

MAGIQ TECHNOLOGIES,  
INC.

MagiQ Technologies  
275 Seventh Ave.  
New York, NY  
10001

TEL: 646-638-1001  
FAX: 646-638-4331

---

# QPN White Paper

---

Presenting the First Commercially Available  
Quantum Cryptography Solution

---

April

2004

## QPN™ White Paper

### CURRENT SECURITY PROTOCOLS

The fundamental part of any cryptographic protocol is the key – a string of random bits that are used to encode the data to be communicated between parties. In classical cryptography communicating parties need to share a secret sequence of random numbers, the key, that is exchanged by physical means and thus open to security loopholes. Because of the difficulty of dissemination of large and secret keys, most of today's cryptographic protocols rely on public key distribution and the assumed computational difficulty of breaking the protocol. To be useful and to provide security the key must be absolutely random, must be kept completely secret from anyone but the communicating parties, and must be refreshed frequently enough to keep the channel safe from eavesdropping.

#### **How and Why Current Security Protocols Are Vulnerable**

The current encryption protocols based on mathematical algorithms introduce potential security holes related to the key refresh rate and key expansion ratio, the most crucial parameters in the security of any cryptographic protocol. As sophisticated as new cryptographic products are, they are all built with digital technology and they all rely on computational difficulty as the source of their protection. Both of these facts contribute to their ultimate vulnerability.

Classical and conventional cryptographic solutions are vulnerable for a variety of reasons. Most systems **rarely refresh their cryptographic keys** which results in large key-expansion rates that are detrimental to the overall security of the system. Keys can be easily compromised in many ways by using brute-force deciphering, by espionage from within the company or by hacking using Trojan horses or sniffer software to gather key information. For systems that have very low key refresh rates, a reality that applies to most settings, a compromised key provides an eavesdropper with full access to information encrypted with the compromised key.

### STATE OF THE ART PROTOCOL - QKD

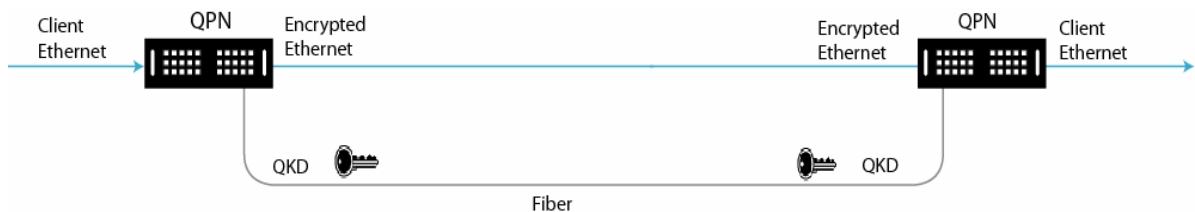
Quantum cryptography is a fool-proof technology that gives a solution to the key distribution and key management problems. The keys generated and disseminated using quantum cryptography are proven to be absolutely random and secure. The security of quantum cryptography is based upon the laws of quantum mechanics, which guarantees that keys can not be captured without being altered and therefore rendered useless, and not upon the assumed security of complex mathematical algorithms that can eventually be broken. Currently, quantum cryptography provides key generation rates of up to 10kbps. When combined with conventional encryption methods, quantum cryptography provides a fast, truly random automated cryptographic key refresh capability. Progress in computational power, advances in hardware design or the discovery of new mathematical algorithms will not compromise the security provided by systems using quantum cryptography technologies. Because it is based on a totally different concept from conventional cryptography, quantum key distribution (QKD) is the most secure replacement for conventional key negotiation schemes.

#### **How and Why Quantum Cryptography Works**

The security of quantum cryptography lies in its ability to exchange the encryption key with absolute security – QKD. By sending the key encoded at the single photon level on a photon-by-photon basis, **quantum mechanics guarantees that the act of an eavesdropper intercepting a photon, even if it is just to observe or to read it, irretrievably changes the information encoded on that photon.** Therefore, the eavesdropper can neither copy nor clone a photon nor read the information encoded on the photon without modifying it, a process that is provably detectable. The use of quantum keys and truly random numbers makes data encryption uncompromisingly secure.

## WHAT IS QPN ?

QPN systems are hybrid components that contain an encrypted communication channel and QKD capability. The QPN is an embedded system that contains hardware and software developed by MagiQ Technologies, Inc. QPN contains an embedded PC running Windows or Linux (both versions are available) to perform QKD protocols, including a hard drive that can be used to cache unused key data. The QPN's tamperproof enclosure prevents unauthorized access to the key storage area. By using an encryption card (see details in Appendix A), MagiQ QPN provides continuous key regeneration that enhances the security of the communication channels, protecting against both cryptographic deciphering and internal espionage, i.e., a compromised key in the MagiQ QPN system could only be used to decrypt a small fraction of the information exchanged as the cryptographic key in the system is flipped (refreshed) at least once every second. Thus not only does MagiQ QPN protect against cryptographic attacks, it enhances the physical security of the system in the face of internal threats.



## WHO NEEDS QPN ?

Protecting financial information is one of the highest priorities of corporations and entities involved in financial management and securities exchange. With QPN, corporations can secure their most critical communication links to prevent intrusion and theft of information. MagiQ QPN supports a variety of network architectures and provides the cryptographic keys used to protect the information channel over an optical fiber. The fiber can be physically separate from the information channel so that the QKD system can be added with little or no modification to existing infrastructure.

Storage area networks offer the promise of protecting corporate assets offsite by creating electronic copies of critical information for later retrieval. Protecting corporate information when it is stored and retrieved from physically distinct locations used in the storage area network requires cryptography for in-transit protection. QPN guarantees high-security in storage area network applications. By guaranteeing that the cryptographic keys are uncompromisingly secured by QKD, an option that is not available today, storage area network providers can address their customer's requirements for cryptographic protection of information.

In addition to, and included in, the above situations are the following enterprises that could benefit from QPN's uncompromising security:

- R&D companies whose concerns are trade secrets, intellectual properties, patents and business plans;
- Financial services where security of both funds transfer and other transaction based data is imperative;
- Service Providers of voice and data to many customers where there is a real danger of internal or external threats to confidential customer data and access to the network command channel;
- Large Power Grid Providers open to terrorist or malicious hacking into the command and control channel interfaces;
- Government Agencies with a need for secured fiber.

## SUMMARY

By adding the MagiQ QPN system to a communication channel, both the problems of truly random key generation and fool proof key dissemination are solved. MagiQ QPN can be configured to several network topologies and can be used to augment security on point-to-point links with little modification to existing infrastructure. All that is required is an optical fiber over which the keys can be exchanged. In any application where classical cryptography is used to protect the exchange of information, the addition of a QKD solution is a must. The system that provides QKD and ultimate security and protection is MagiQ QPN.

## APPENDIX A

The simplest and most visual way to explain the basics of QKD is by describing photon polarization based on a QKD scheme. A photon is an electromagnetic quantum, i.e., a discrete, elementary particle that has measurable properties, such as energy, momentum, and polarization. Photon polarization can be measured in different bases, for example, rectilinear, and diagonal. Polarization can then be used to encode binary data (0s and 1s) between a sender and recipient in one of these bases.

To generate symmetric key material, the sender and recipient can run the BB84 protocol [bb84], invented by Bennet and Brassard in 1984. This protocol assumes that the sender and recipient share a dark fiber and that they also have a classical (non-quantum) unsecured communication channel available. A summary of the protocol is as follows:

The sender randomly picks a basis, encodes a key bit in that basis, and sends the photon to the recipient.

The recipient also randomly picks a basis and measures the photon polarization. The recipient will guess the basis correctly approximately 50% of the time.

The sender and recipient then exchange the basis information on a public channel; however, they do not reveal the key bit or photon measurement outcomes.

When their bases coincide, the recipient obtains the value of the bit the sender was communicating. Otherwise, both sender and recipient disregard the result of the transmission.

Quantum cryptography makes use of quantum encoding by exploiting the Heisenberg Uncertainty Principle, where measuring a photon in one basis will affect the outcome of the measurement in the other basis. Specifically, to determine the photon's polarization (i.e. correctly determine a key bit), a receiver must measure the photon even though the correct basis is unknown. For example, the receiver must pass the photon through a filter oriented to a basis, but this will change the photon's polarization state if the filter's basis is incorrect. As shown in, a vertically polarized photon will pass through a vertical filter unchanged, but passing through a diagonal filter changes the photon's polarization.

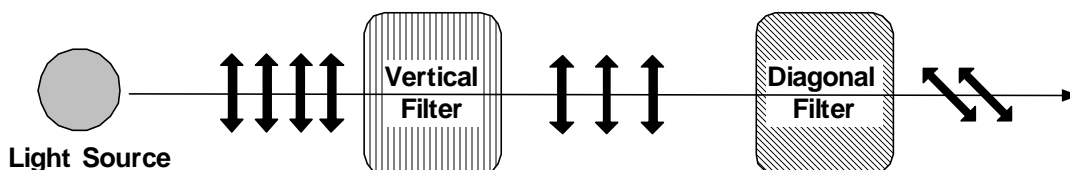


Figure 1 Polarization Measurement Affects Polarization

On average, only half the recipient's measurements can be used for key material, since the bases of the sender and recipient will only coincide for approximately half the photons. This makes undetected eavesdropping even more difficult. In Figure 2, a sender generates a stream of photons with random polarizations and attempts to send them to a receiver. Unknown to the sender and receiver, an eavesdropper is between them. The eavesdropper doesn't know the polarizations and so must guess the correct photon filter to use. Since the eavesdropper has no way of knowing the bases, the eavesdropper will guess the wrong basis with a 50% probability, thus affecting the photons that pass through the eavesdropper's filters to the recipient. This will be noticed by the sender and the recipient as an increase in the error rate (the last measurement in figure 2).

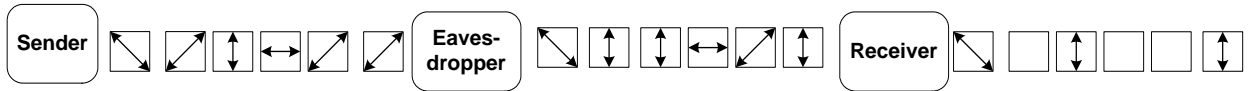


Figure 2 Quantum Transmission with an Eavesdropper

When the quantum transmission is finished, the sender and the recipient run an error correction protocol over the public channel. During this protocol, they reveal a fraction of the key bits to each other (and to the eavesdropper). The result of error correction is an error-free key shared both by sender and recipient. This key is not completely secure as part of it may be known to the eavesdropper.

After error correction, the sender and receiver can determine the key error rate (and detect the eavesdropper). At this point, the sender and receiver can perform an additional privacy amplification protocol to remove all unsecured bits. After this protocol, the eavesdropper will have zero knowledge about the remaining key bits. Note that the number of key bits is reduced in privacy amplification; thus, there is a possibility that zero bits may be left after privacy amplification. A QKD device must still operate below this threshold value.

The BB84 protocol is secure even when all of the information sent over the public channel is accessible to the eavesdropper. The only requirement is that messages transmitted during the sifting procedure (when sender and receiver check their bases for agreement) are authenticated. This can be done by using standard message authentication techniques like adding HMAC tags to the messages.