Supporting Unconditionally Secure Authentication within e-Government Infrastructure based on QKD

Sufyan T. Faraj Al-Janabi (Ph.D., Prof.)

College of Computer Science and IT

University of Anbar, Ramadi, Iraq

saljanabi@fulbrightmail.org

Contents

Problem Statement

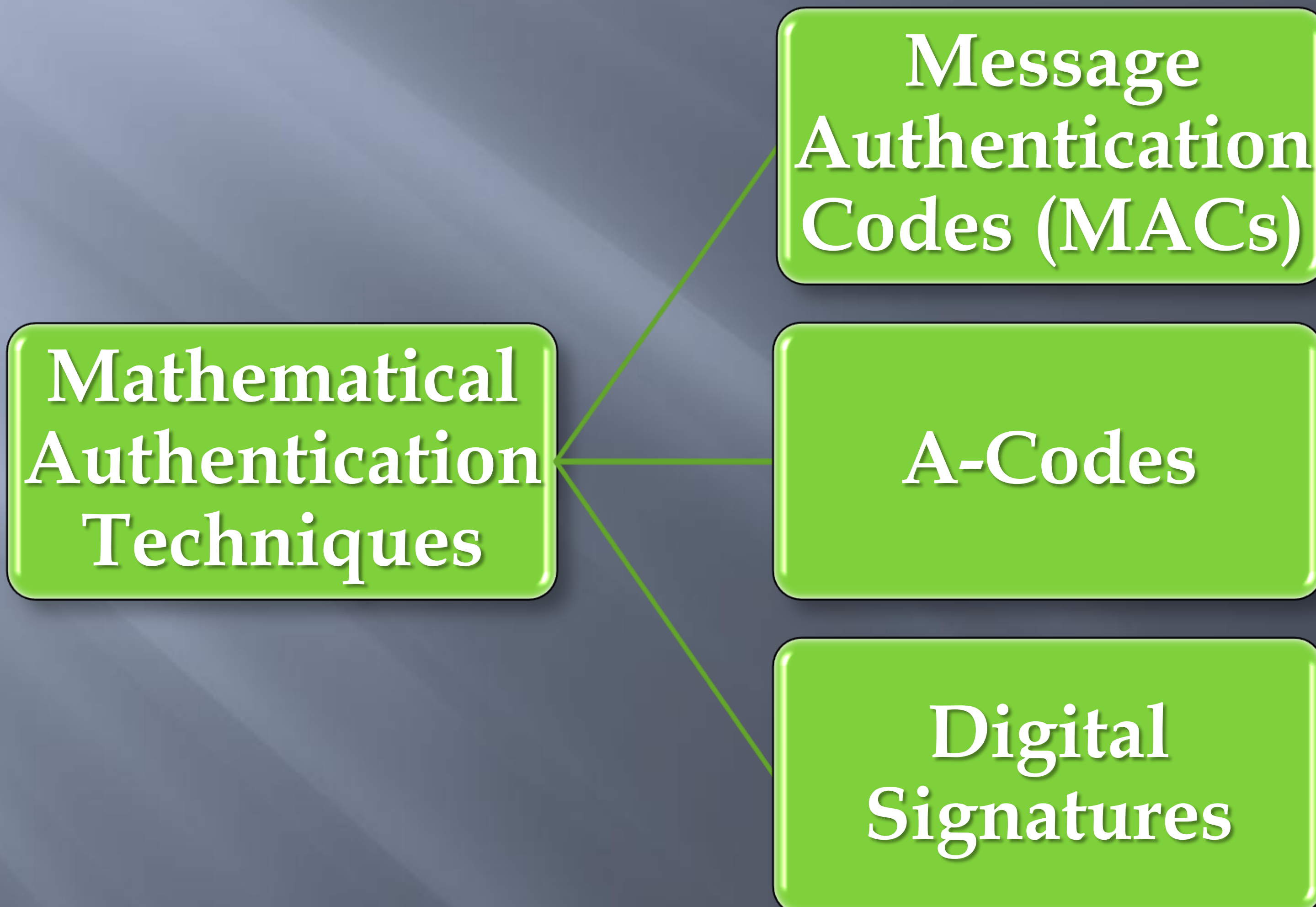
- It has been noticed that the speed of ICT advancement in developing, deploying, and using e-government infrastructures is much faster than the development and deployment of security services.
- Therefore, government organizations are still suffering from the existence and emerging of security risks.
- All available security solutions are only computationally-secure!

Work Objective

- The aim of this work is to show the importance and validation of including unconditionally-secure authentication services within e-government infrastructure based on QKD.

- The work highlights the basic requirements for a general framework that facilitates such inclusion and also introduces sample protocol modification.

Authentication Techniques



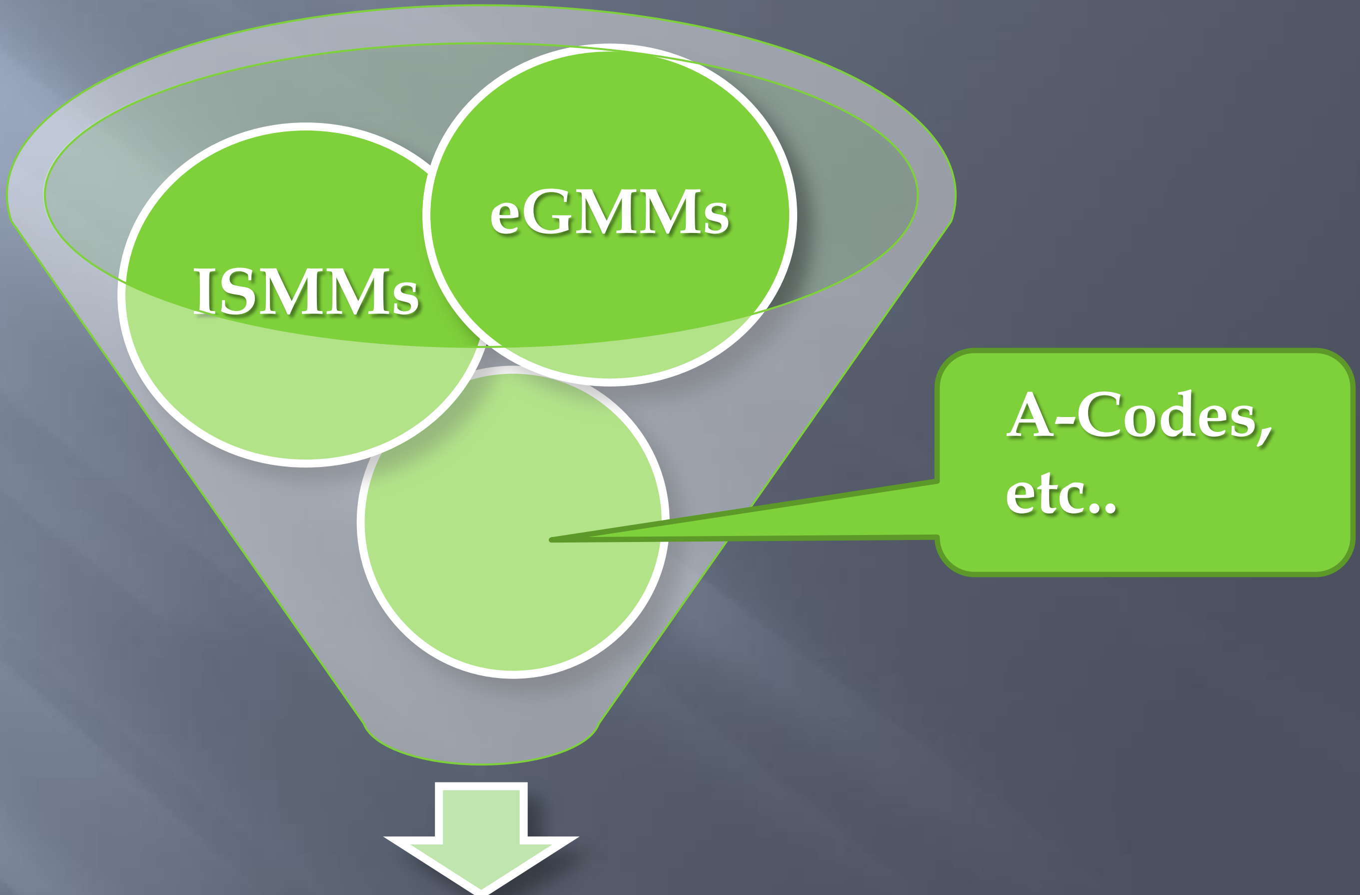
MACs vs. A-Codes

- MACs and A-codes can provide data integrity and data origin authentication.
- It is important to emphasize that MACs are only proven to be computationally secure while the security of A-codes is unconditional.
- Thus, MACs are suitable for short-term security but they are not useful for long-term (say 20 years) requirements, especially when considering new technologies like quantum computers.

Digital Signatures

- Digital signatures are very widely used technology for ensuring unforgeability and non-repudiation of information.
- Digital signature schemes can be constructed for both computational security and unconditional security.

eGMMs vs. ISMMs



General Convergence Maturity Model

The proposed N-Tier framework architecture

Basic security-related functions

Signature-creation

Signature-verification

Info-box access

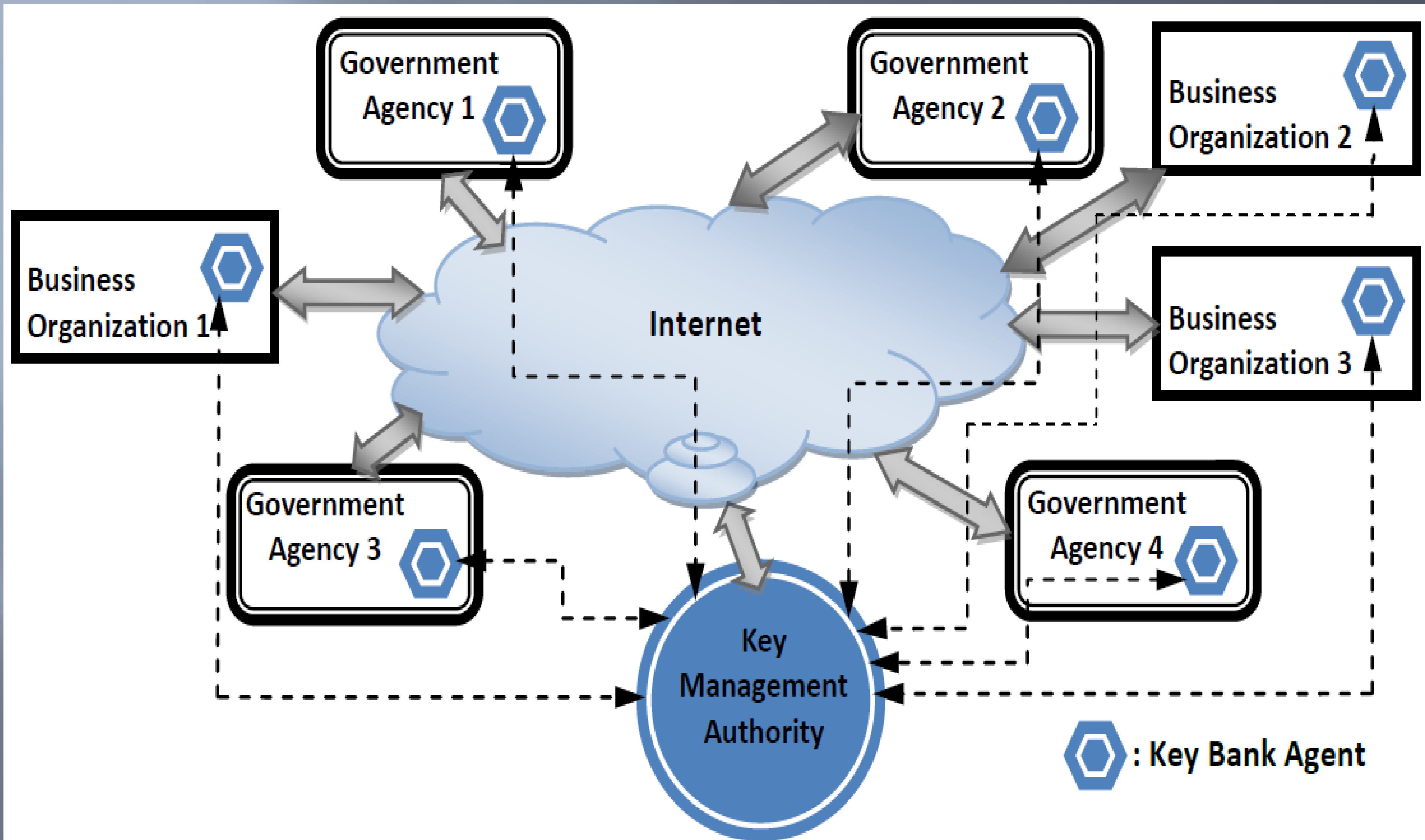
Session certificates

Session encryption

Session decryption

Key-synchronization

Typical deployment of key bank agents



Proposed key management and distribution approaches

Courier-based approach:

- *This is the most traditional approach*

Quantum cryptographic-based approach:

- *Recently, there have been significant advancements in Quantum Key Distribution (QKD)*

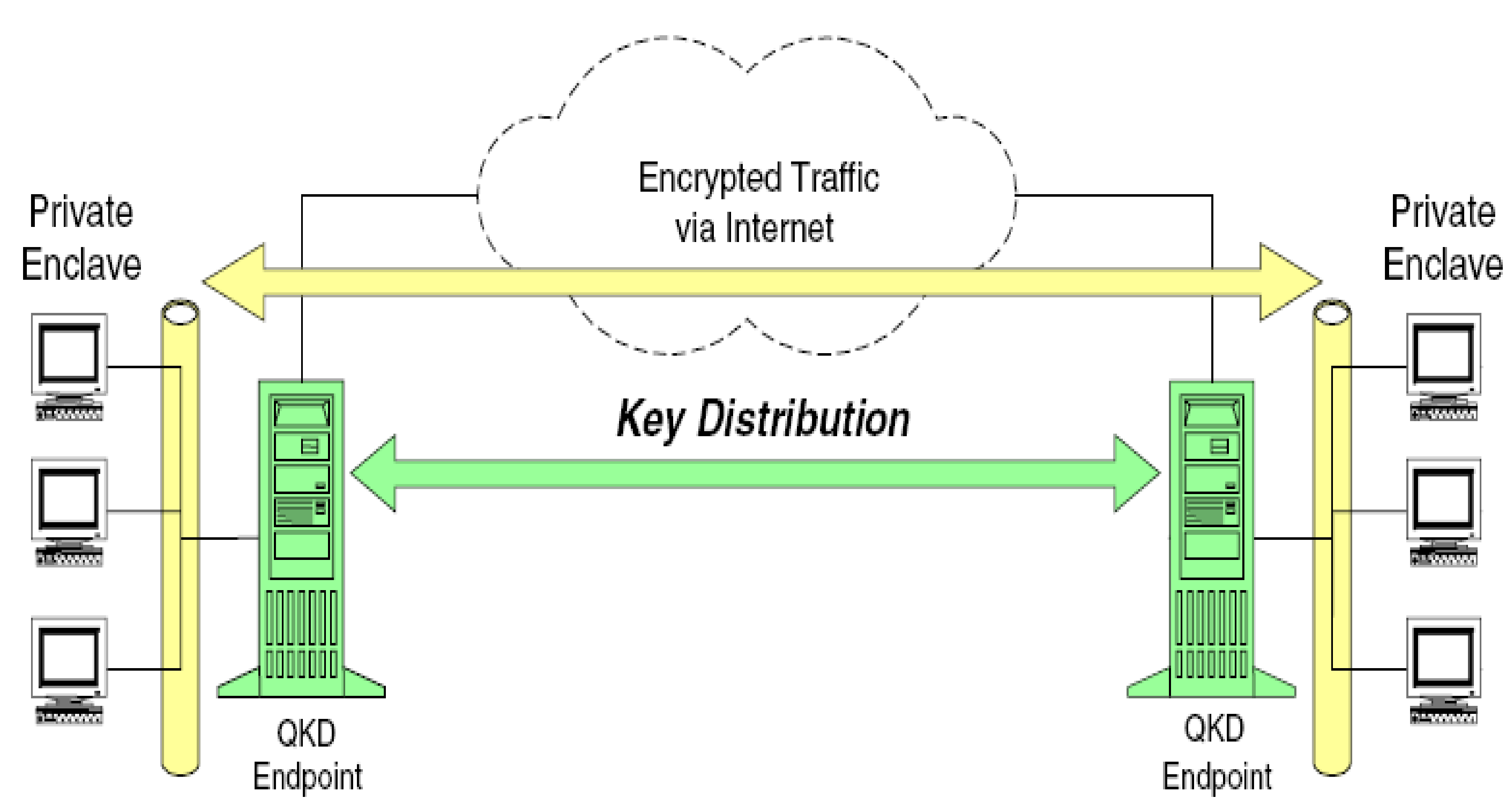
Hybrid PKI-based approach:

- *Properly combining QKD with public-key based authentication*

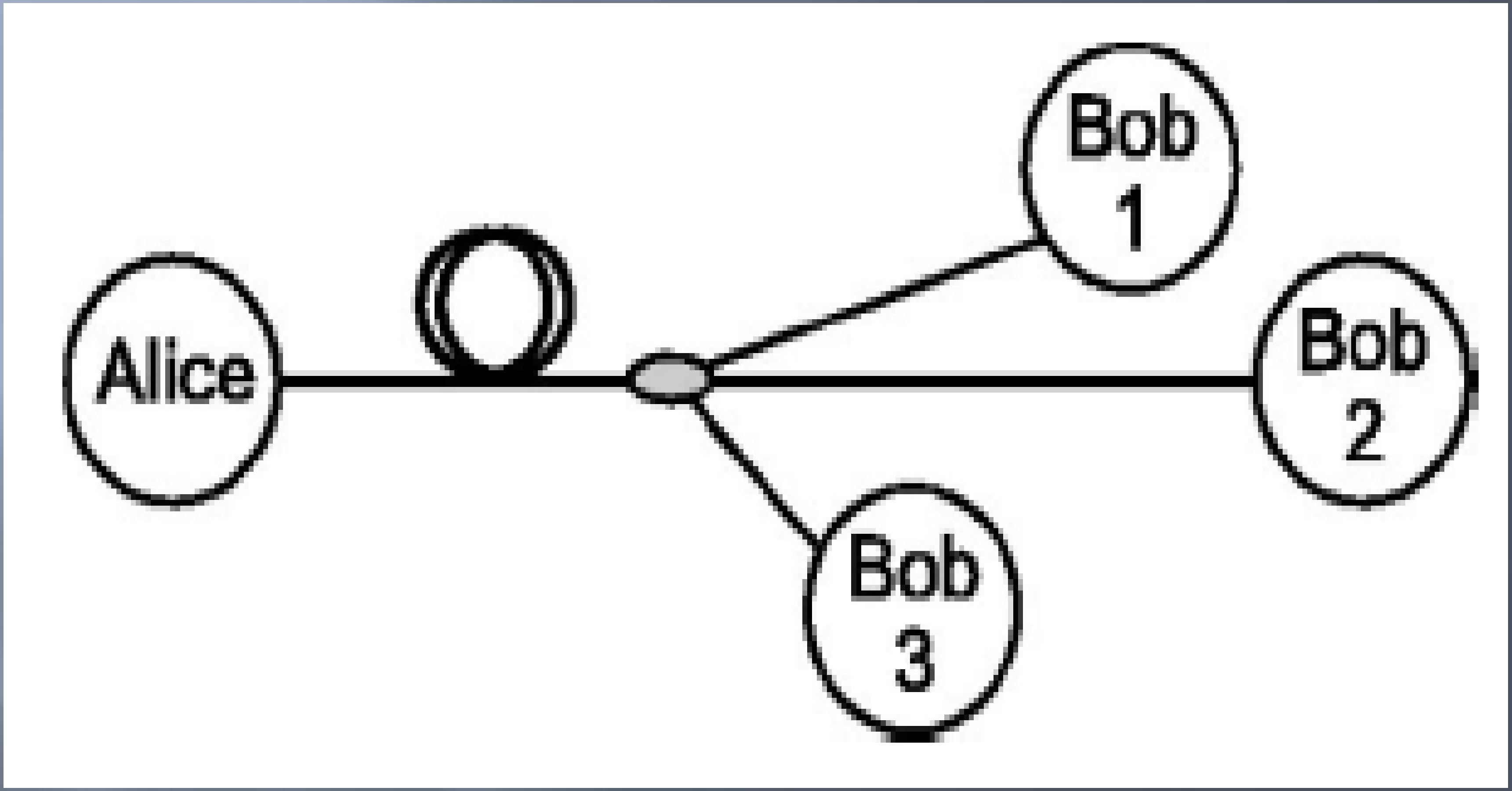
Why QKD?

- QC delivers cryptographic keys whose secrecy is guaranteed by the laws of physics.
- QC offers new methods of secure communications that are not threatened even by the power of quantum computers.
- In quantum cryptography, physically secure quantum key distribution can be combined with the mathematical security of the OTP cipher and/or information-theoretically secure authentication (based on universal hashing) .

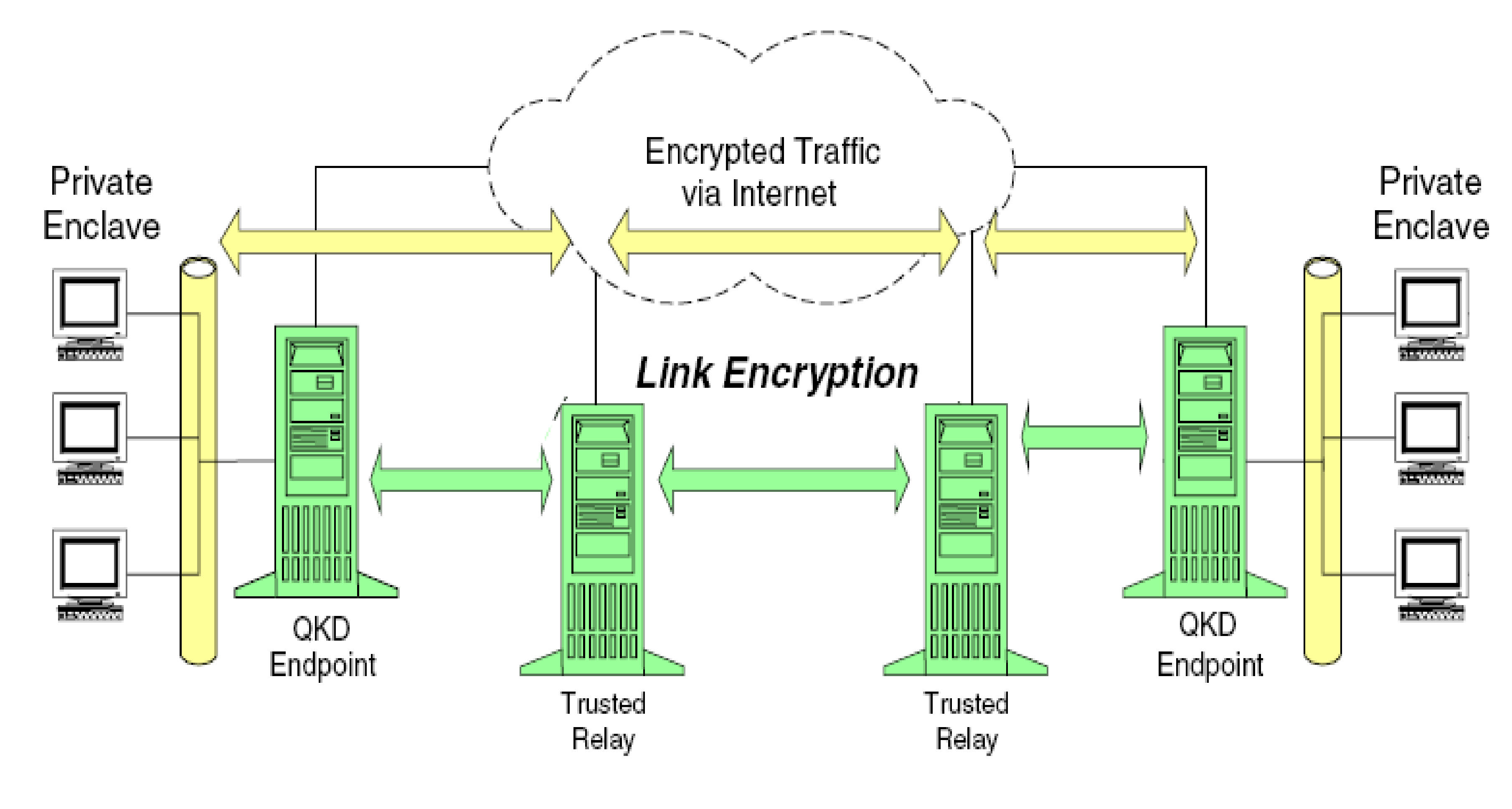
Stand-alone QKD PTP link



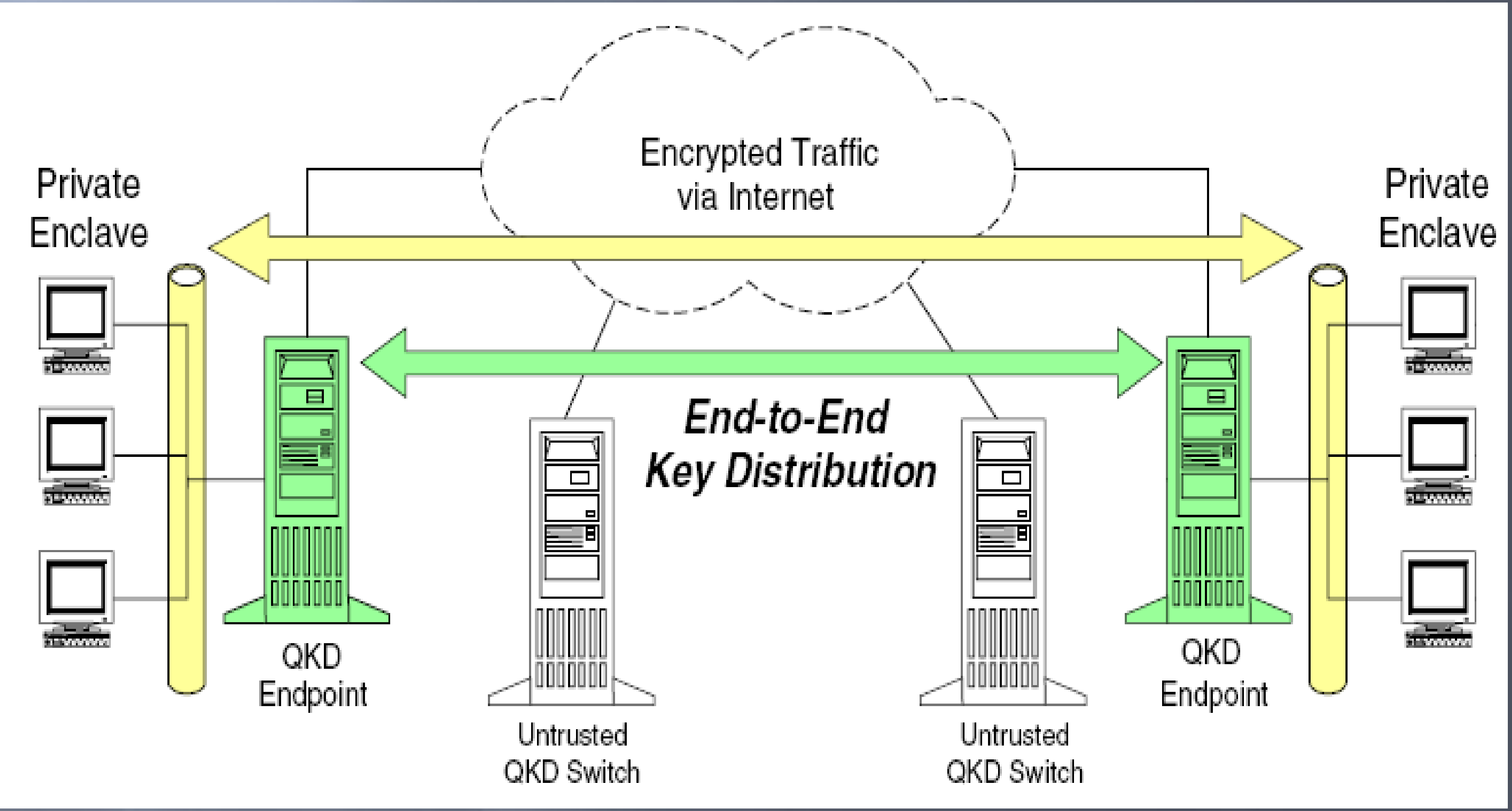
Optically switched QKD network



Trusted relays QKD network



"Full" quantum network

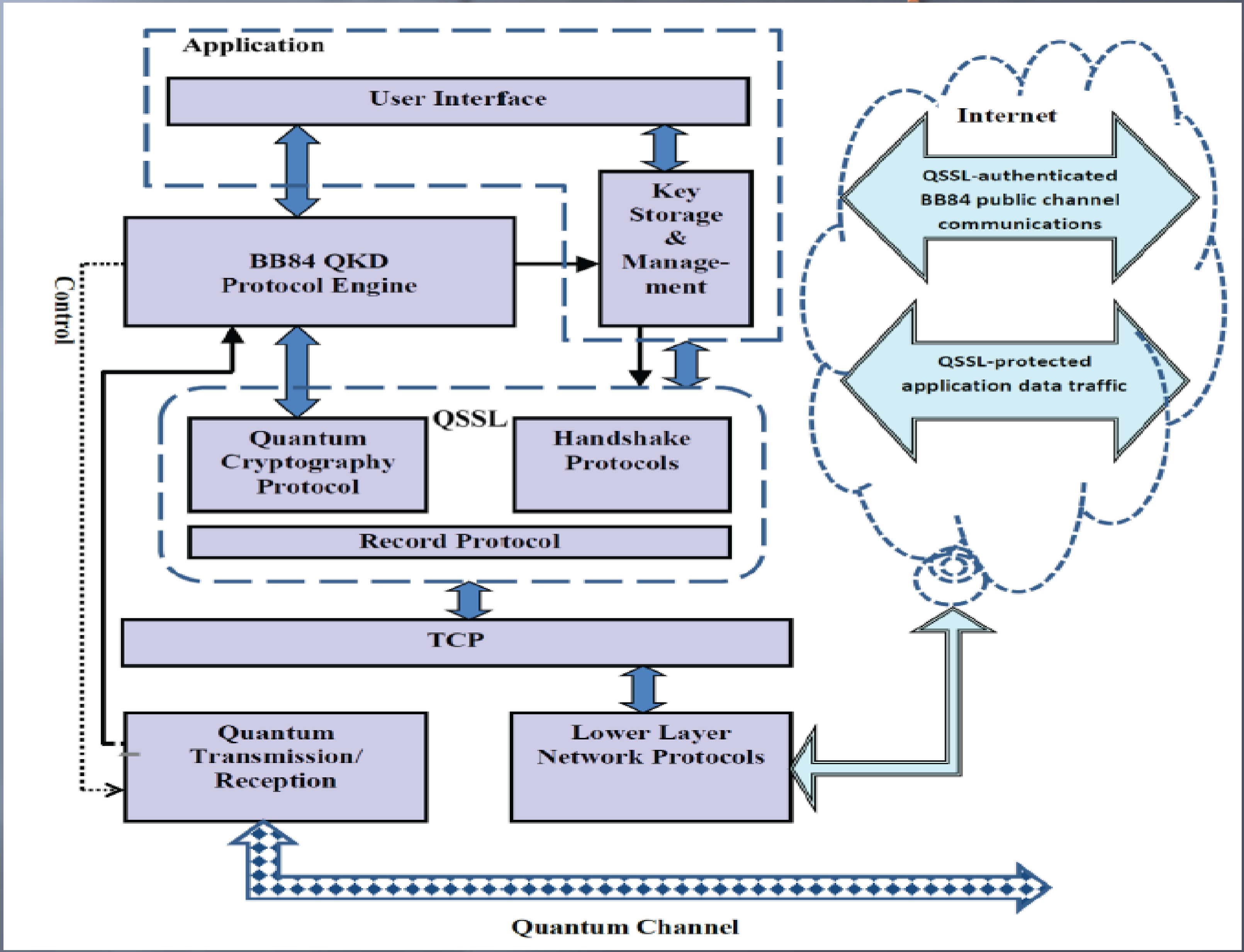


QKDNs (Software)

- Tightly-coupled protocol stack strategy; secret random bits obtained from QKD (which is mainly a physical layer technology) are merged directly somehow into a conventional higher-layer security protocol suite. Thus, the consumer security protocol has to be modified to enable the integration of QKD within it.

- Loosely-coupled protocol stack strategy; the focus here is to develop original multi-layer protocol infrastructures that are dedicated to QKD networks. In such a case, the QKD network infrastructure can be viewed as a "new cryptographic primitive“.

SSL/TLS Example



QKD Protocol Message Types.

	Message Type	Content
1-	start-quantum-transmission	null
2-	start-acknowledgement	null
3-	end-quantum-transmission	null
4-	end-acknowledgement	null
5-	synchronize-quantum-channel	timing information
6-	receiver-sifting	indices of detected pulses, detection bases
7-	sender-sifting	pulses' indices, transmission bases
8-	receiver-error-correction	reconciliation technique dependent
9-	sender-error-correction	reconciliation technique dependent
10-	set-equality	hashes of chosen sets
11-	equality-acknowledgement	null
12-	privacy-amp-parameters	parameters of the privacy amplification method
13-	privacy-amp-acknowledgement	null
14-	receiver-discussion	situation dependent
15-	sender-discussion	situation dependent

Conclusion

- Using A-codes can offer additional security benefits especially in situations when long-term and/or significantly high level of security is required.
- We advise A-codes based services for **G2G** and **G2B** settings only in the first adaptation stage.
- It is possible in next stages to include **e-democracy** (especially e-voting)

Future Work

- Since our current implementation is mainly limited to simulation. Future work might consider prototype implementation on Intranet level.
- Further investigation of hardware and software requirements of such systems for wired and/or wireless settings can also be considered.

Thank you