1)

Image: (c) Austrian Research Centers



Development of a Global Network for Secure
Communication based on Quantum Cryptography



Image: (c) Austrian Research Centers



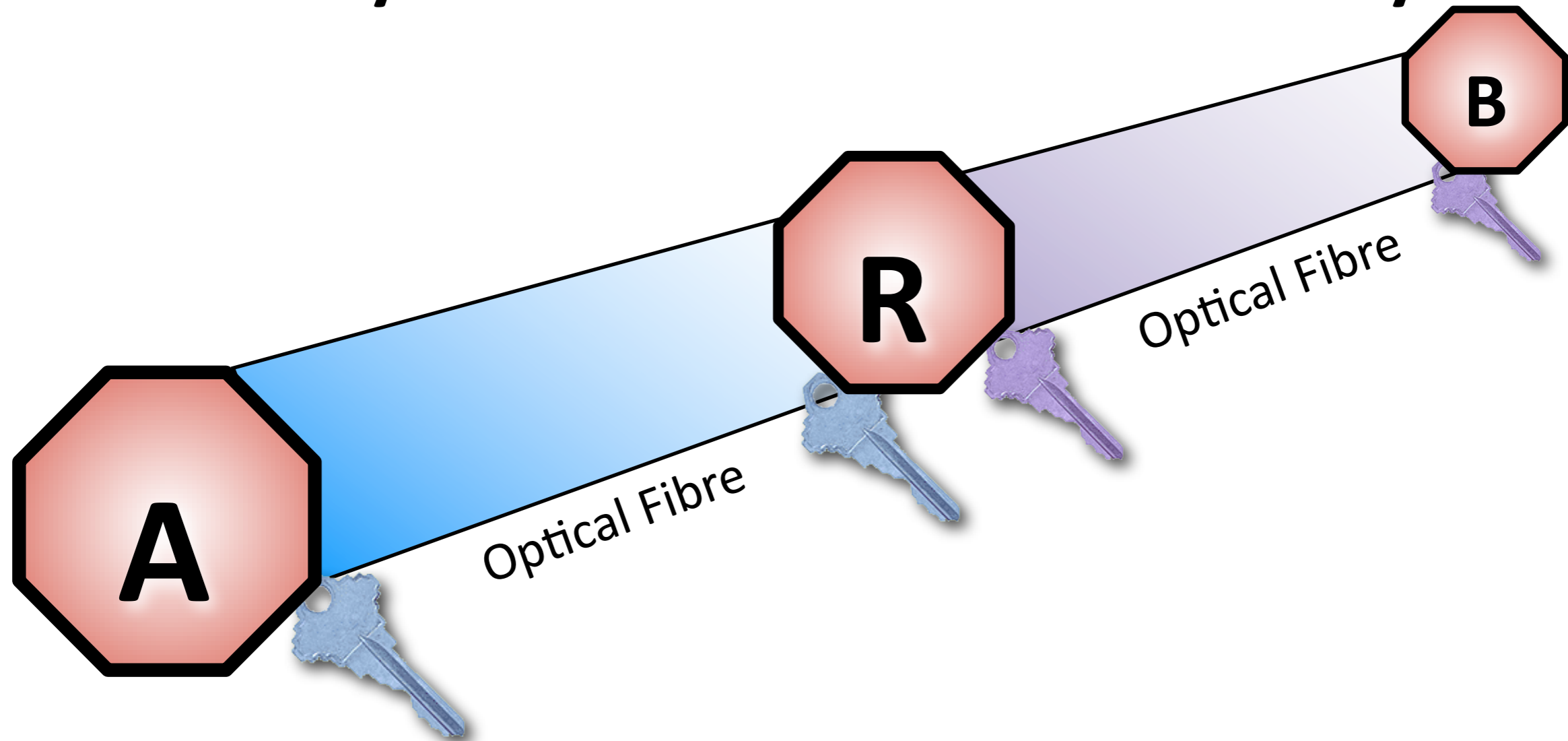
Development of a Global Network for Secure
Communication based on Quantum Cryptography

**QKD requires dedicated point-to-point links
that have PHYSICAL DISTANCE LIMITATIONS**

Image: (c) Austrian Research Centers

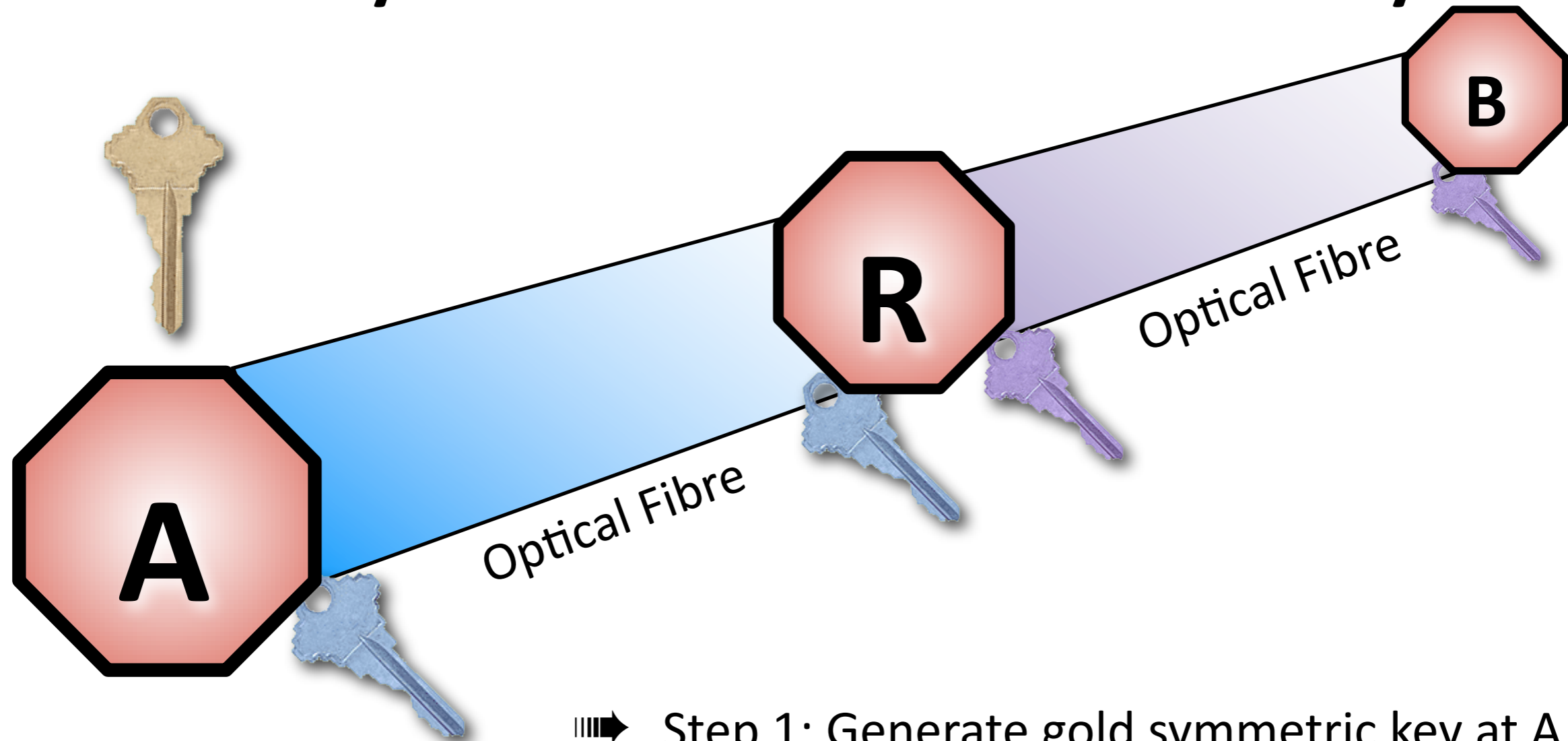


**To overcome the distance limitation in QKD Networks,
trusted relays are often used to forward key material**





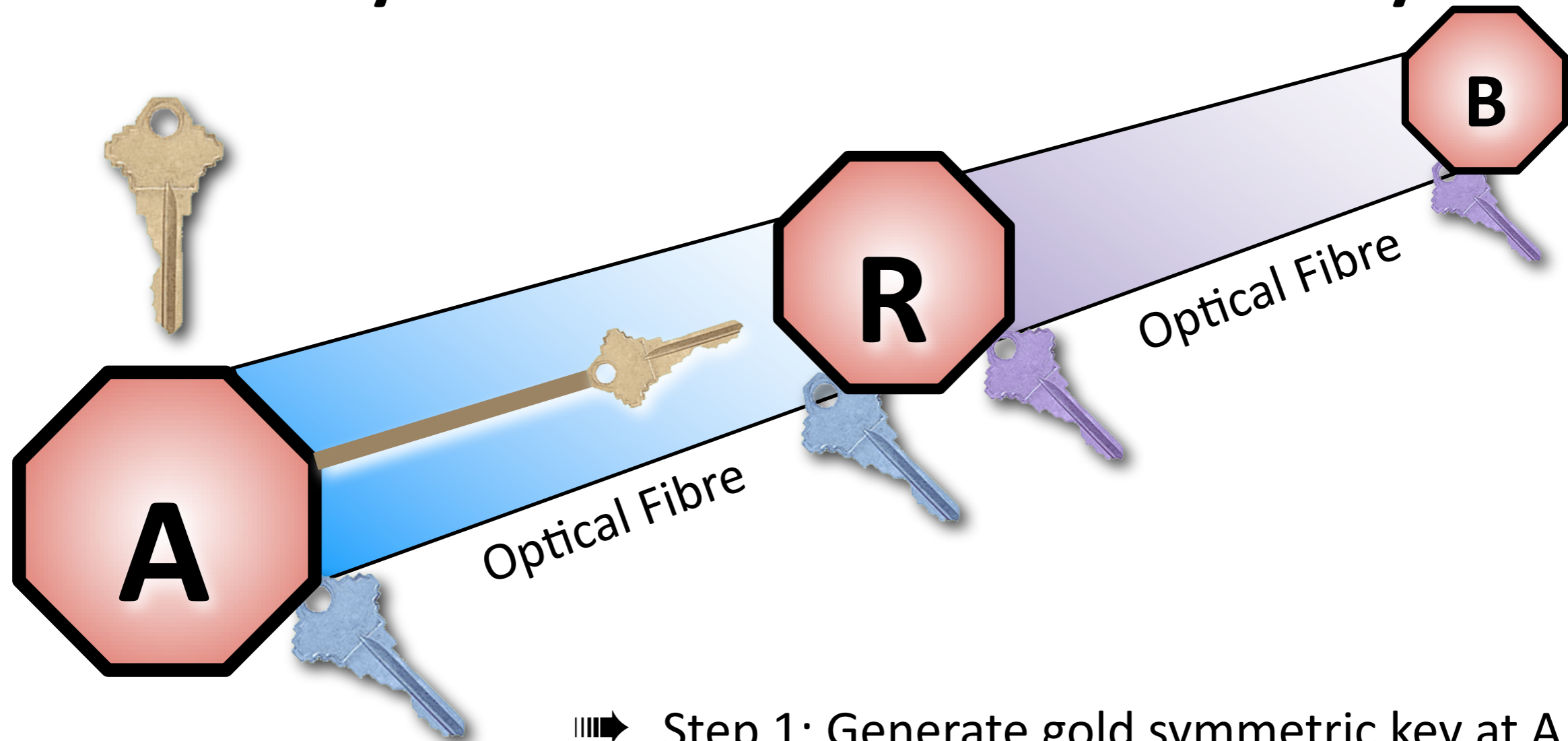
**To overcome the distance limitation in QKD Networks,
trusted relays are often used to forward key material**



➡ Step 1: Generate gold symmetric key at A



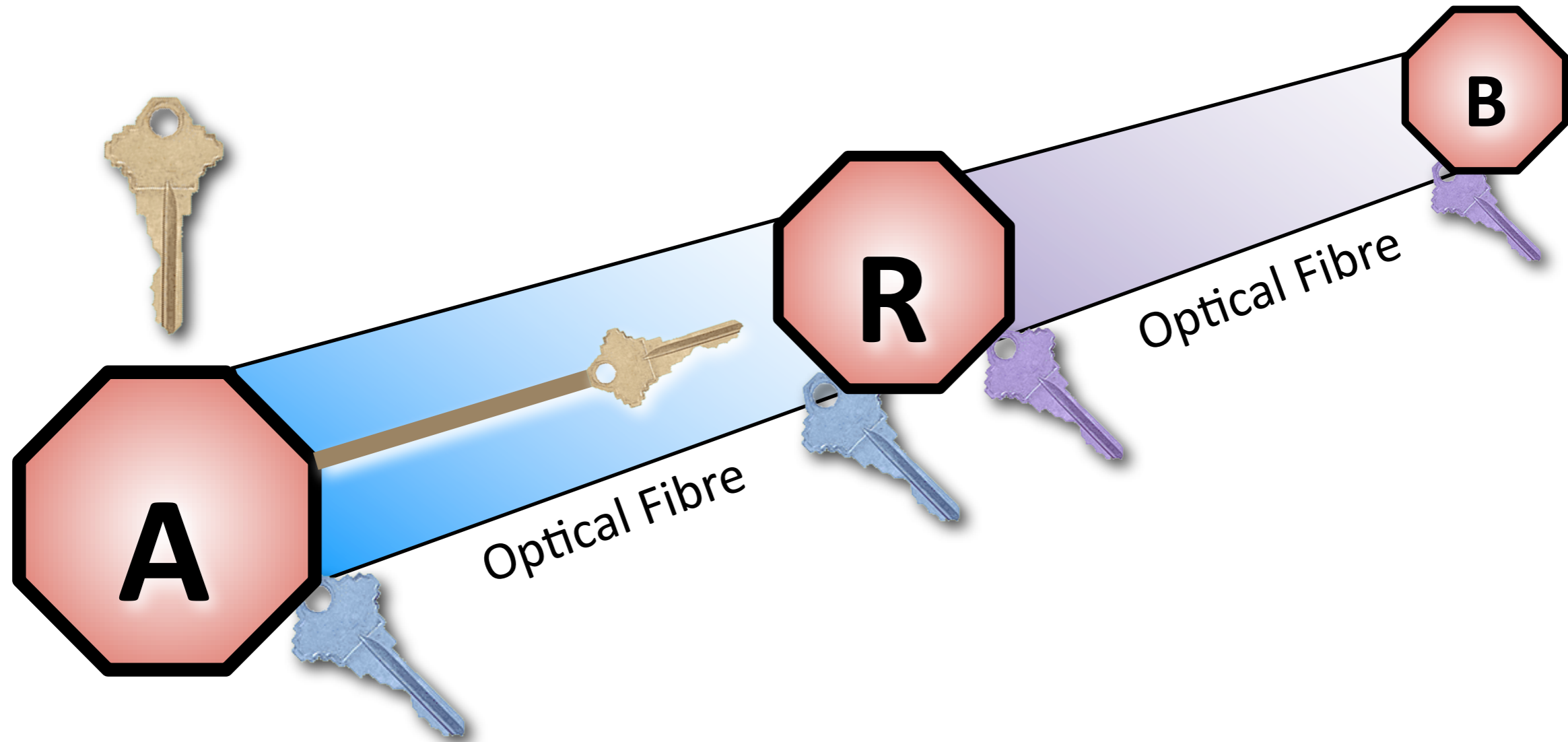
**To overcome the distance limitation in QKD Networks,
trusted relays are often used to forward key material**



- ➡ Step 1: Generate gold symmetric key at A
- ➡ Step 2: Transmit gold key over first QKD LINK

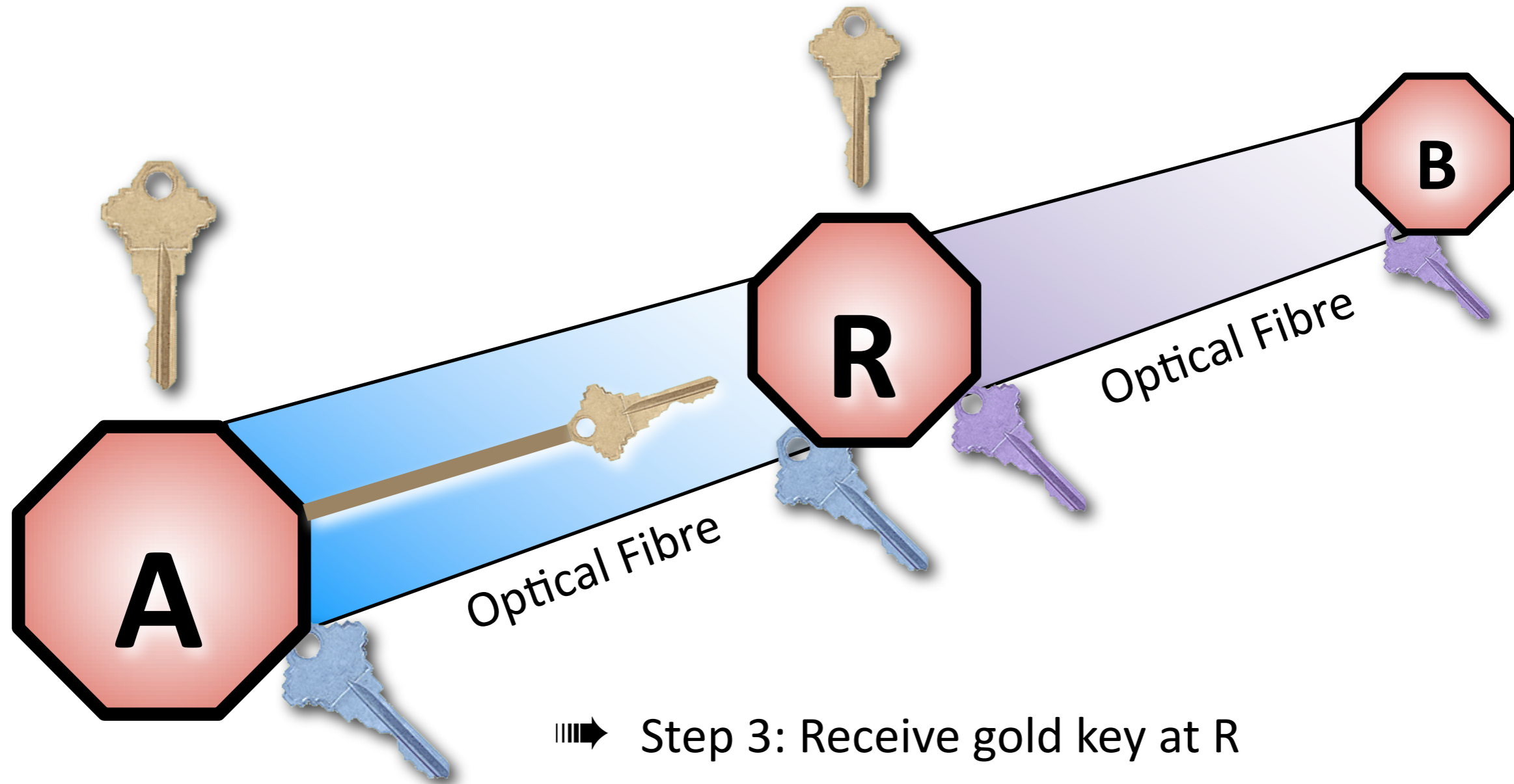


To overcome the distance limitation...



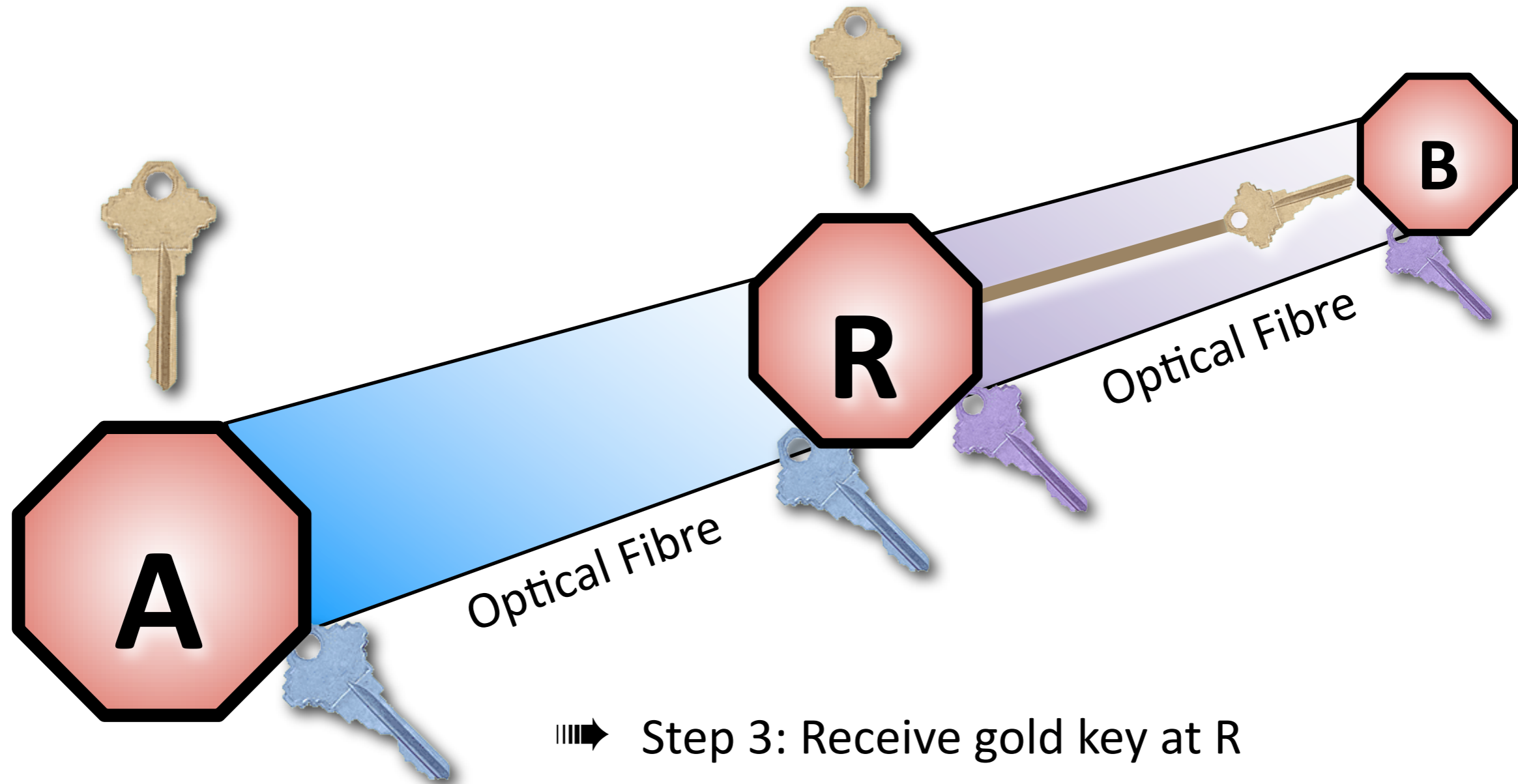


To overcome the distance limitation...





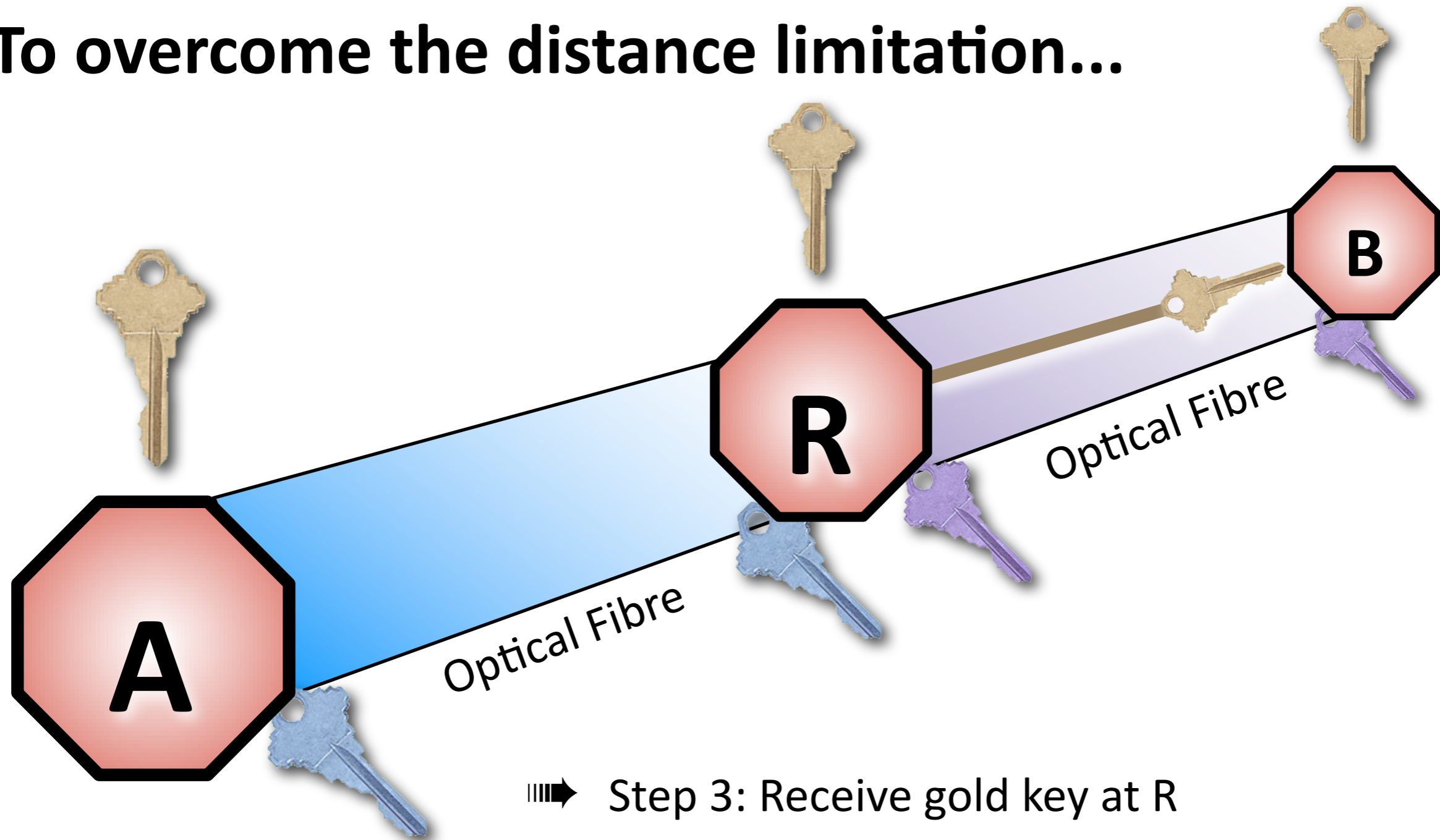
To overcome the distance limitation...



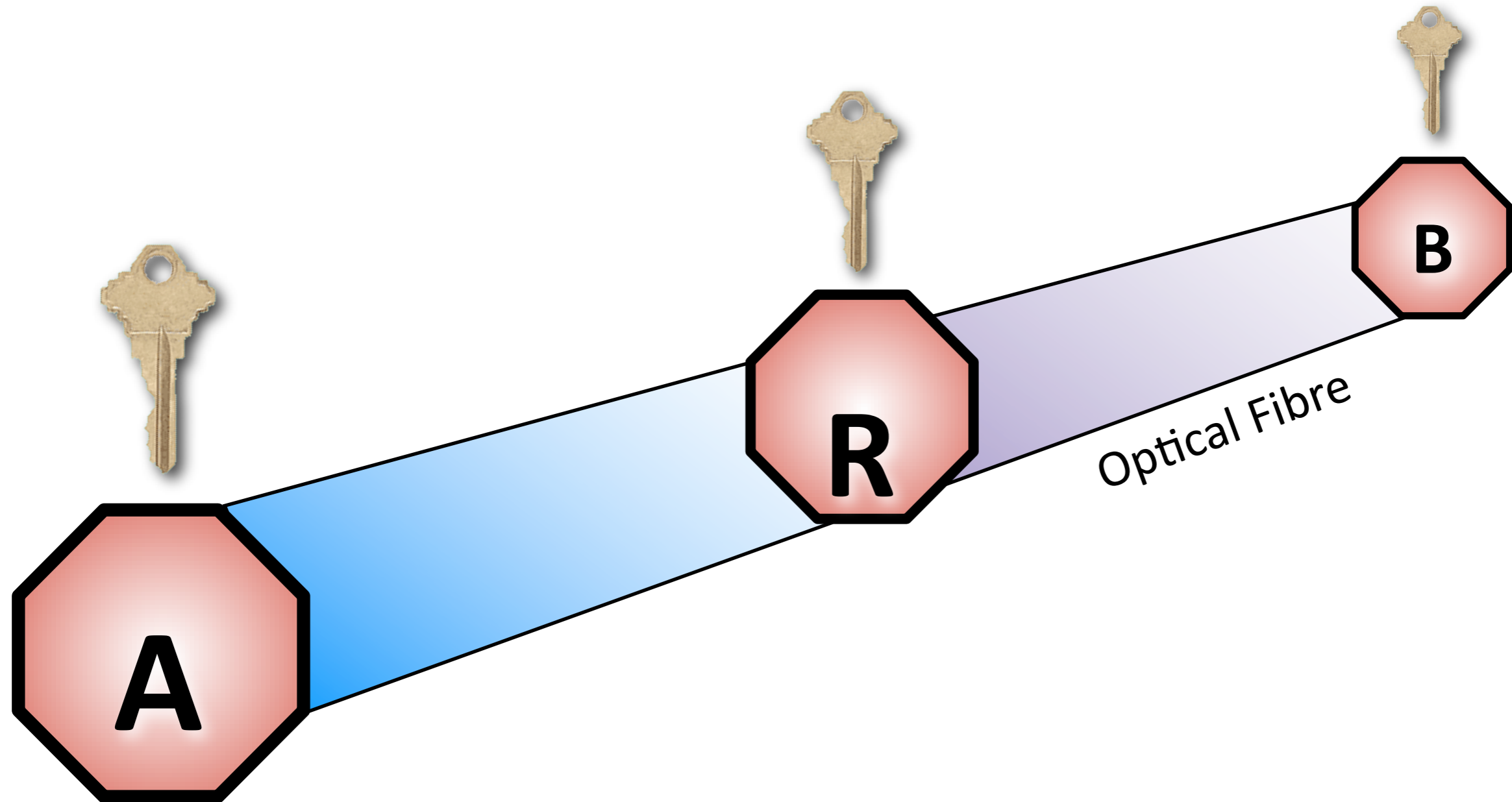
- ➡ Step 3: Receive gold key at R
- ➡ Step 4: Transmit gold key over second QKD link

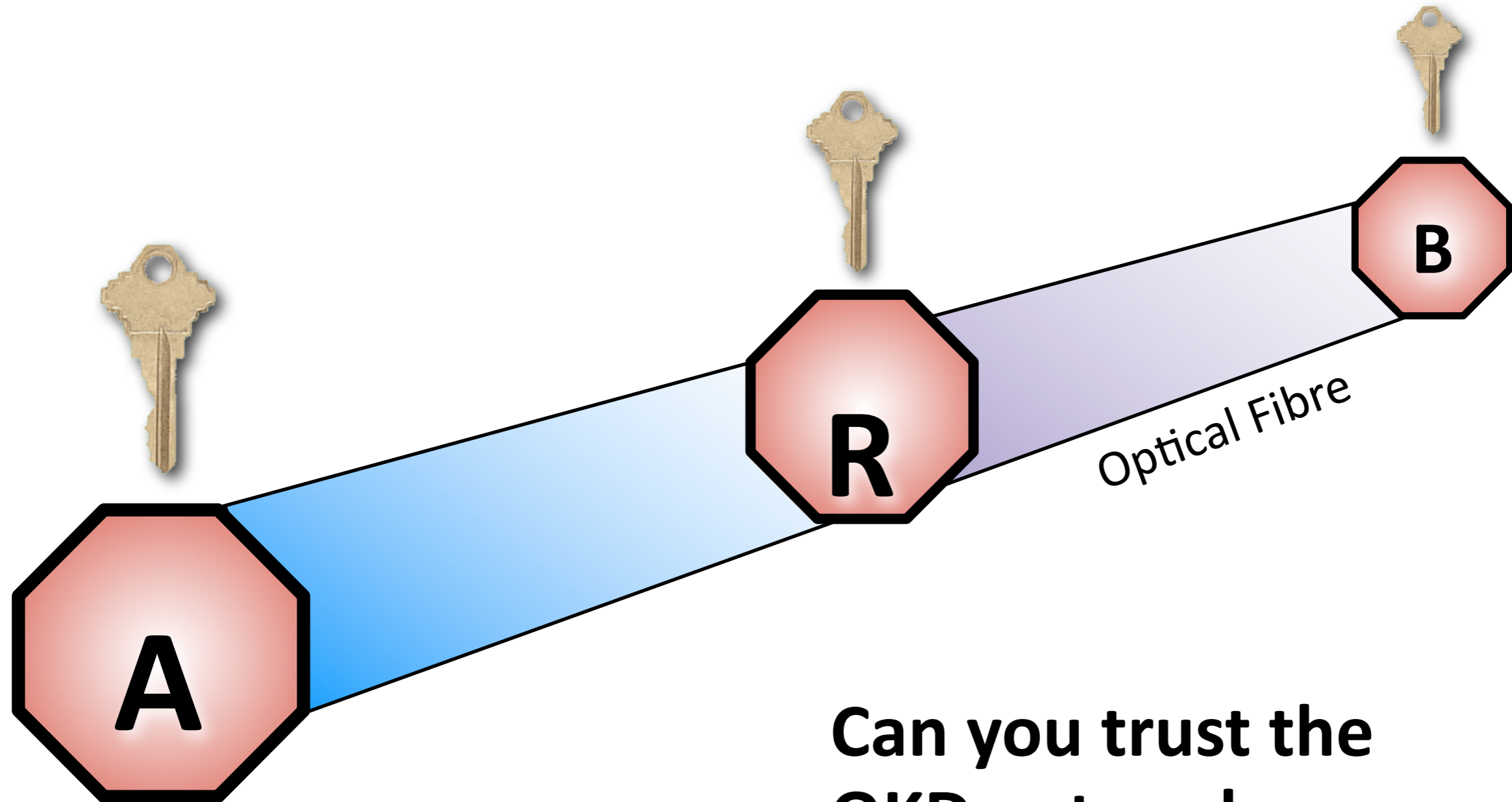


To overcome the distance limitation...

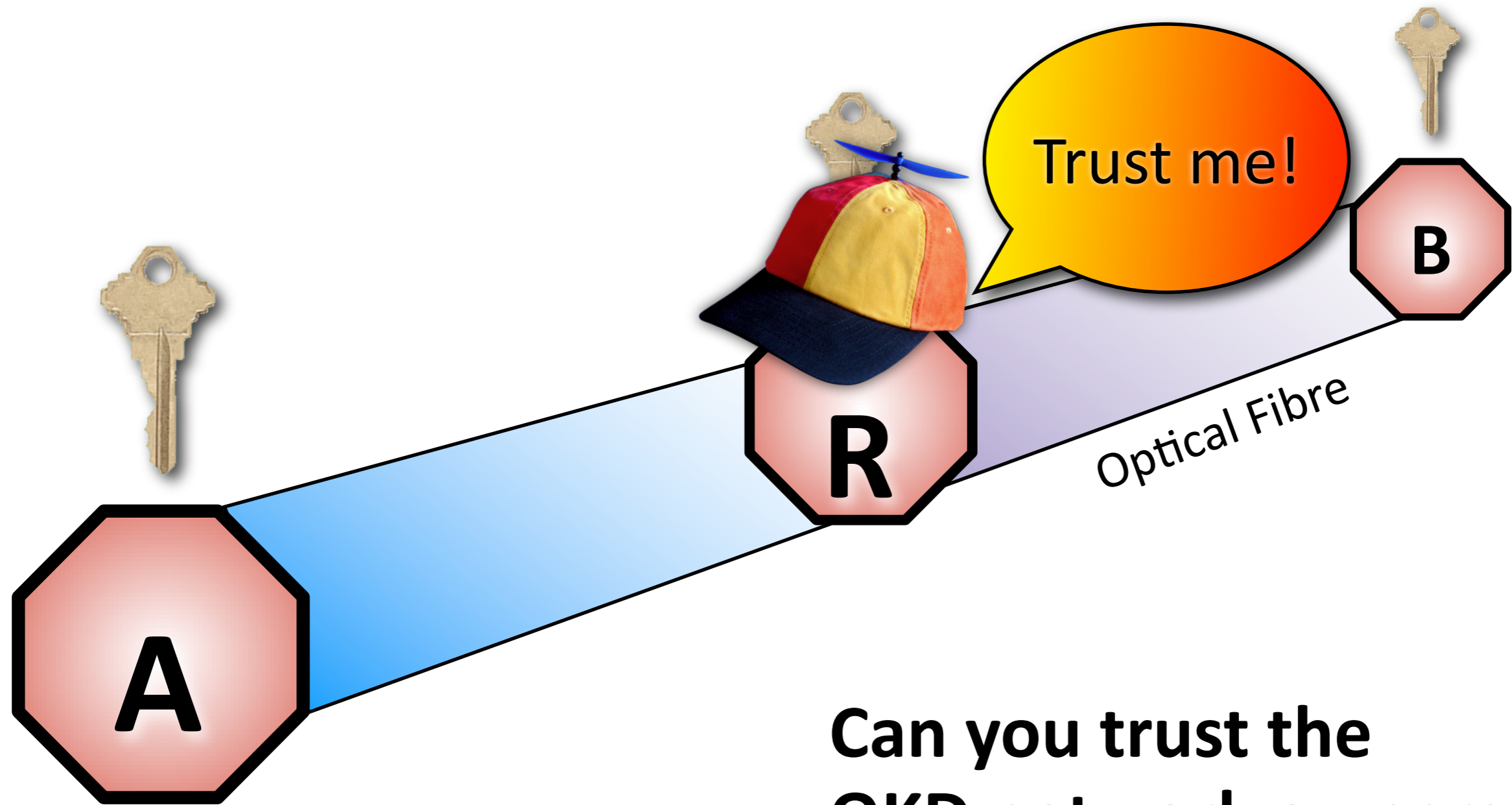


- ➡ Step 3: Receive gold key at R
- ➡ Step 4: Transmit gold key over second QKD link
- ➡ Step 5: Receive gold key at B





**Can you trust the
QKD network owners
or their technicians?**



**Can you trust the
QKD network owners
or their technicians?**



Addressing the 'single point of trust failure' problem

Addressing the 'single point of trust failure' problem

Problem:



If one party can discover
(or is entrusted with) the
value of the key, the 2 end
users have a very low level of
assurance wrt. security

Chain images © iStockPhoto. Used with permission.



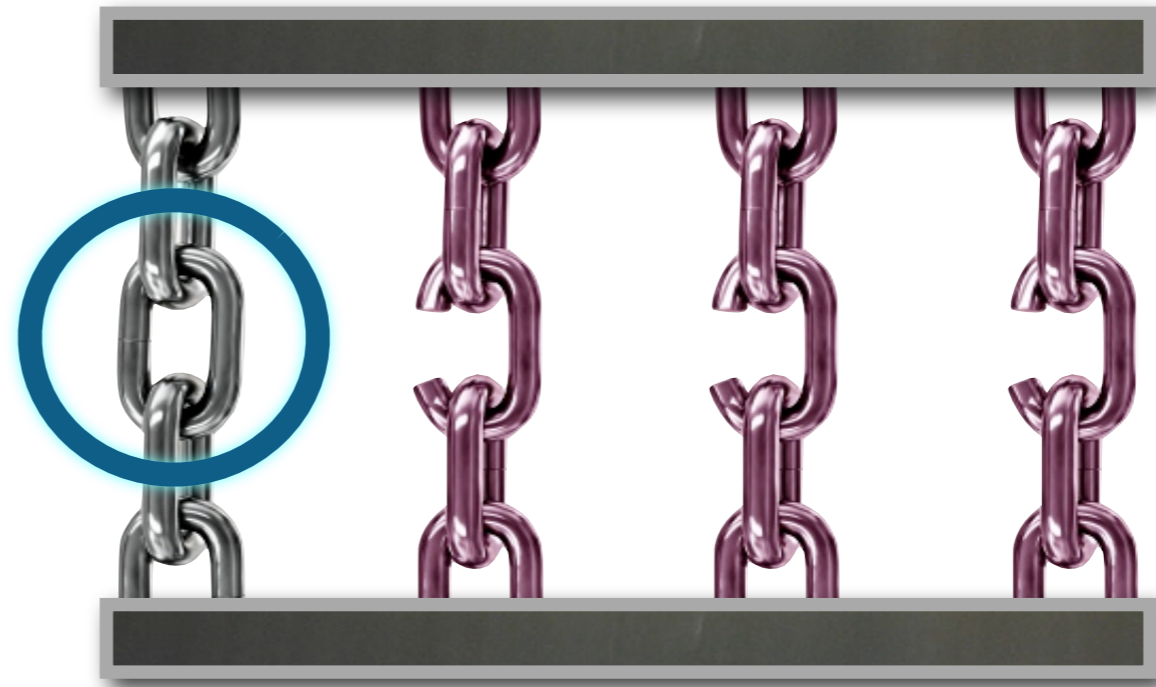
Addressing the 'single point of trust failure' problem

Problem:



If one party can discover
(or is entrusted with) the
value of the key, the 2 end
users have a very low level of
assurance wrt. security

Solution:



Introduce redundancy and distribute
secrets across m independent parties

However, this redundancy must be
added carefully

Chain images © iStockPhoto. Used with permission.



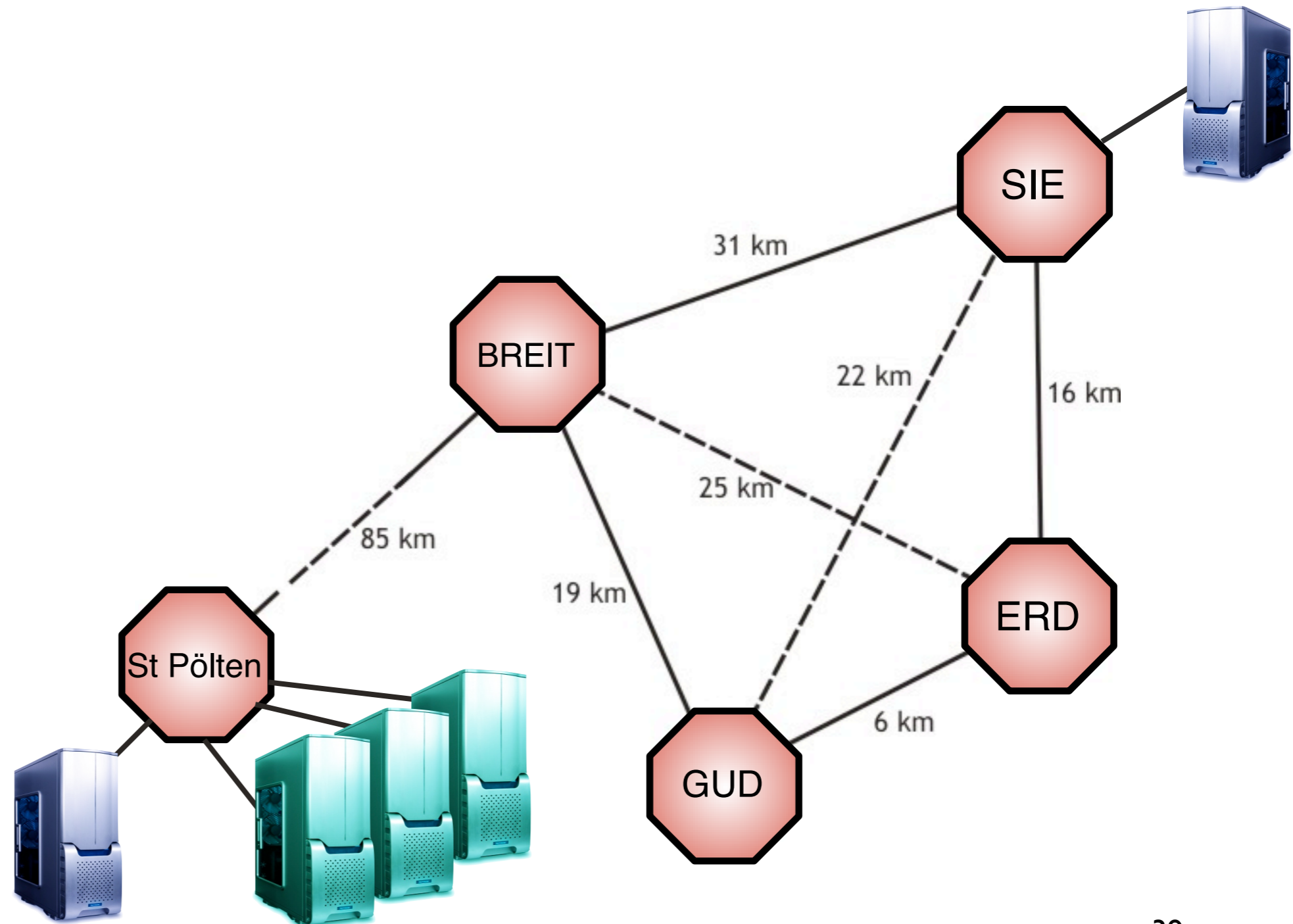
QKD Research Agenda

PART 3: Scaling QKDN (Global QKD Networks?)

Image: (c) Austrian Research Centers



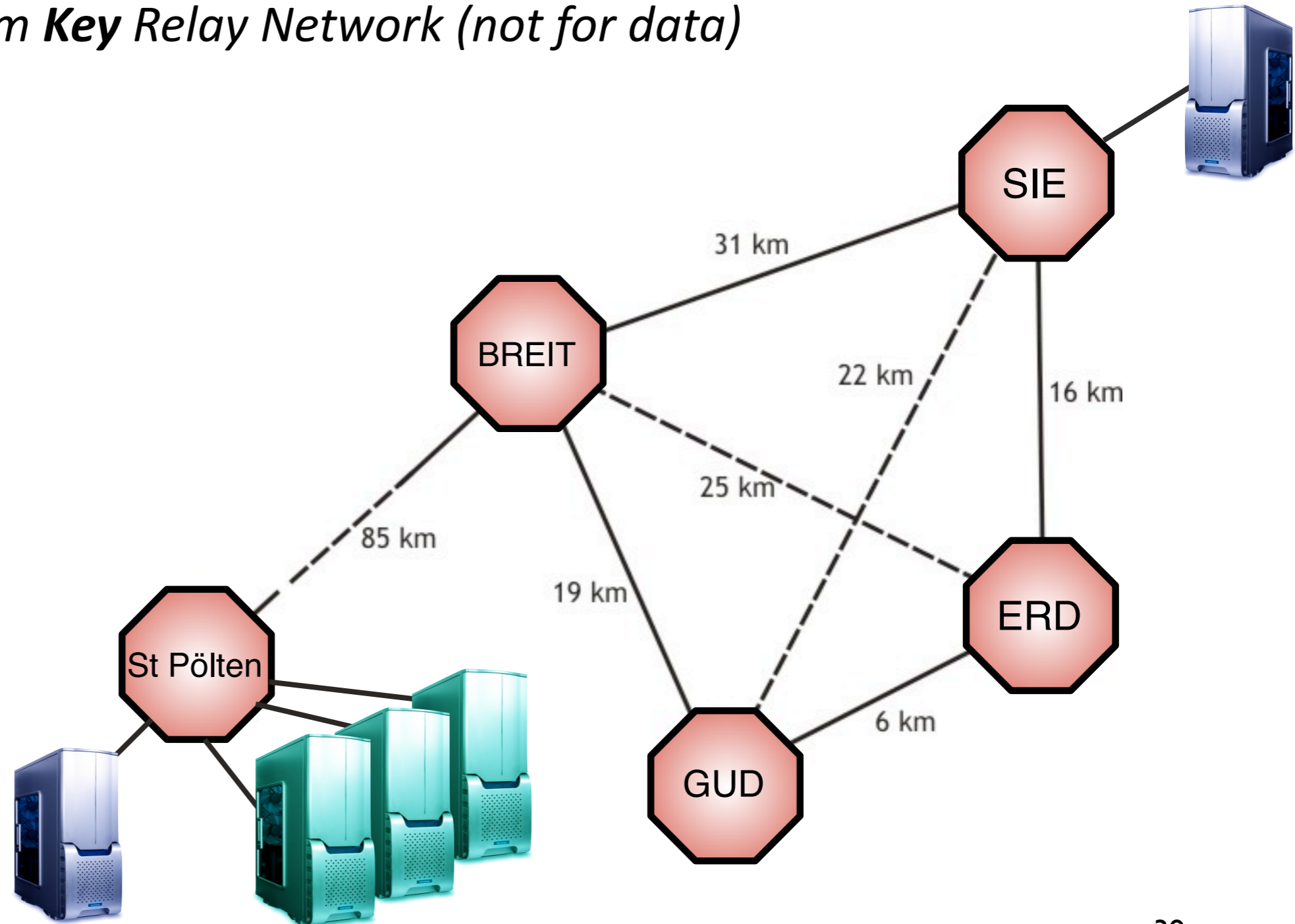
SECOQC QKD Network: Vienna AUSTRIA





SECOQC QKD Network: Vienna AUSTRIA

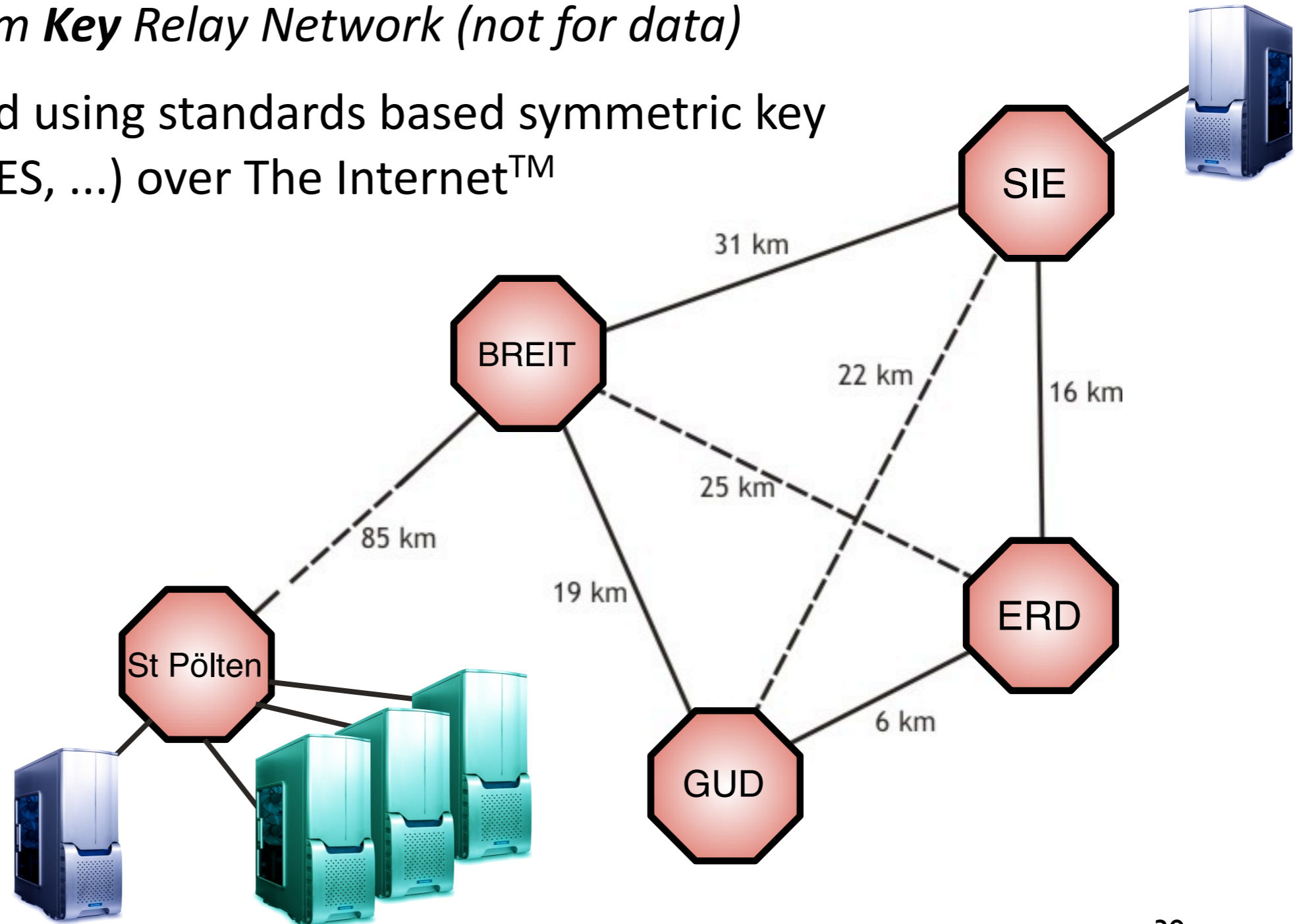
➡ This is a Quantum *Key* Relay Network (not for data)





SECOQC QKD Network: Vienna AUSTRIA

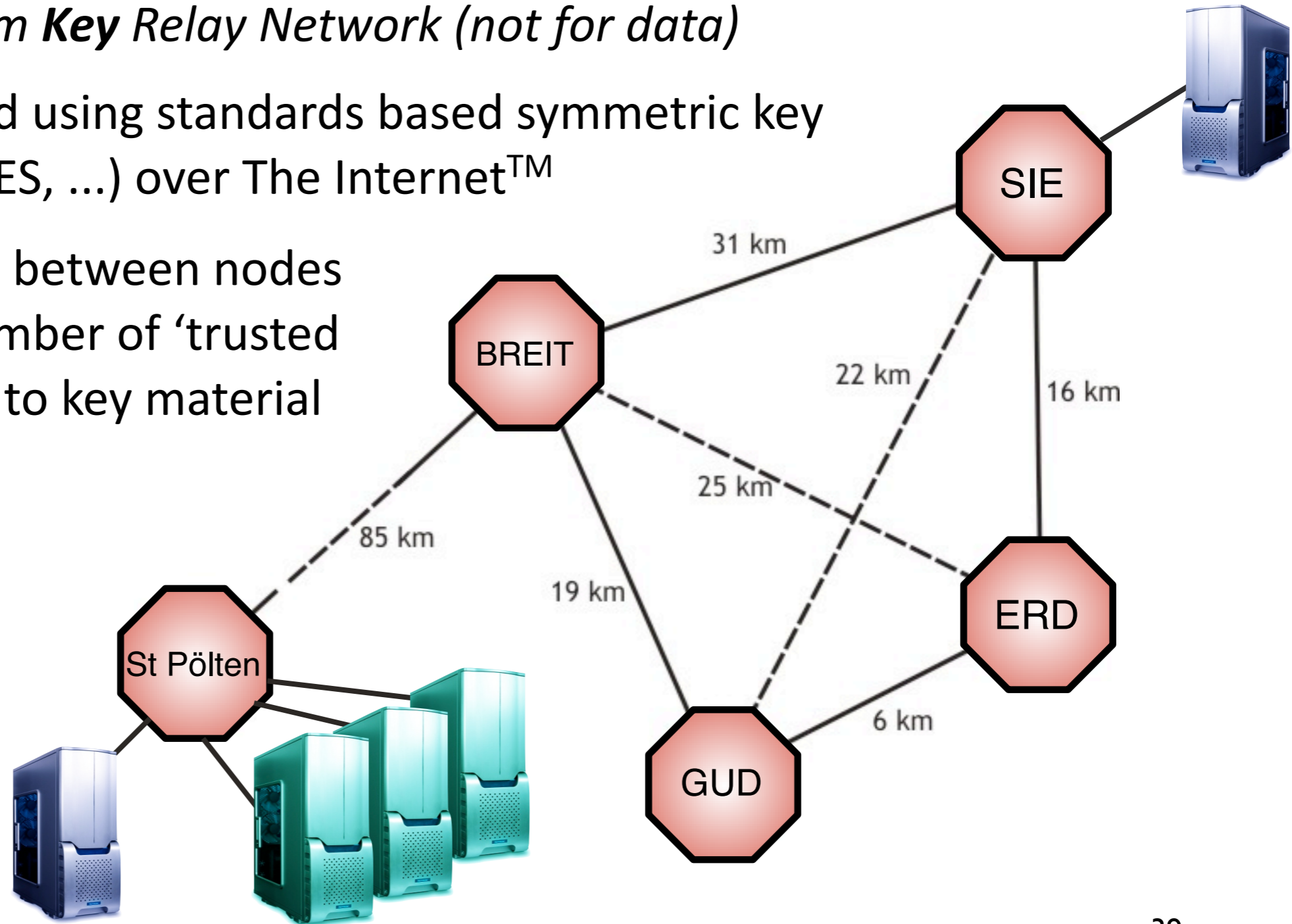
- ➡ This is a Quantum **Key** Relay Network (not for data)
- ➡ Data is encrypted using standards based symmetric key ciphers (AES, 3DES, ...) over The Internet™





SECOQC QKD Network: Vienna AUSTRIA

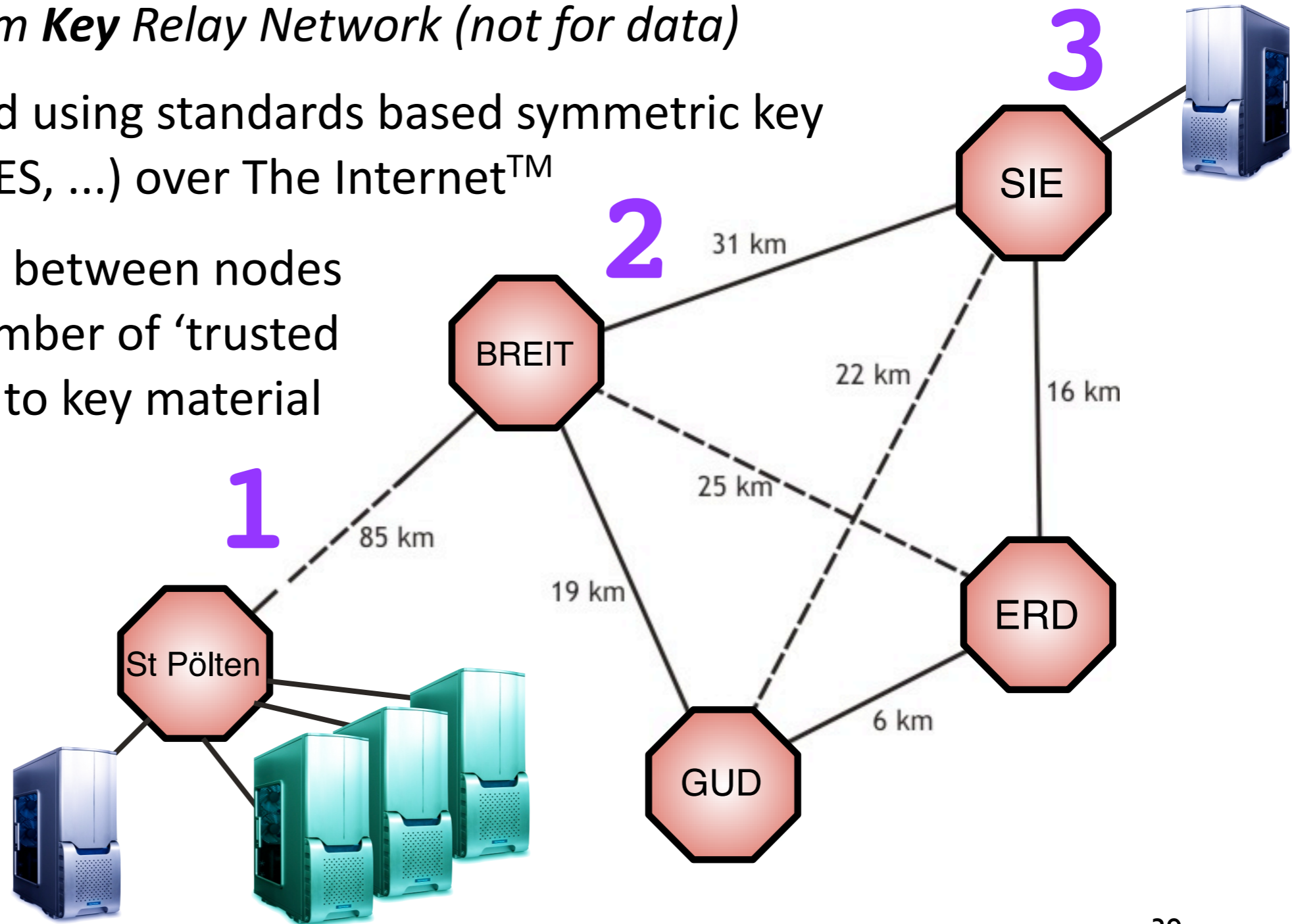
- ➡ This is a Quantum **Key** Relay Network (not for data)
- ➡ Data is encrypted using standards based symmetric key ciphers (AES, 3DES, ...) over The Internet™
- ➡ Physical distance between nodes increases the number of 'trusted parties' exposed to key material





SECOQC QKD Network: Vienna AUSTRIA

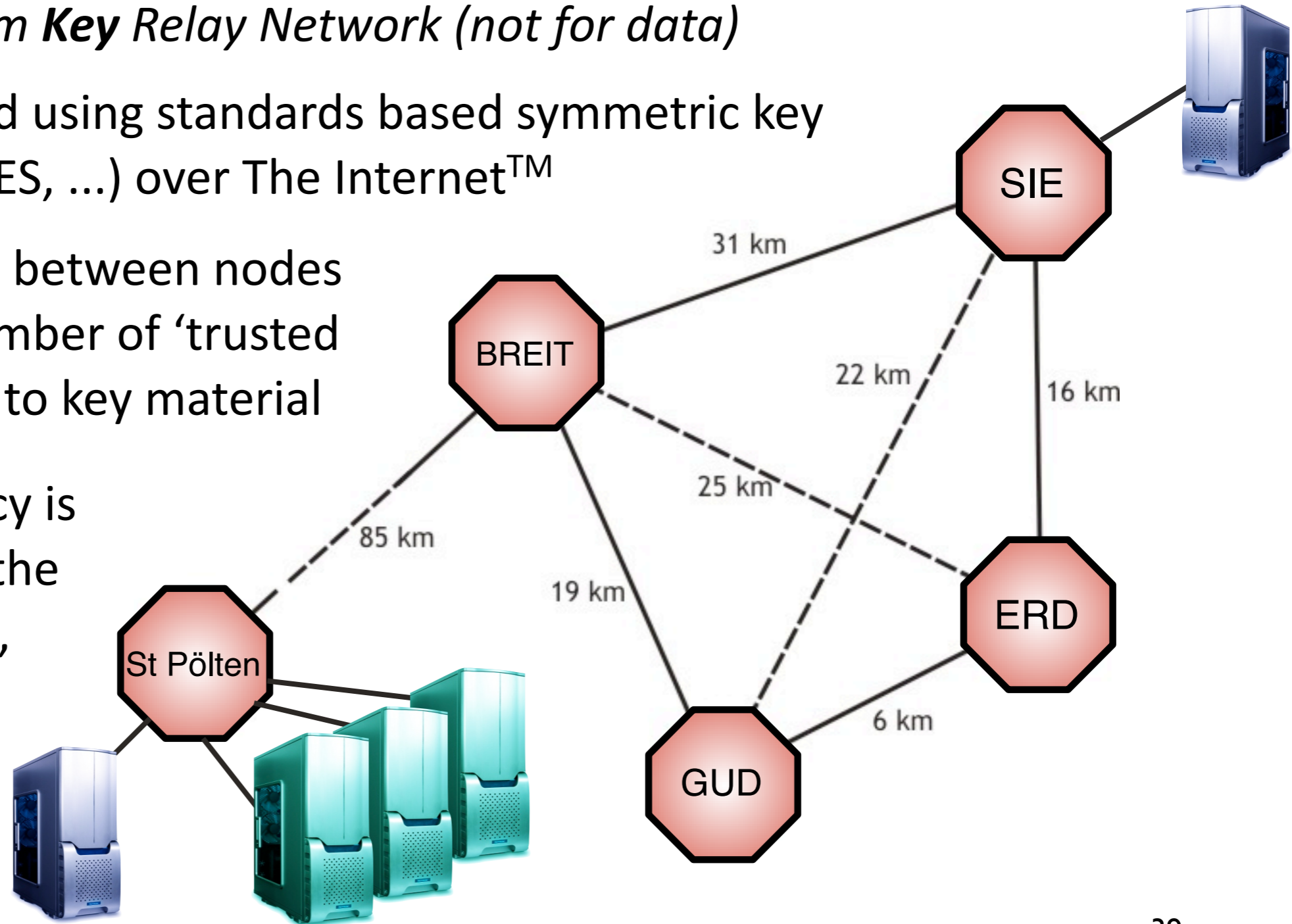
- ➡ This is a Quantum **Key** Relay Network (not for data)
- ➡ Data is encrypted using standards based symmetric key ciphers (AES, 3DES, ...) over The Internet™
- ➡ Physical distance between nodes increases the number of 'trusted parties' exposed to key material





SECOQC QKD Network: Vienna AUSTRIA

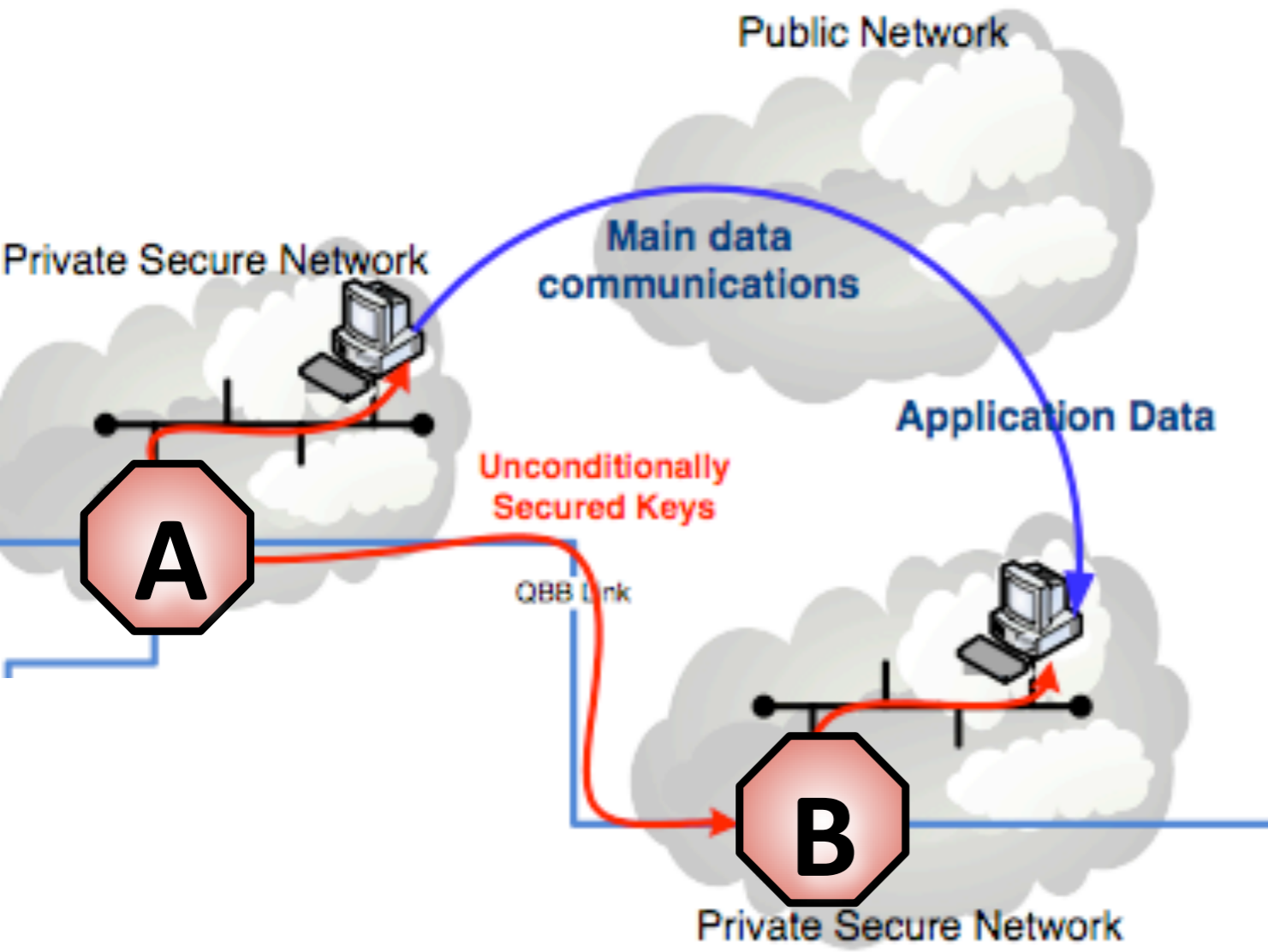
- ➡ This is a Quantum **Key** Relay Network (not for data)
- ➡ Data is encrypted using standards based symmetric key ciphers (AES, 3DES, ...) over The Internet™
- ➡ Physical distance between nodes increases the number of 'trusted parties' exposed to key material
- ➡ Some redundancy is introduced into the mesh back-bone, however it does NOT reach the user





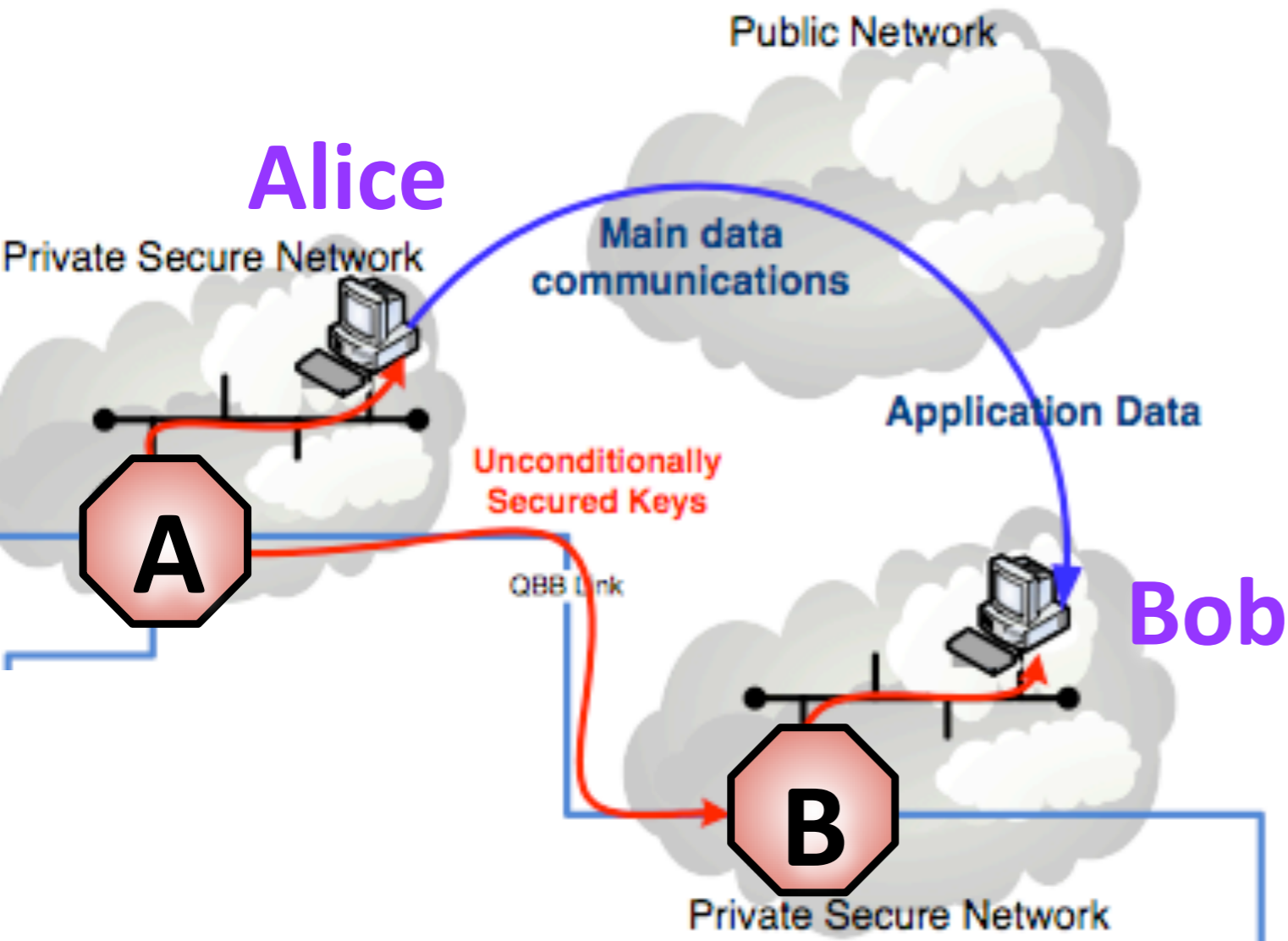
Expanding mesh QKD Back Bone with a LAN

Alice and Bob exchange keys, with the assistance of the **QKD back bone** (Only the red link between **A** and **B** uses Quantum techniques). Alice and Bob use that key to encrypt application data which is sent **over the public network**.



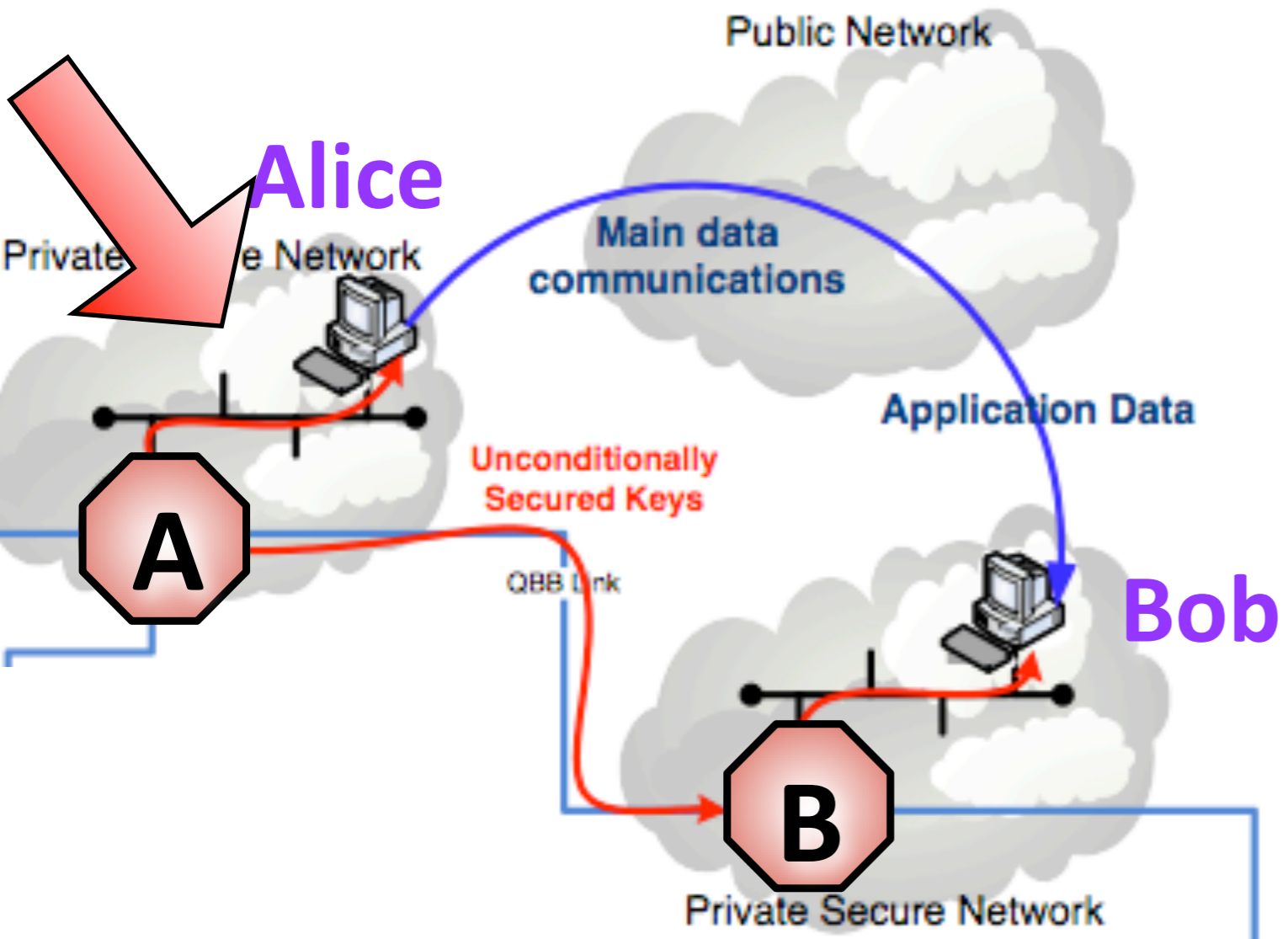
Expanding mesh QKD Back Bone with a LAN

Alice and Bob exchange keys, with the assistance of the **QKD back bone** (Only the red link between **A** and **B** uses Quantum techniques). Alice and Bob use that key to encrypt application data which is sent **over the public network**.



Expanding mesh QKD Back Bone with a LAN

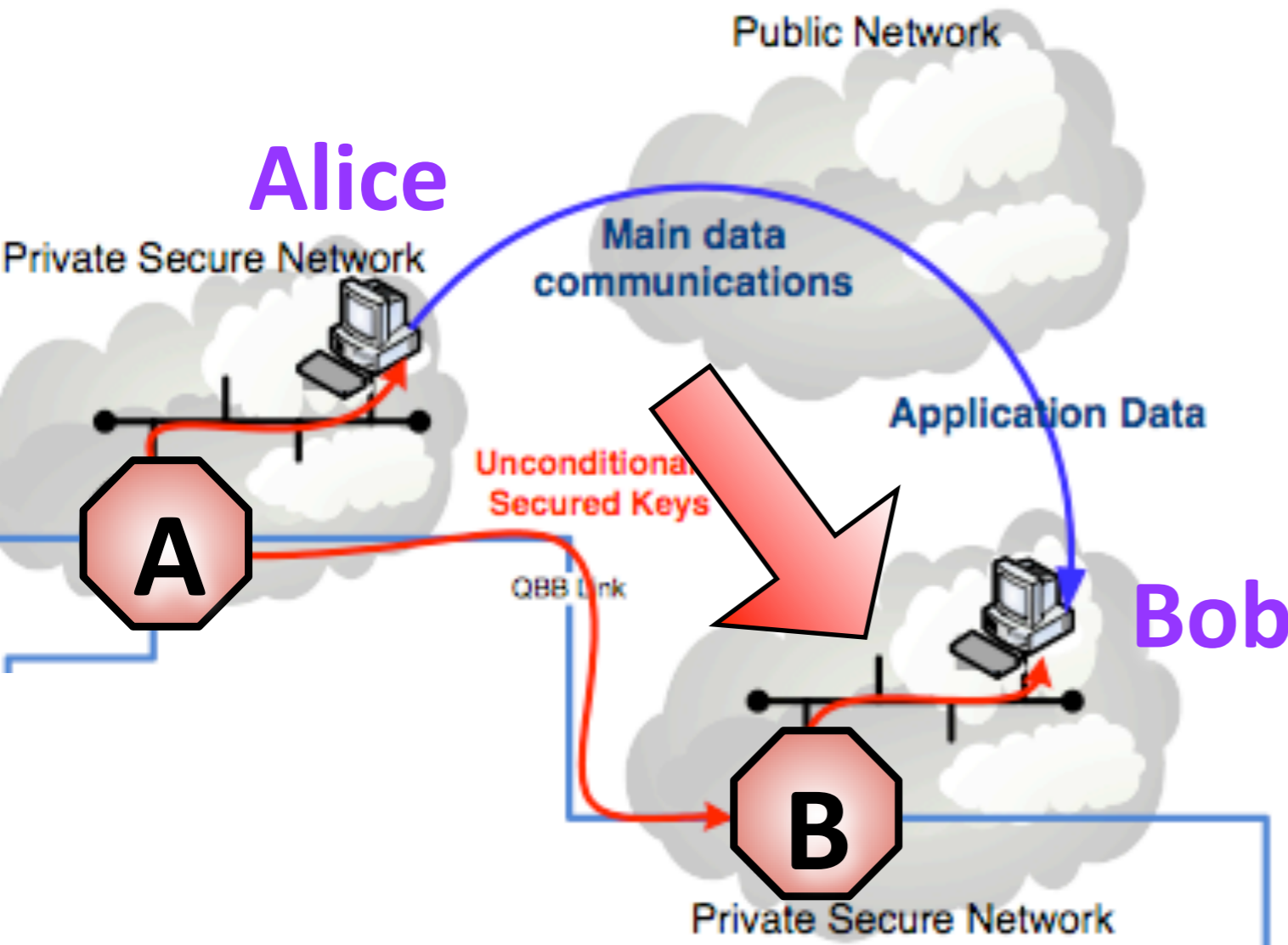
Alice and Bob exchange keys, with the assistance of the QKD back bone (Only the red link between A and B uses Quantum techniques). Alice and Bob use that key to encrypt application data which is sent over the public network.



➡ Alice needs a secure link to her QKD device A over LAN (no redundancy)

Expanding mesh QKD Back Bone with a LAN

Alice and Bob exchange keys, with the assistance of the **QKD back bone** (Only the red link between **A** and **B** uses Quantum techniques). Alice and Bob use that key to encrypt application data which is sent **over the public network**.

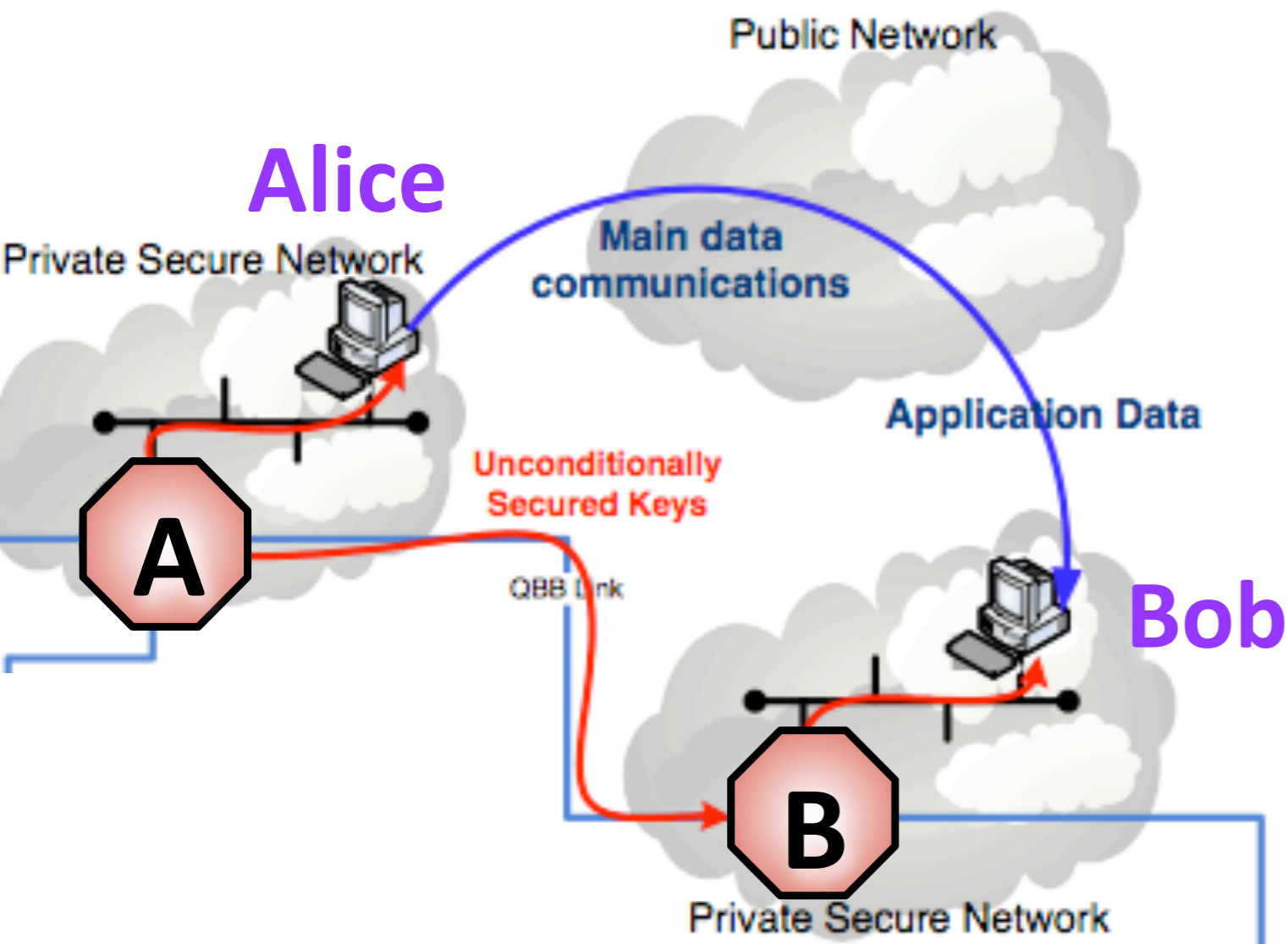


- ➡ Alice needs a secure link to her QKD device A over LAN (no redundancy)
- ➡ So does Bob



Expanding mesh QKD Back Bone with a LAN

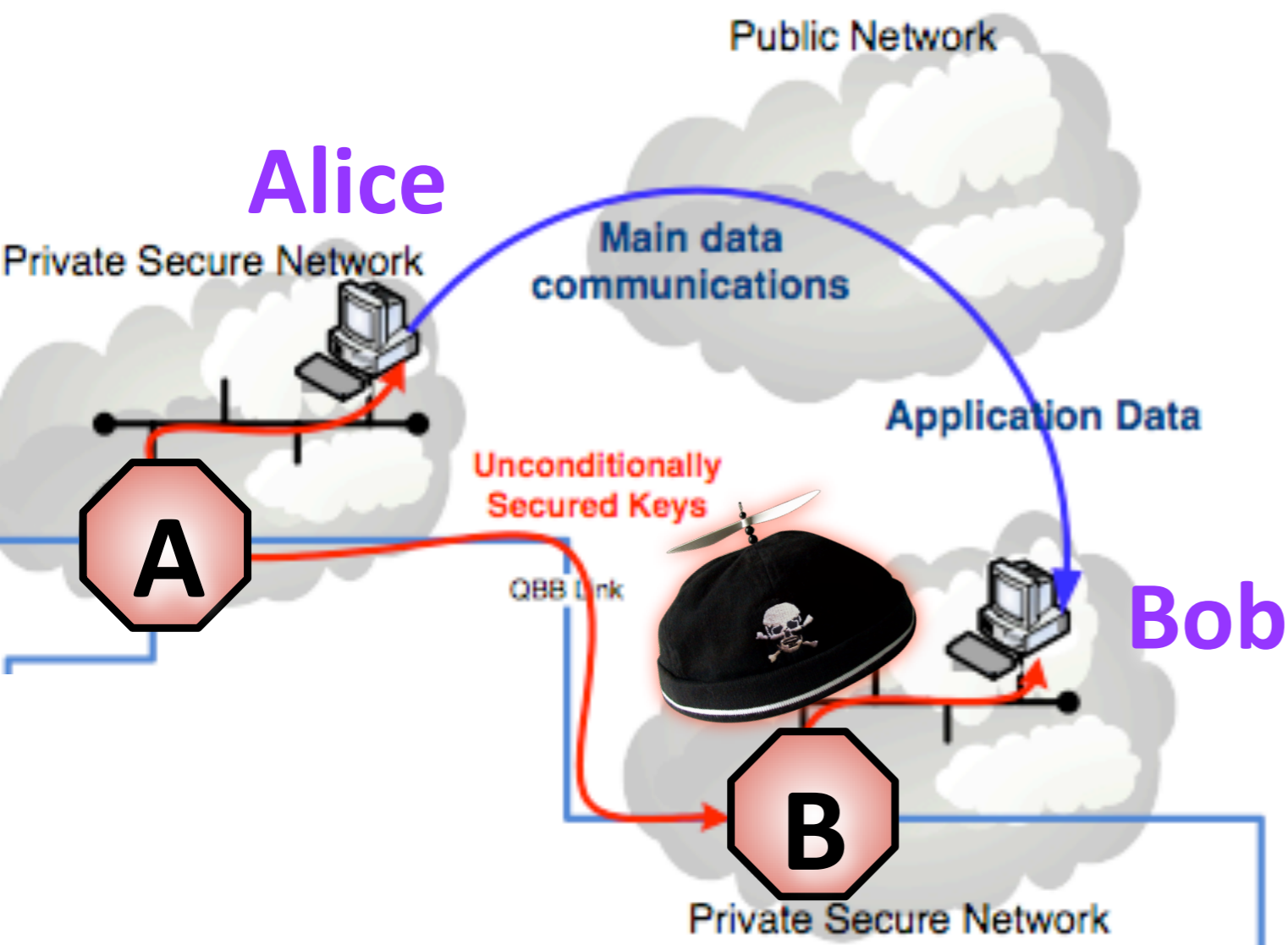
Alice and Bob exchange keys, with the assistance of the QKD back bone (Only the red link between A and B uses Quantum techniques). Alice and Bob use that key to encrypt application data which is sent over the public network.



➡ Can Alice and Bob trust the owners or administrators of their QKD nodes, today or tomorrow? When will they know if they have been compromised? What if the operator changes?

Expanding mesh QKD Back Bone with a LAN

Alice and Bob exchange keys, with the assistance of the QKD back bone (Only the red link between A and B uses Quantum techniques). Alice and Bob use that key to encrypt application data which is sent over the public network.



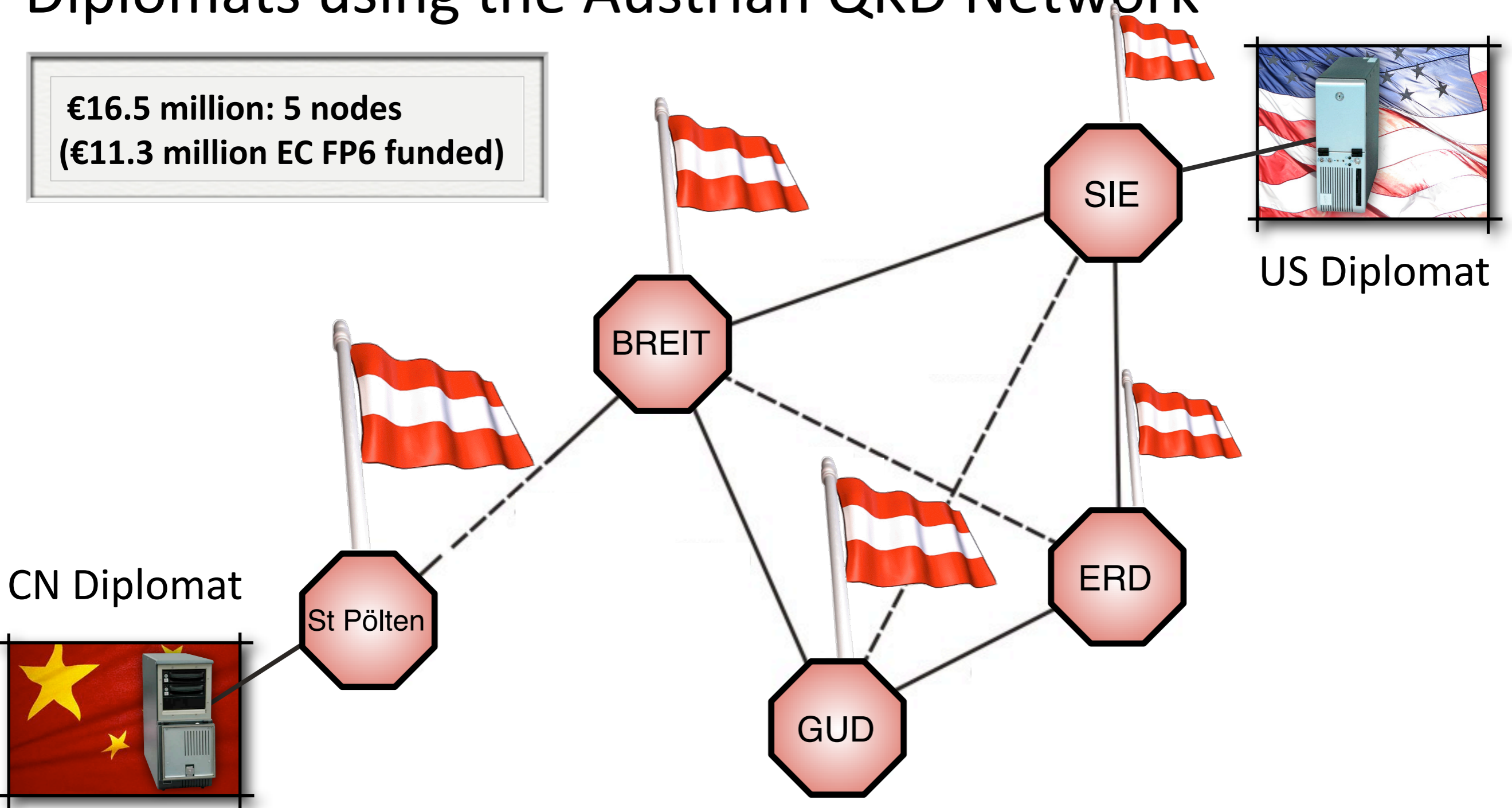
➡ Can Alice and Bob trust the owners or administrators of their QKD nodes, today or tomorrow? When will they know if they have been compromised? What if the operator changes?



A hypothetical case use study

Diplomats using the Austrian QKD Network

€16.5 million: 5 nodes
(€11.3 million EC FP6 funded)

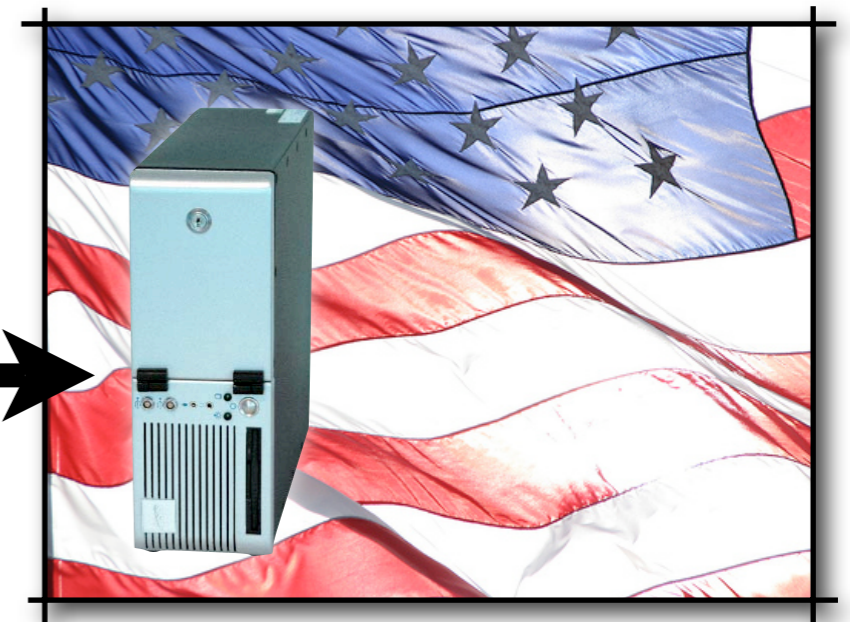


Are first generation Global QKD Networks possible?

Chinese Diplomat



American Diplomat



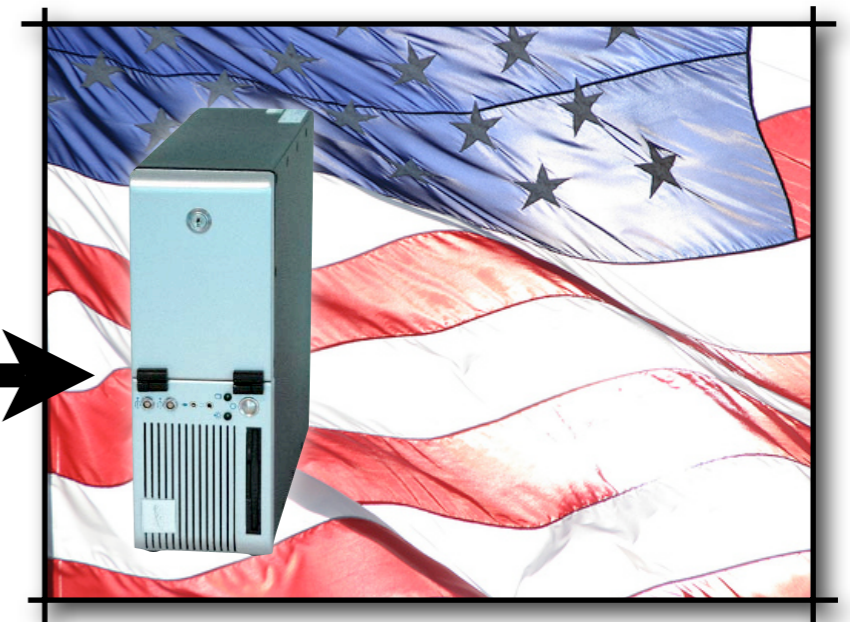


Are first generation Global QKD Networks possible?

Chinese Diplomat



American Diplomat

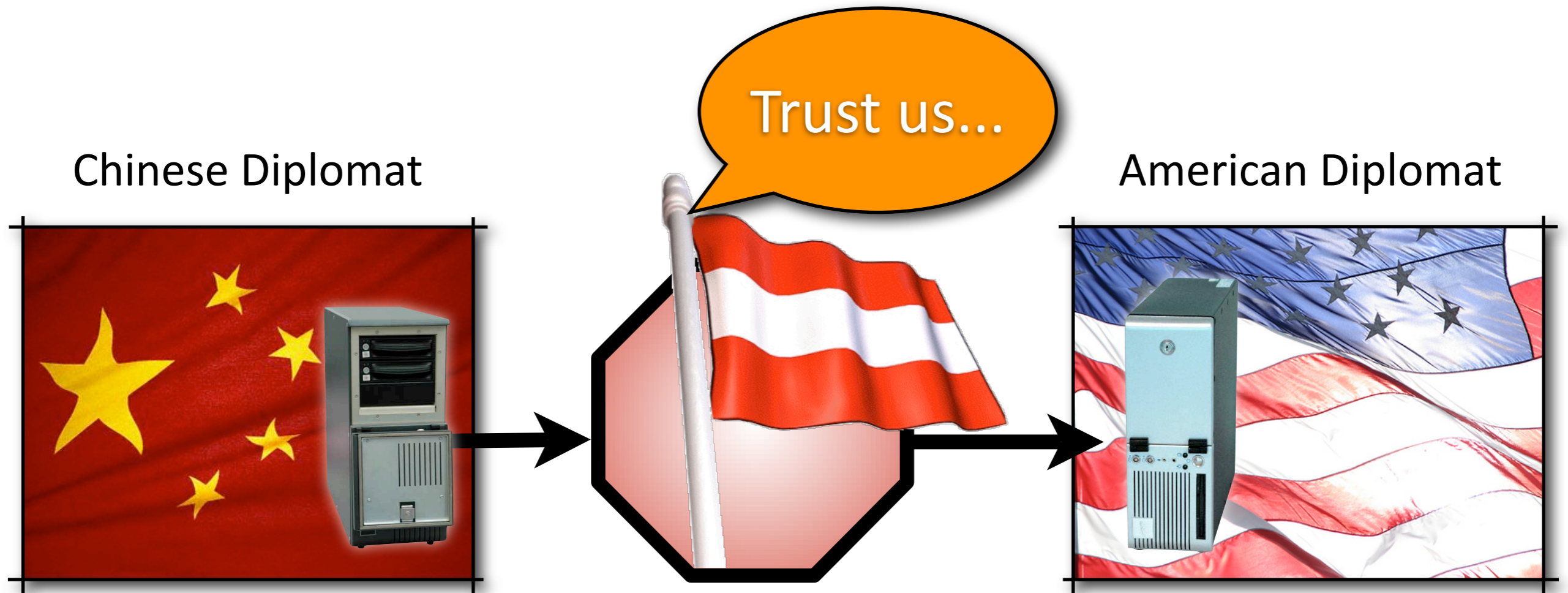


Trusting Vienna QKD Network would require
total trust in Austria AND its network operators





Are first generation Global QKD Networks possible?



Trusting Vienna QKD Network would require *total trust in Austria AND its network operators*





Lessons learned so far



Image: (c) Austrian Research Centers



Lessons learned so far

- ▶ We need to ensure that we protect devices against side-channel attacks, otherwise we undermine one of the core tenants of security

Image: (c) Austrian Research Centers



Lessons learned so far

- ➡ We need to ensure that we protect devices against side-channel attacks, otherwise we undermine one of the core tenants of security
- ➡ We need to ensure that all pre-shared keys are negotiated using a information-theoretic technique that is secure against insiders



Lessons learned so far

- We need to ensure that we protect devices against side-channel attacks, otherwise we undermine one of the core tenants of security
- We need to ensure that all pre-shared keys are negotiated using a information-theoretic technique that is secure against insiders
- Key distribution overlay networks
 - that map 1:1 against the underlying physical network topology become less secure as the size of the network grows



Lessons learned so far

- We need to ensure that we protect devices against side-channel attacks, otherwise we undermine one of the core tenants of security
- We need to ensure that all pre-shared keys are negotiated using a information-theoretic technique that is secure against insiders
- Key distribution overlay networks
 - that map 1:1 against the underlying physical network topology become less secure as the size of the network grows
 - cannot be trusted by users (outsiders) if all relays are controlled by one organisation, or if the relay ownership is irregular/uncontrolled



Lessons learned so far

- We need to ensure that we protect devices against side-channel attacks, otherwise we undermine one of the core tenants of security
- We need to ensure that all pre-shared keys are negotiated using a information-theoretic technique that is secure against insiders
- Key distribution overlay networks
 - that map 1:1 against the underlying physical network topology become less secure as the size of the network grows
 - cannot be trusted by users (outsiders) if all relays are controlled by one organisation, or if the relay ownership is irregular/uncontrolled
- We must prevent against single-point-of-trust-failure, and ensure end-to-end redundancy reaches all the way to the end user (token)

Image: (c) Austrian Research Centers



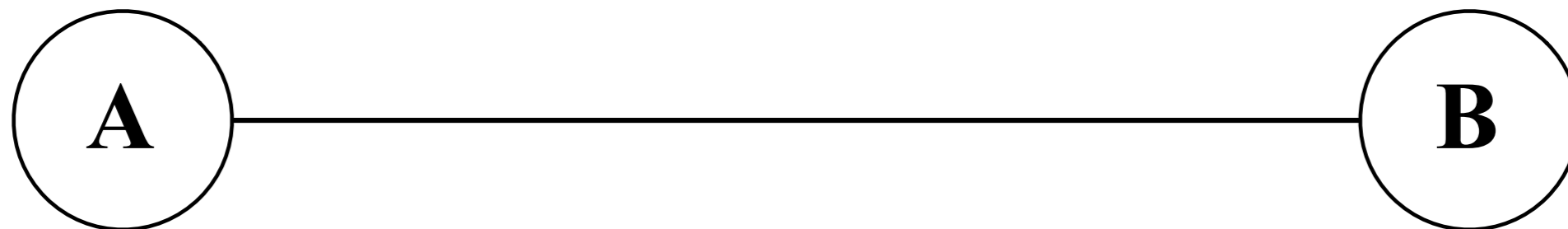
Kerberos

Symmetric Key Distribution for Identity Management
WITH integrated Cryptographic Key Management



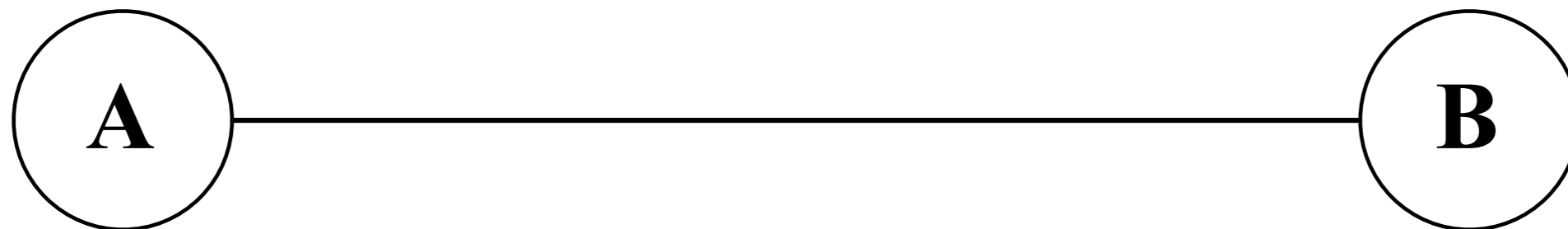


Kerberos 4 (1980)



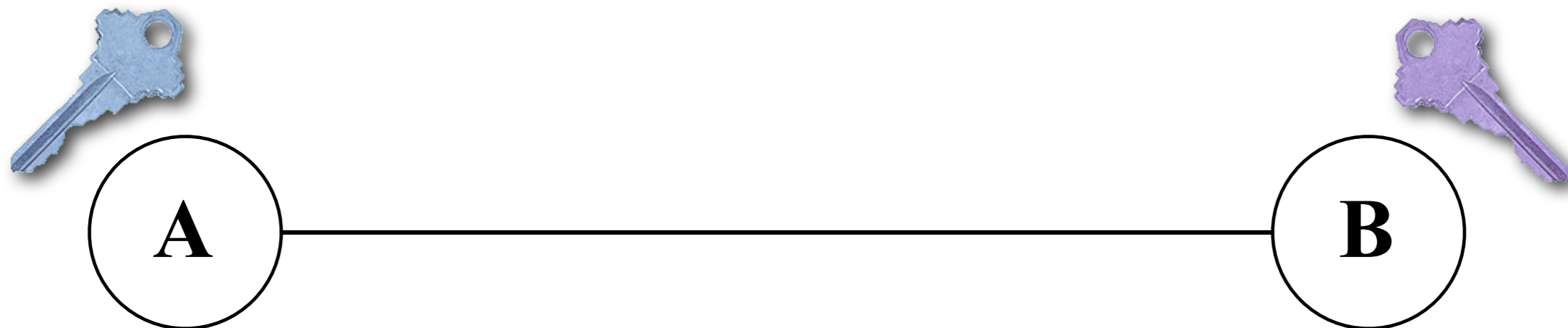
Kerberos 4 (1980)

➡ Based on techniques by Branstad 1973 and Needham-Schroeder 1978:



Kerberos 4 (1980)

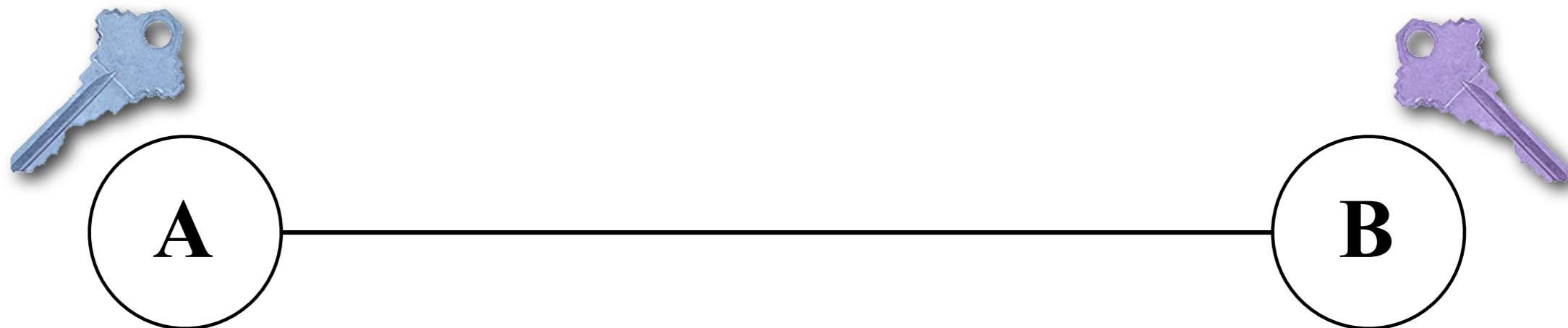
➡ Based on techniques by Branstad 1973 and Needham-Schroeder 1978:



➡ User A and Server B have not met and share no common secrets

Kerberos 4 (1980)

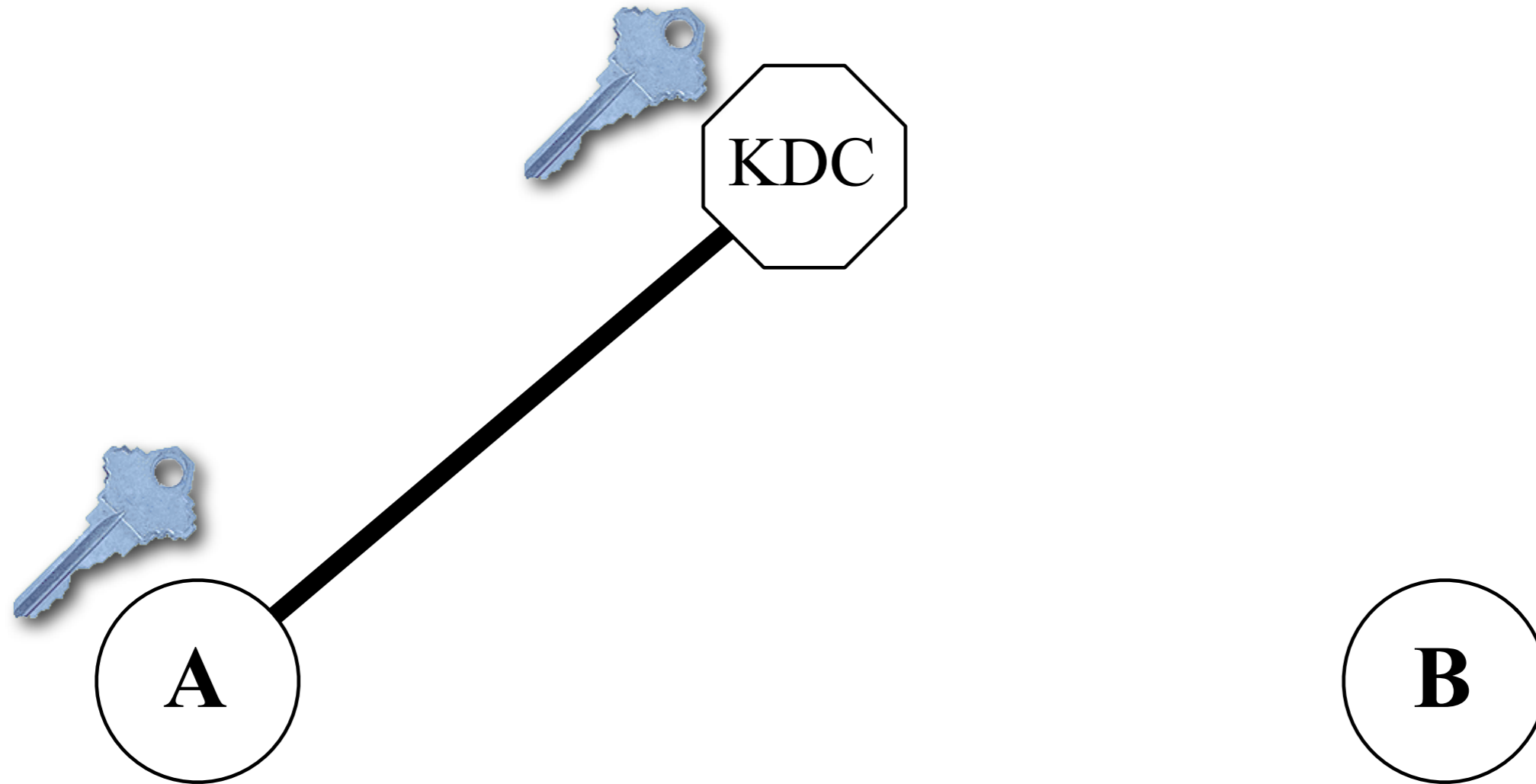
➡ Based on techniques by Branstad 1973 and Needham-Schroeder 1978:



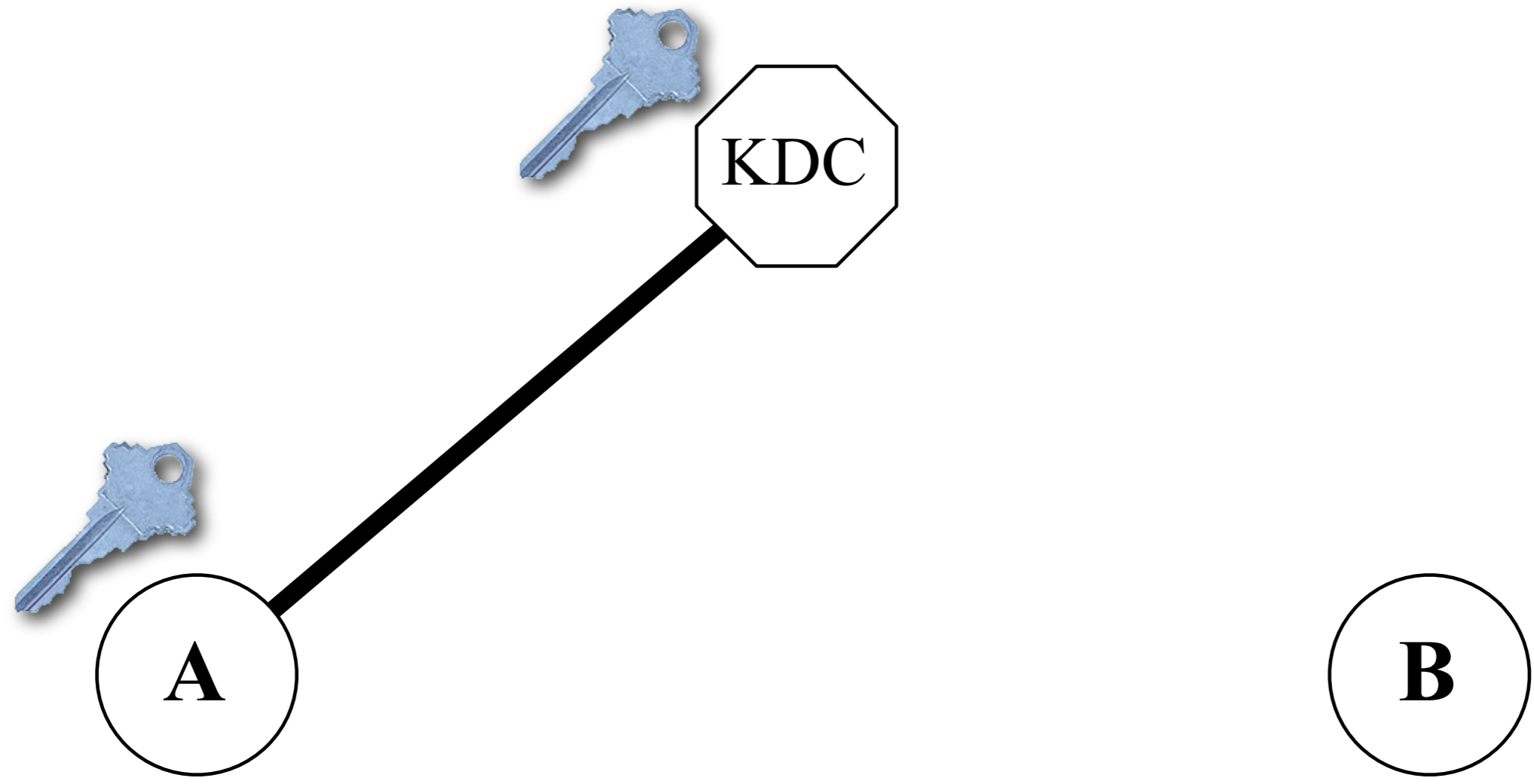
➡ User A and Server B have not met and share no common secrets

➡ User A wants secure mutual authenticated communications with Server B

Kerberos 4 (1980)



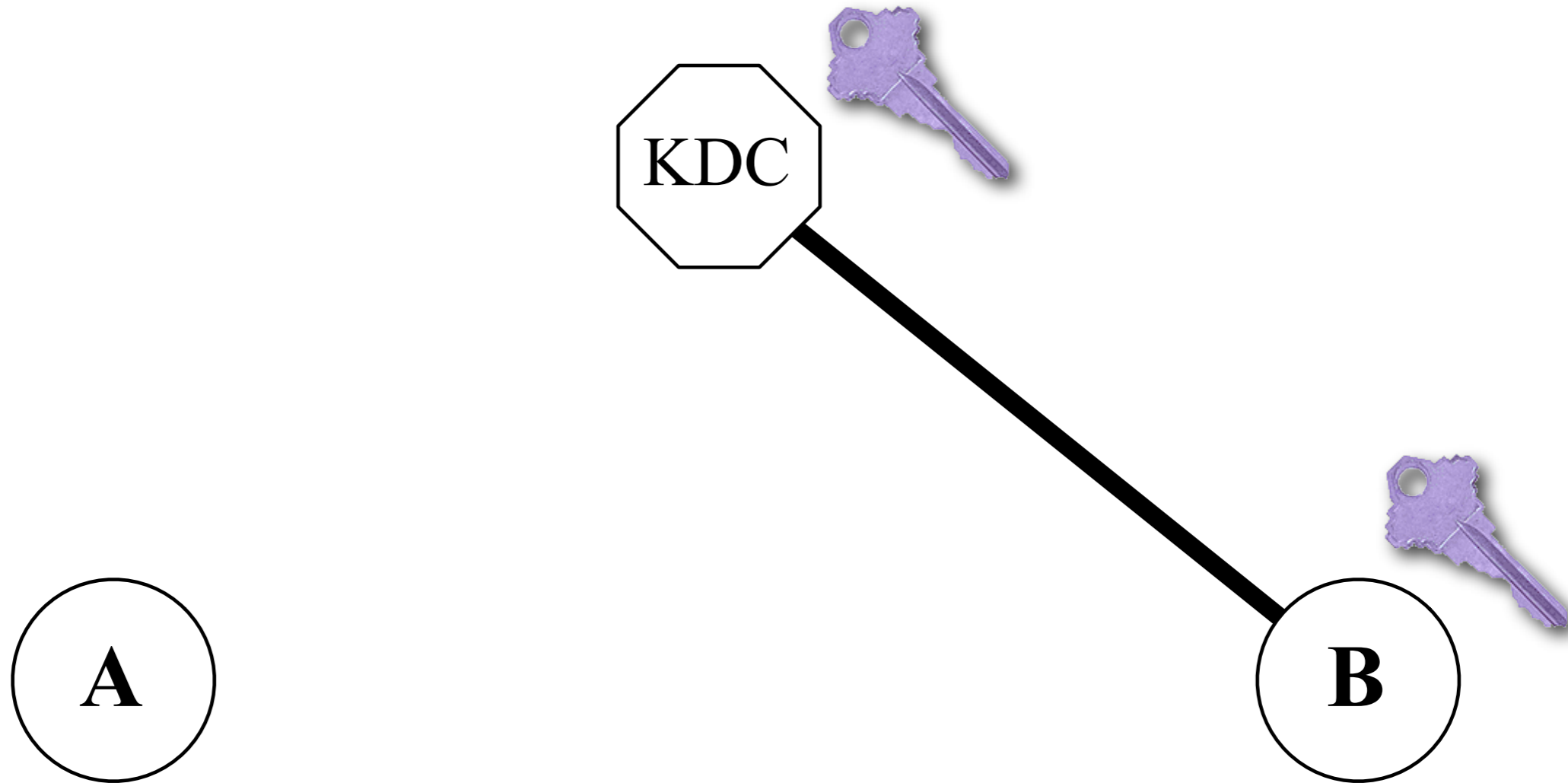
Kerberos 4 (1980)



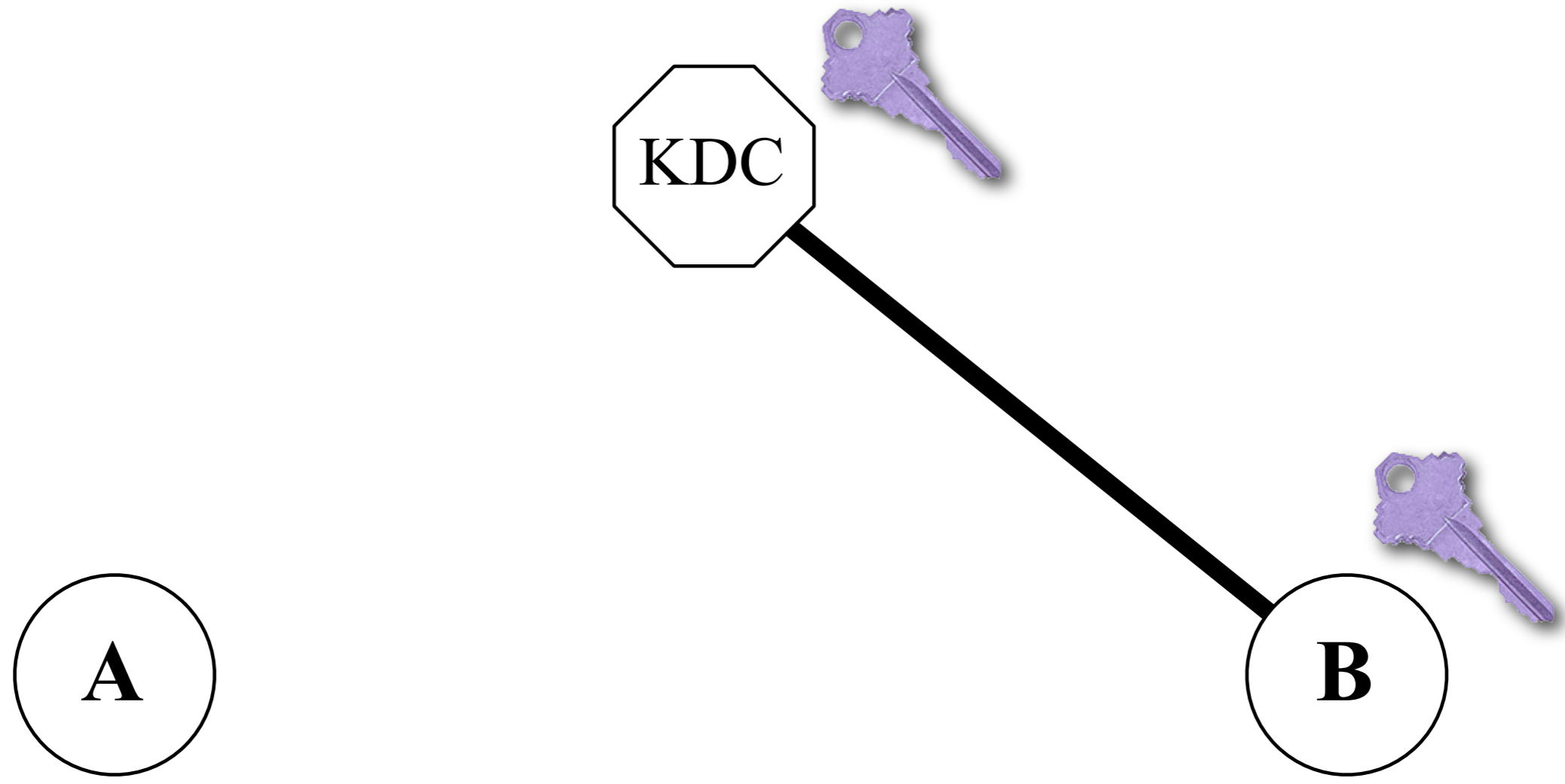
- User A shares a pairwise unique secret (a secret password) with a key distribution center (KDC).



Kerberos 4 (1980)



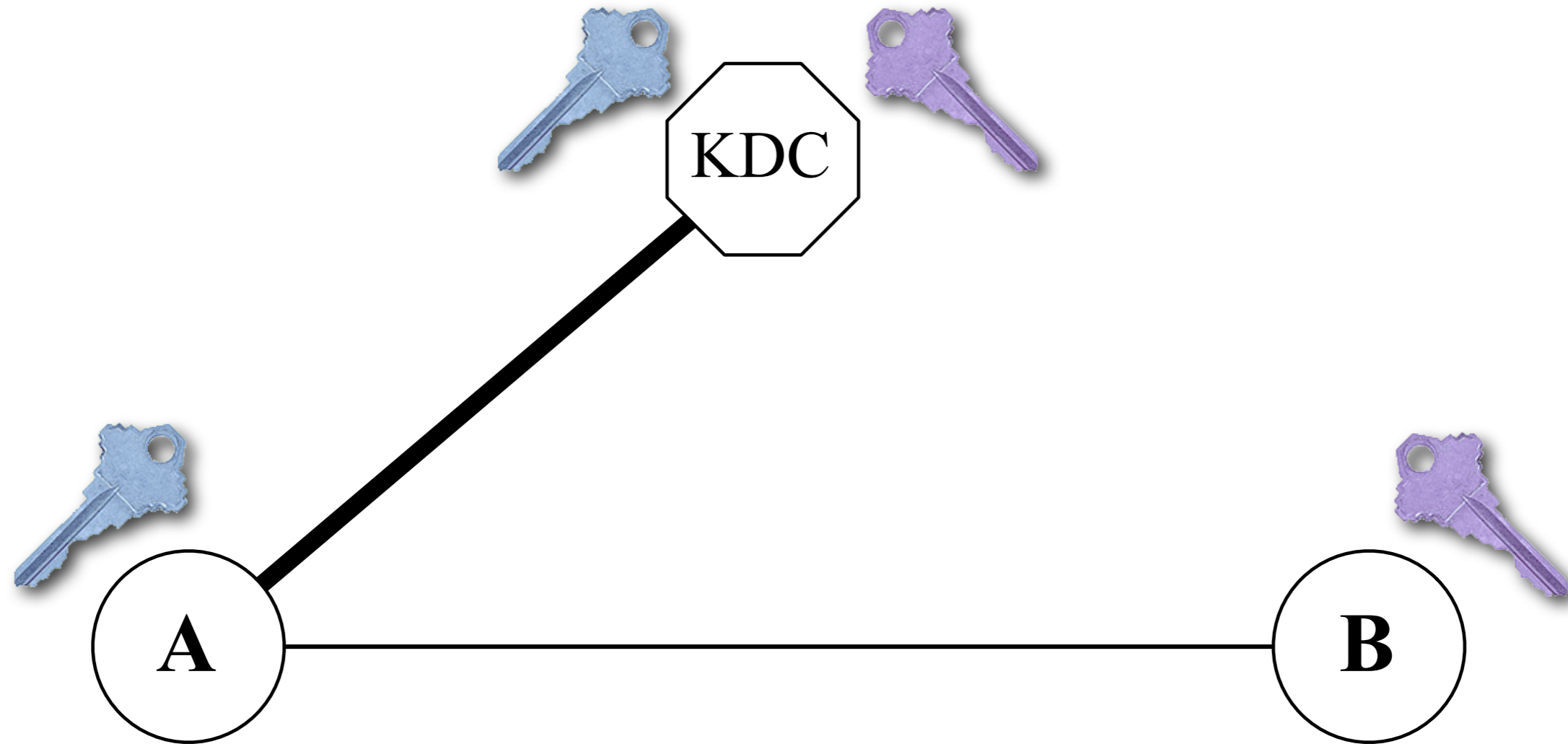
Kerberos 4 (1980)



- Server B shares a different pairwise unique pre-shared-key (password) with the same key distribution center

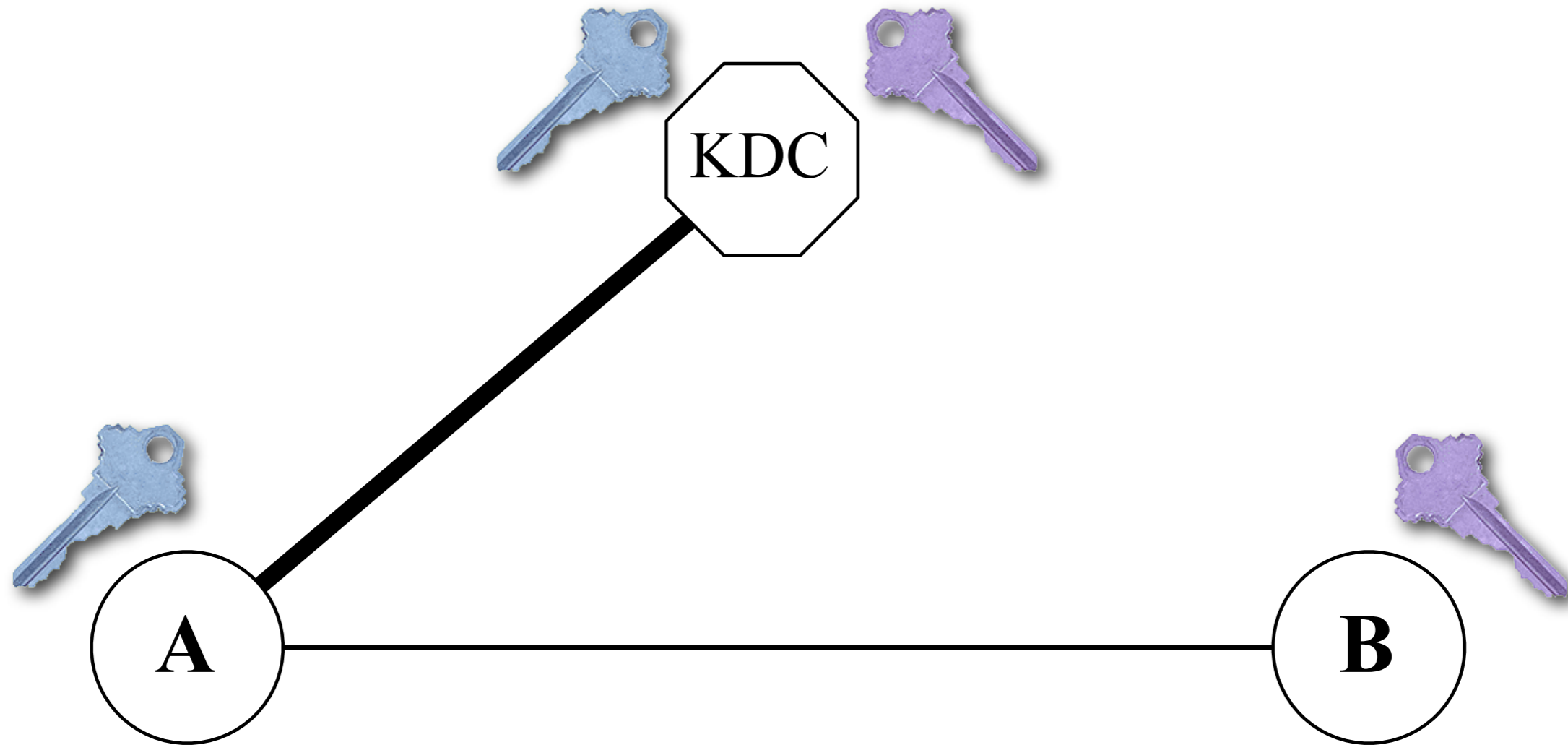


Kerberos 4 (1980)





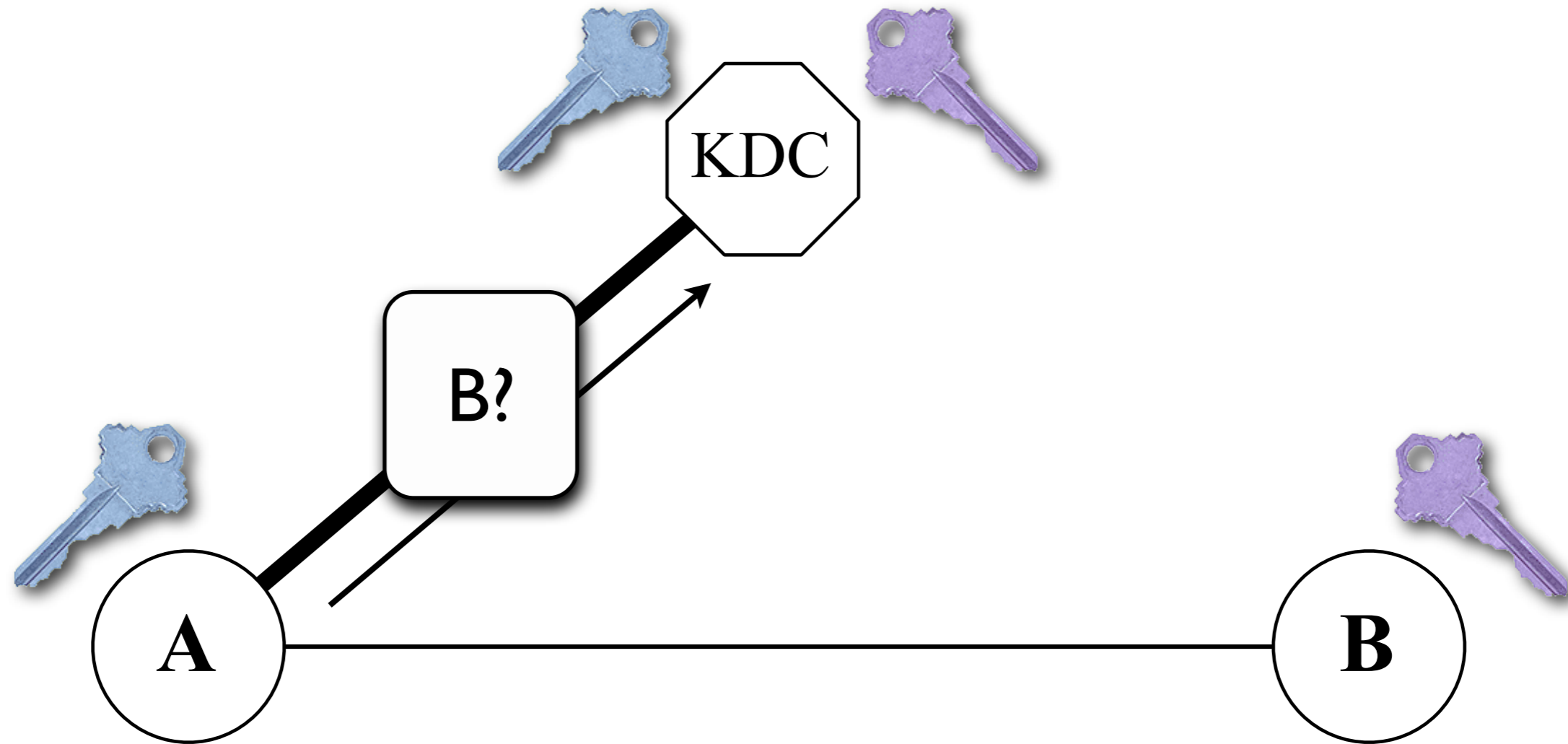
Kerberos 4 (1980)



➡ The Key Distribution Center acts as an introduction service



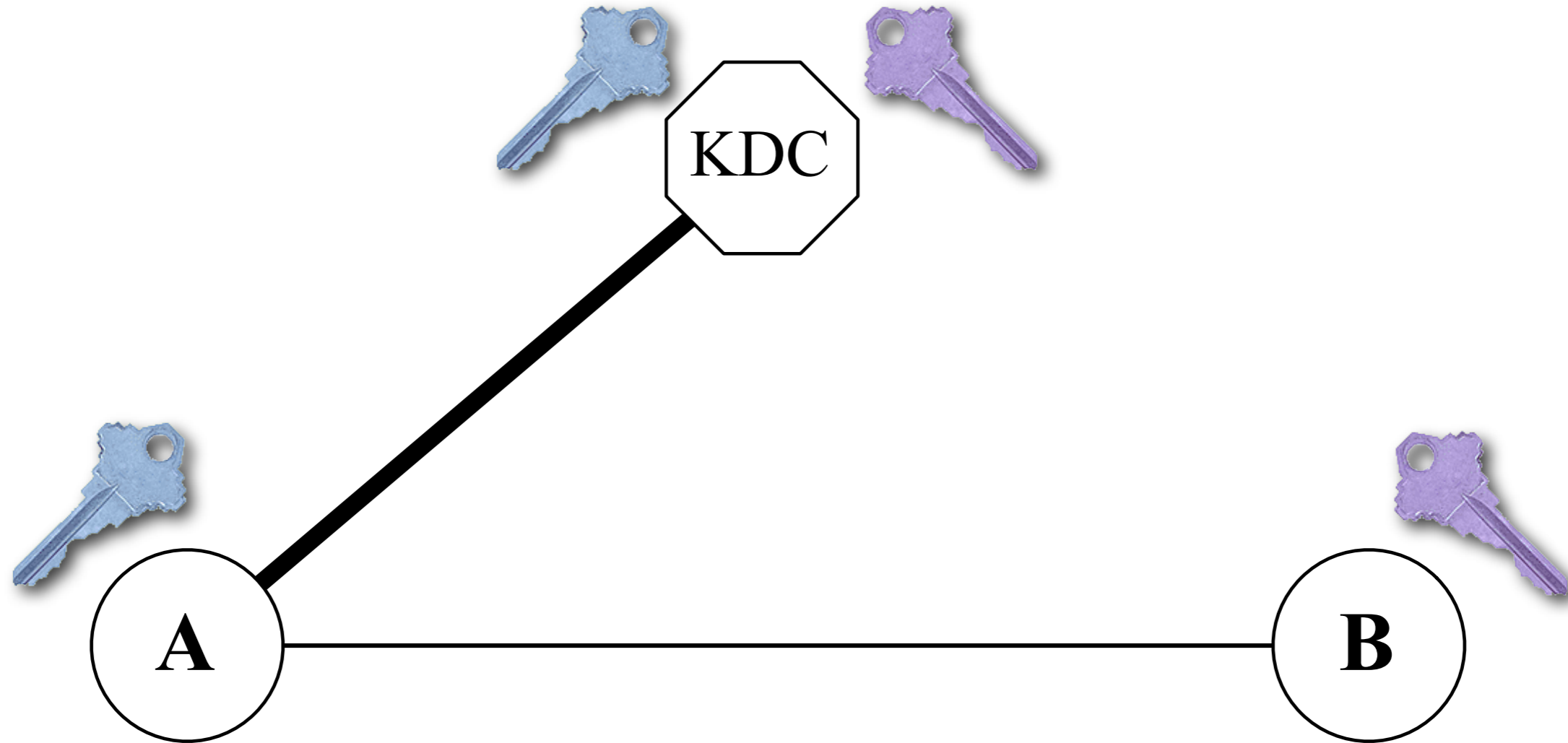
Kerberos 4 (1980)



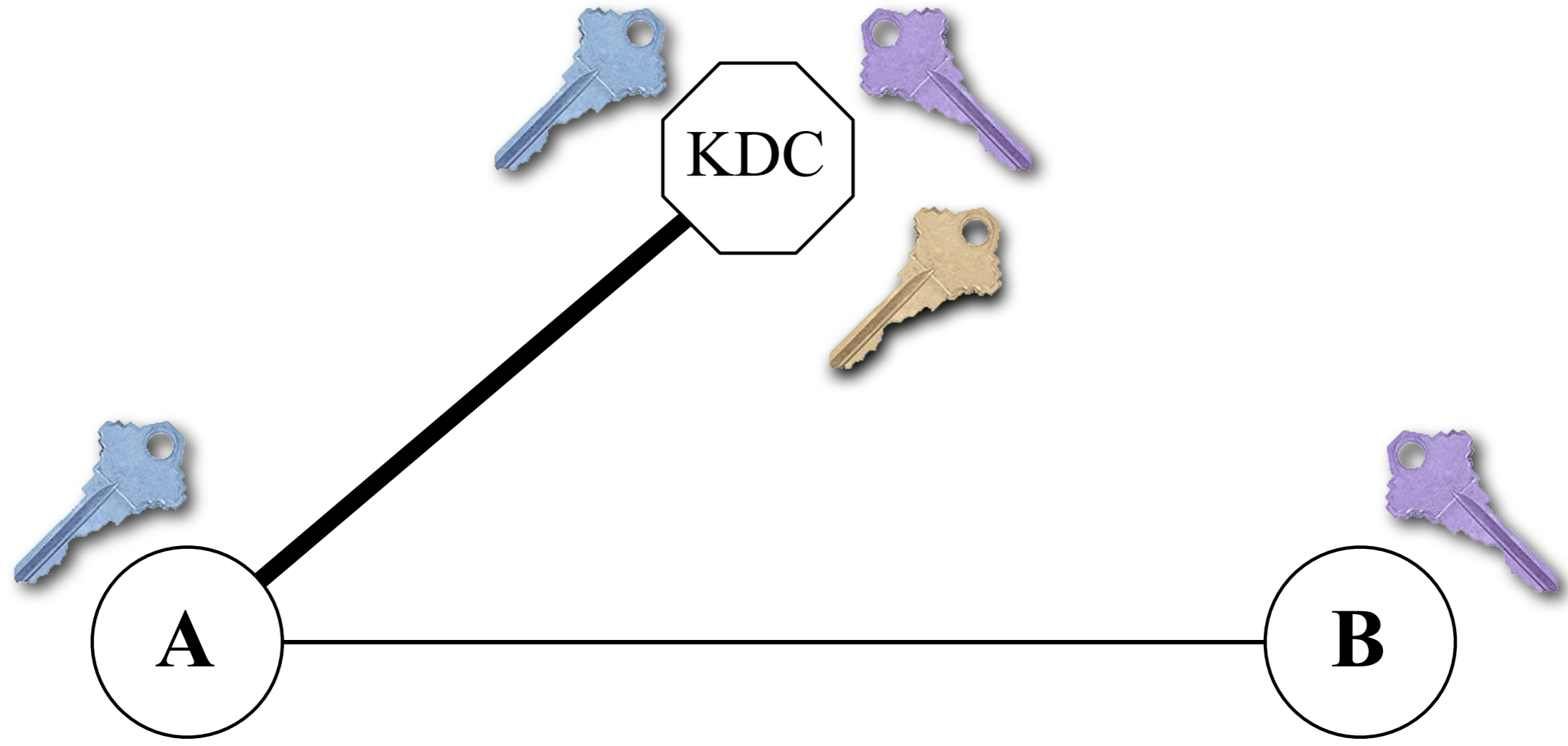
- **The Key Distribution Center acts as an introduction service**
- **User A sends a cleartext request to be introduced to Server B**



Kerberos 4 (1980)



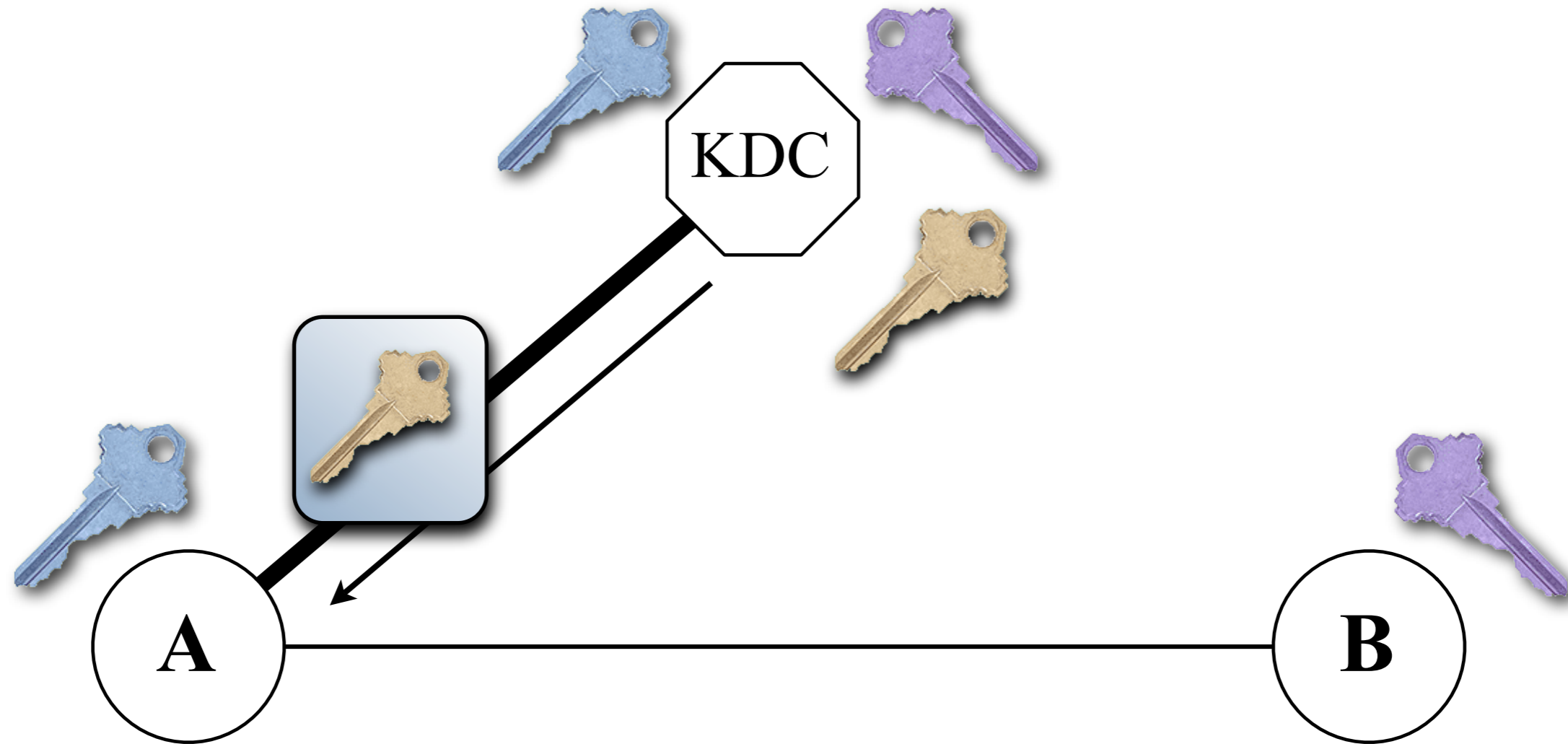
Kerberos 4 (1980)



➡ Server B generates a fresh nonce (random number)



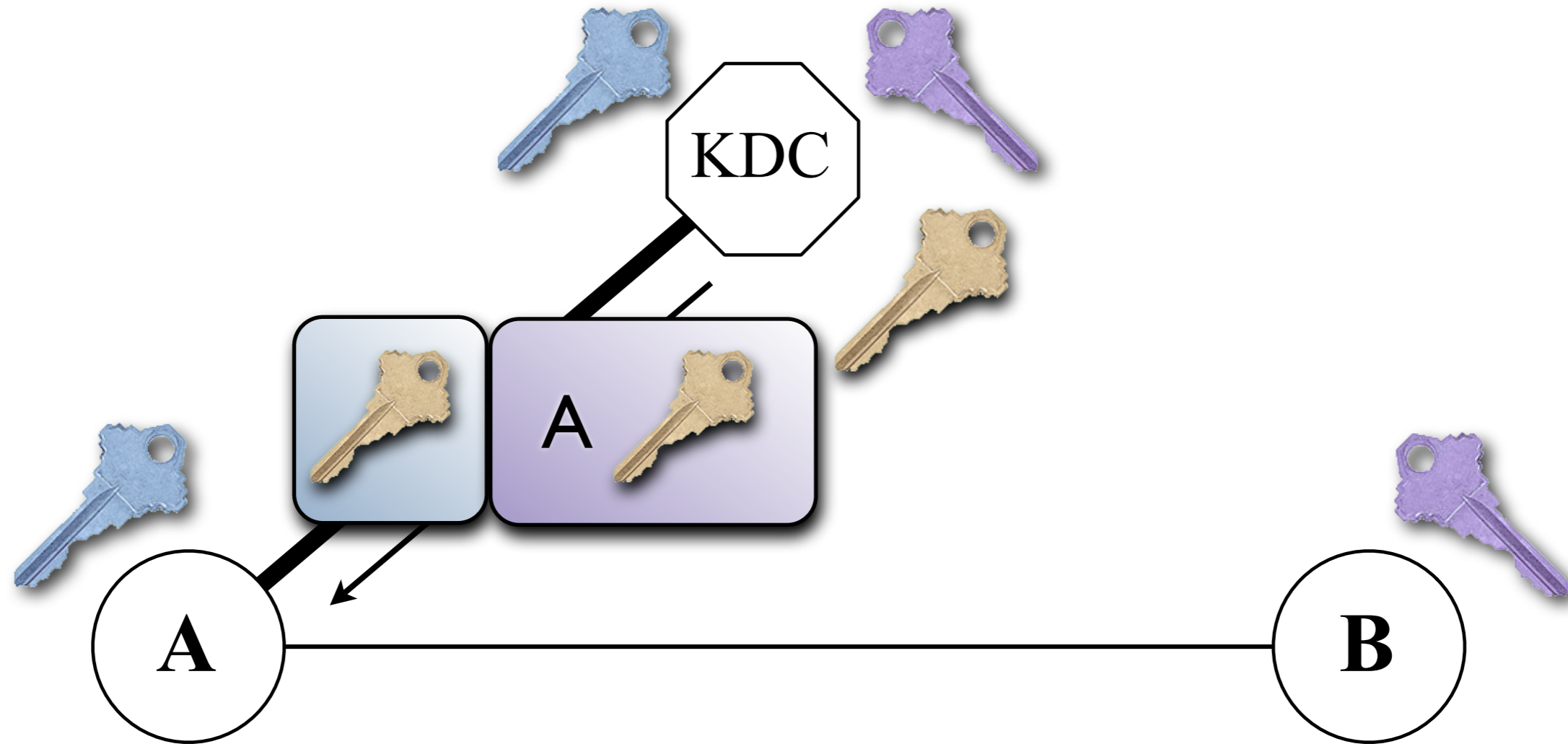
Kerberos 4 (1980)



- ➡ Server B generates a fresh nonce (random number)
- ➡ Server B encrypts that nonce and sends to User A



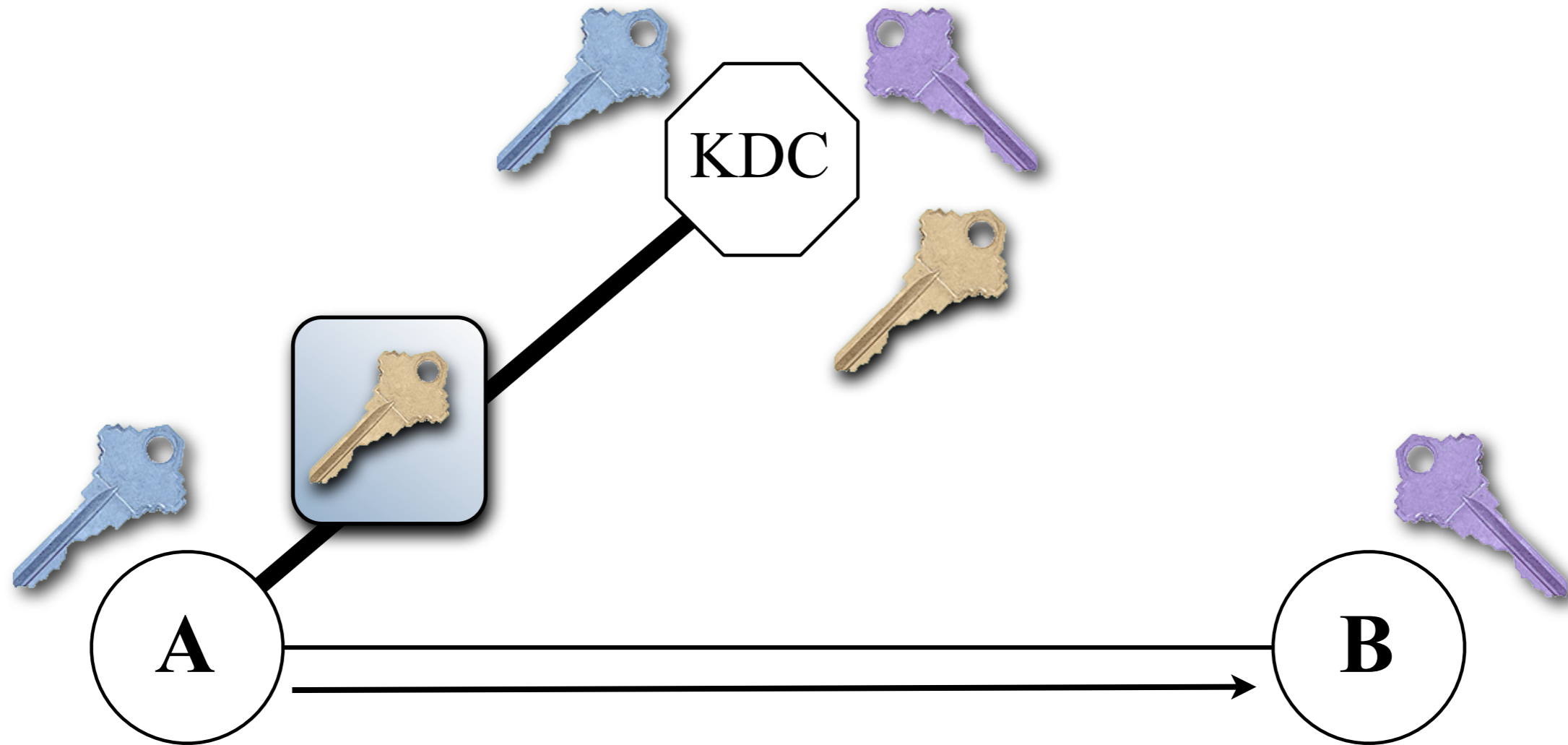
Kerberos 4 (1980)



- ➡ Server B generates a fresh nonce (random number)
- ➡ Server B encrypts that nonce and sends to User A
- ➡ Server B encrypts the same nonce along with ID of User A for Server B

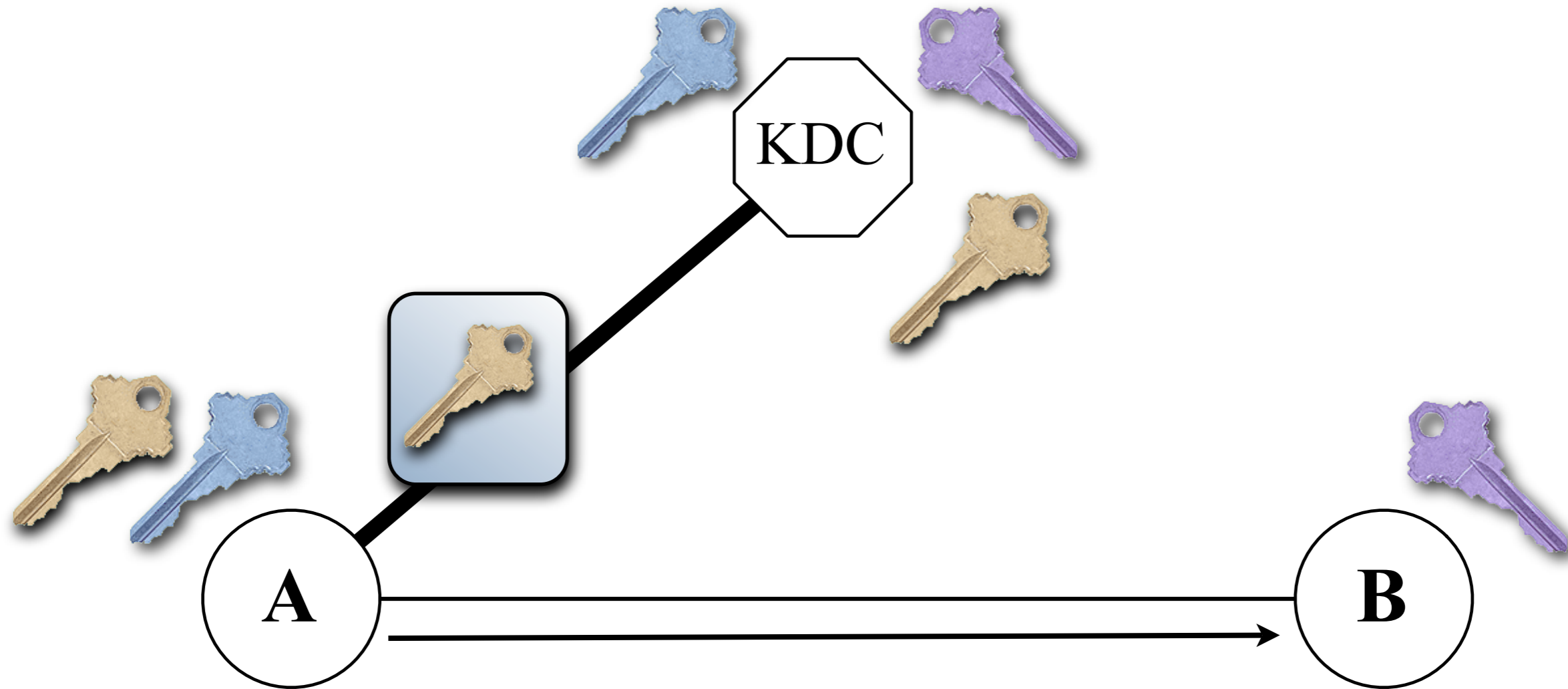


Kerberos 4 (1980)





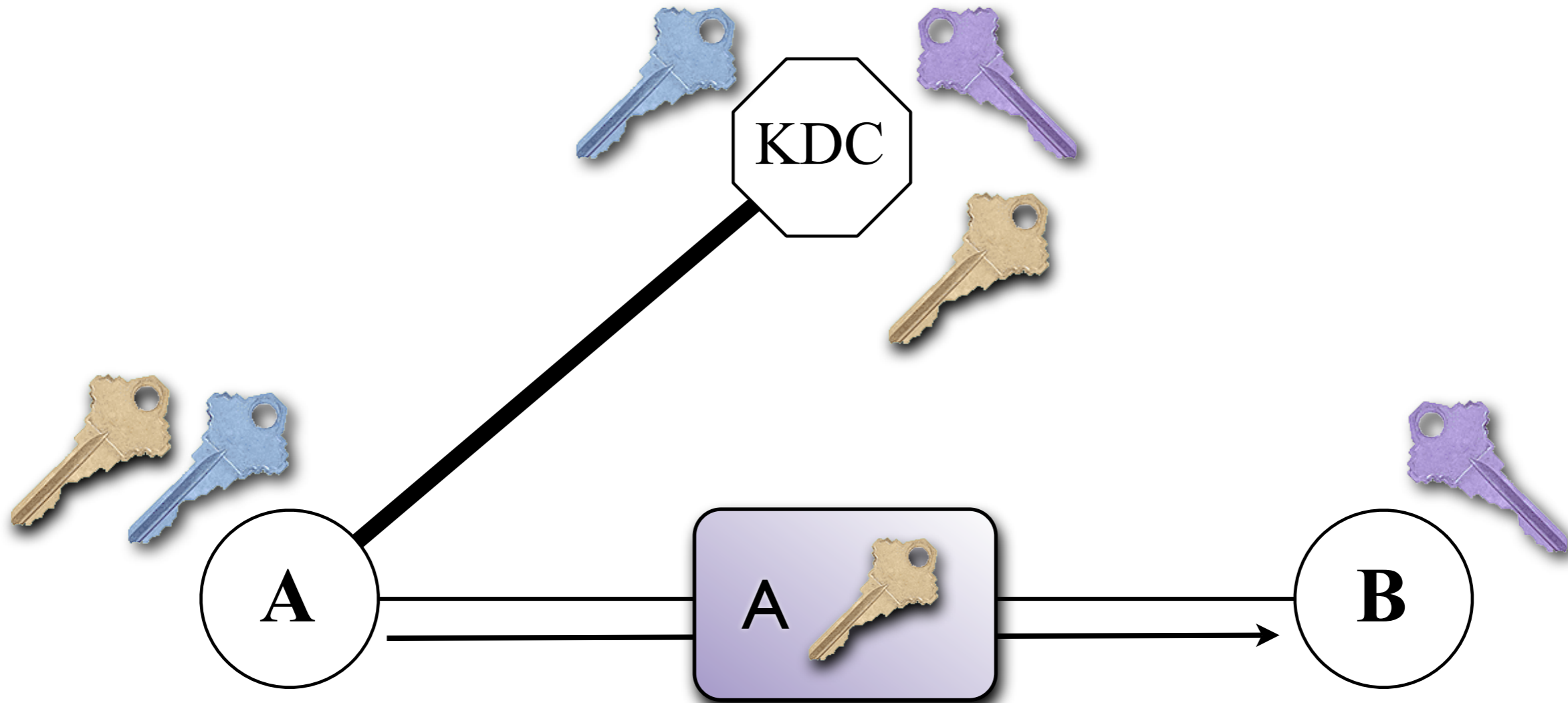
Kerberos 4 (1980)



➡ User A decrypts the encrypted session key using it's key with KDC



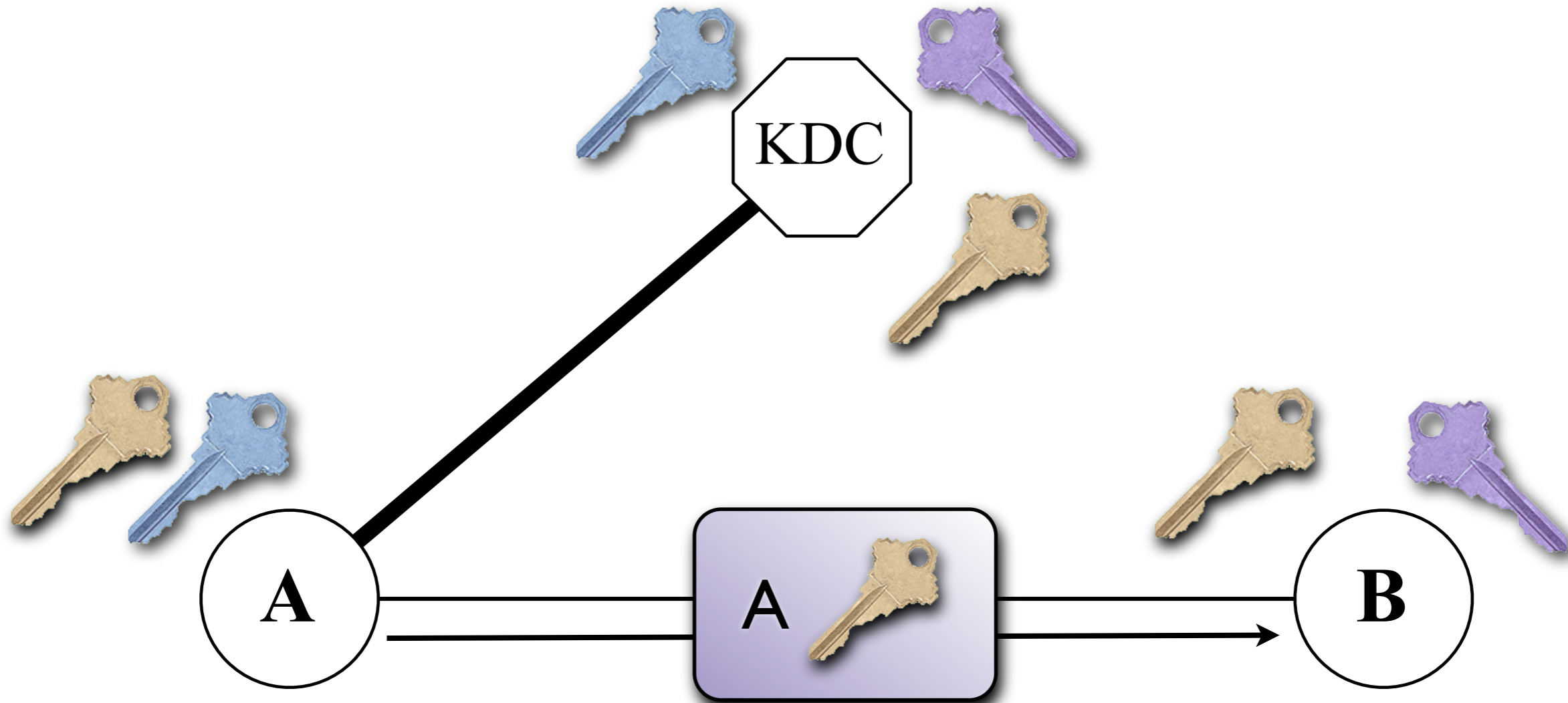
Kerberos 4 (1980)



- ➡ User A decrypts the encrypted session key using it's key with KDC
- ➡ User A forwards the encrypted session key to Server B



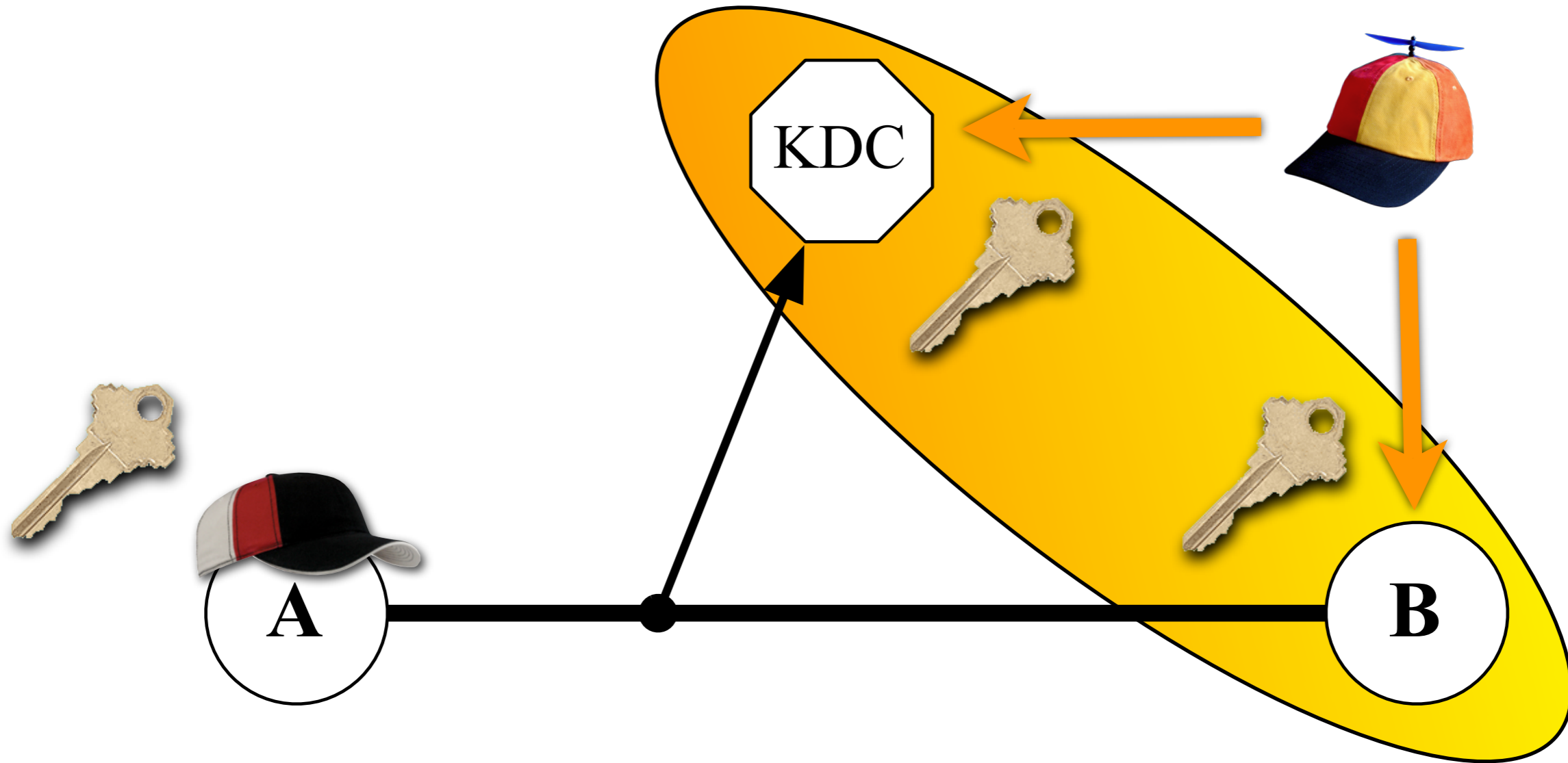
Kerberos 4 (1980)



- ➡ User A decrypts the encrypted session key using it's key with KDC
- ➡ User A forwards the encrypted session key to Server B
- ➡ Server B decrypts the message, receives identity of A and session key

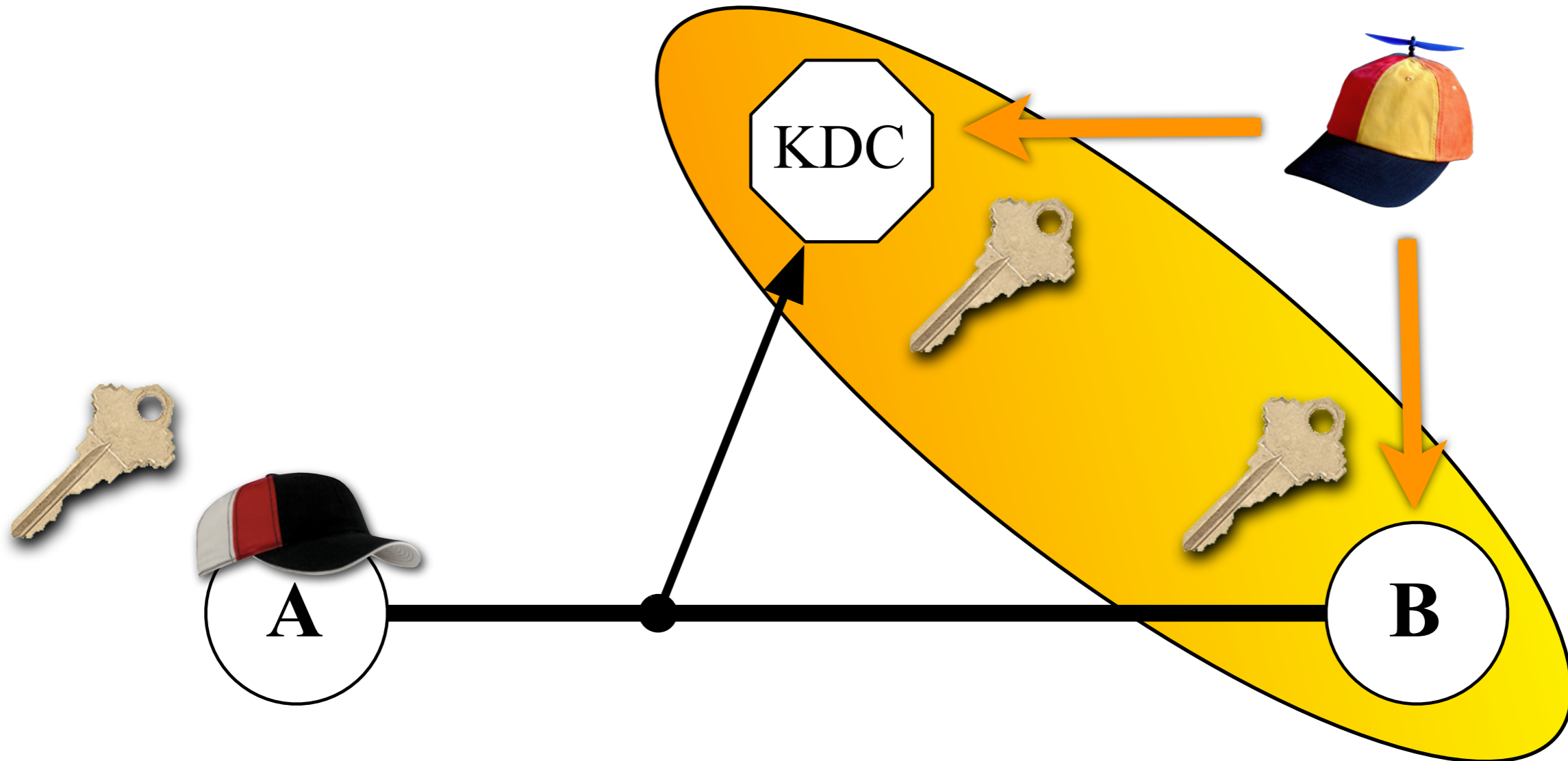


Kerberos 4 (1980)





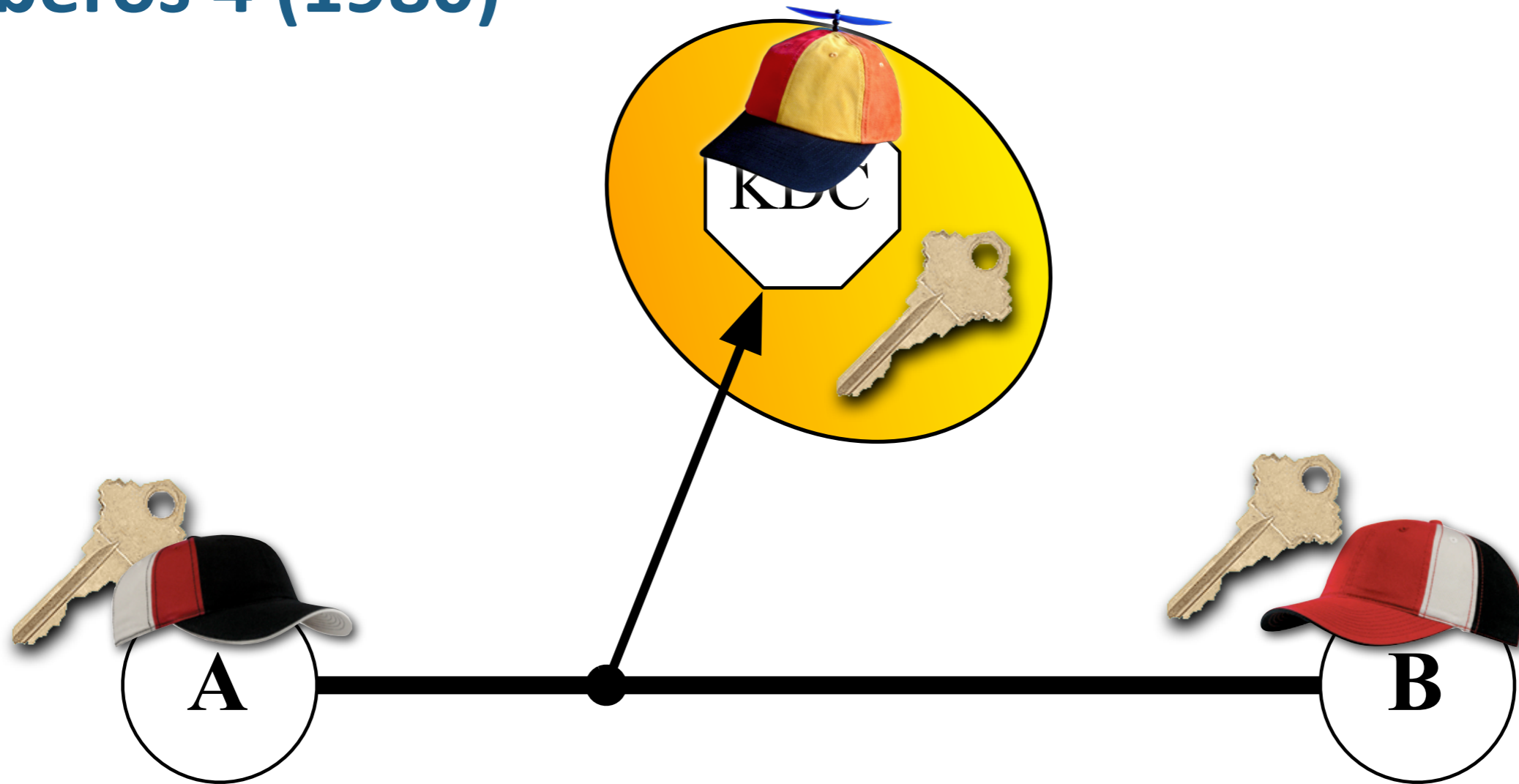
Kerberos 4 (1980)



- Kerberos assumes that the KDC Authentication Server and Server B are managed by the same organisation. In this context, User A and Server B achieve secure authenticated communications.

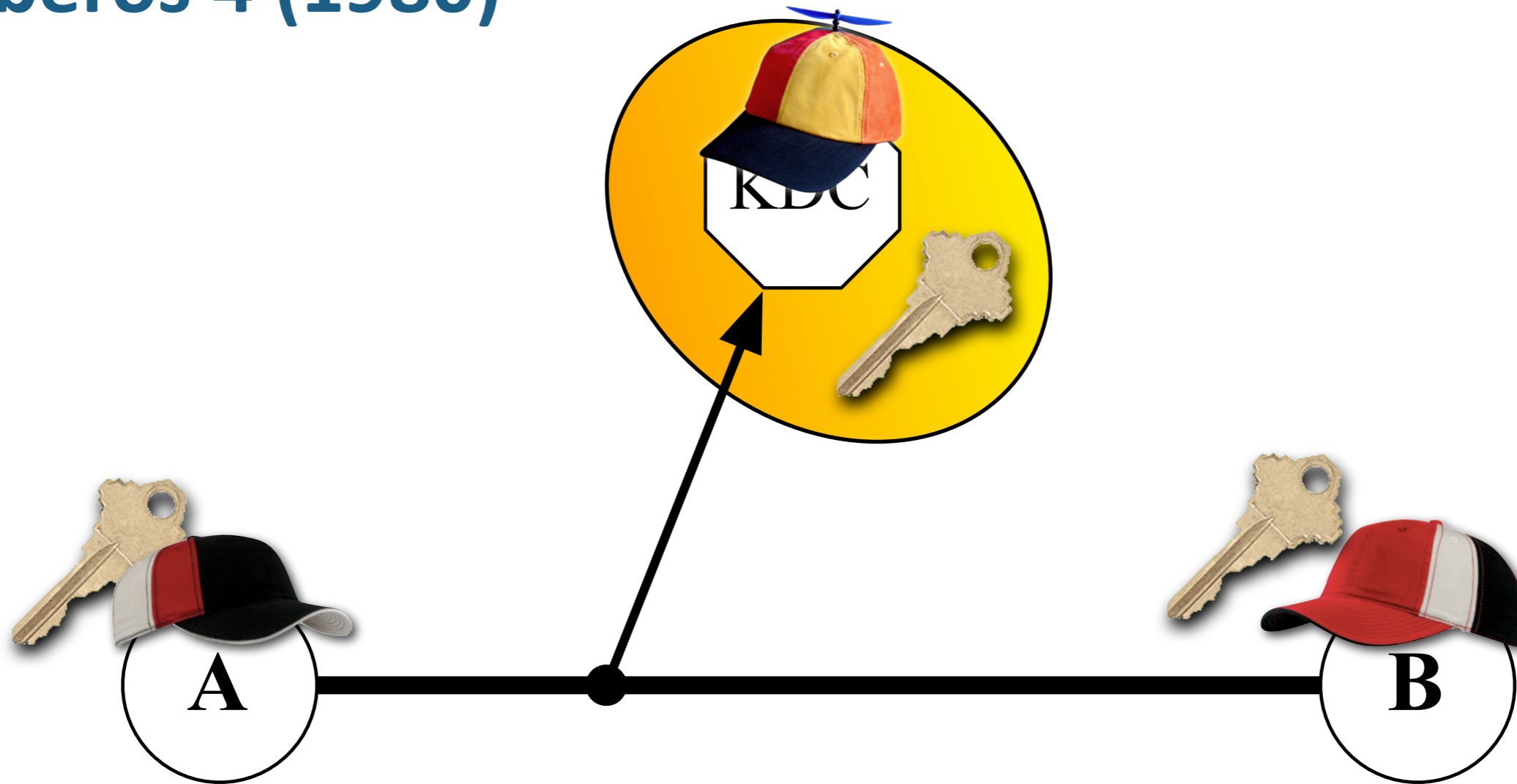


Kerberos 4 (1980)





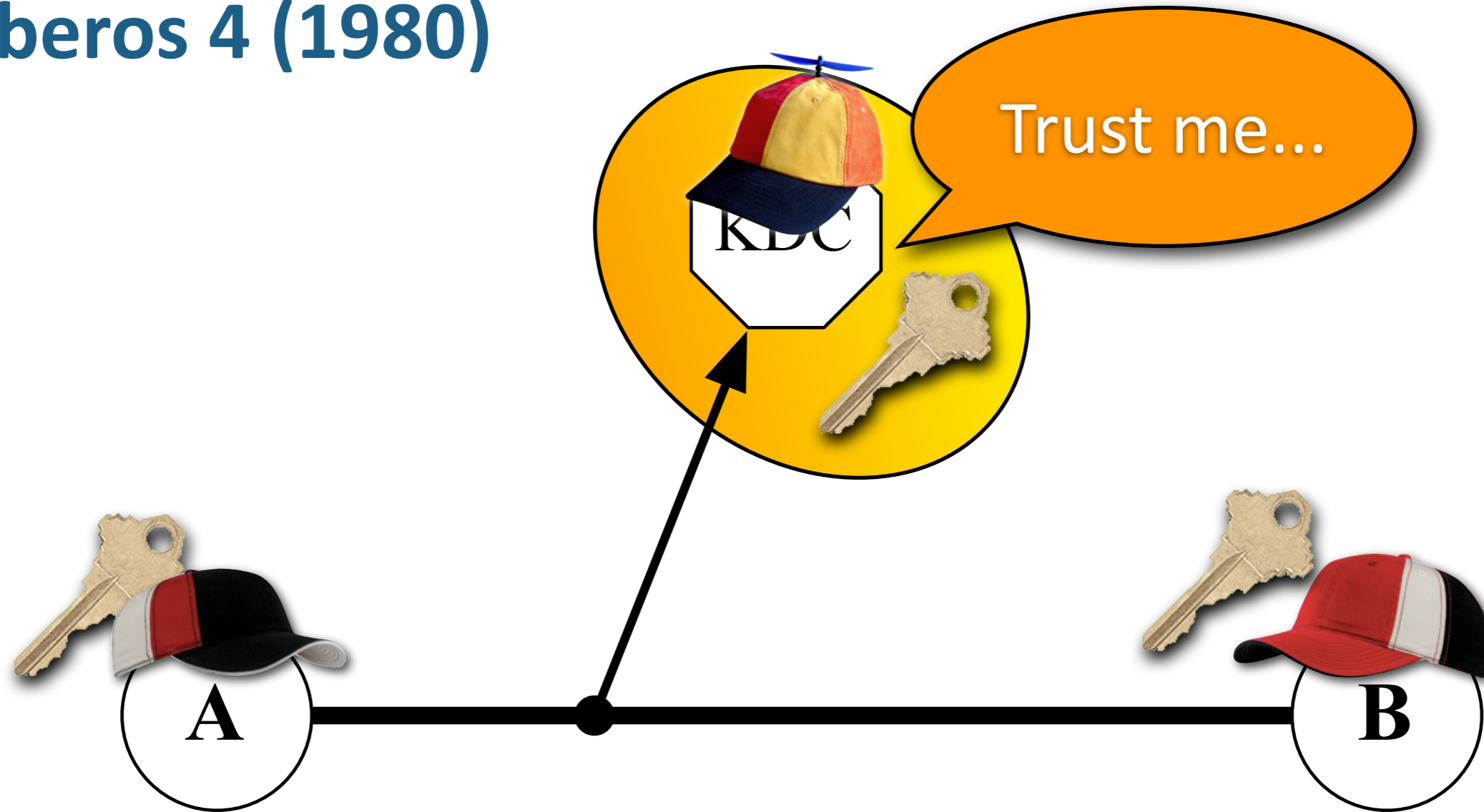
Kerberos 4 (1980)



- However it is not intended or suitable for applications where the KDC Authentication Server is under different control to user A and user B



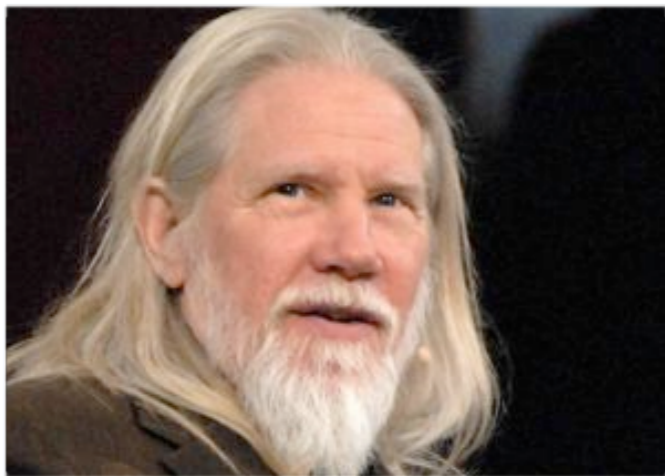
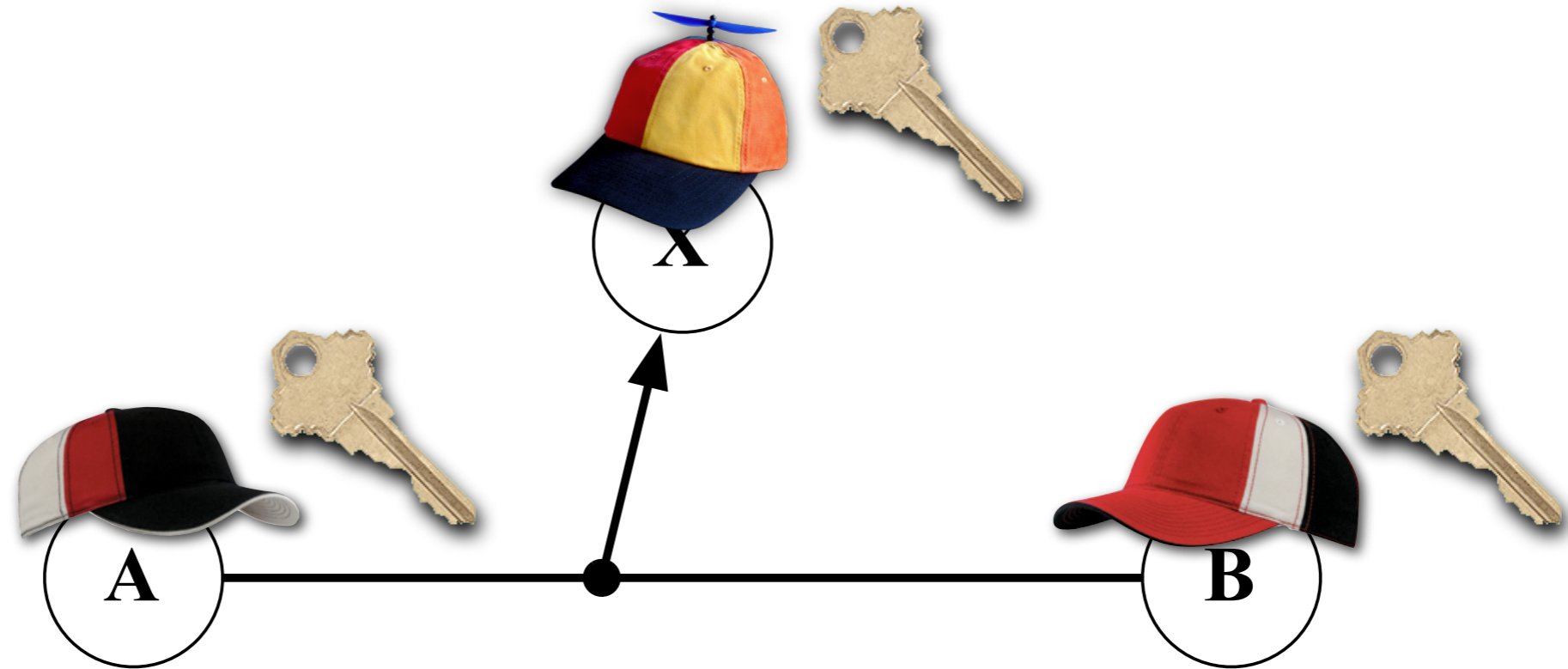
Kerberos 4 (1980)



- However it is not intended or suitable for applications where the KDC Authentication Server is under different control to user A and user B



Kerberos 4 (1980)



“(ed. In the 1970’s) I could not understand the (ed. sense of) cryptography in which more than two people (ed. *the two end users*) knew the key”

- Whitfield DIFFIE (2006)
Co-inventor of public key crypto

Kerberos 4 (1980) - Pros and Cons

Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'

Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'
- ✓ Key Distribution Center can introduce all agents within a system

Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'
- ✓ Key Distribution Center can introduce all agents within a system
- ✓ Always the freshest key material and identity assertions!



Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'
- ✓ Key Distribution Center can introduce all agents within a system
- ✓ Always the freshest key material and identity assertions!
- ✓ Network communications overhead is upper bound



Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'
- ✓ Key Distribution Center can introduce all agents within a system
- ✓ Always the freshest key material and identity assertions!
- ✓ Network communications overhead is upper bound
- ✓ Works over all networks types

Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'
- ✓ Key Distribution Center can introduce all agents within a system
- ✓ Always the freshest key material and identity assertions!
- ✓ Network communications overhead is upper bound
- ✓ Works over all networks types
- ✗ Relies on simple {Username, Passwords} (not post quantum secure)



Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'
- ✓ Key Distribution Center can introduce all agents within a system
- ✓ Always the freshest key material and identity assertions!
- ✓ Network communications overhead is upper bound
- ✓ Works over all networks types
- ✗ Relies on simple {Username, Passwords} (not post quantum secure)
- ✗ Server(s) can perform identity fraud



Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'
- ✓ Key Distribution Center can introduce all agents within a system
- ✓ Always the freshest key material and identity assertions!
- ✓ Network communications overhead is upper bound
- ✓ Works over all networks types
- ✗ Relies on simple {Username, Passwords} (not post quantum secure)
- ✗ Server(s) can perform identity fraud
- ✗ Server(s) can listen into, and corrupt, communications between users



Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'
- ✓ Key Distribution Center can introduce all agents within a system
- ✓ Always the freshest key material and identity assertions!
- ✓ Network communications overhead is upper bound
- ✓ Works over all networks types
- ✗ Relies on simple {Username, Passwords} (not post quantum secure)
- ✗ Server(s) can perform identity fraud
- ✗ Server(s) can listen into, and corrupt, communications between users
- ✗ Problems with availability (replication is a partial solution)



Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'
- ✓ Key Distribution Center can introduce all agents within a system
- ✓ Always the freshest key material and identity assertions!
- ✓ Network communications overhead is upper bound
- ✓ Works over all networks types
- ✗ Relies on simple {Username, Passwords} (not post quantum secure)
- ✗ Server(s) can perform identity fraud
- ✗ Server(s) can listen into, and corrupt, communications between users
- ✗ Problems with availability (replication is a partial solution)
- ✗ We have to trust the system administrators/management



Kerberos 4 (1980) - Pros and Cons

- ✓ Upper bound number of 'trusted actors'
- ✓ Key Distribution Center can introduce all agents within a system
- ✓ Always the freshest key material and identity assertions!
- ✓ Network communications overhead is upper bound
- ✓ Works over all networks types
- ✗ Relies on simple {Username, Passwords} (not post quantum secure)
- ✗ Server(s) can perform identity fraud
- ✗ Server(s) can listen into, and corrupt, communications between users
- ✗ Problems with availability (replication is a partial solution)
- ✗ We have to trust the system administrators/management
- ✗ Version 5 scales using Public Key Cyptography but has known flaws





Based on hundreds of actual fraud investigations conducted by KPMG Forensic departments within the Europe, Middle East and Africa region in 2007 approximately 86% of fraud is instigated by management level staff against their own organization and > 50% percent of offenders have been with their company for more than six years.



Based on hundreds of actual fraud investigations conducted by KPMG Forensic departments within the Europe, Middle East and Africa region in 2007 approximately 86% of fraud is instigated by management level staff against their own organization and > 50% percent of offenders have been with their company for more than six years.

Part of the identified problem is that senior management are often able to circumvent the internal security mechanisms intended to prevent fraud.

Recent FBI White Paper values cybercrime at USD1,000 billion

Recent FBI White Paper values cybercrime at USD1,000 billion

To quote R. Morris,
a former Chief Scientist of the
United States National Security Agency:

Recent FBI White Paper values cybercrime at USD1,000 billion

To quote R. Morris,
a former Chief Scientist of the
United States National Security Agency:

**“It’s not good enough to have a system where everyone
(using/supporting the system) must be trusted.**

It must also be made robust against insiders!”



Photograph by Alessio Damato (<http://commons.wikimedia.org/wiki/User:Alejo2083>). This file is licensed under the Creative Commons Attribution ShareAlike 3.0 (<http://creativecommons.org/licenses/by-sa/3.0/>)



I have tried, but it appears impossible to provision genuinely secure cryptographic services, on behalf of the global community, on my own. The burden of responsibility is too large.



Photograph by Alessio Damato (<http://commons.wikimedia.org/wiki/User:Alejo2083>). This file is licensed under the Creative Commons Attribution ShareAlike 3.0 (<http://creativecommons.org/licenses/by-sa/3.0/>)



I have tried, but it appears impossible to provision genuinely secure cryptographic services, on behalf of the global community, on my own. The burden of responsibility is too large.



- ➔ Global Identity Management and Cryptographic Key Management architectures with **system-wide**, single points of trust failure are just too vulnerable to insider attacks

Photograph by Alessio Damato (<http://commons.wikimedia.org/wiki/User:Alejo2083>). This file is licensed under the Creative Commons Attribution ShareAlike 3.0 (<http://creativecommons.org/licenses/by-sa/3.0/>)



I have tried, but it appears impossible to provision genuinely secure cryptographic services, on behalf of the global community, on my own. The burden of responsibility is too large.



- Global Identity Management and Cryptographic Key Management architectures with **system-wide**, single points of trust failure are just too vulnerable to insider attacks
- IdM/CKM systems with MULTIPLE system-wide single points of trust failure exasperate the vulnerability from insider attacks

Photograph by Alessio Damato (<http://commons.wikimedia.org/wiki/User:Alejo2083>). This file is licensed under the Creative Commons Attribution ShareAlike 3.0 (<http://creativecommons.org/licenses/by-sa/3.0/>)



I have tried, but it appears impossible to provision genuinely secure cryptographic services, on behalf of the global community, on my own. The burden of responsibility is too large.



- Global Identity Management and Cryptographic Key Management architectures with **system-wide**, single points of trust failure are just too vulnerable to insider attacks
- IdM/CKM systems with MULTIPLE system-wide single points of trust failure exasperate the vulnerability from insider attacks
- Kerberos V5, X.509, OpenID, ...

Photograph by Alessio Damato (<http://commons.wikimedia.org/wiki/User:Alejo2083>). This file is licensed under the Creative Commons Attribution ShareAlike 3.0 (<http://creativecommons.org/licenses/by-sa/3.0/>)



Omnicrypt Security Architecture

A modern *Enterprise Symmetric Key Proposal*
(by Omnicrypt AG)

Omniscrypt OSA: A command and control architecture

*This summary **may contain material errors**, as we do not have detailed product specifications.*



Omniscrypt OSA: A command and control architecture

*This summary **may contain material errors**, as we do not have detailed product specifications.*

- ▣▣▣▣➤ **OSA is a complex system that exploits a combination of choices between the following features and options:**
 - ▣▣▣▣➤ Supports symmetric key + public key modes of operation
 - ▣▣▣▣➤ Standard and proprietary ciphers



Omniscrypt OSA: A command and control architecture

*This summary **may contain material errors**, as we do not have detailed product specifications.*

- |||➤ **OSA is a complex system that exploits a combination of choices between the following features and options:**
 - |||➤ Supports symmetric key + public key modes of operation
 - |||➤ Standard and proprietary ciphers

- |||➤ **Enterprise deployment (2 to 3000 devices)**
 - |||➤ The OSA system does not appear to be intended to support secure communications between adversaries/competitors



Omniscrypt OSA: A command and control architecture

*This summary **may contain material errors**, as we do not have detailed product specifications.*

- |||➤ **OSA is a complex system that exploits a combination of choices between the following features and options:**
 - |||➤ Supports symmetric key + public key modes of operation
 - |||➤ Standard and proprietary ciphers

- |||➤ **Enterprise deployment (2 to 3000 devices)**
 - |||➤ The OSA system does not appear to be intended to support secure communications between adversaries/competitors

- |||➤ **Appears to be centralised “command-and-control” architecture**
 - |||➤ Central administrators are responsible for enabling key exchanges between devices
 - |||➤ A single central HSM (Programmable Security Module) appears to have knowledge of most (if not all) keys used by the enrolled devices

Omniscrypt: A command and control architecture



**Security Module
Programmer**



Security Module



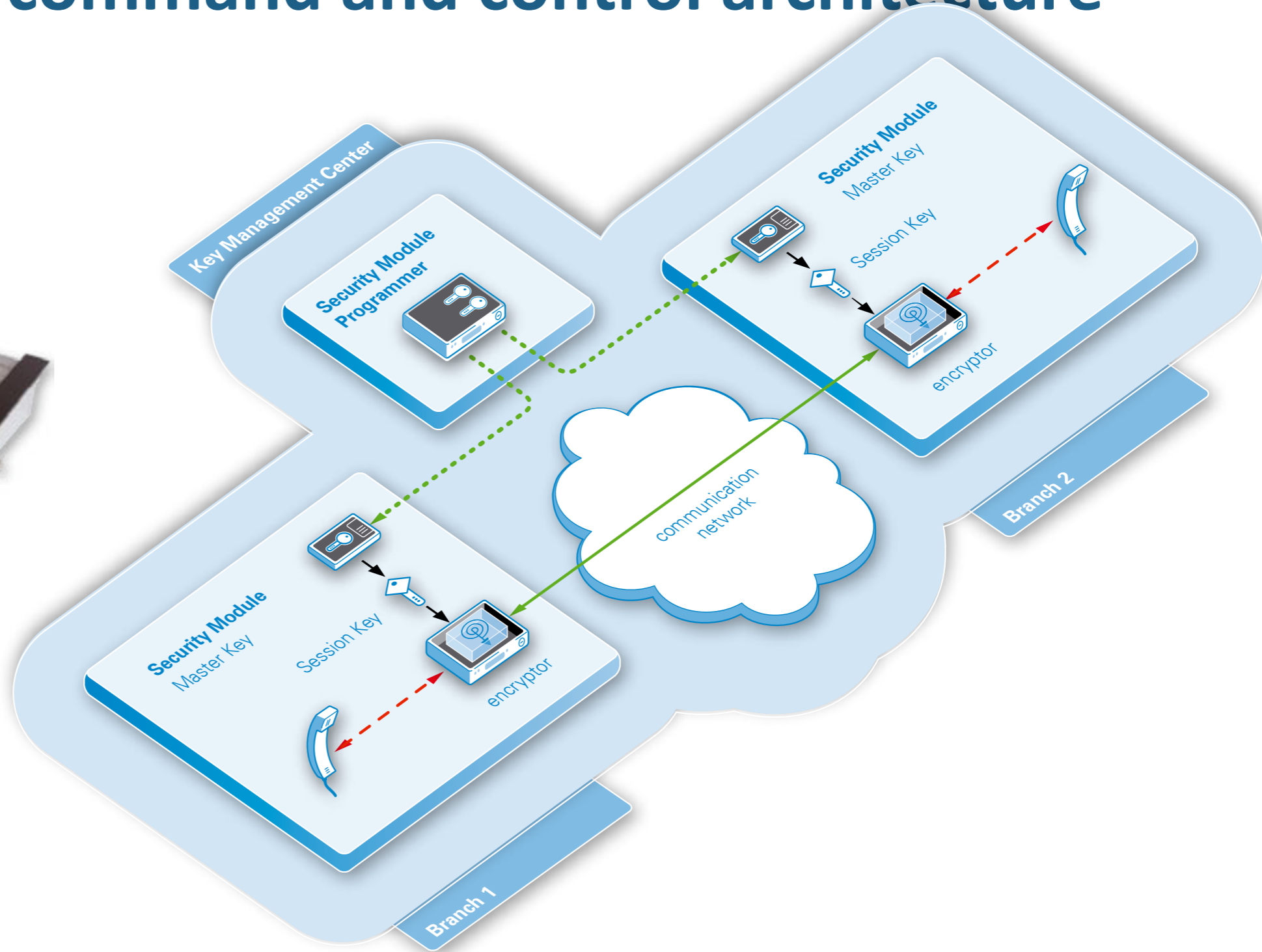
Omniscrypt: A command and control architecture



**Security Module
Programmer**



Security Module





Omniscrypt: A command and control architecture

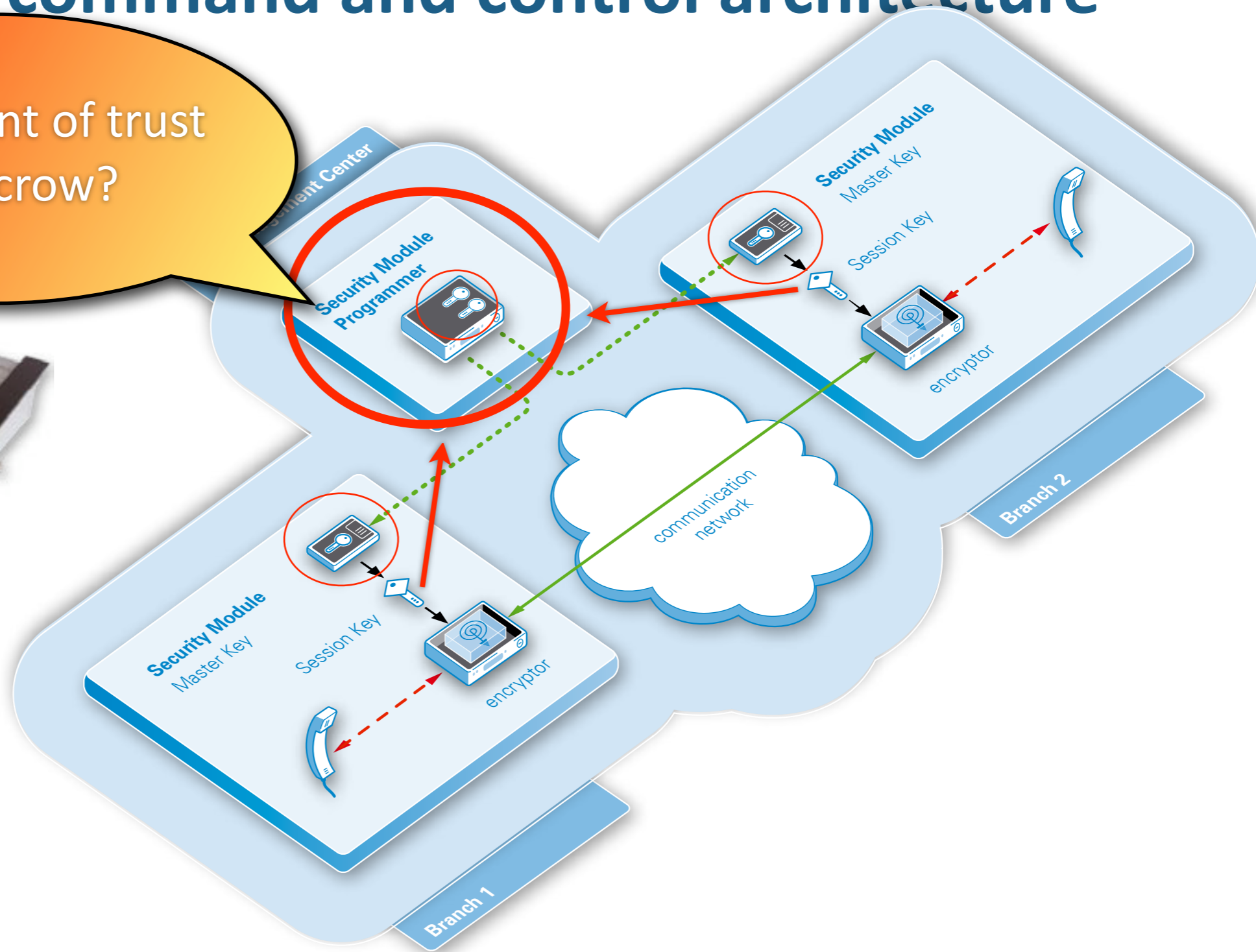
Single point of trust
failure/escrow?



**Security Module
Programmer**



Security Module



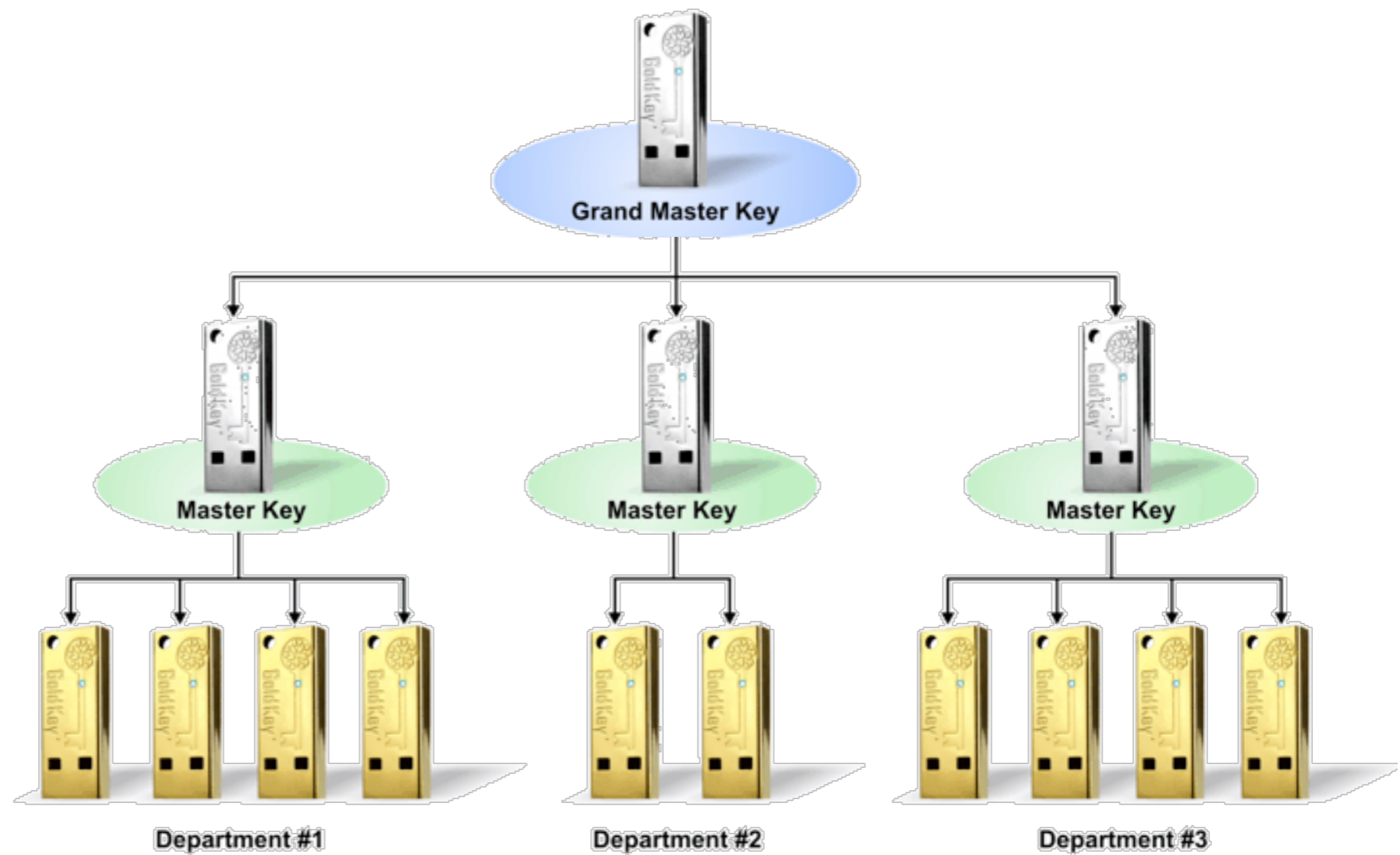


GOLDKEY

A modern *Enterprise* Symmetric Key Distribution Proposal
(by GoldKey Security Corporation)



GOLDKEY: A command and control architecture

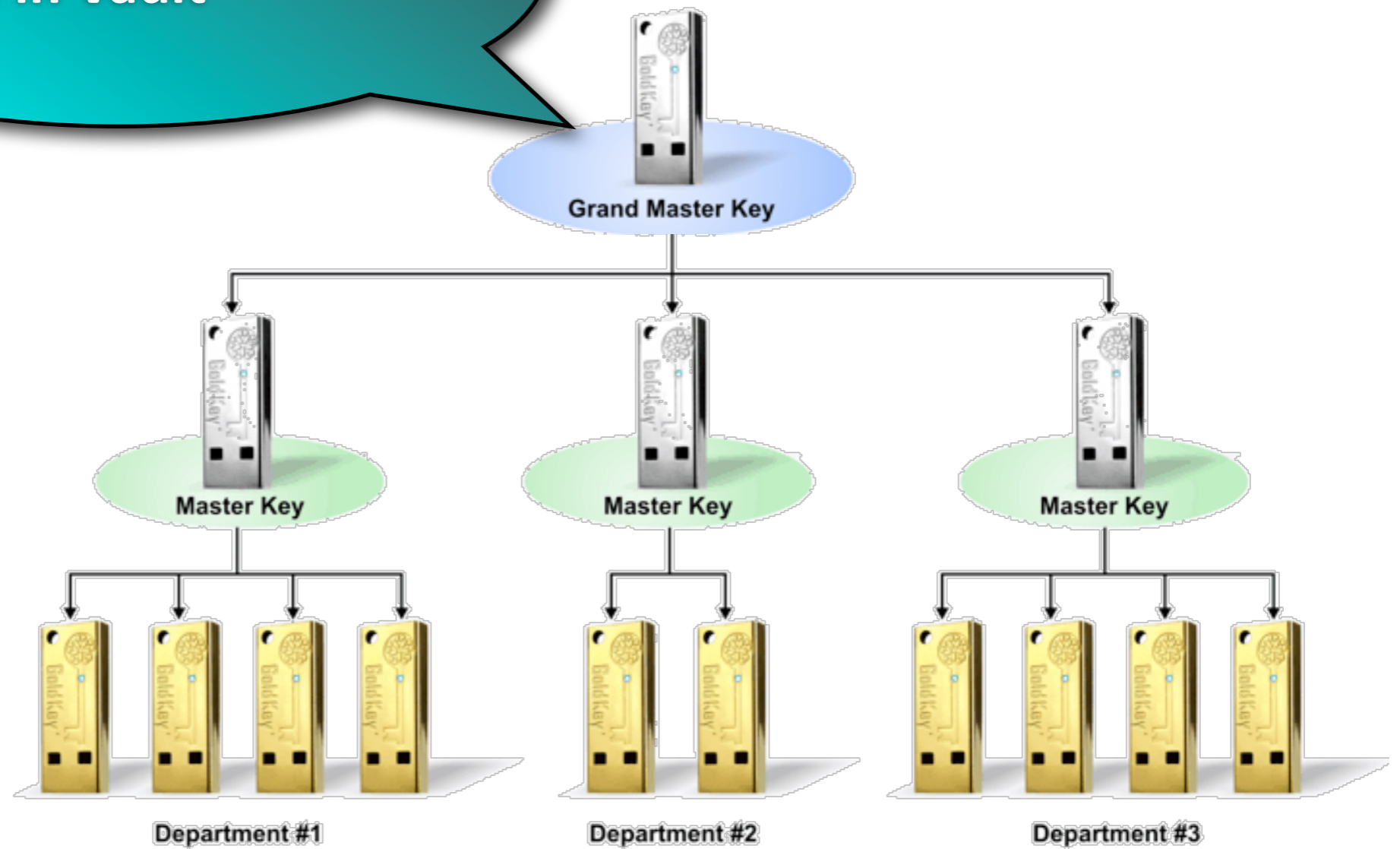


This summary **may contain material errors**, as we do not have detailed product specifications.



GOLDKEY: A command and control architecture

Master Symmetric Key
"Store in Vault"



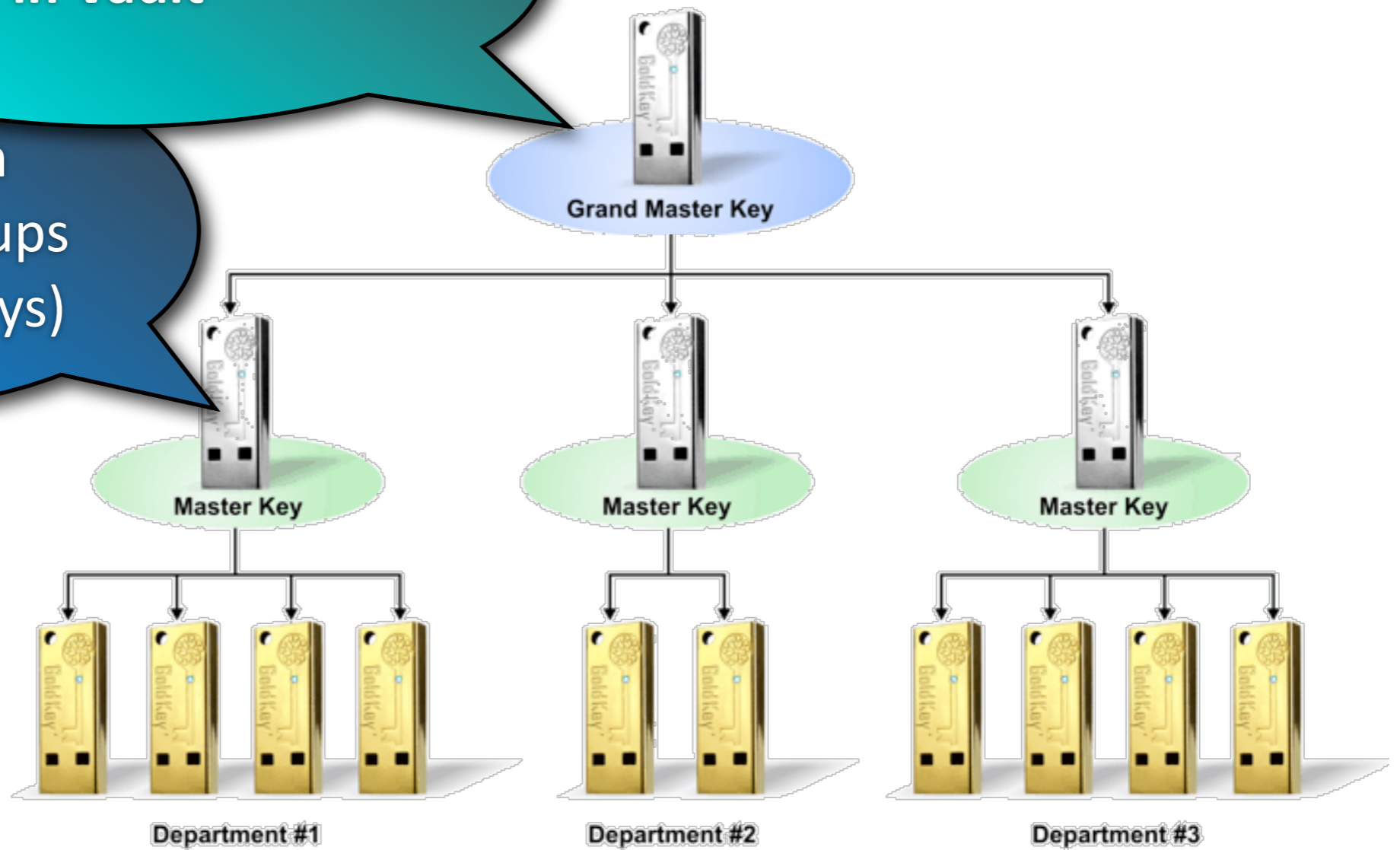
This summary **may contain material errors**, as we do not have detailed product specifications.



GOLDKEY: A command and control architecture

Master Symmetric Key
"Store in Vault"

Key Derivation
Create 64 groups
(symmetric keys)



This summary **may contain material errors**, as we do not have detailed product specifications.

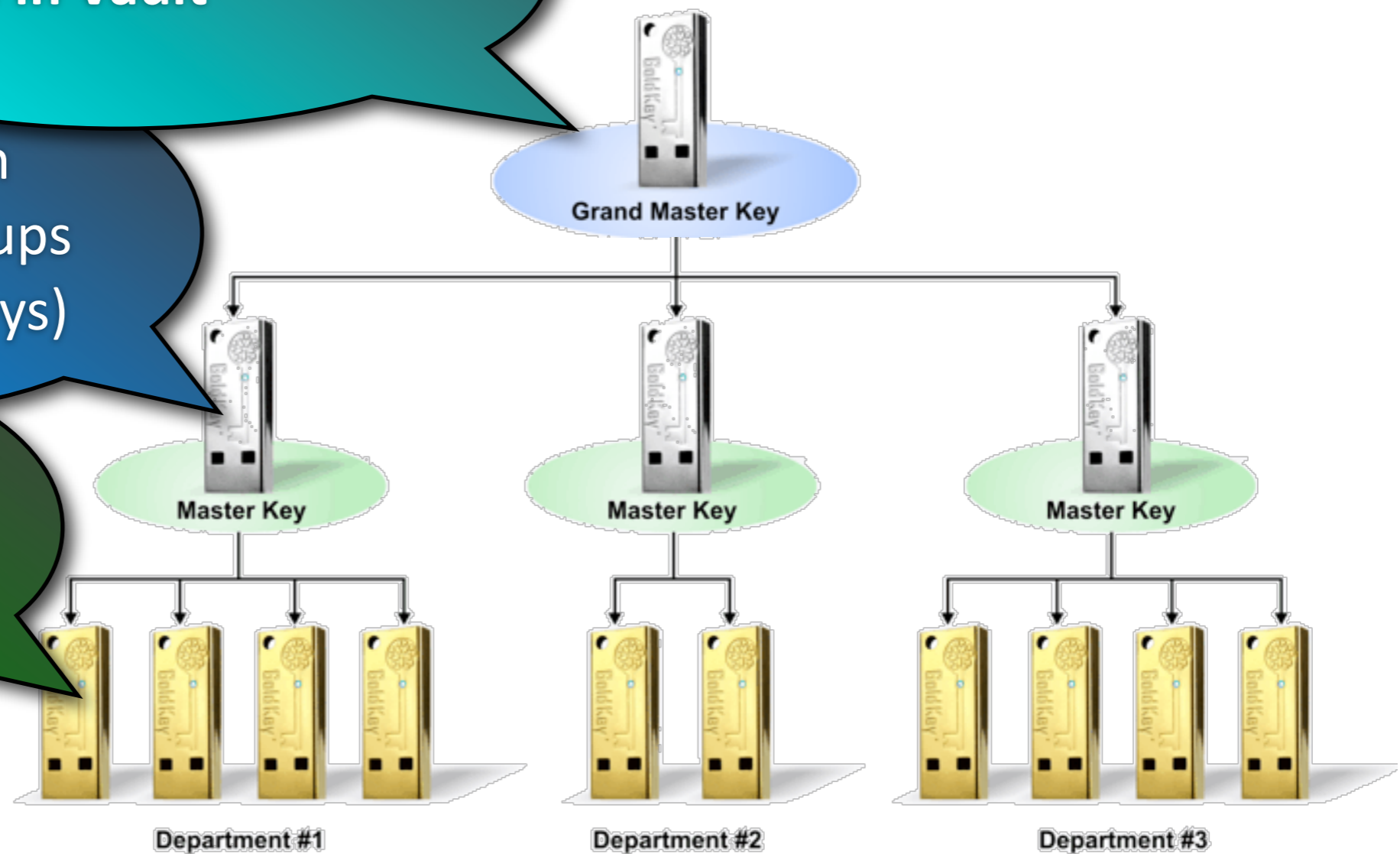


GOLDKEY: A command and control architecture

Master Symmetric Key
"Store in Vault"

Key Derivation
Create 64 groups
(symmetric keys)

Assigned (secrets)
to access some of
the 64 groups



This summary **may contain material errors**, as we do not have detailed product specifications.



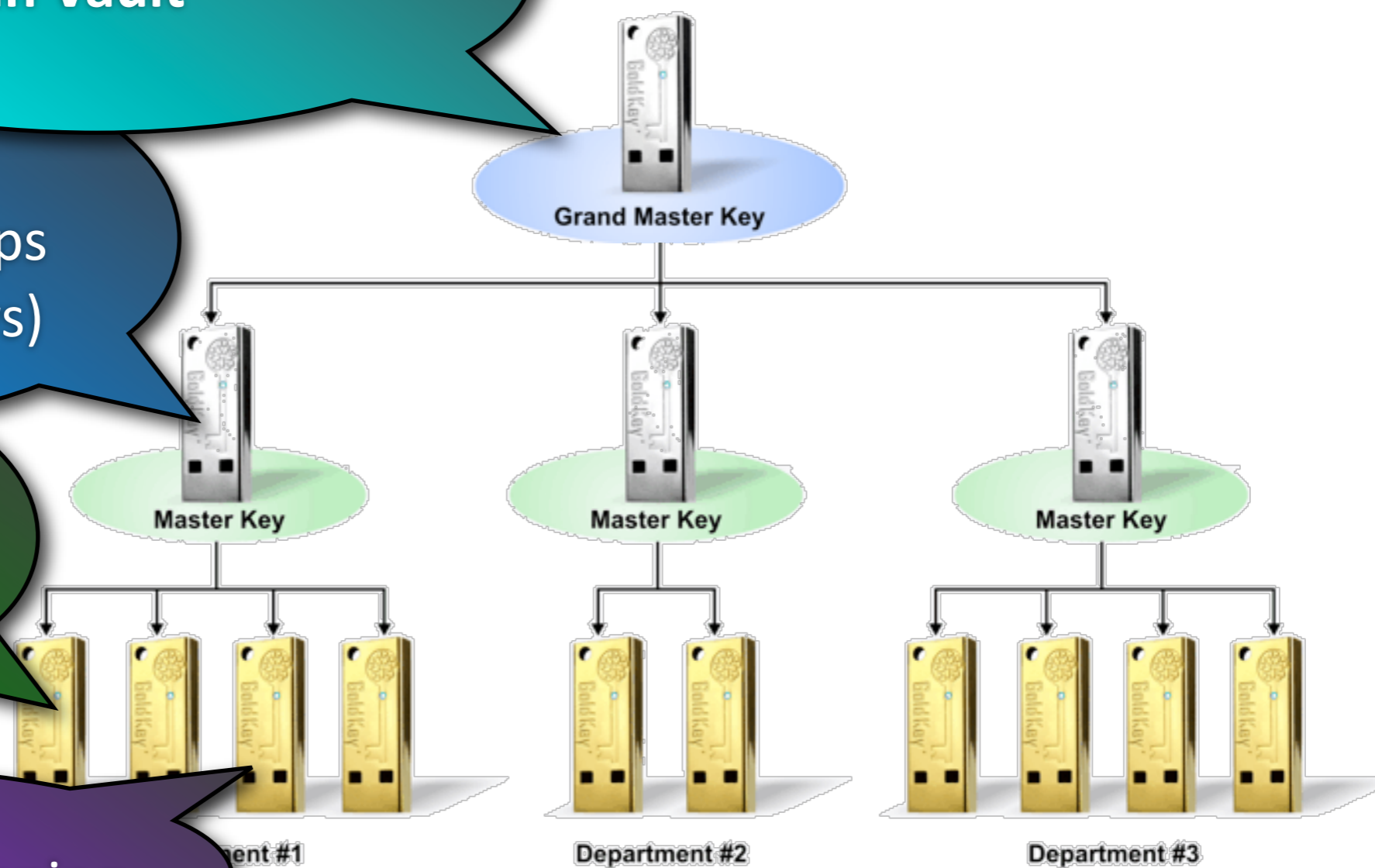
GOLDKEY: A command and control architecture

Master Symmetric Key
"Store in Vault"

Key Derivation
Create 64 groups
(symmetric keys)

Assigned (secrets)
to access some of
the 64 groups

No {Token, ID} mapping



This summary **may contain material errors**, as we do not have detailed product specifications.



GOLDKEY: A command and control architecture

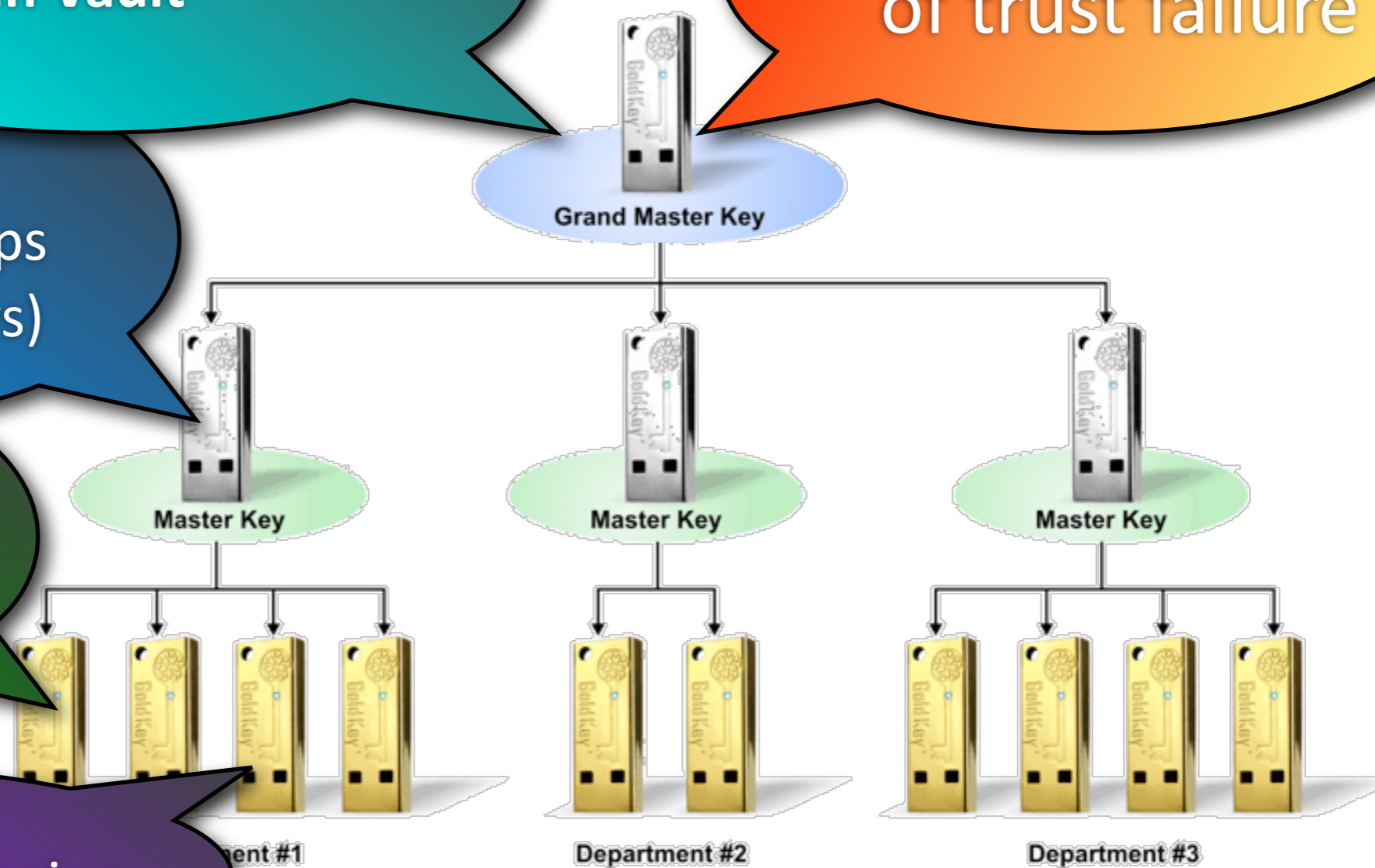
Master Symmetric Key
"Store in Vault"

Single point
of trust failure

Key Derivation
Create 64 groups
(symmetric keys)

Assigned (secrets)
to access some of
the 64 groups

No {Token, ID} mapping



This summary **may contain material errors**, as we do not have detailed product specifications.



GOLDKEY: A command and control architecture

Master Symmetric Key
"Store in Vault"

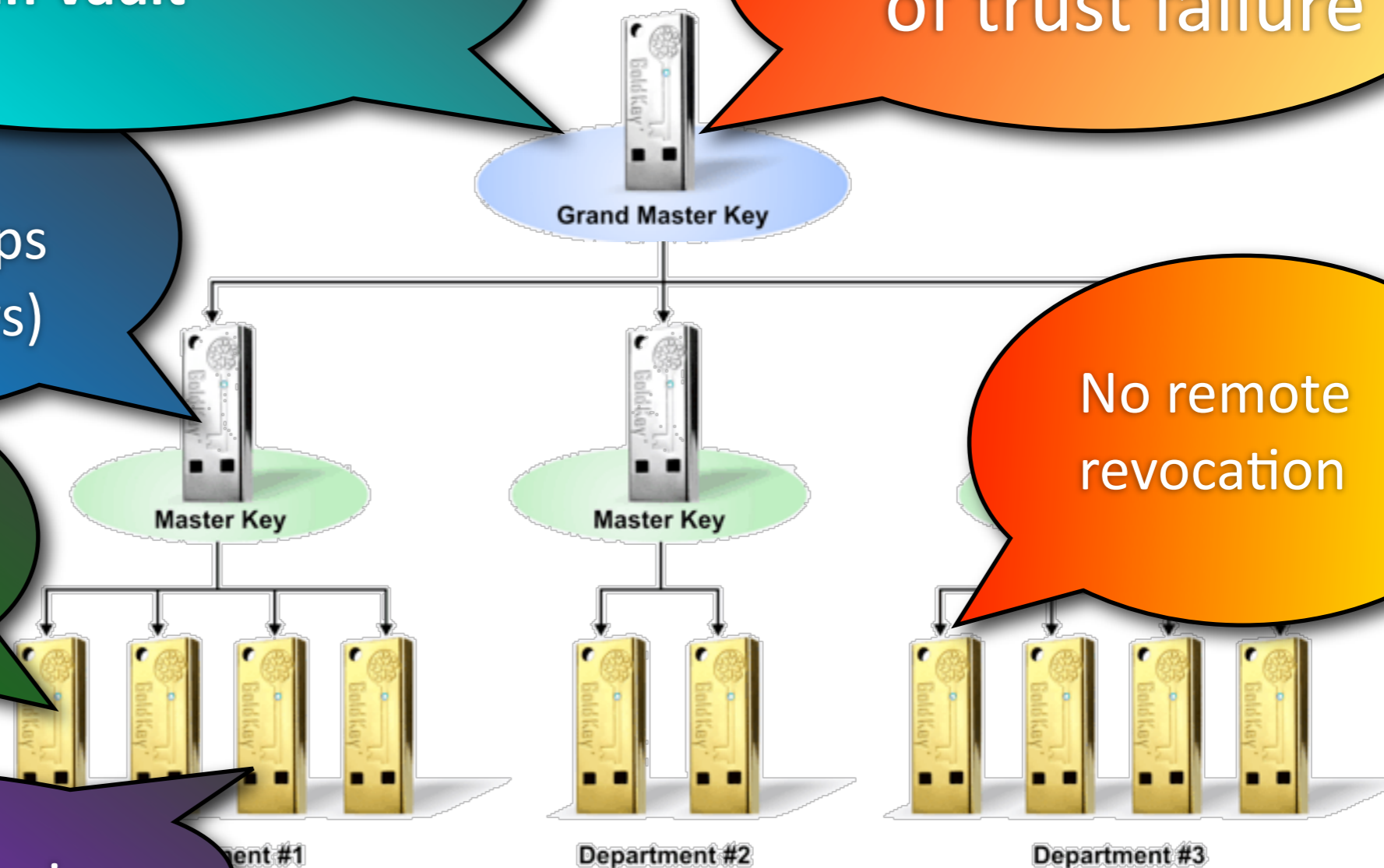
Single point
of trust failure

Key Derivation
Create 64 groups
(symmetric keys)

Assigned (secrets)
to access some of
the 64 groups

No remote
revocation

No {Token, ID} mapping

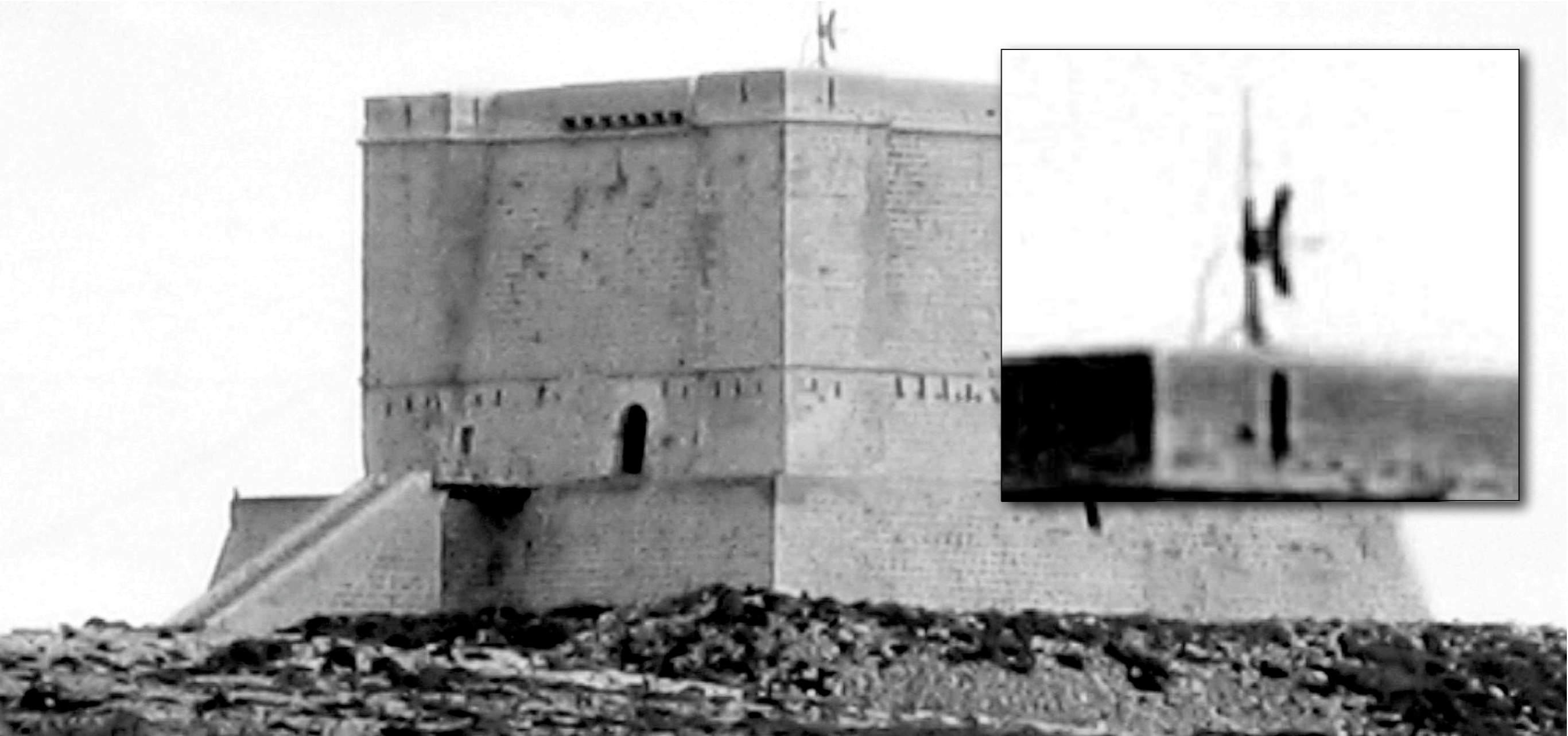


This summary **may contain material errors**, as we do not have detailed product specifications.

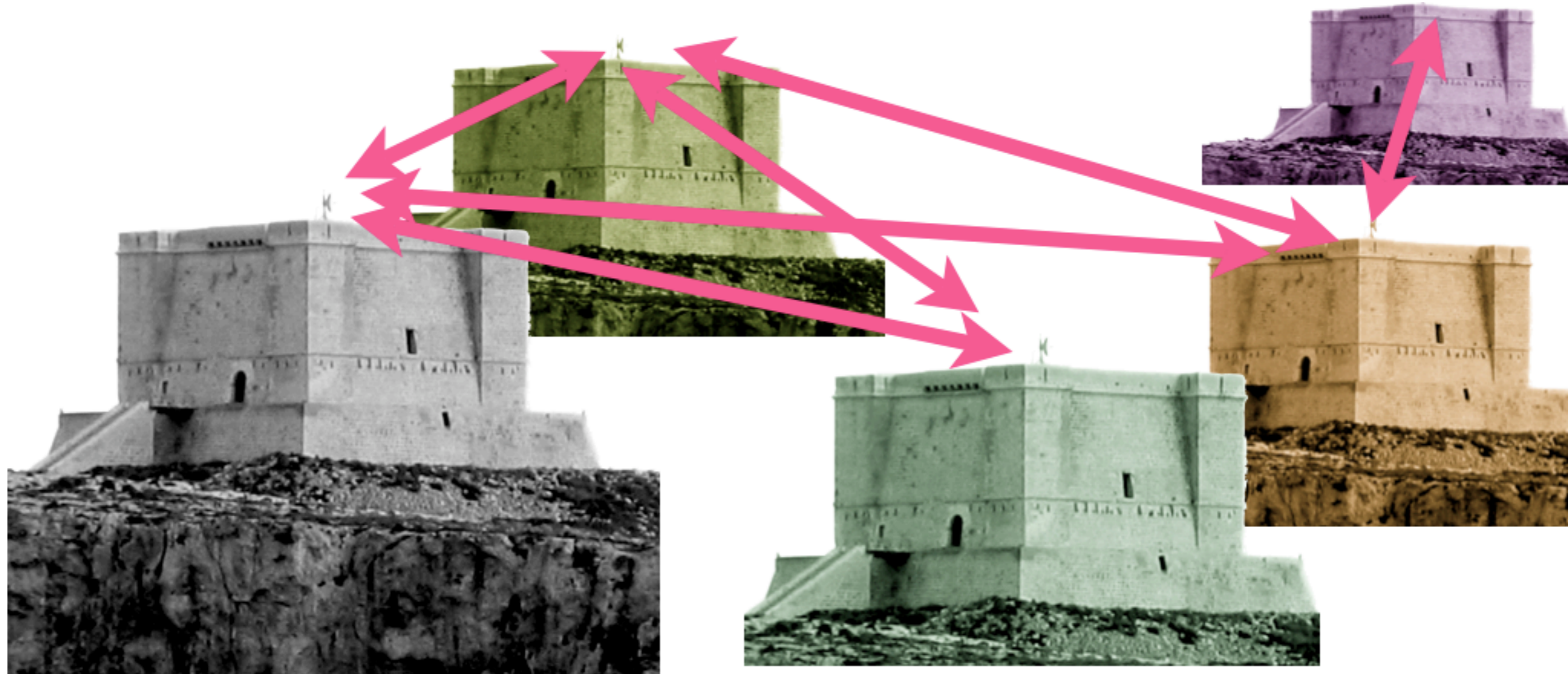


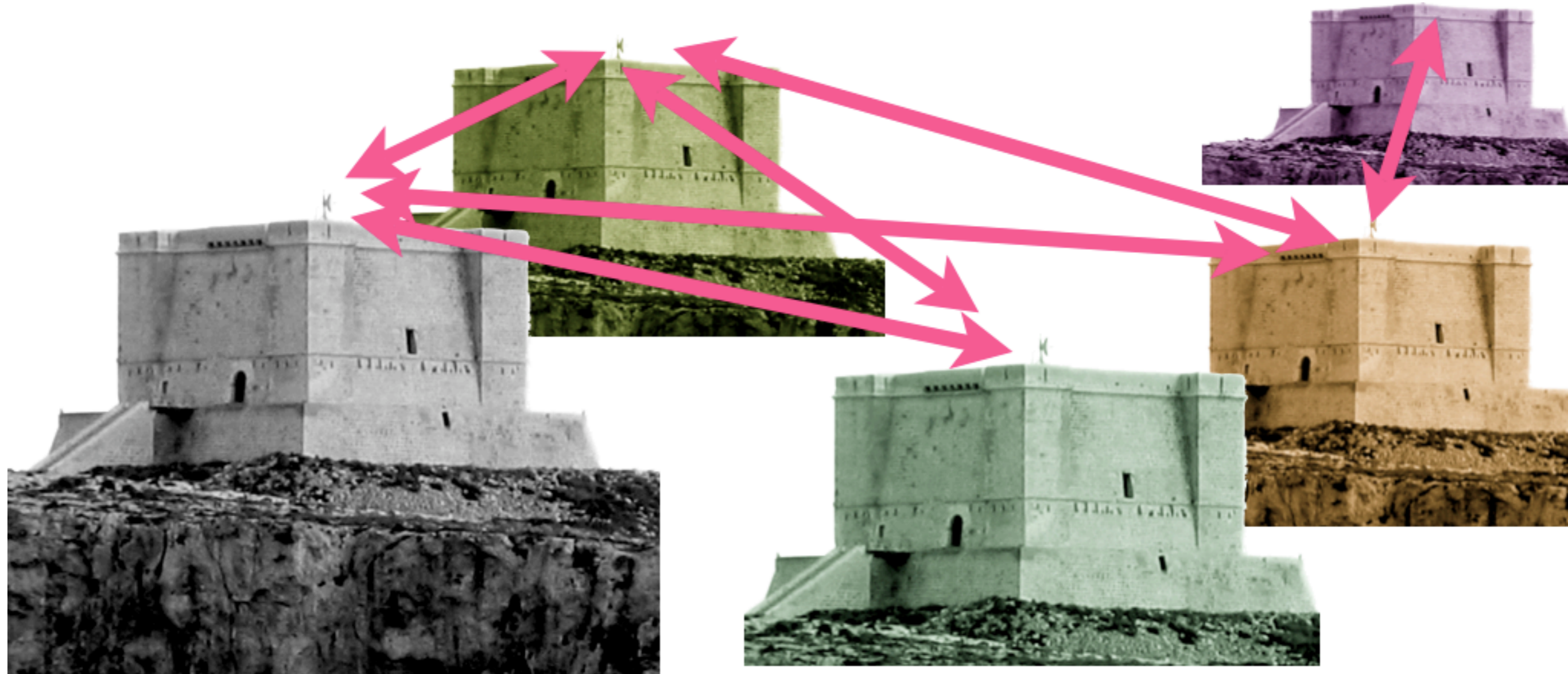


- ➡ *In today's interconnected business environment (with outsourcing, supply chains, distributors, collaborators, remote customer support and so on) the silo fortress (us versus them) trust/threat model doesn't work*

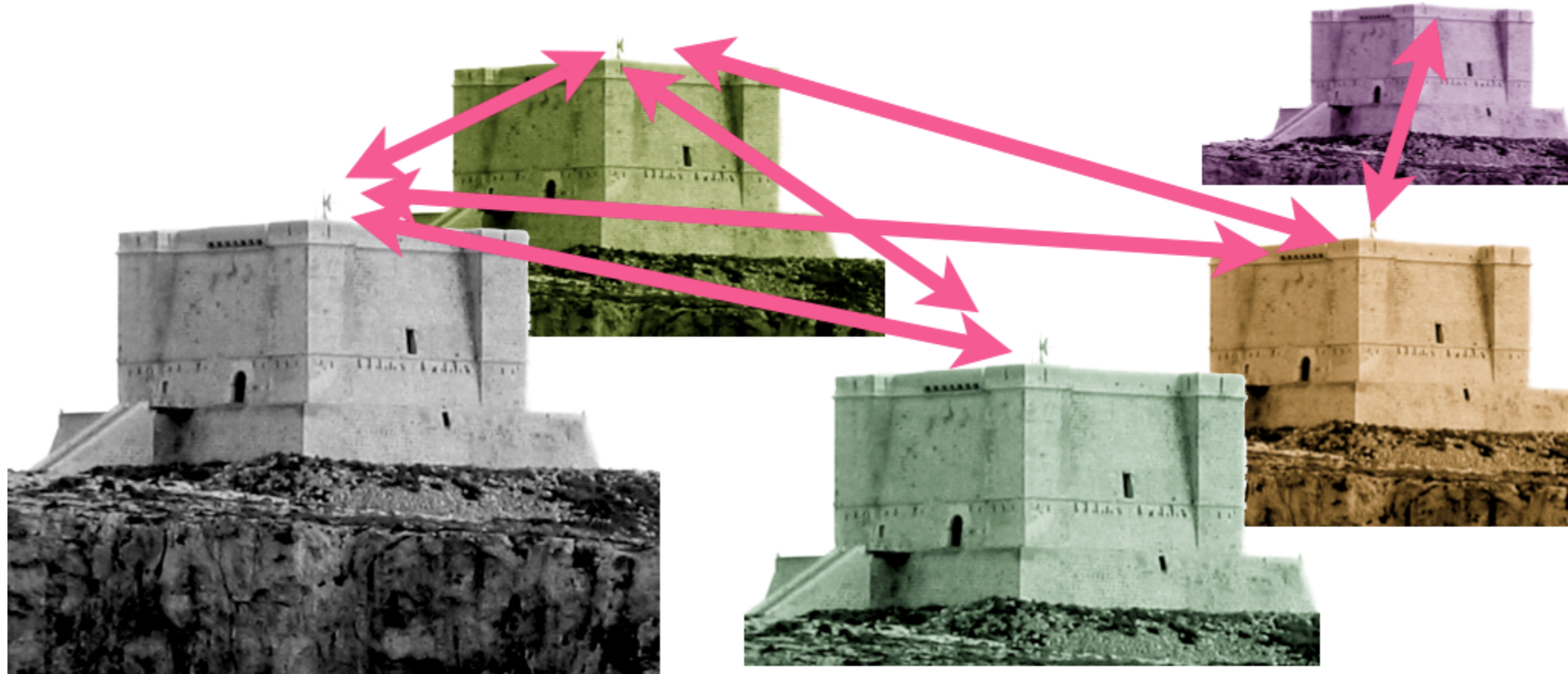


- ➡ *In today's interconnected business environment (with outsourcing, supply chains, distributors, collaborators, remote customer support and so on) the silo fortress (us versus them) trust/threat model doesn't work*

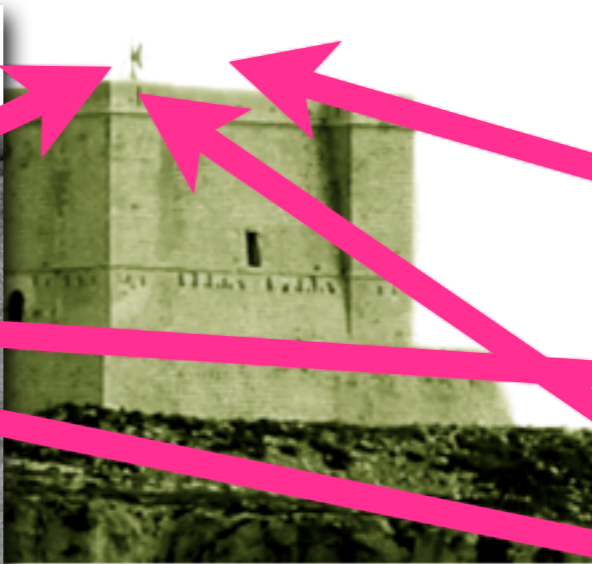
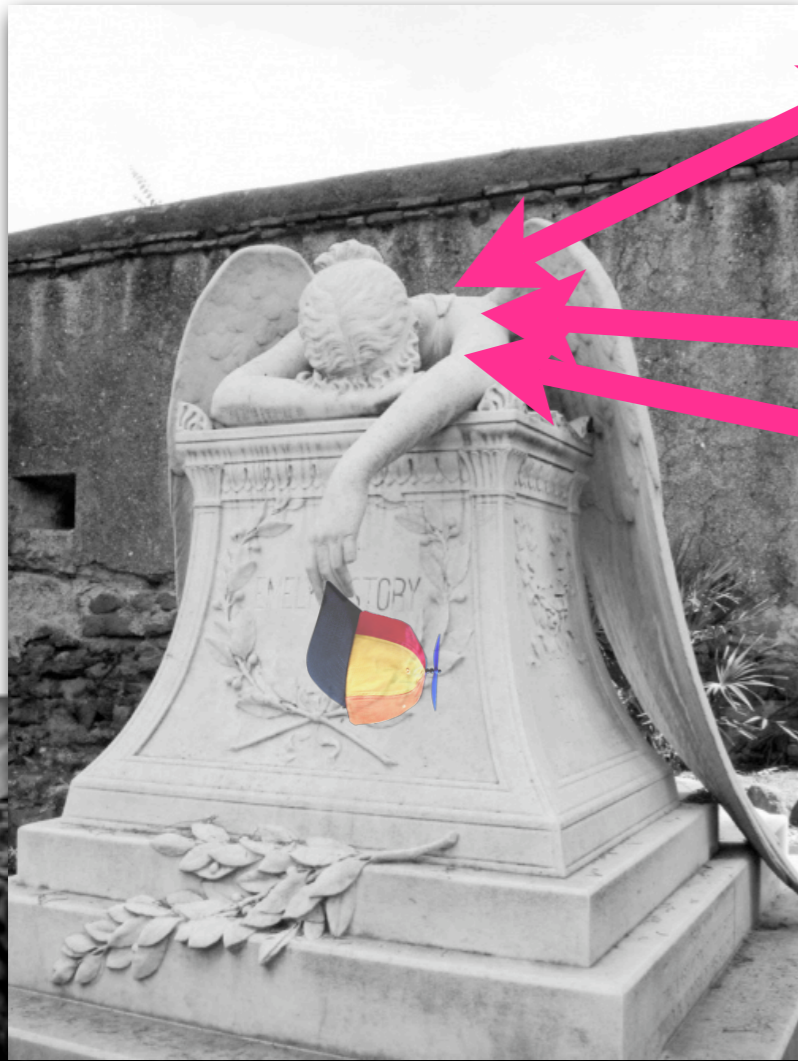


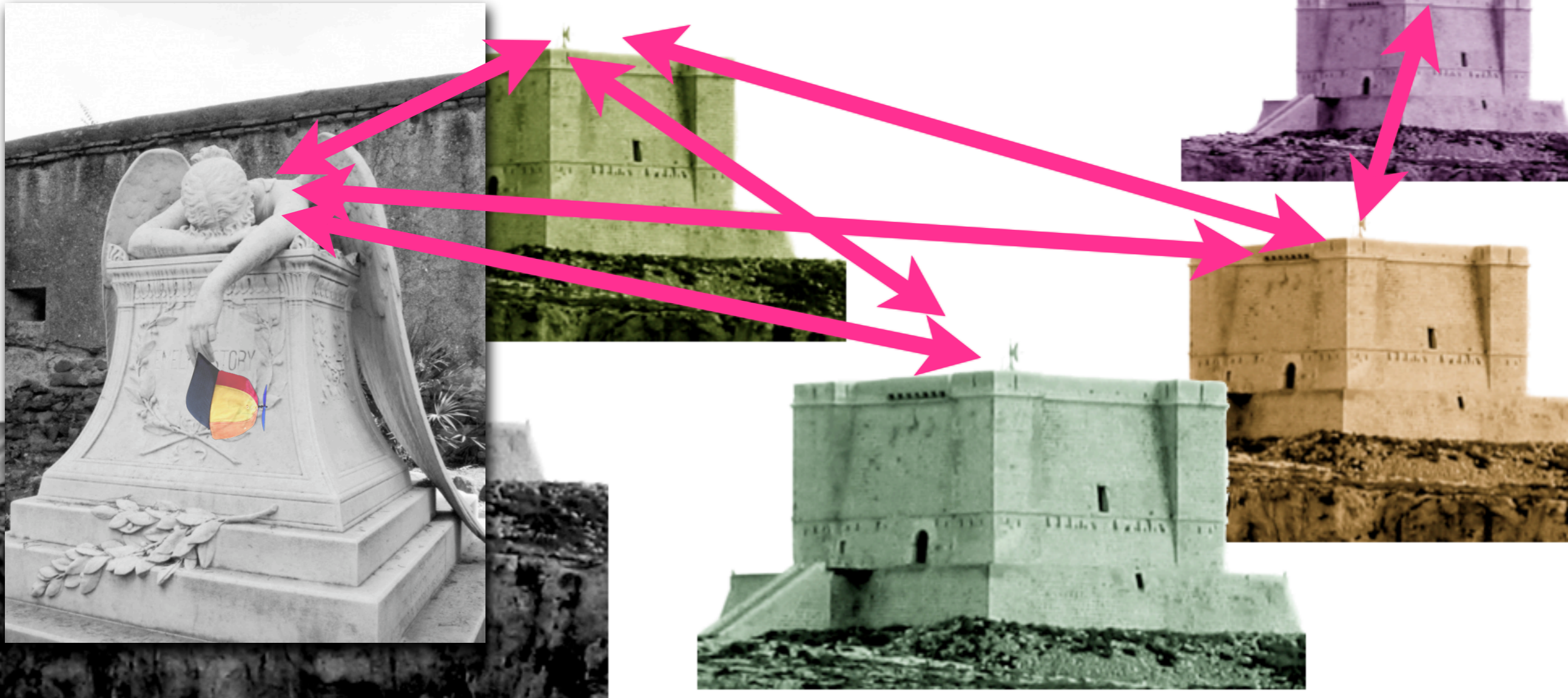


➡ *Each organisation/enterprise/government needs to have assurances that their respective security needs are met, while maintaining internal control*

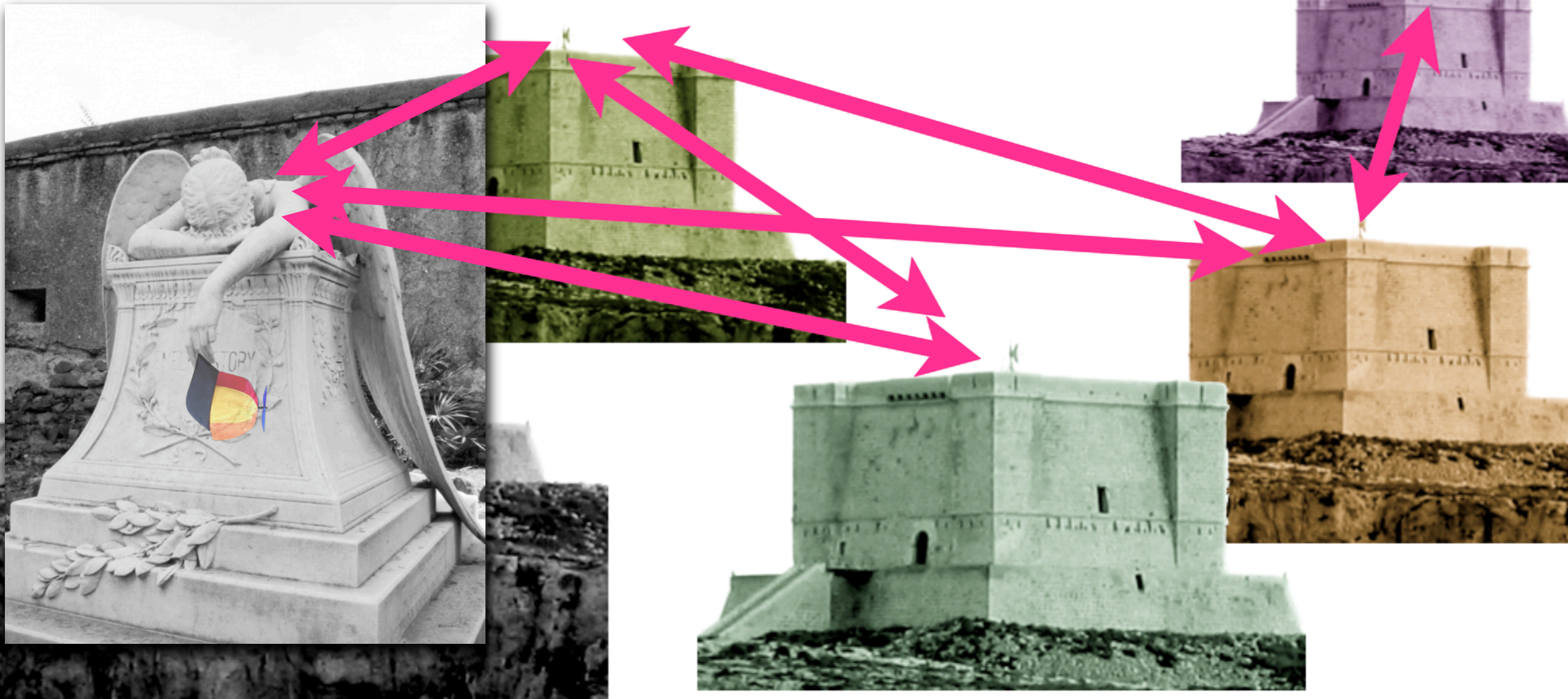


- *Each organisation/enterprise/government needs to have assurances that their respective security needs are met, while maintaining internal control*
- *The previous command-and-control us-vs-them symmetric key designs do not meet the complex commercial/business/trust needs of our community*

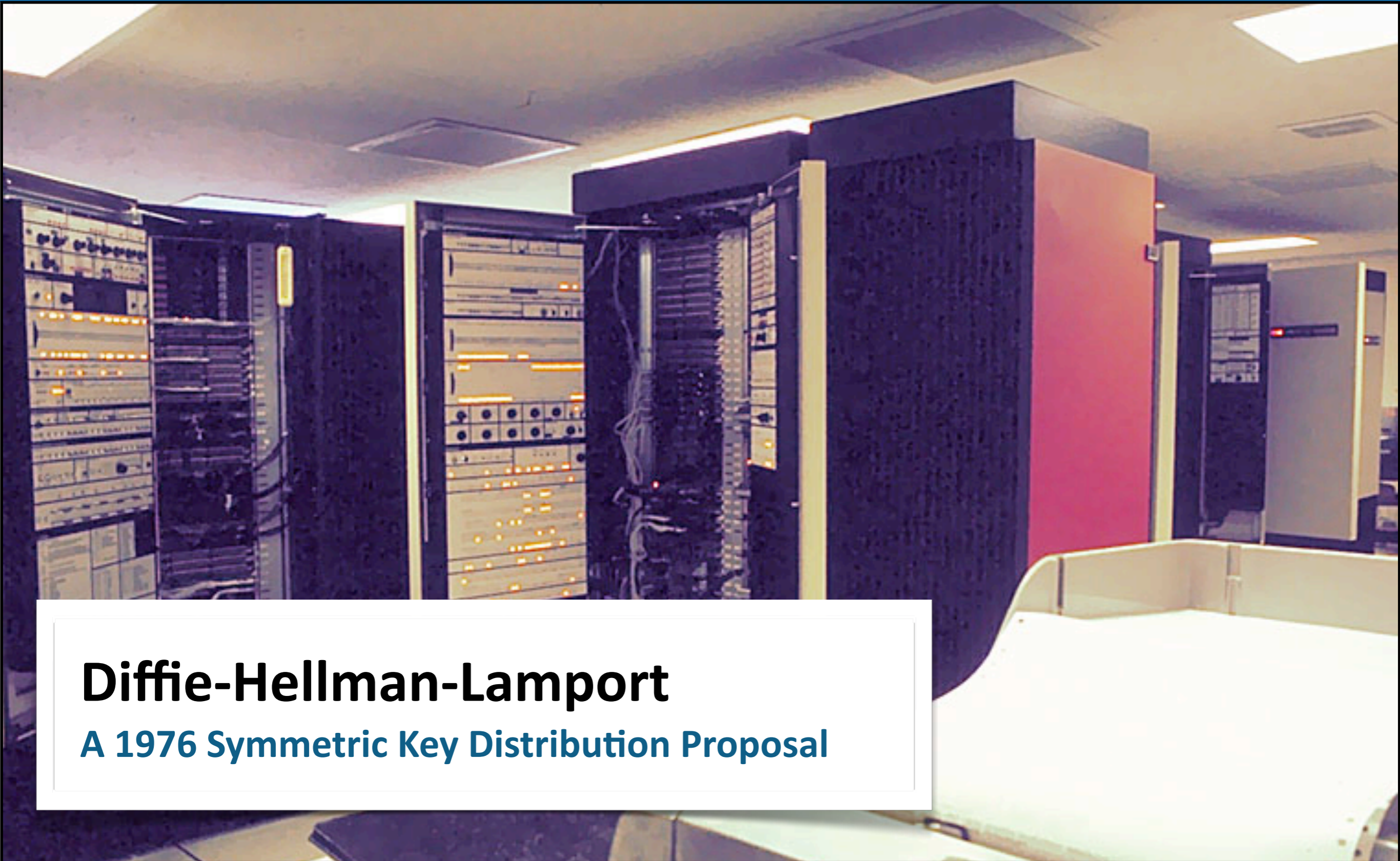




➡ *As mentioned previously, it is not possible for one “security fortress”, acting on their own, to provision trust-worthy solutions for everyone.*

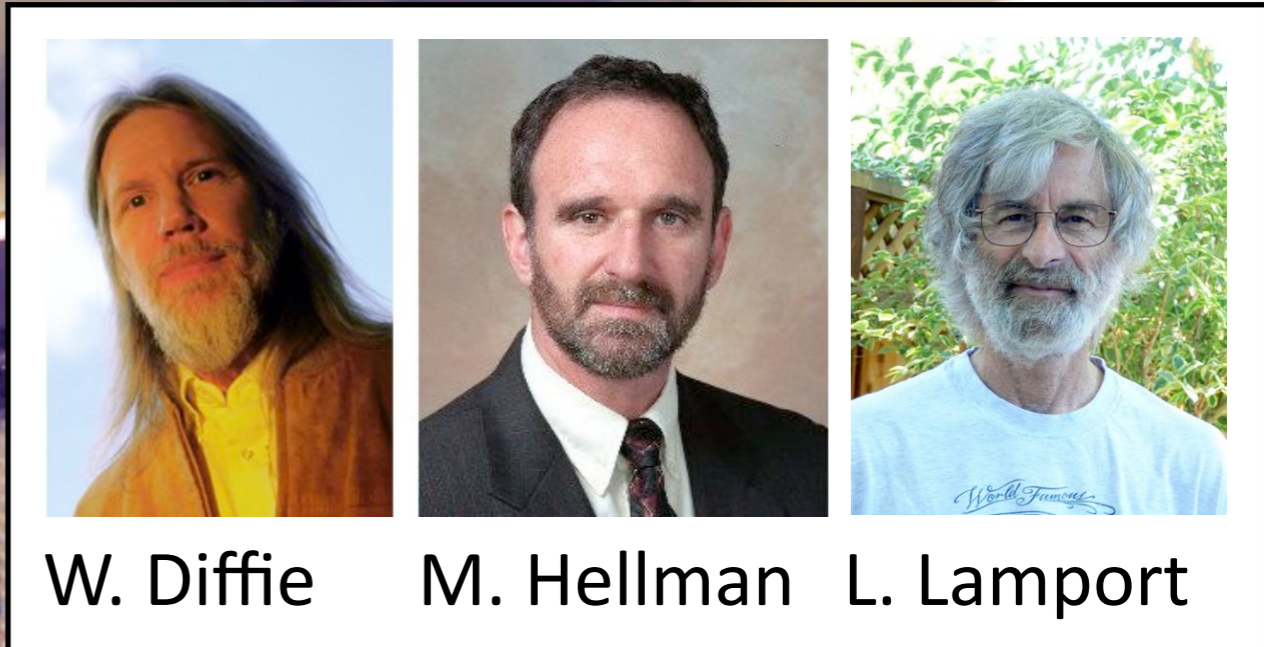
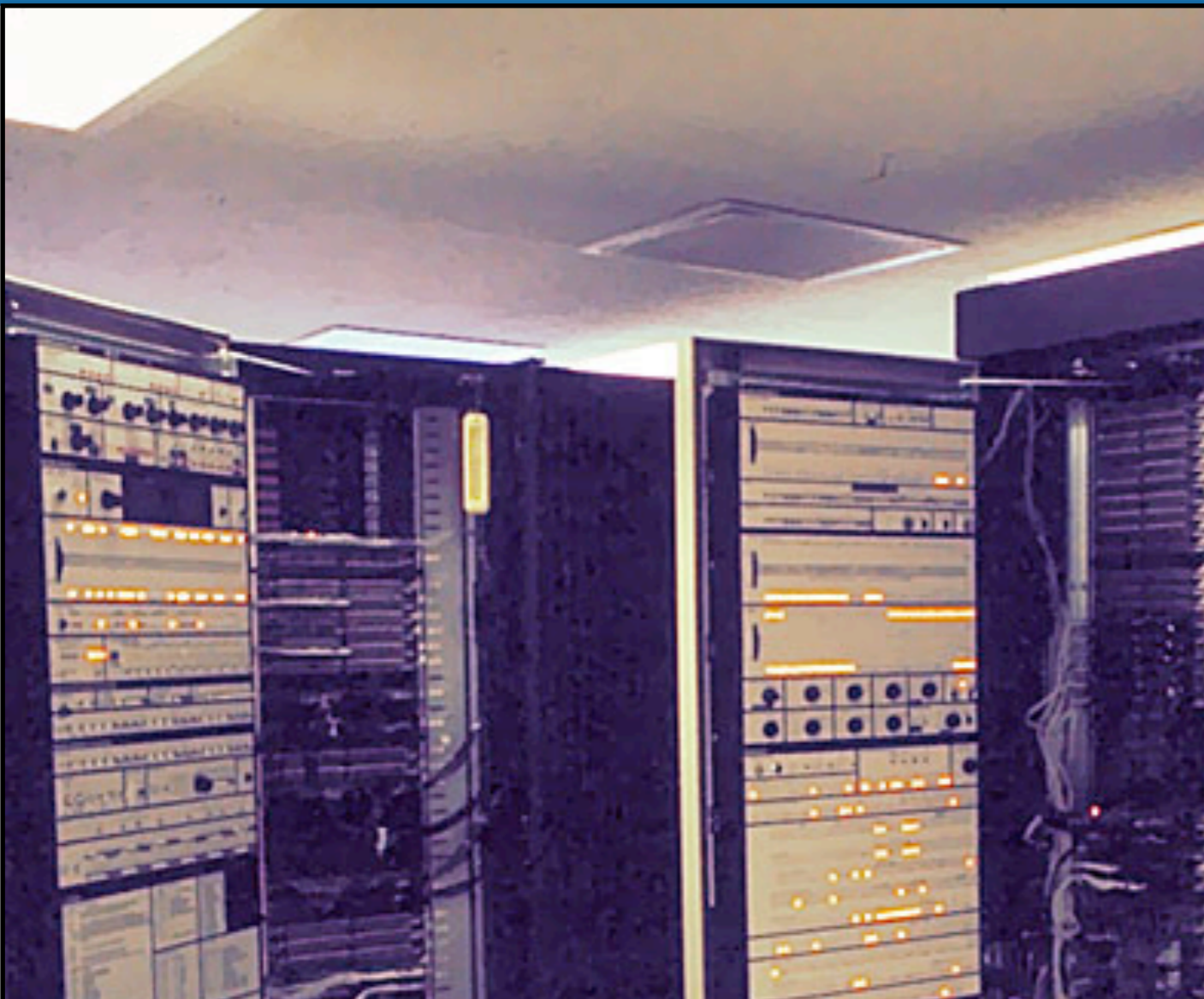


- *As mentioned previously, it is not possible for one “security fortress”, acting on their own, to provision trust-worthy solutions for everyone.*
- *So, is there a way existing security authorities can work together?*



Diffie-Hellman-Lamport

A 1976 Symmetric Key Distribution Proposal



W. Diffie

M. Hellman

L. Lamport

Diffie-Hellman-Lamport

A 1976 Symmetric Key Distribution Proposal

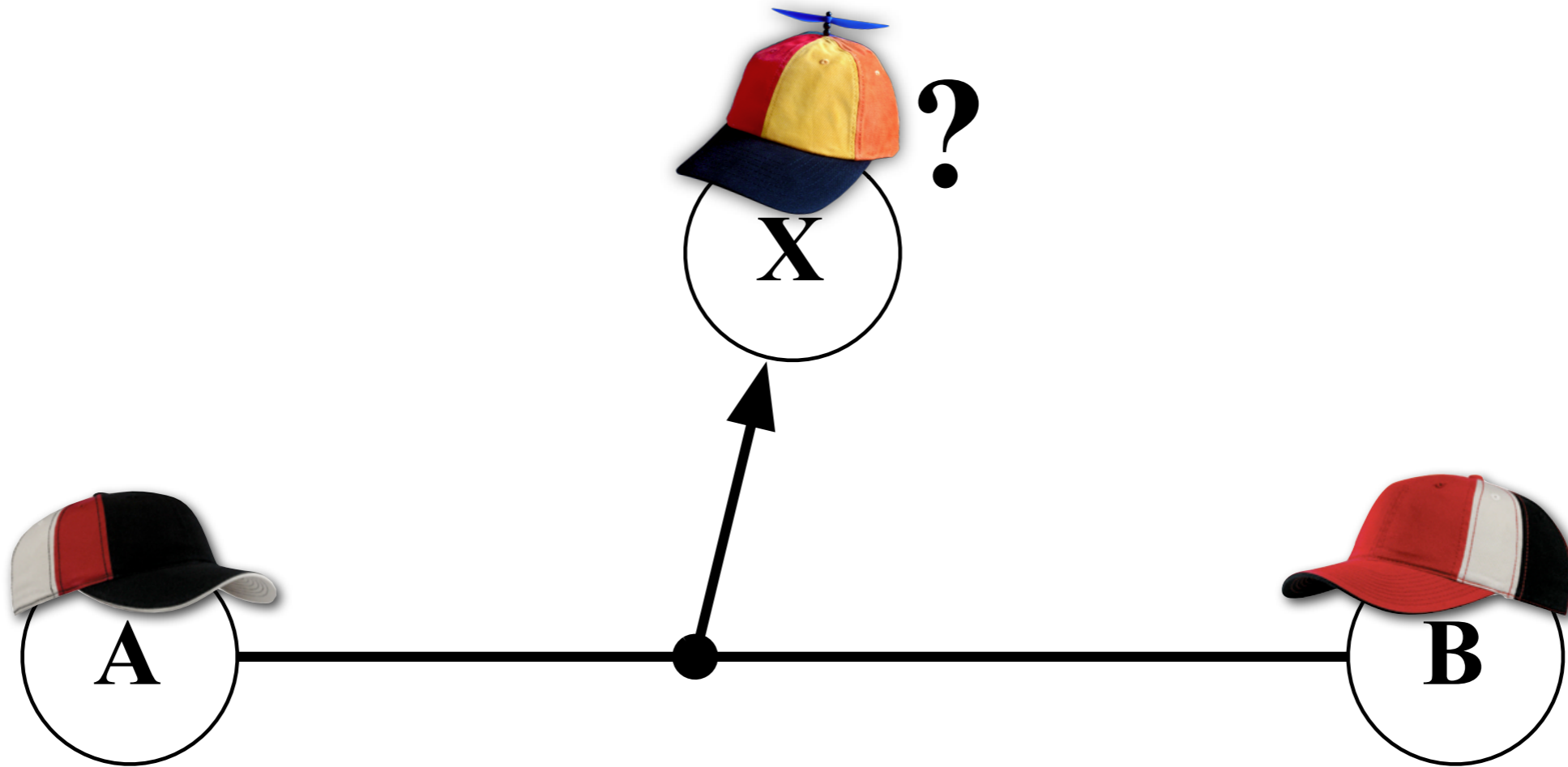


Timeline of symmetric key distribution schemes

Date		Description
1970	SKD	H. Feistel - mutual authentication using symmetric keys
1973	SKDN	D. Branstad - mutual authentication over a network
1976	SKDN	W. Diffie, M. Hellman, L. Lamport - key distribution that is $(m-1)$ secure against Single Points of Trust Failure
1976	SKDN	S. Kent - two factor authentication, symmetric key distribution over a network, backwards secrecy using magnetic cards, authenticated encryption of data
1976	PKC	W. Diffie, M. Hellman, R. Merkle - public key cryptography
1987	SKDN	Kerberos version 4 published (Public version)
1988	PKI	X.509 standard issued

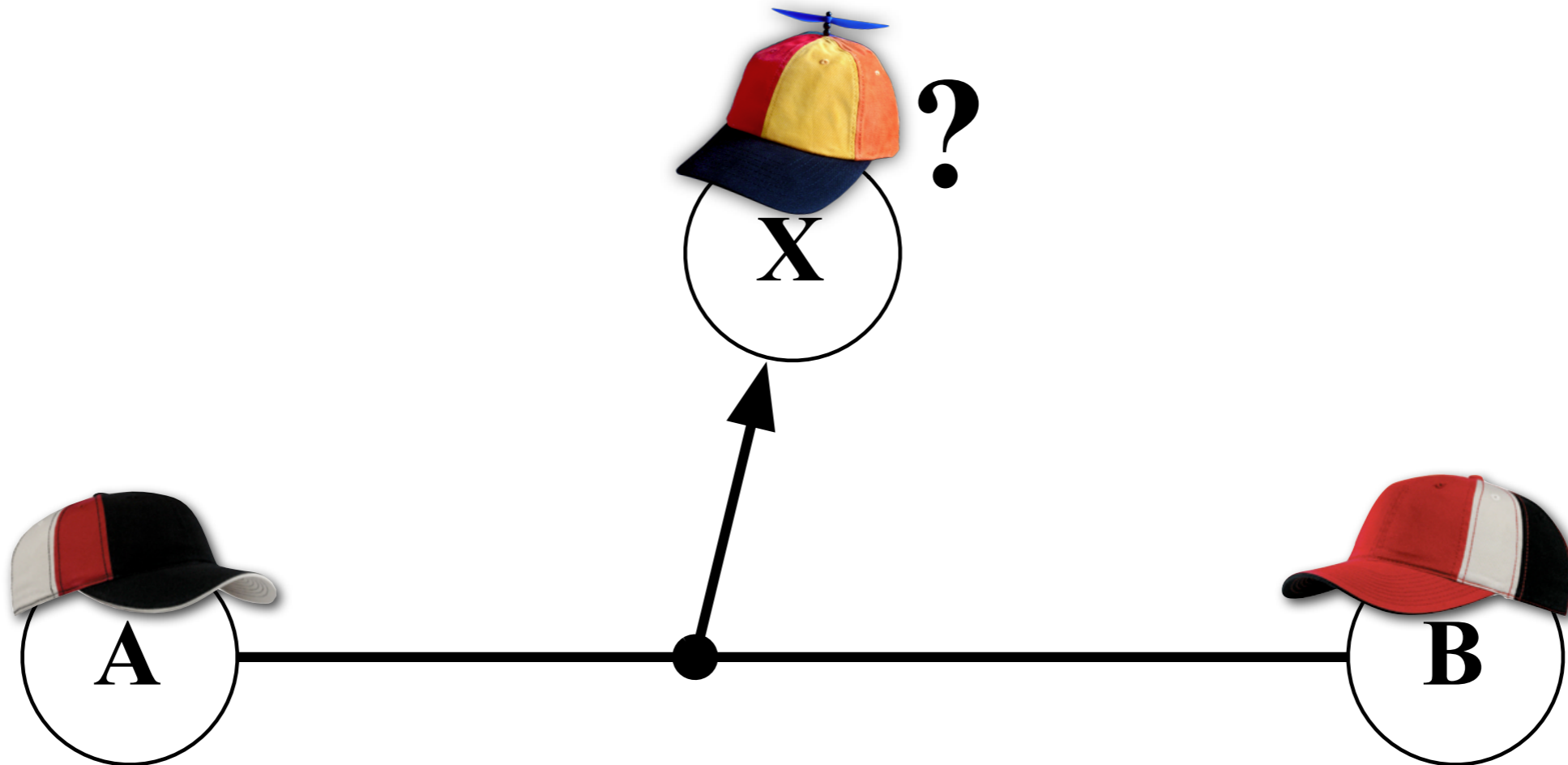


A driver for Diffie-Merkle-Hellman's 1976 SKD design





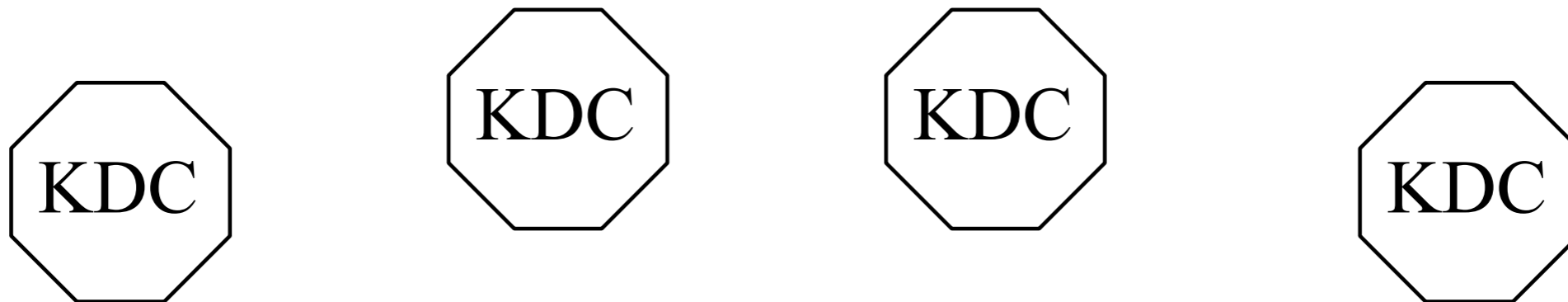
A driver for Diffie-Merkle-Hellman's 1976 SKD design



- ➡ Enable private conversations between any two parties, even if they have not communicated before, while also being secure against 'trusted parties'



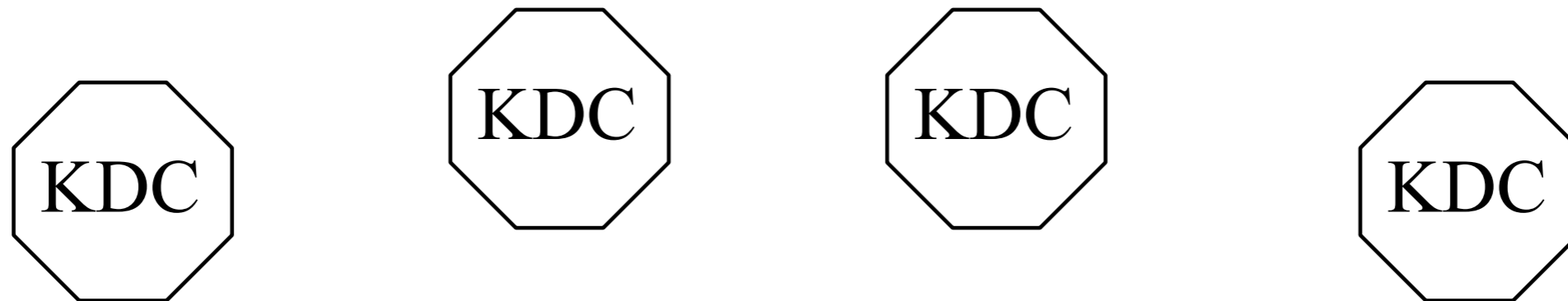
A (m-1) out of m KDC secure SKD overlay network



➡ **Diffie-Hellman-Lamport proposed in 1976:**



A (m-1) out of m KDC secure SKD overlay network



➤ **Diffie-Hellman-Lamport proposed in 1976:**

Increase the number of 'trusted parties' (m), and
distribute trust over these m different key distribution centers



A (m-1) out of m KDC secure SKD overlay network

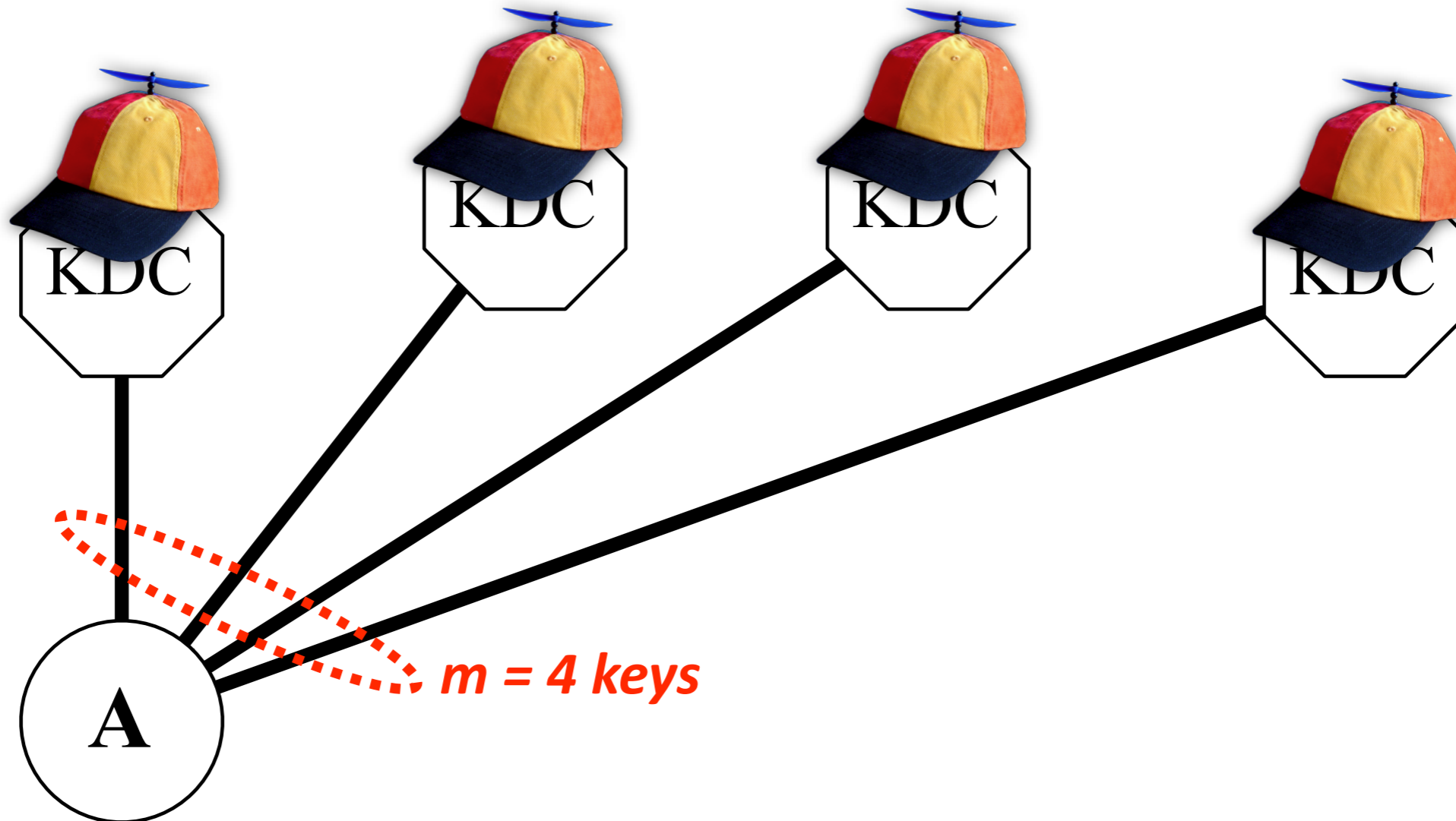


➡ Diffie-Hellman-Lamport proposed in 1976:

Increase the number of 'trusted parties' (m), and
distribute trust over these m different key distribution centers

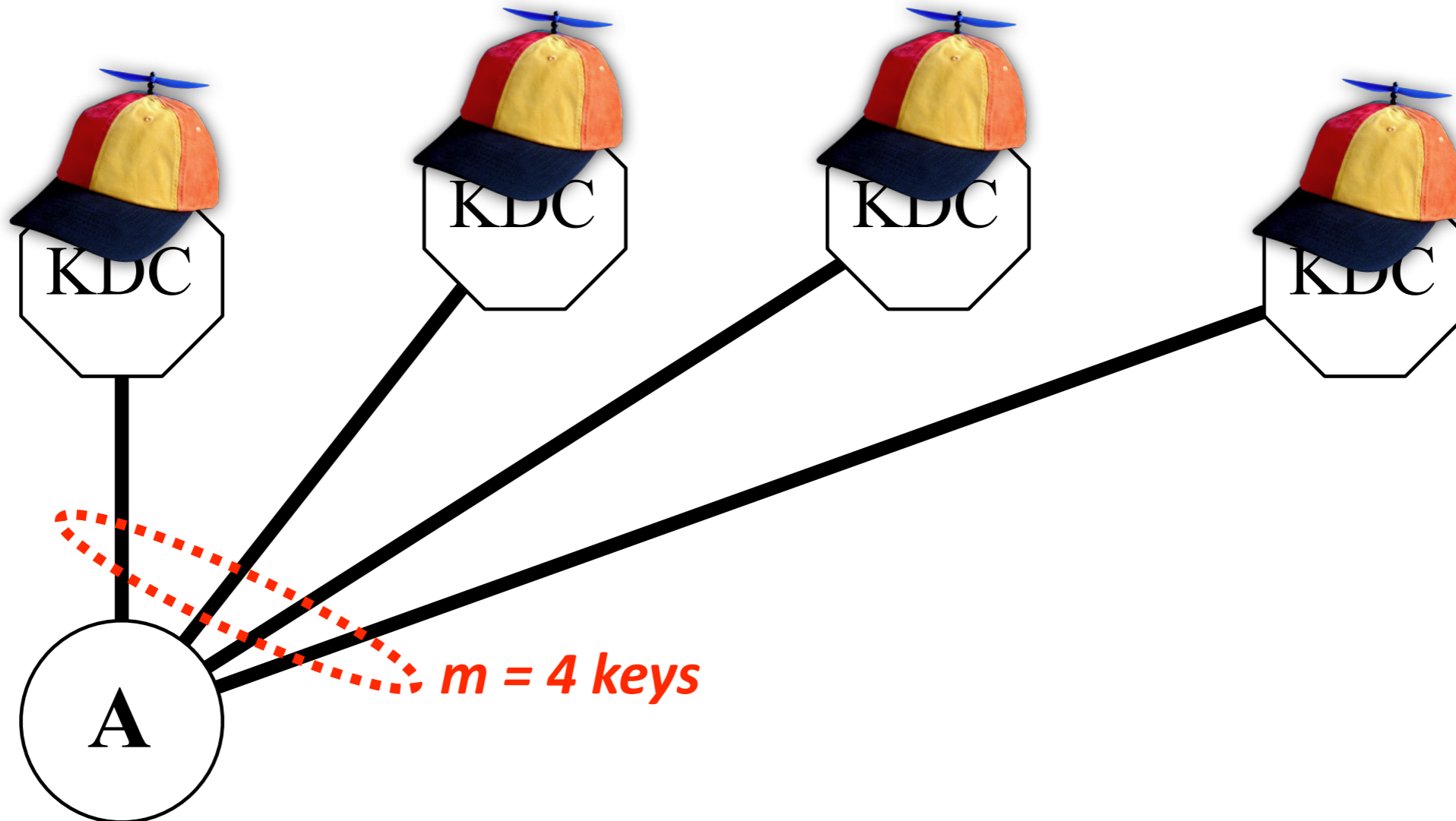


A (m-1) out of m KDC secure SKD overlay network





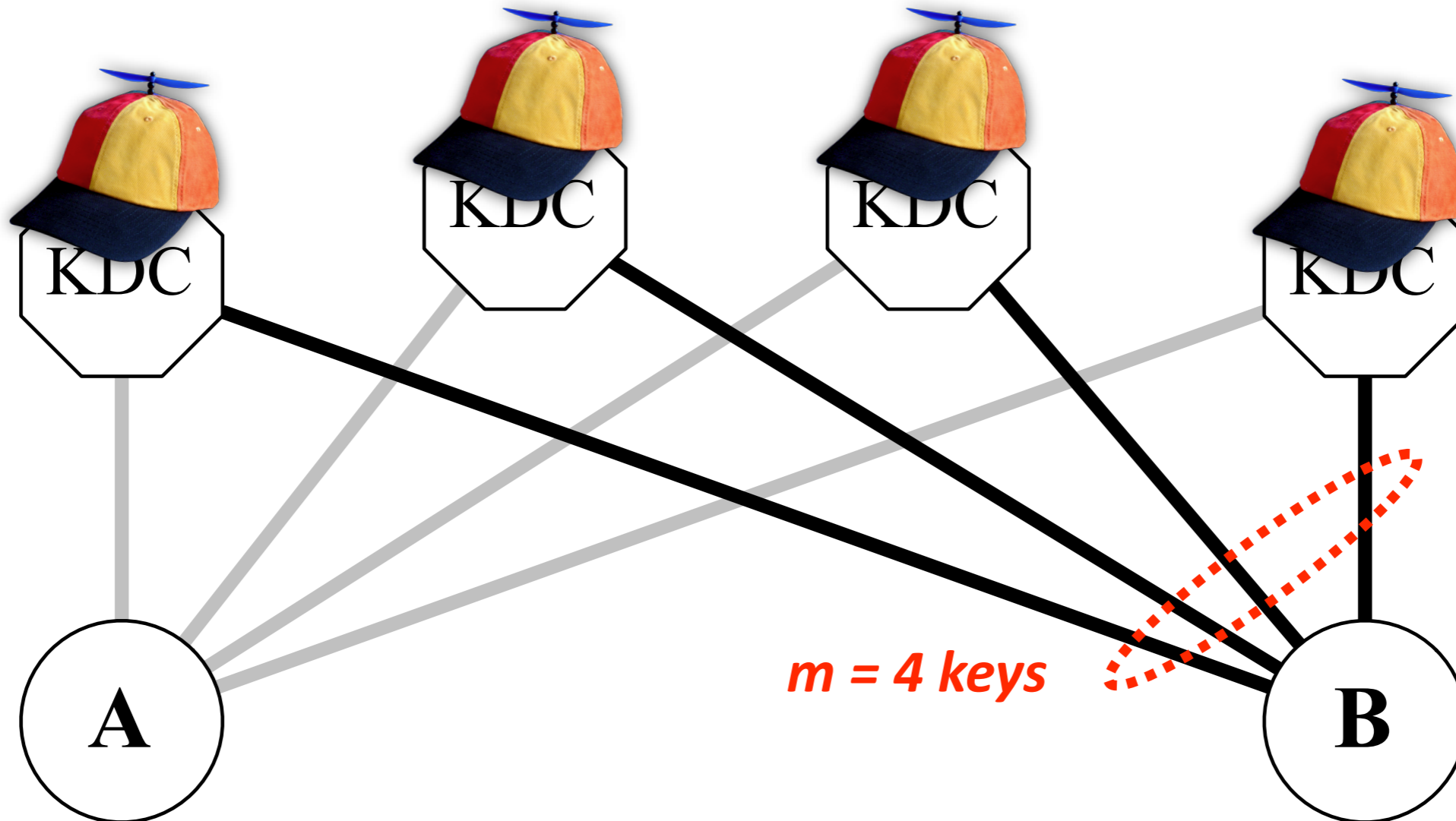
A (m-1) out of m KDC secure SKD overlay network



- ➡ Each token has m pairwise unique pre-shared keys, a different PSK for each of the m key distribution centers



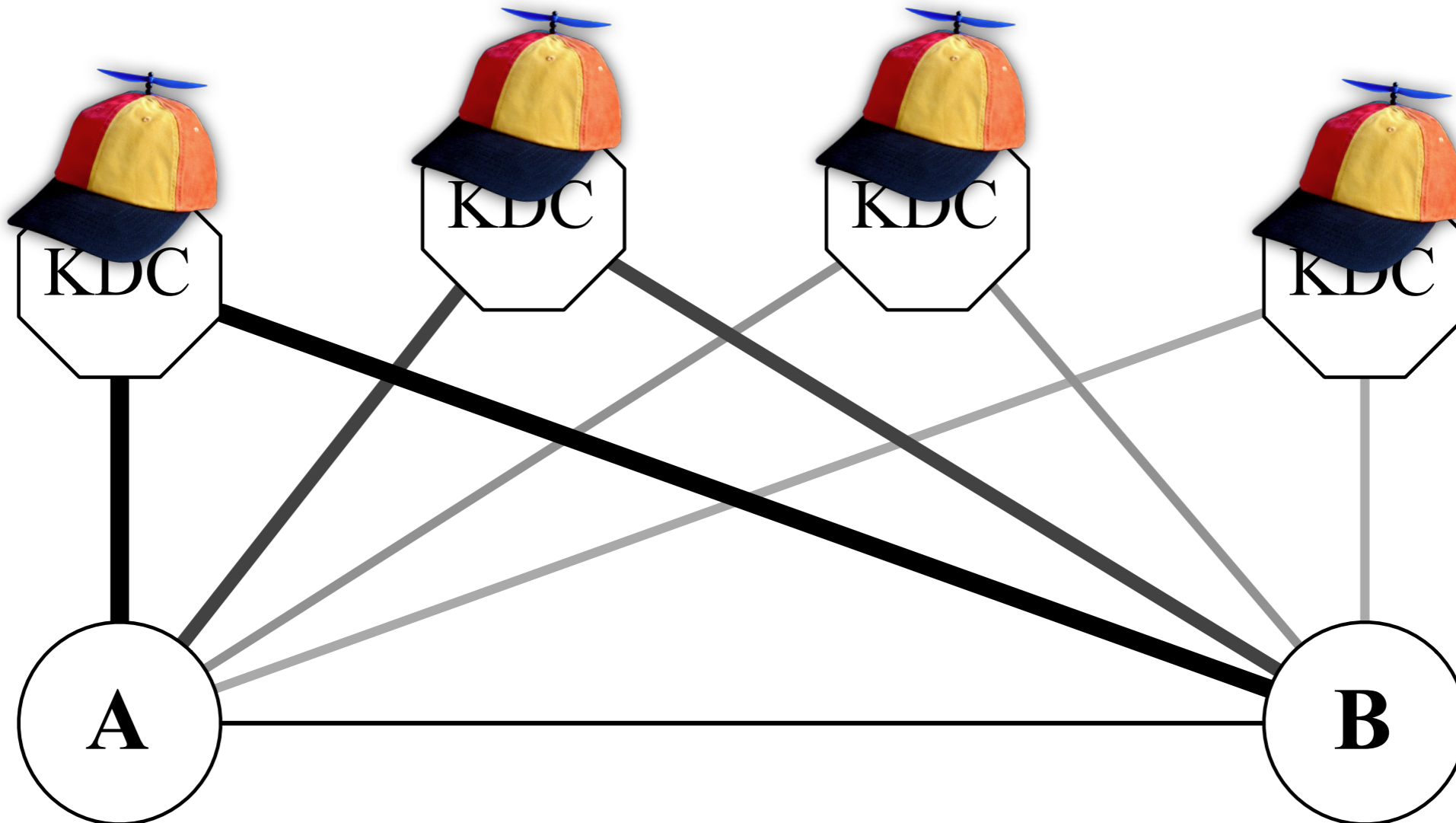
A (m-1) out of m KDC secure SKD overlay network



- Each token has m pairwise unique pre-shared keys, a different PSK for each of the m key distribution centers

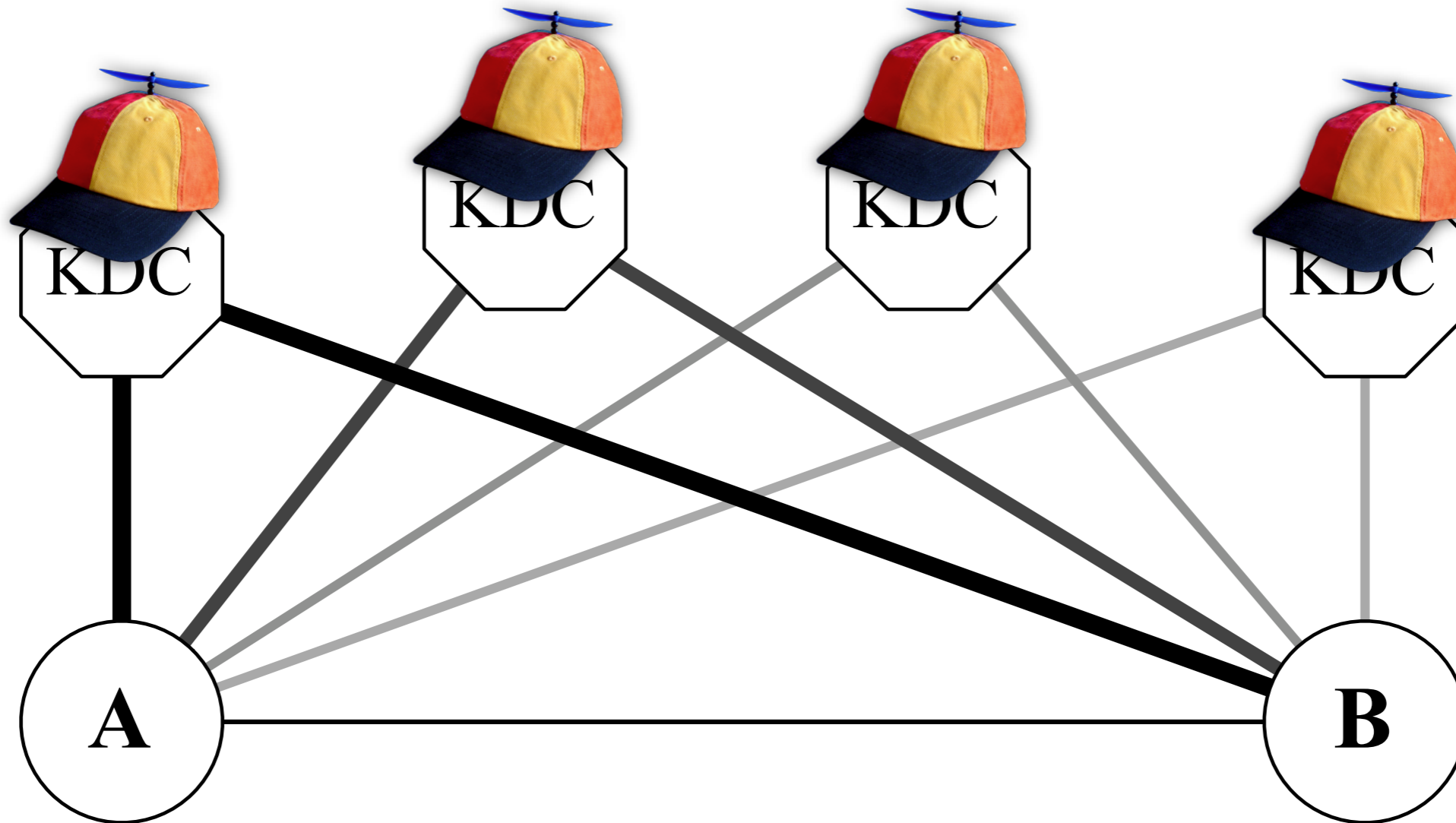


A (m-1) out of m KDC secure SKD overlay network





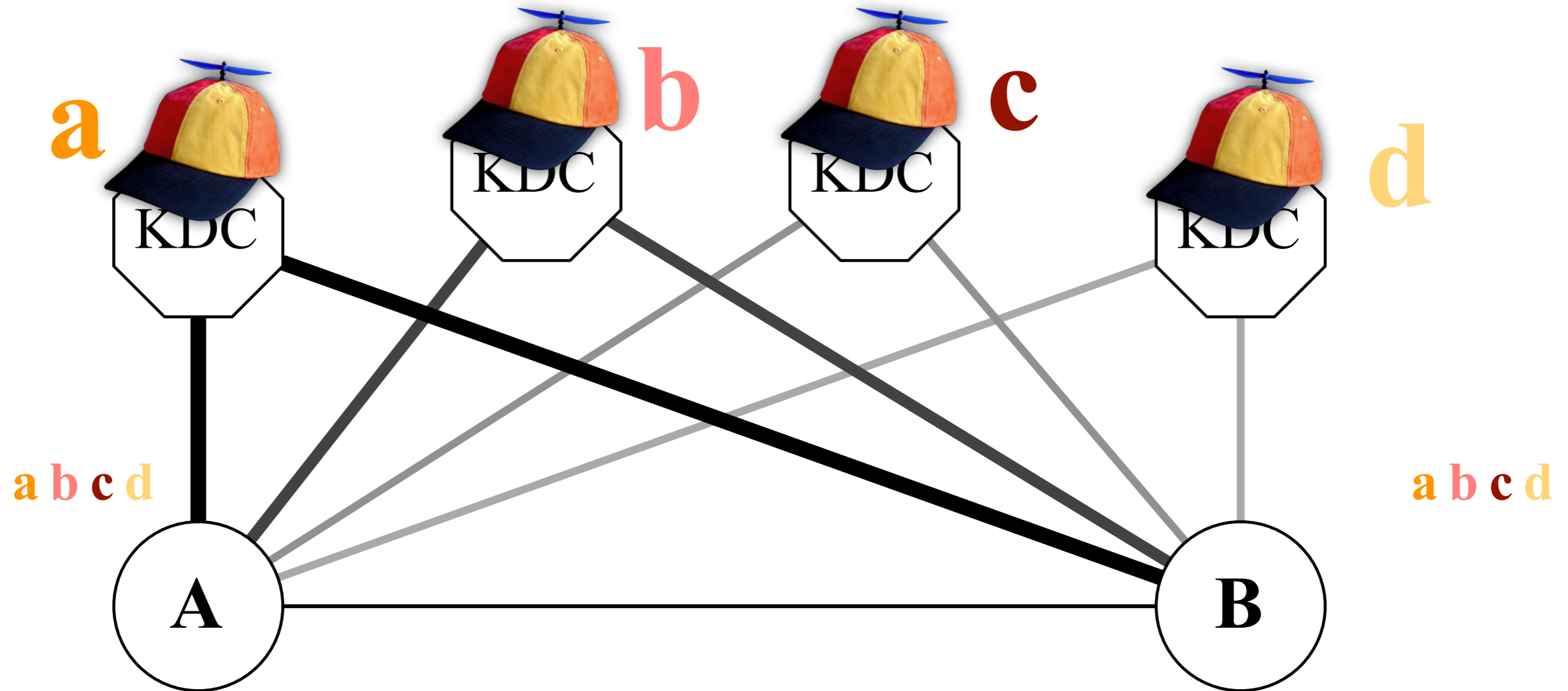
A (m-1) out of m KDC secure SKD overlay network



➡ A and B negotiate m symmetric keys using the m key distribution centers



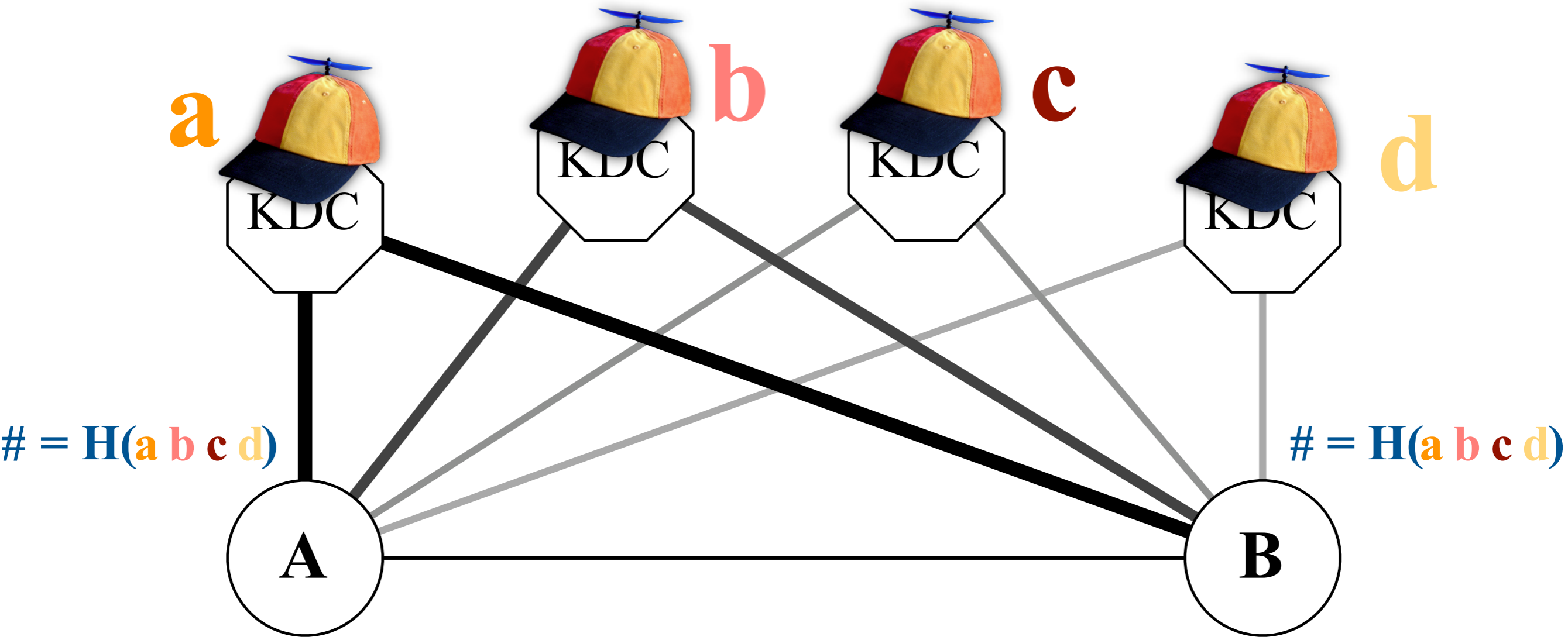
A (m-1) out of m KDC secure SKD overlay network



➡ A and B negotiate m symmetric keys using the m key distribution centers



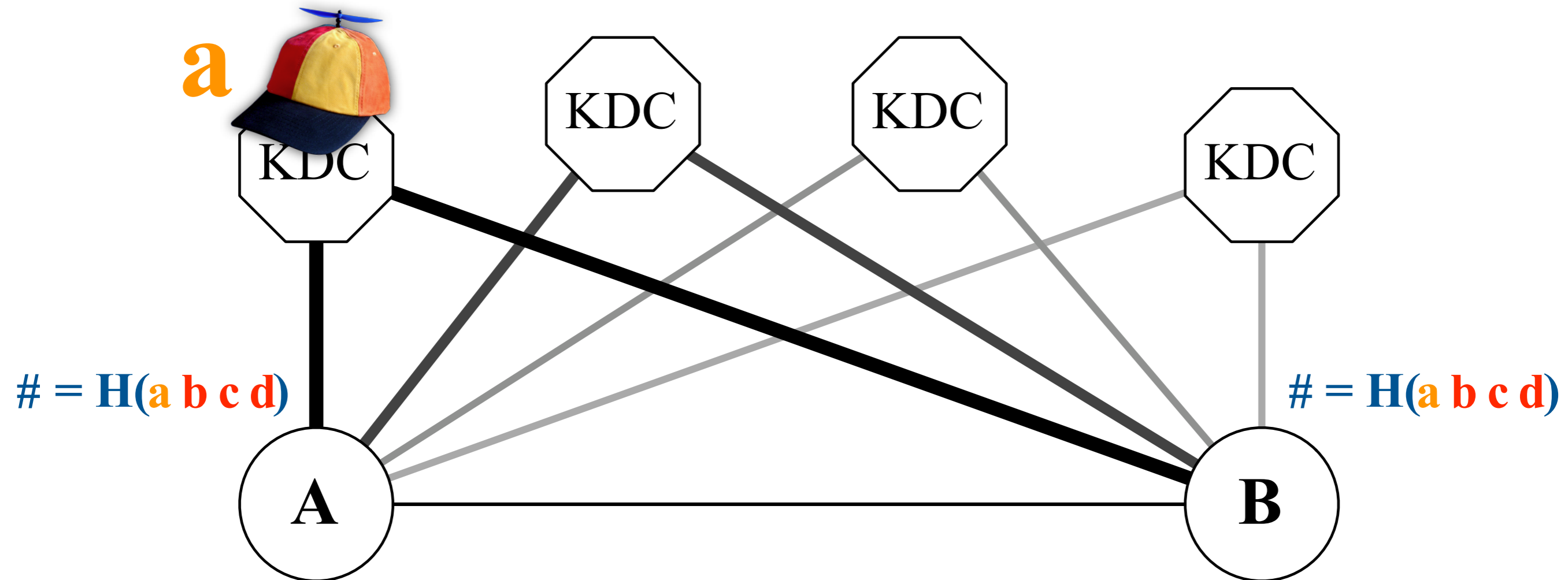
A (m-1) out of m KDC secure SKD overlay network



- ➡ A and B negotiate m symmetric keys using the m key distribution centers
- ➡ Then A and B hash their local copy of the m keys to make 1 shared key #

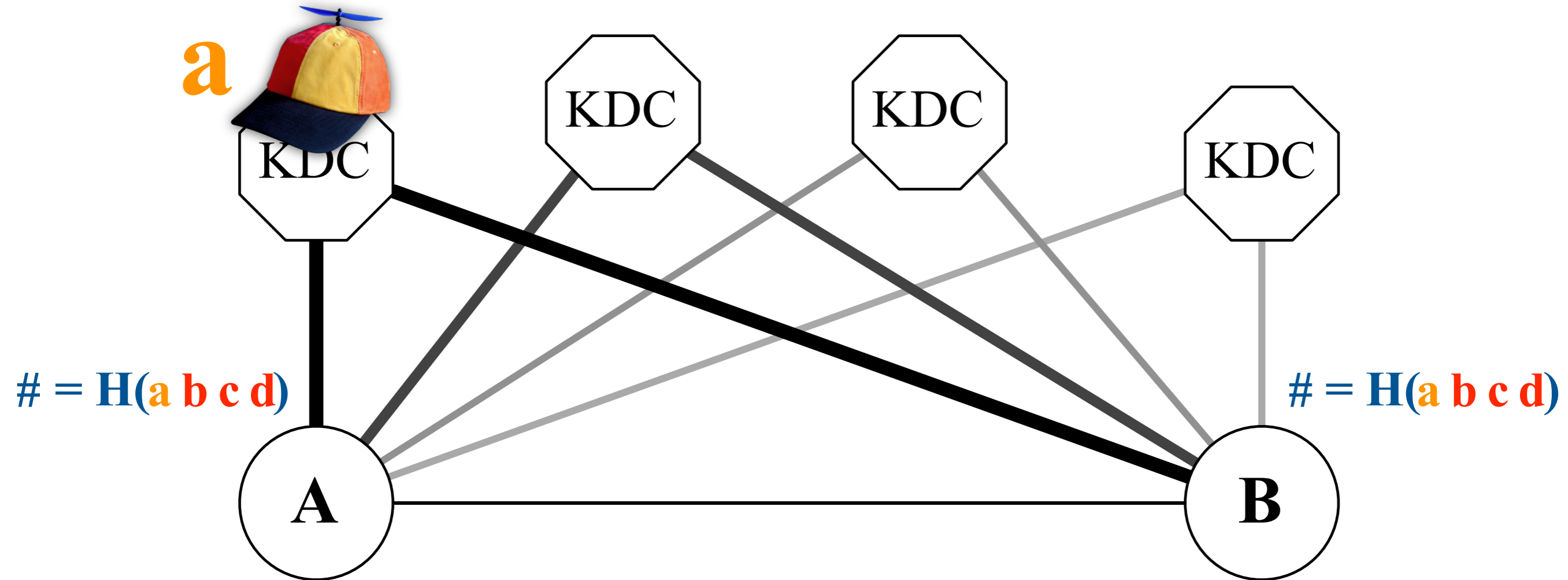


A (m-1) out of m KDC secure SKD overlay network





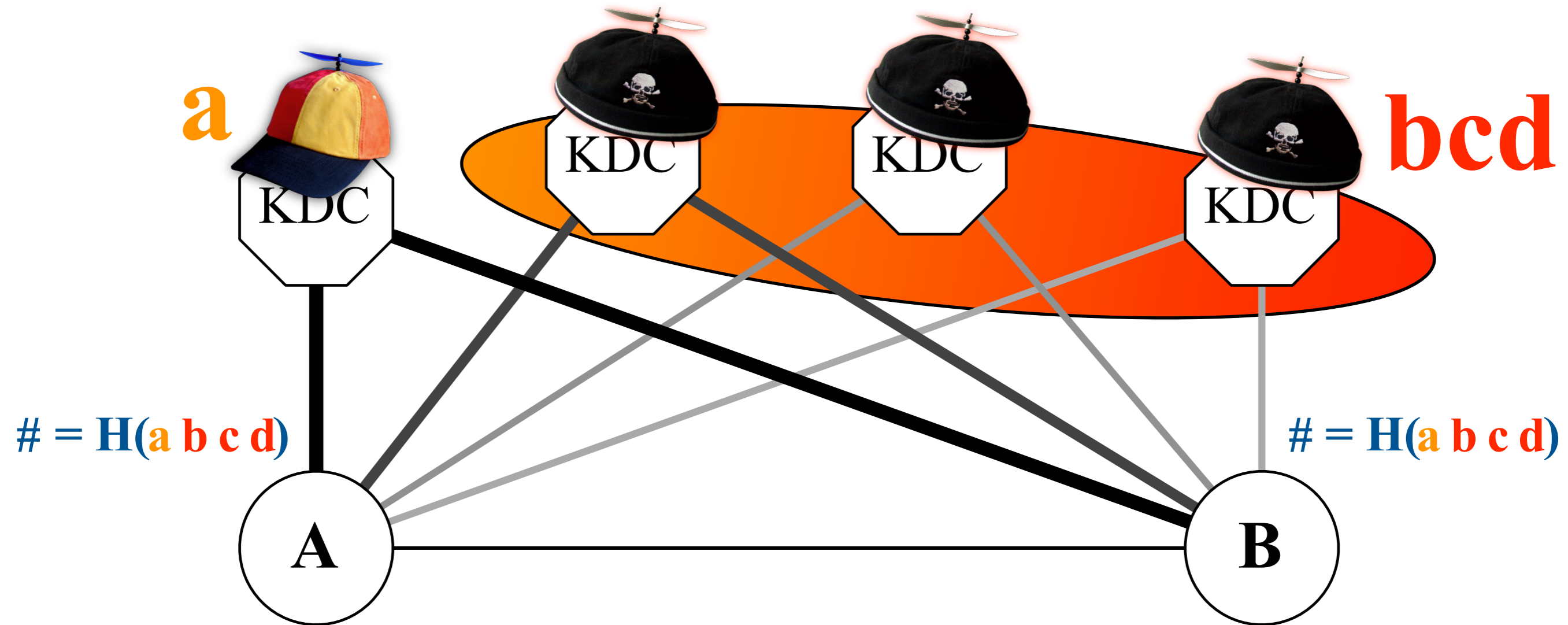
A (m-1) out of m KDC secure SKD overlay network



➡ A and B maintain their privacy so long as 1 KDC refuses to collude
This is because **trust is distributed** across all m service providers



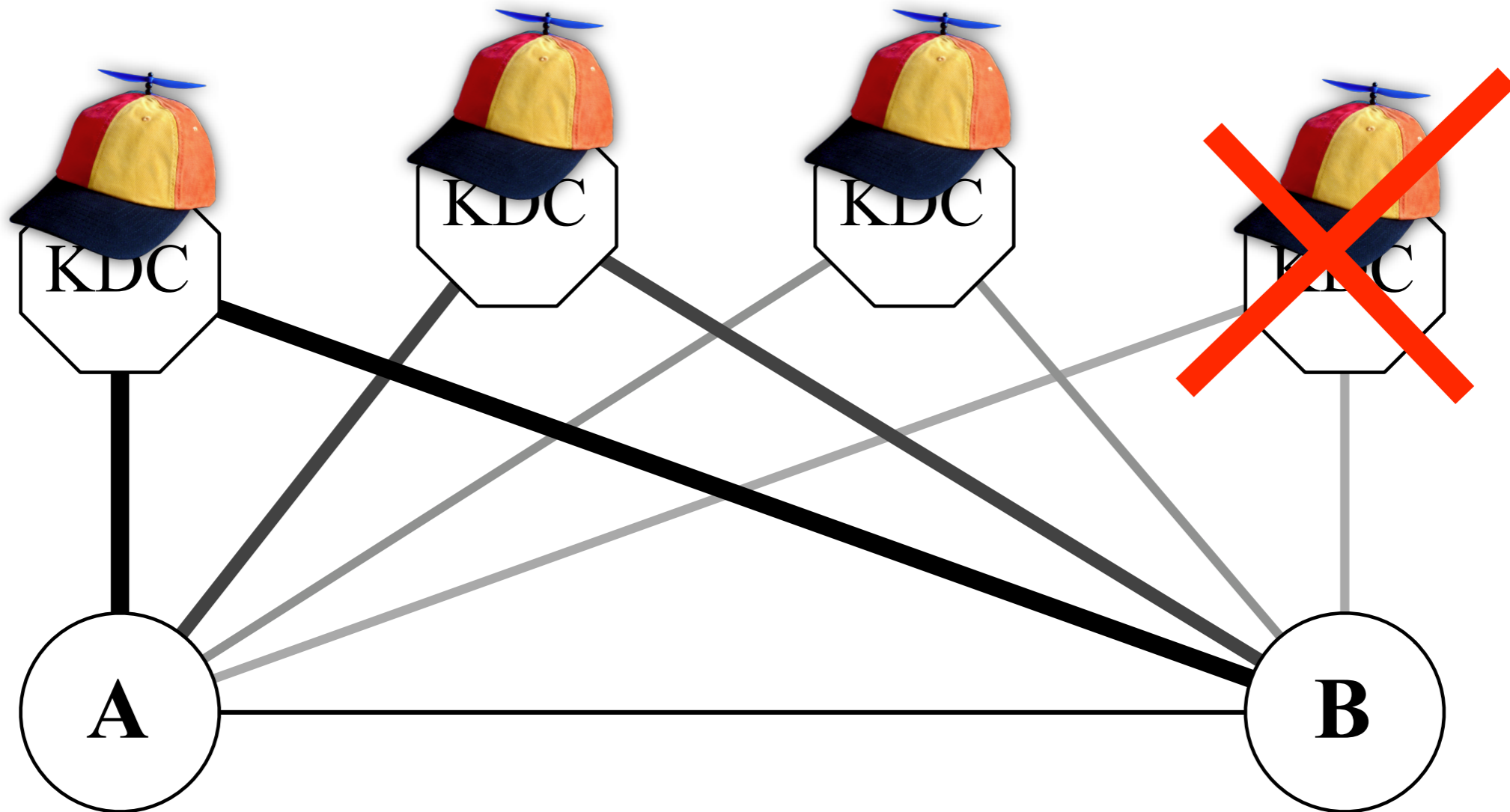
A (m-1) out of m KDC secure SKD overlay network



➡ A and B maintain their privacy so long as 1 KDC refuses to collude
 This is because **trust is distributed** across all m service providers

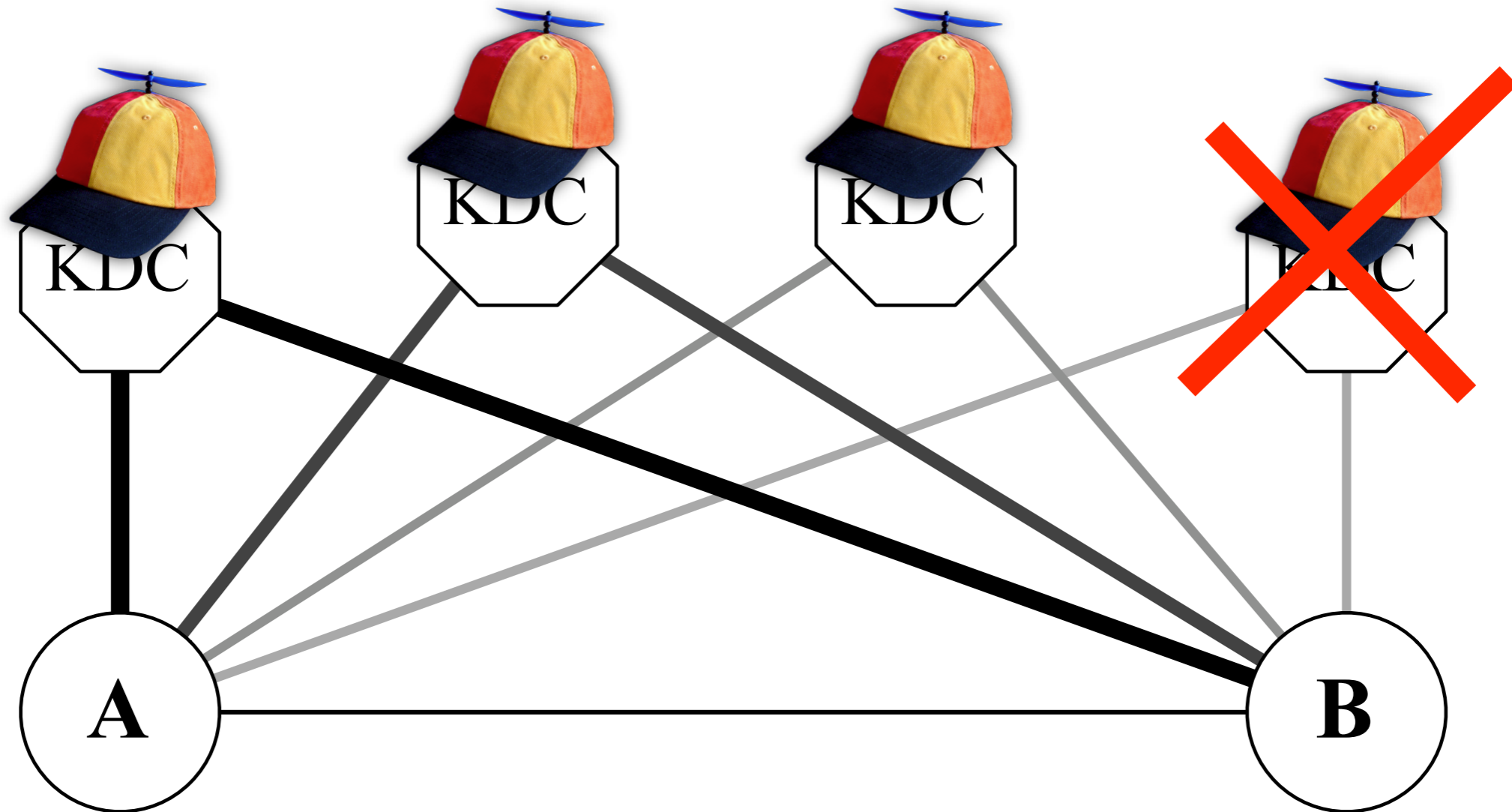


High availability





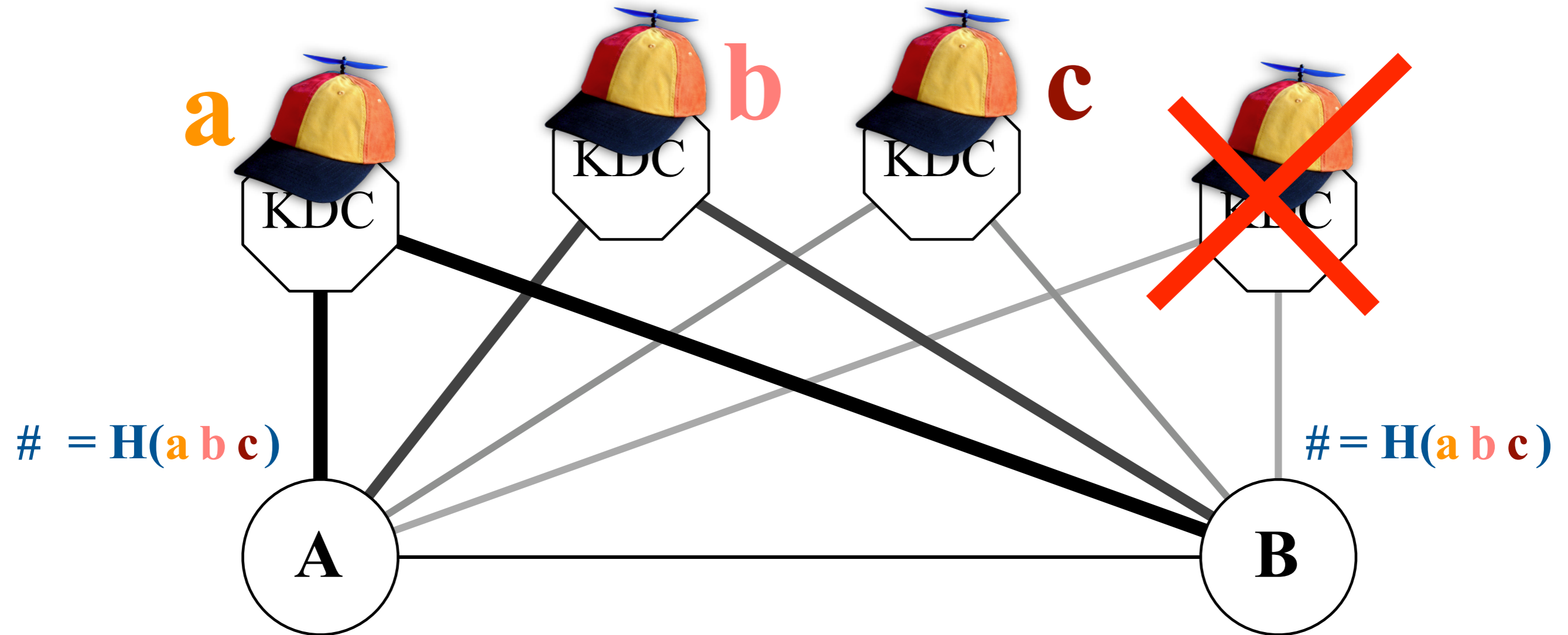
High availability



- If a service provider becomes unavailable, the users A and B can perform key exchanges with the remaining n servers. The security of that transaction reduces gracefully to $(n-1)$.



High availability

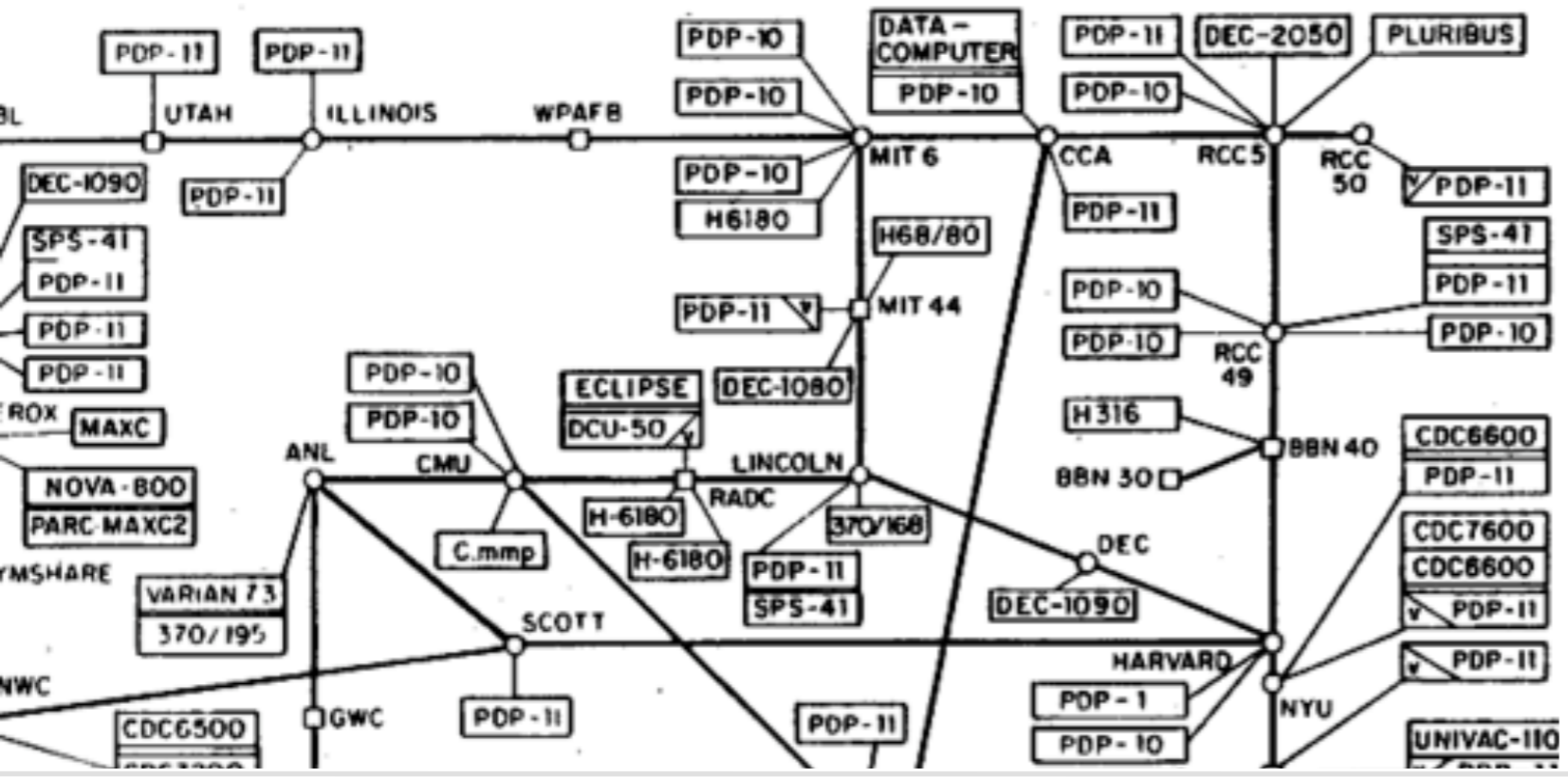


- ➡ If a service provider becomes unavailable, the users A and B can perform key exchanges with the remaining n servers. The security of that transaction reduces gracefully to $(n-1)$.

S. Kent (1976)

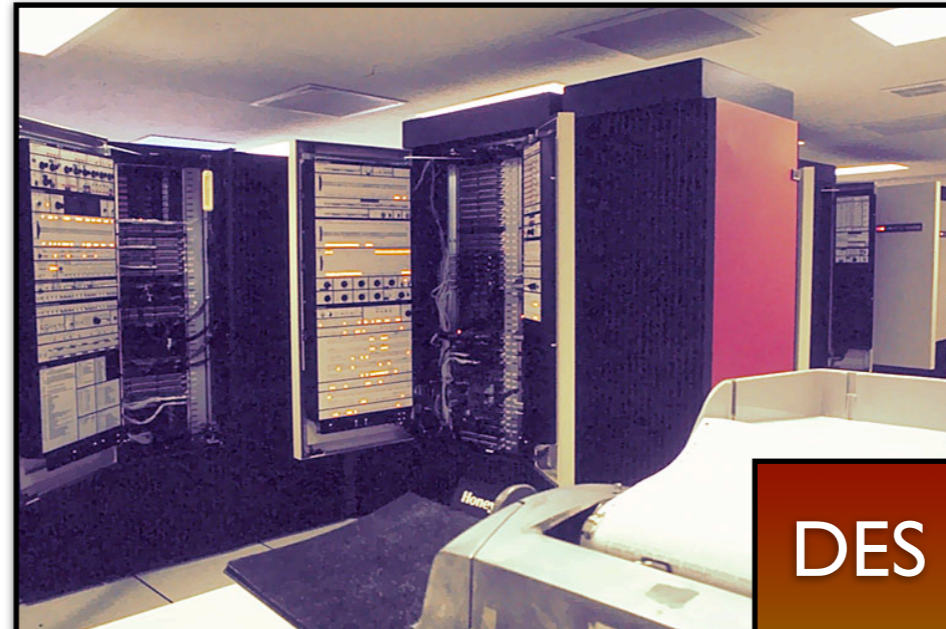
S. Kent (1976)

ARPANET LOGICAL MAP, MARCH 1977

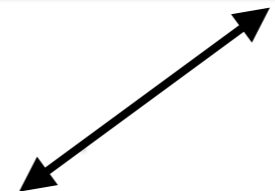
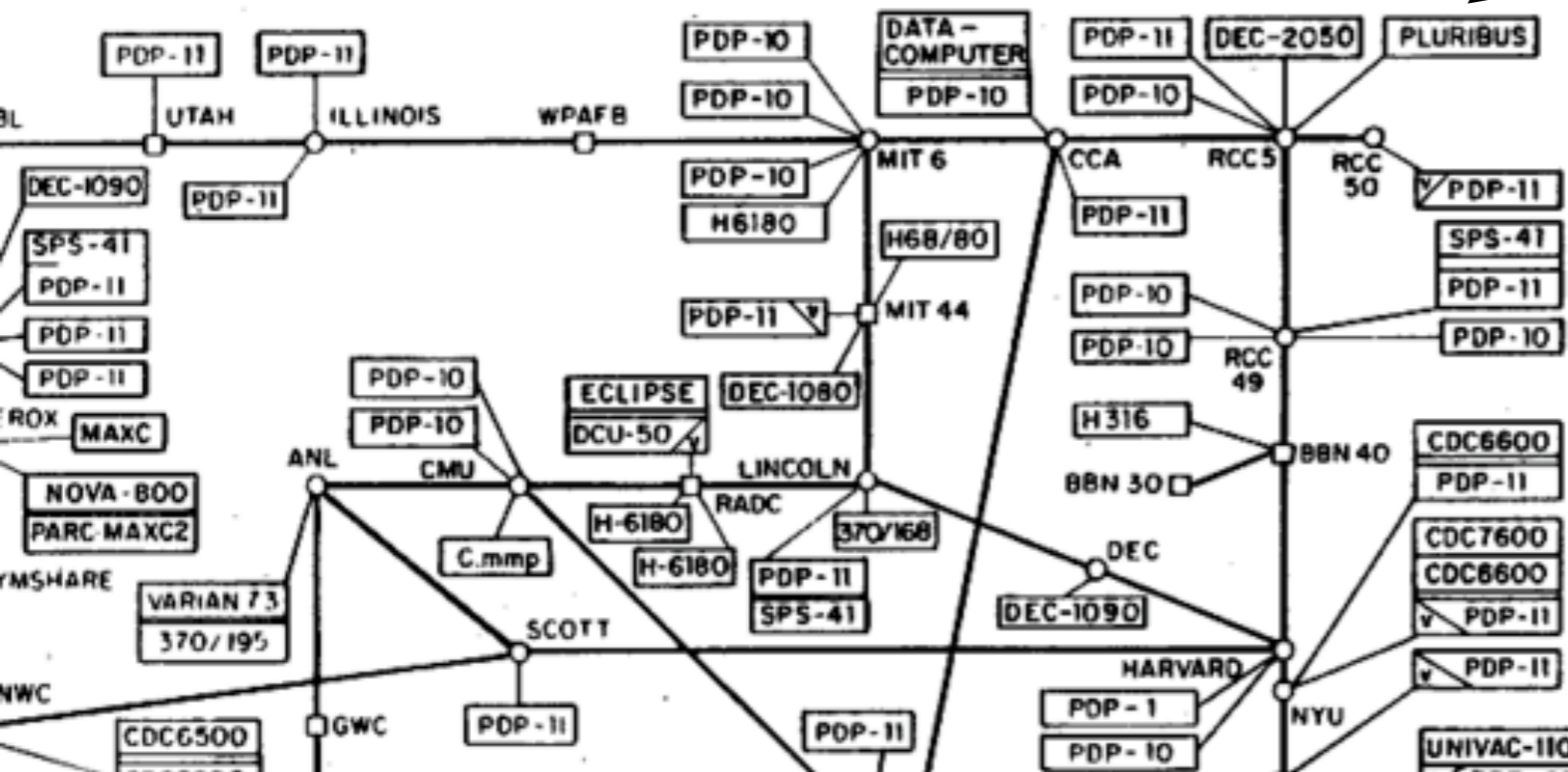




S. Kent (1976)



6180 CPU
(1MIPS)
MULTICS

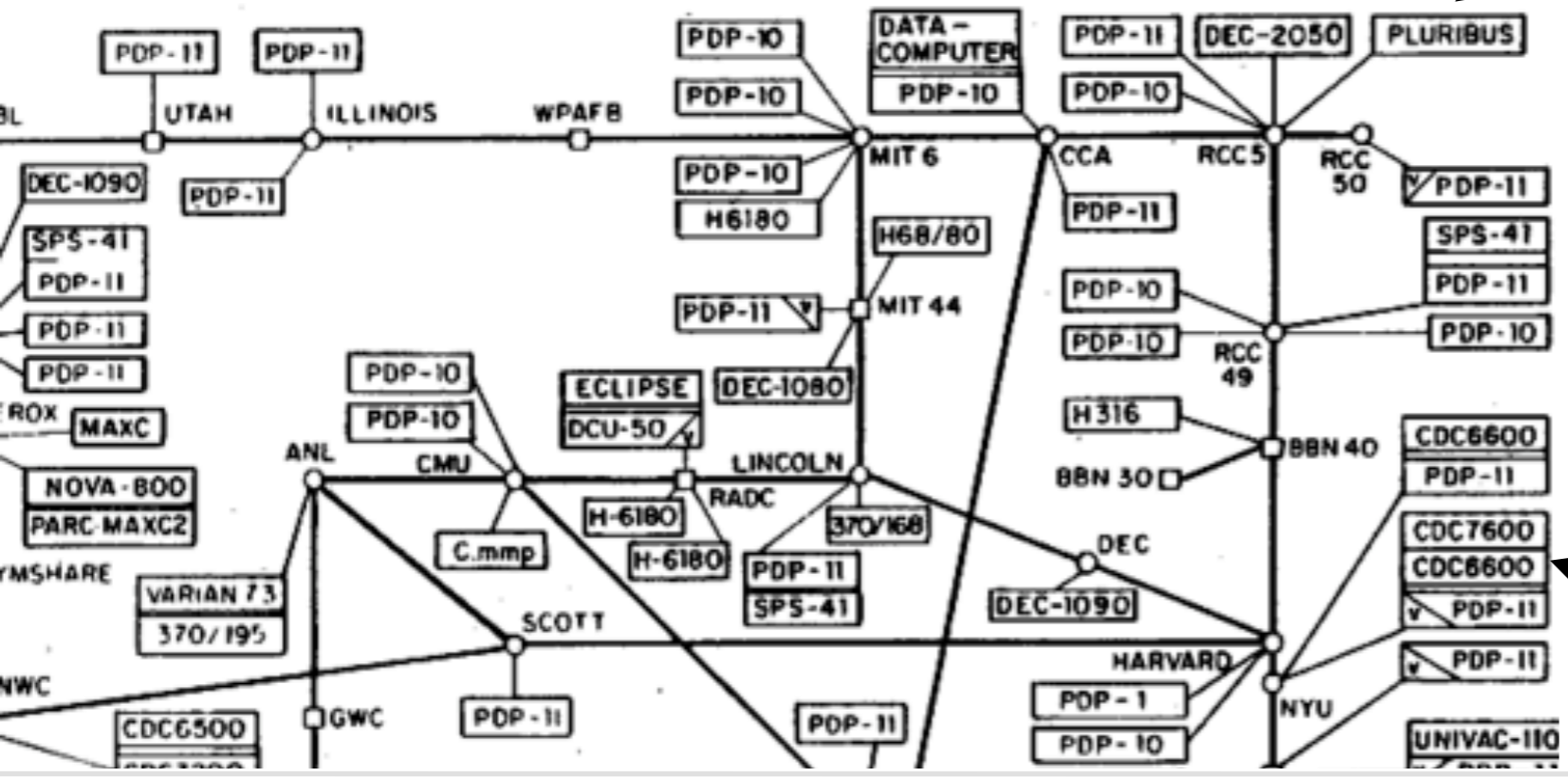


S. Kent (1976)



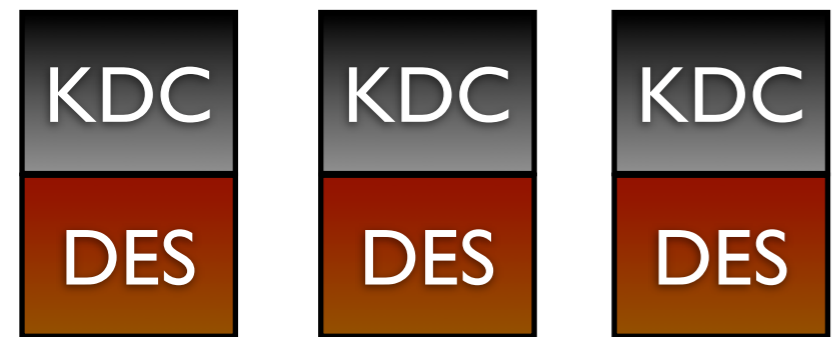
DES

Host Terminal with Card R/W
3 Keys on Magnetic Card

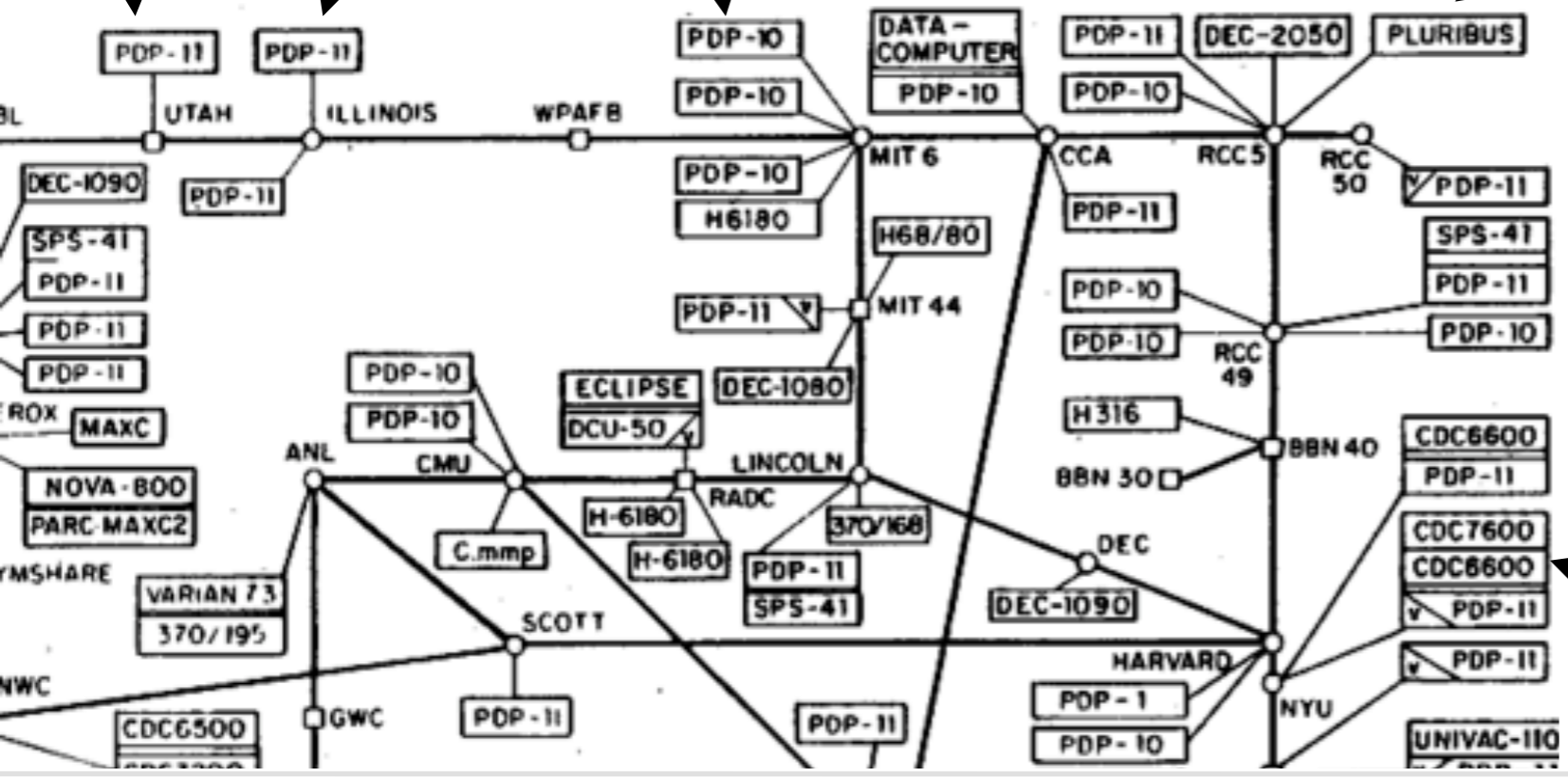


DES

S. Kent (1976)



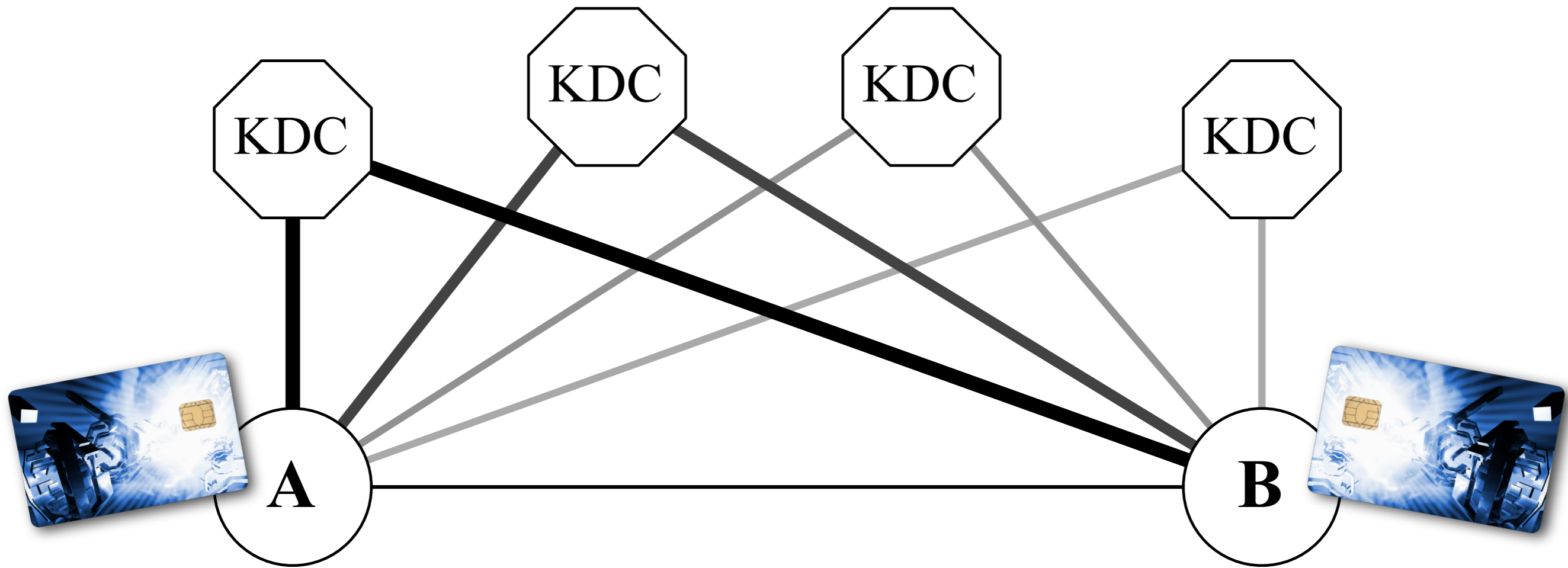
DES



DES

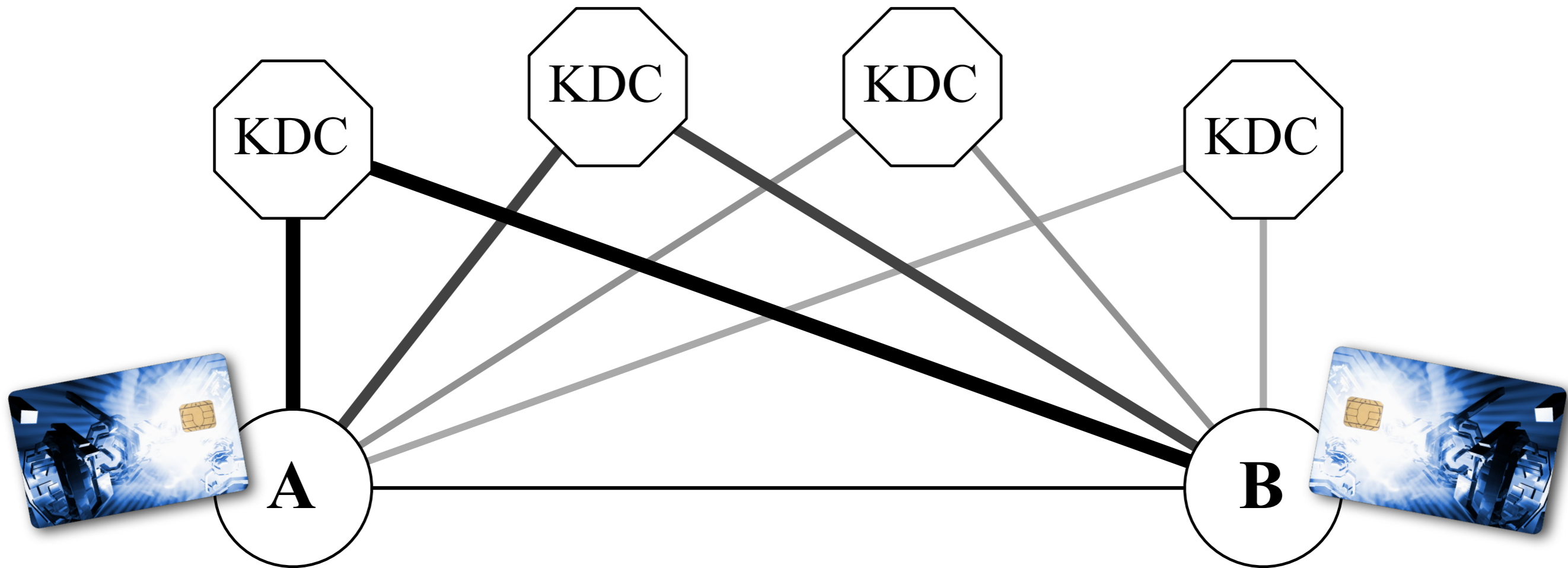


Synaptic's observation on global IdM/CKM services





Synaptic's observation on global IdM/CKM services

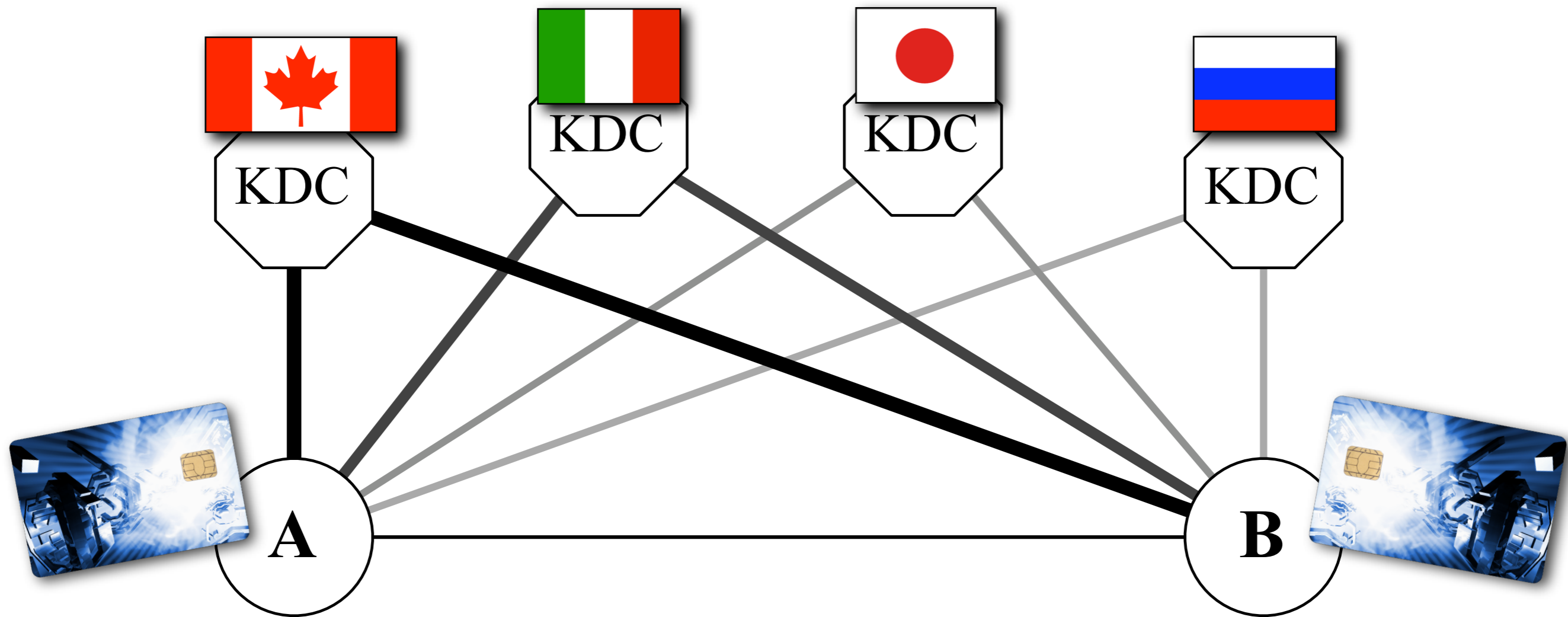


➡ Synaptic's observation:

The security of this proposal tends to increase if the KDC are managed by different organizations, even from different countries (eg. Canada, Italy, Japan, Russia)



Synaptic's observation on global IdM/CKM services



➡ Synaptic's observation:

The security of this proposal tends to increase if the KDC are managed by different organizations, even from different countries (eg. Canada, Italy, Japan, Russia)



Diffie-Hellman-Lamport-Synaptic design properties

Diffie-Hellman-Lamport-Synaptic design properties

- ➡ All pre-shared keys stored on smart cards can be negotiated using Synaptic's information-theoretic technique with ESE that is secure against insiders



Diffie-Hellman-Lamport-Synaptic design properties

- ▣▣▣▣➤ All pre-shared keys stored on smart cards can be negotiated using Synaptic's information-theoretic technique with ESE that is secure against insiders
- ▣▣▣▣➤ In this key distribution overlay network:
 - ▣▣▣▣➤ We ignore the underlying network topology



Diffie-Hellman-Lamport-Synaptic design properties

- ▣▣▣▣➤ All pre-shared keys stored on smart cards can be negotiated using Synaptic's information-theoretic technique with ESE that is secure against insiders
- ▣▣▣▣➤ In this key distribution overlay network:
 - ▣▣▣▣➤ We ignore the underlying network topology
 - ▣▣▣▣➤ We upper-bound the number of participating service providers, irrespective of the number of users



Diffie-Hellman-Lamport-Synaptic design properties

- All pre-shared keys stored on smart cards can be negotiated using Synaptic's information-theoretic technique with ESE that is secure against insiders
- In this key distribution overlay network:
 - We ignore the underlying network topology
 - We upper-bound the number of participating service providers, irrespective of the number of users
 - The participating service providers can be owned and managed by different organisations, preferably from different countries



Diffie-Hellman-Lamport-Synaptic design properties

- ▣▣▣▣➤ All pre-shared keys stored on smart cards can be negotiated using Synaptic's information-theoretic technique with ESE that is secure against insiders
- ▣▣▣▣➤ In this key distribution overlay network:
 - ▣▣▣▣➤ We ignore the underlying network topology
 - ▣▣▣▣➤ We upper-bound the number of participating service providers, irrespective of the number of users
 - ▣▣▣▣➤ The participating service providers can be owned and managed by different organisations, preferably from different countries
 - ▣▣▣▣➤ Non-aligned users may trust the competitive/adversarial service providers not to collude against them



Diffie-Hellman-Lamport-Synaptic design properties

- All pre-shared keys stored on smart cards can be negotiated using Synaptic's information-theoretic technique with ESE that is secure against insiders
- In this key distribution overlay network:
 - We ignore the underlying network topology
 - We upper-bound the number of participating service providers, irrespective of the number of users
 - The participating service providers can be owned and managed by different organisations, preferably from different countries
 - Non-aligned users may trust the competitive/adversarial service providers not to collude against them
 - There is no system-wide single-point-of-trust-failure in the architecture



Diffie-Hellman-Lamport-Synaptic design properties

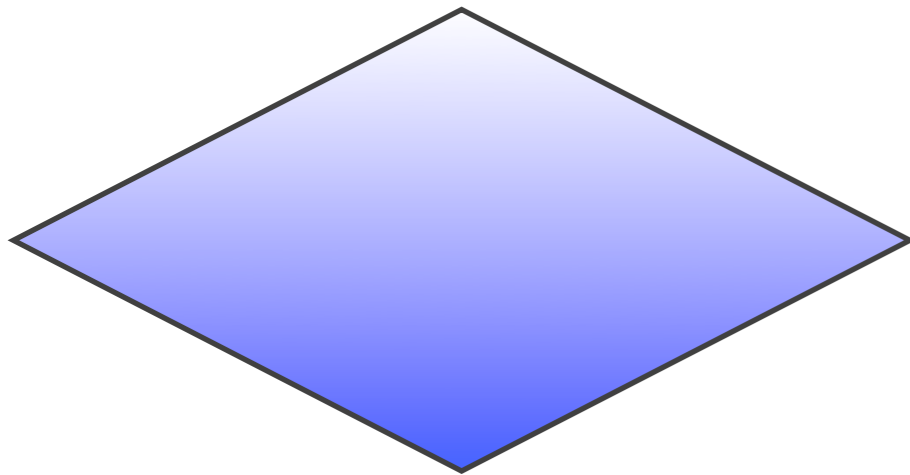
- All pre-shared keys stored on smart cards can be negotiated using Synaptic's information-theoretic technique with ESE that is secure against insiders
- In this key distribution overlay network:
 - We ignore the underlying network topology
 - We upper-bound the number of participating service providers, irrespective of the number of users
 - The participating service providers can be owned and managed by different organisations, preferably from different countries
 - Non-aligned users may trust the competitive/adversarial service providers not to collude against them
 - There is no system-wide single-point-of-trust-failure in the architecture
 - End-to-end redundancy reaches all the way to the end user (token)



**A step towards a defense-in-depth solution , that
extends the life, availability and functionality of our
existing security investments:**



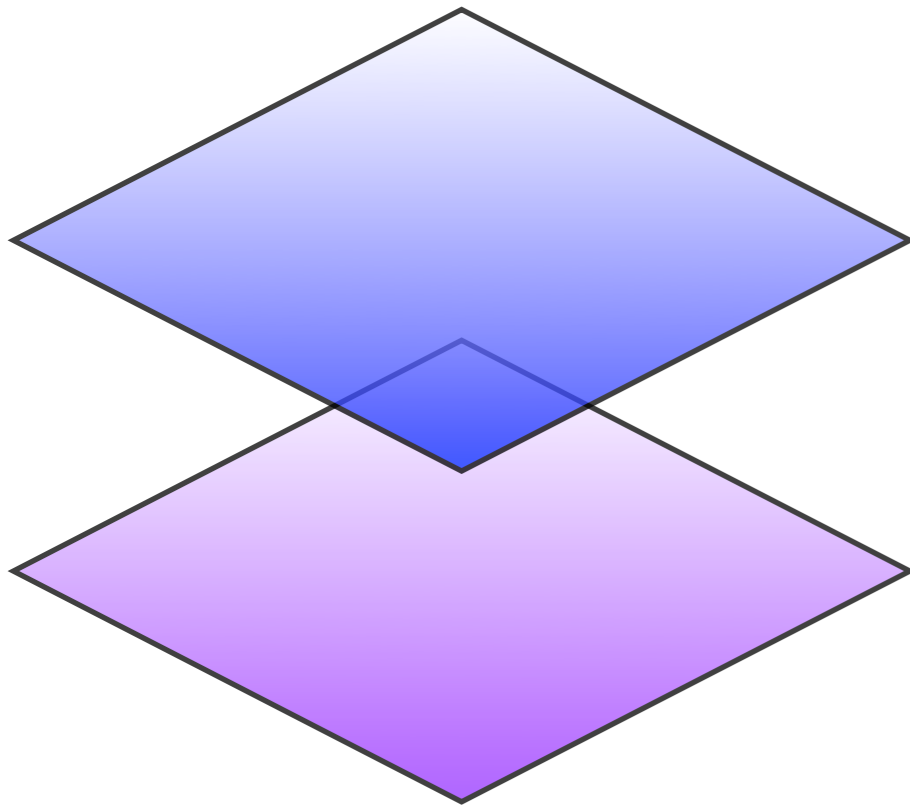
**A step towards a defense-in-depth solution , that
extends the life, availability and functionality of our
existing security investments:**



⇐ **Asymmetric**
Unmodified SSL/TLS, etc



A step towards a defense-in-depth solution , that extends the life, availability and functionality of our existing security investments:



⇐ **Asymmetric**

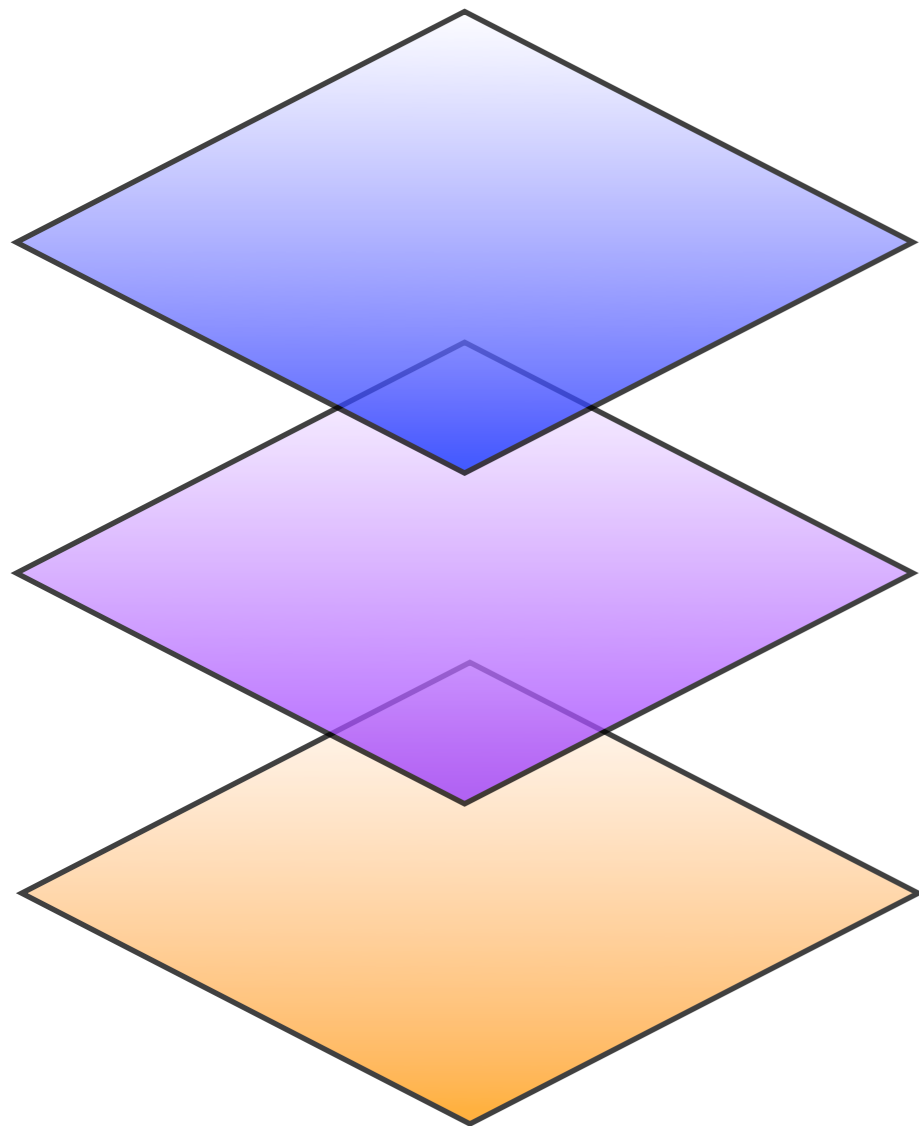
Unmodified SSL/TLS, etc

⇐ **Symmetric Systems**

Designs based on Diffie-Hellman-Lampert that wrap around output of SSL/TLS



A step towards a defense-in-depth solution , that extends the life, availability and functionality of our existing security investments:



⇐ **Asymmetric**

Unmodified SSL/TLS, etc

⇐ **Symmetric Systems**

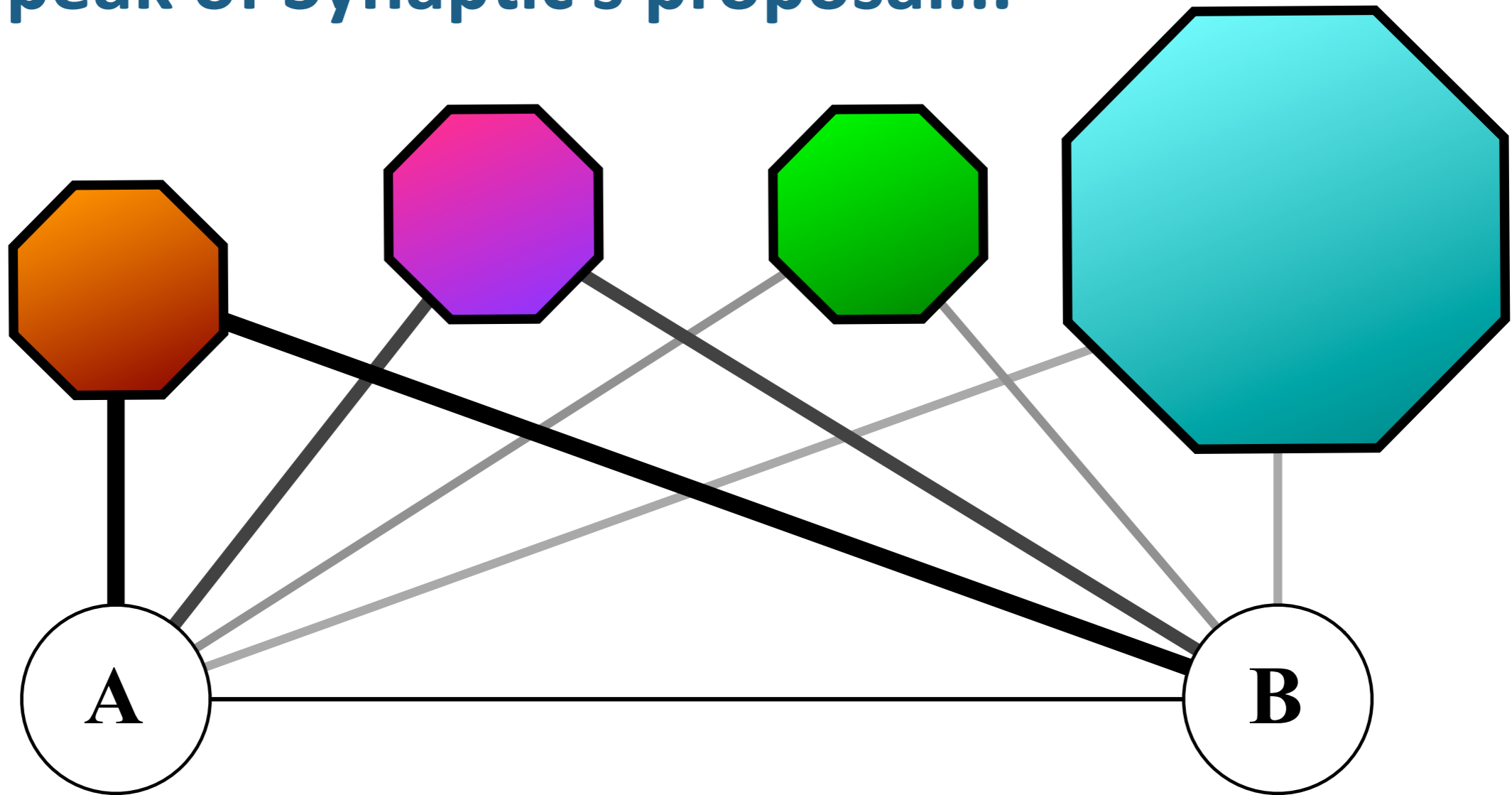
Designs based on Diffie-Hellman-Lampert that wrap around output of SSL/TLS

⇐ **Quantum Key Distribution**

QKD network single-point-of-trust failures protected by PQS (m-1) secure symmetric key distribution architecture

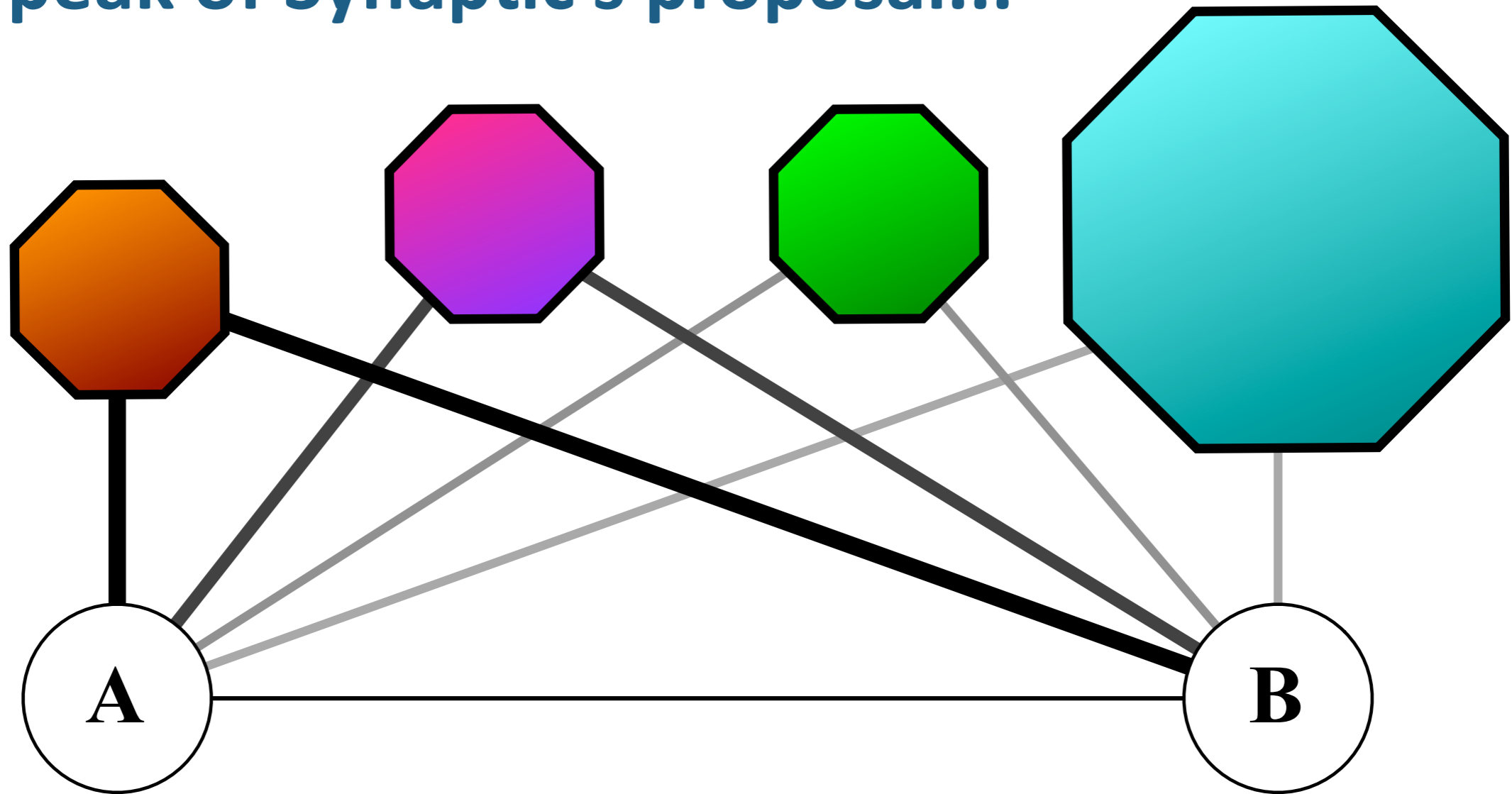


Sneak peak of Synaptic's proposal...





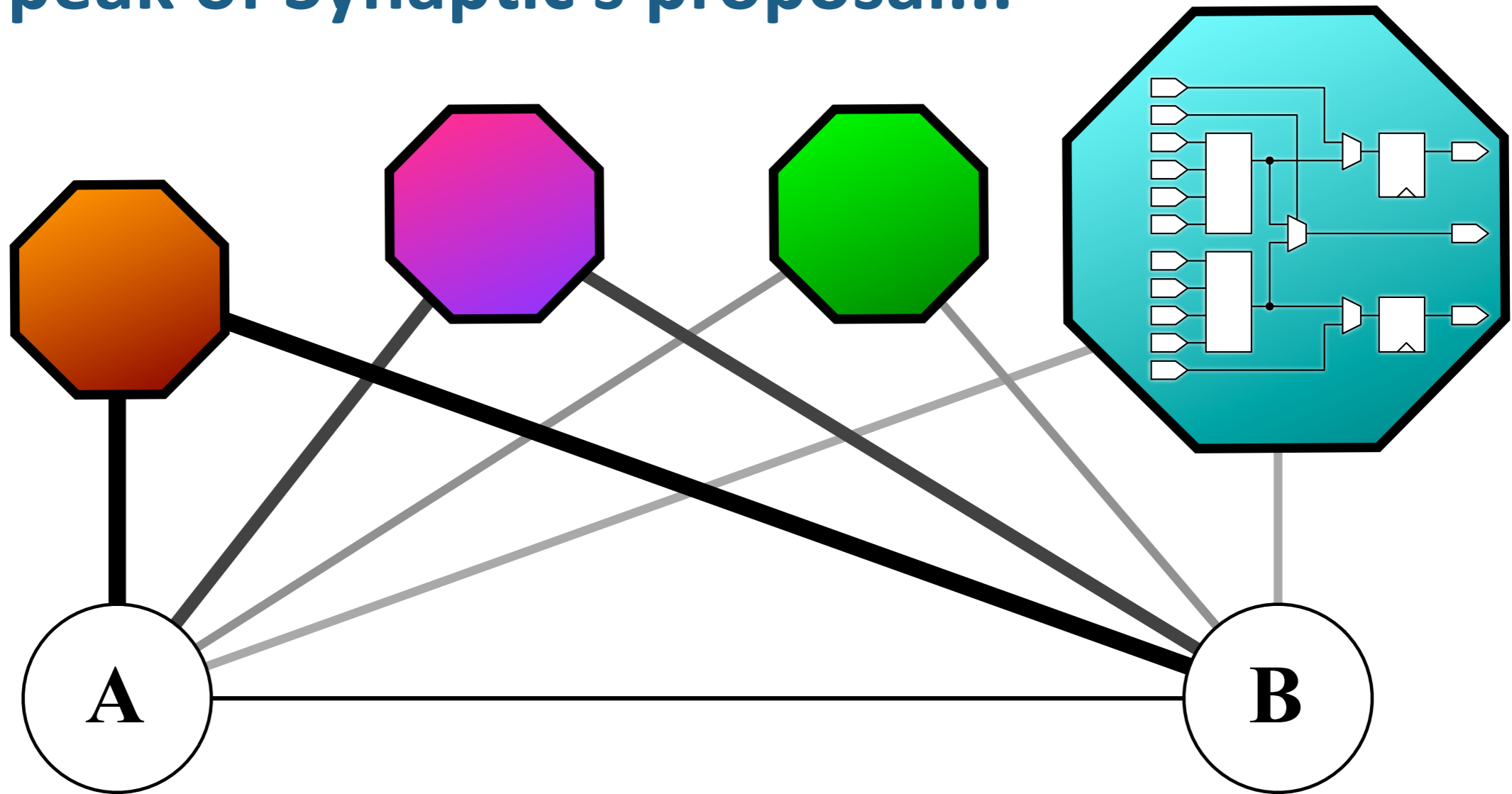
Sneak peak of Synaptic's proposal...



➡ But how do we achieve global scalability of DHL's proposal?



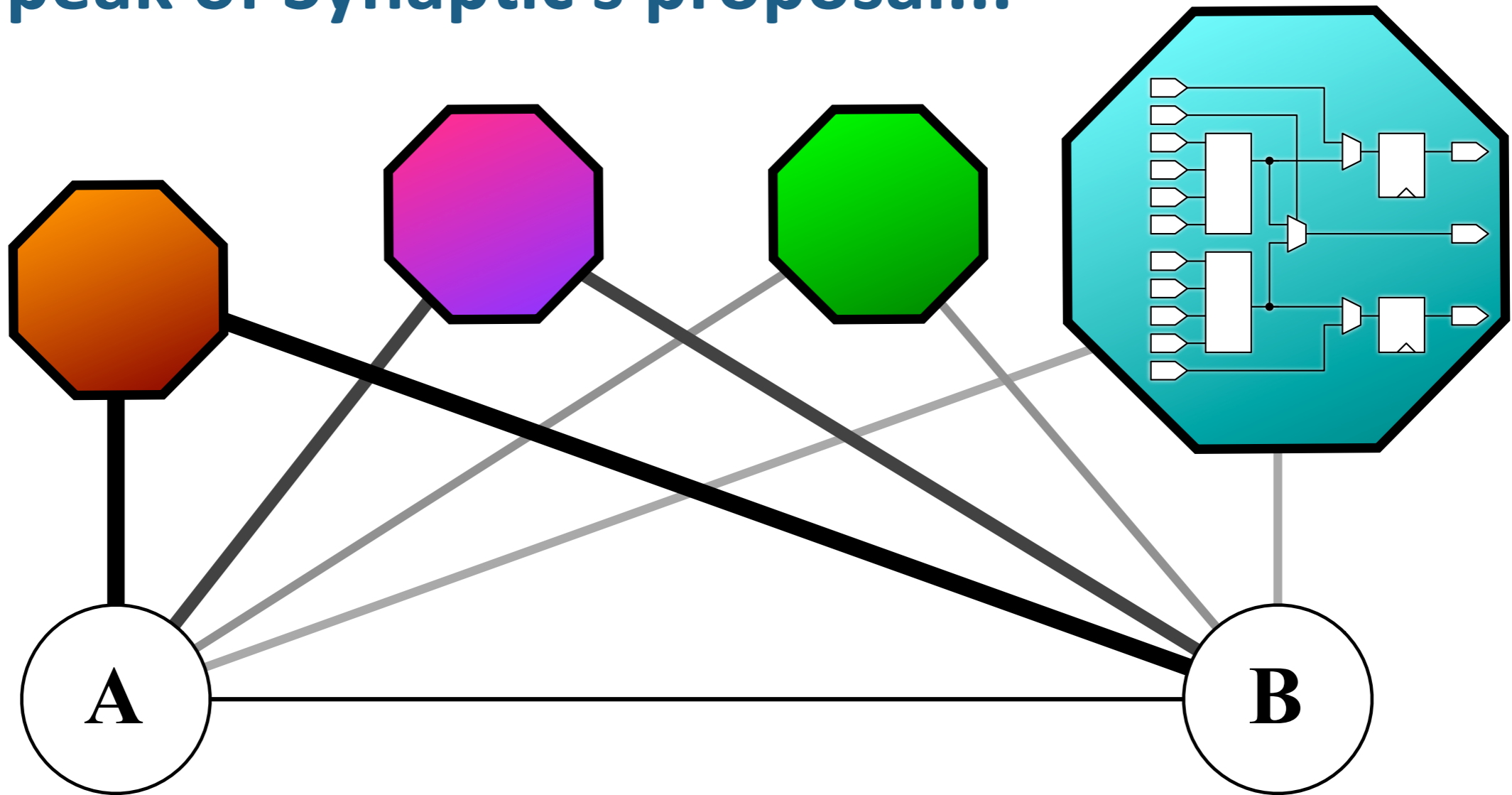
Sneak peak of Synaptic's proposal...



➡ But how do we achieve global scalability of DHL's proposal?



Sneak peak of Synaptic's proposal...



➡ But how do we achieve global scalability of DHL's proposal?

Every key distribution center is a service run by a computer, where that computer is itself built from a network of processing and storage elements...

Closing statement

Closing statement

We need IdM/CKM designs that **empower existing (semi-)autonomous Authorities** to work together with other (semi-)autonomous **Authorities** both **inter/intra domain** and **internationally** to fulfil their respective **mission objectives**

Closing statement

We need IdM/CKM designs that **empower existing (semi-)autonomous Authorities** to work together with other (semi-)autonomous **Authorities** both **inter/intra domain** and **internationally** to fulfil their respective **mission objectives**

We need **inclusive** electronic systems that support a thriving **ecosystem** of autonomous organisations **collaborating** to improve **global security**





“Team Earth”



Contact: **Benjamin Gittins**

Chief Technical Officer and Architect
Synaptic Laboratories Limited

Email: cto@pqs.io

Phone: +356 7956 2164

Web: <http://synaptic-labs.com>