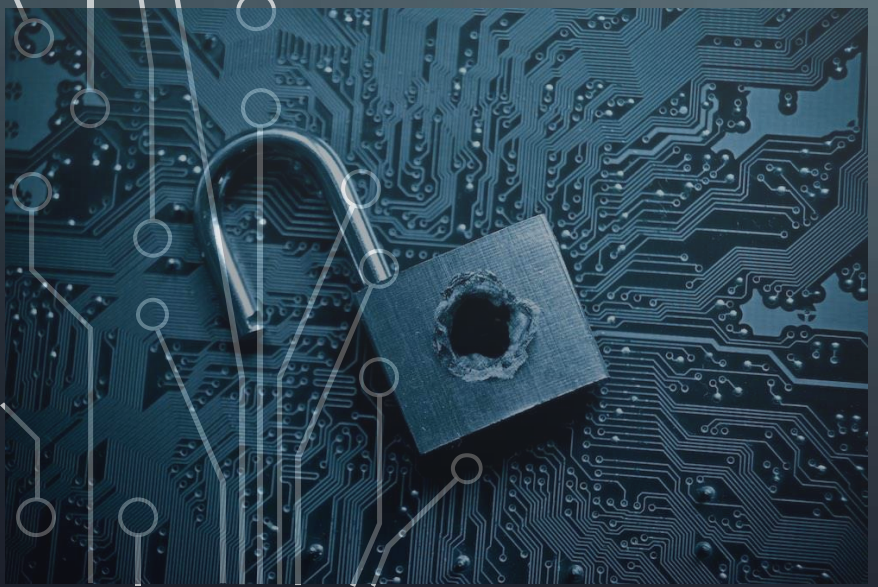


SECnet

*PATENT US 11,108,550

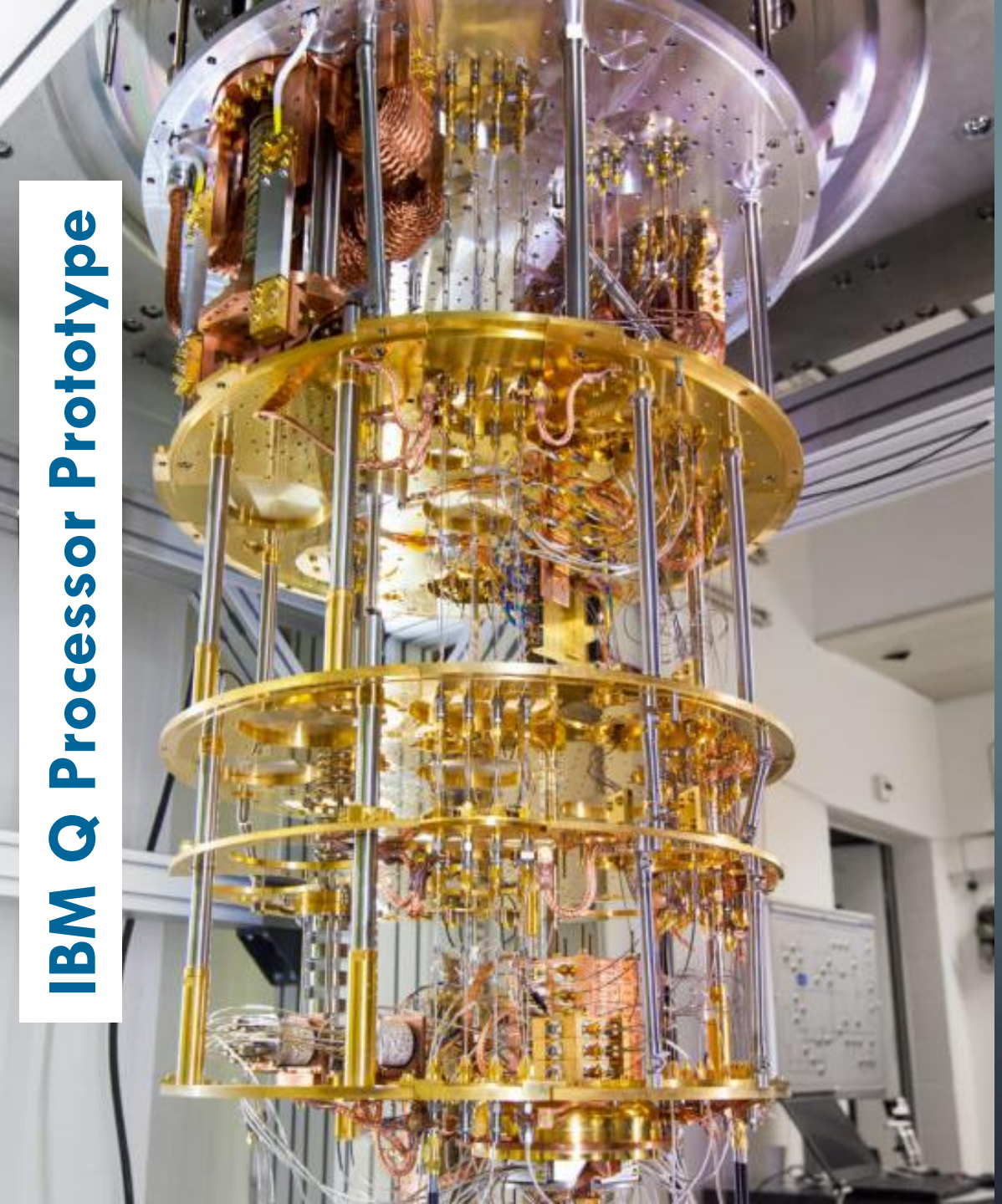
Secure Data Transmission Across Networks

Once secured by SECnet, encrypted transmitted data is invulnerable to all cryptographic attack methods – including "brute force" and quantum assaults

INVENTORS:

Daniel Esbensen

Steve Omohundro, PhD



IBM Q Processor Prototype

PROBLEM SCOPE

- Researchers at Google and Sweden's KTH Royal Institute of Technology have developed a technique that a quantum computer could use to crack 2,048-bit RSA encryption in just eight hours (previously estimated at 30 trillion years). (*Technology Review,* June 5, 2019)
- *"Anyone that wants to make sure that their data is protected for longer than 10 years should move to alternate forms of encryption now…"* (Arvind Krishna, Director of IBM Research)
- *"There is little to no margin of safety for beginning the migration to [post-quantum cryptography] PQC."* (2020 RAND Corporation report)

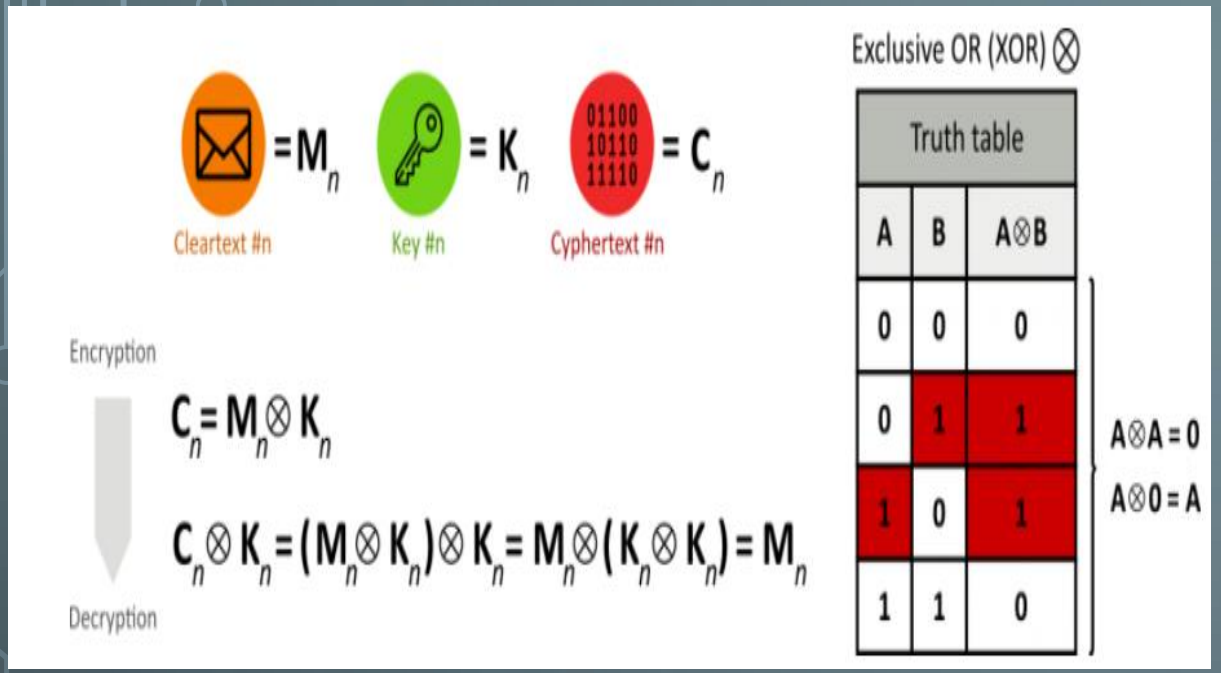
PROBLEM SCOPE (CONTINUED)

- **Quantum Computing Poses An Existential Security Threat, But Not Today (Forbes – October 31, 2019)**
- With the advent of realizable Quantum Computers, everything that has been transmitted or stored and that has been protected by one of the known to be vulnerable algorithms, or that will ever be stored or transmitted, will become unprotected and thus vulnerable to public disclosure.“ (European Telecommunications Standards Institute 2017)
- It is an inevitability that cryptographers dread: the arrival of powerful quantum computers that can break the security of the Internet. Although these devices are thought to be a decade or more away, researchers are adamant that preparations must begin now. (Scientific American https://www.scientificamerican.com/article/cryptographers-brace-for-quantum-revolution/)
- It’s a matter of time until the day arrives when quantum computers will crack traditional encryption. This moment, often referred to as “Y2Q,” may be as little as three to five years away, given the billions of dollars of investment flowing into the field. (https://securityboulevard.com/2020/11/why-its-time-to-quantum-proof-your-communications-infrastructure/)

SECnet Solution: Benefits Summary

- Data transmitted 100% securely via networks without fear of hacking or data discovery.
- If desired, data tunneled through SECnet using any network protocols, creating a perfectly secure VPN.
- The secured data is “future proof” and mathematically proven impossible to break, even applying quantum computing methods.

The SECnet Solution Overview



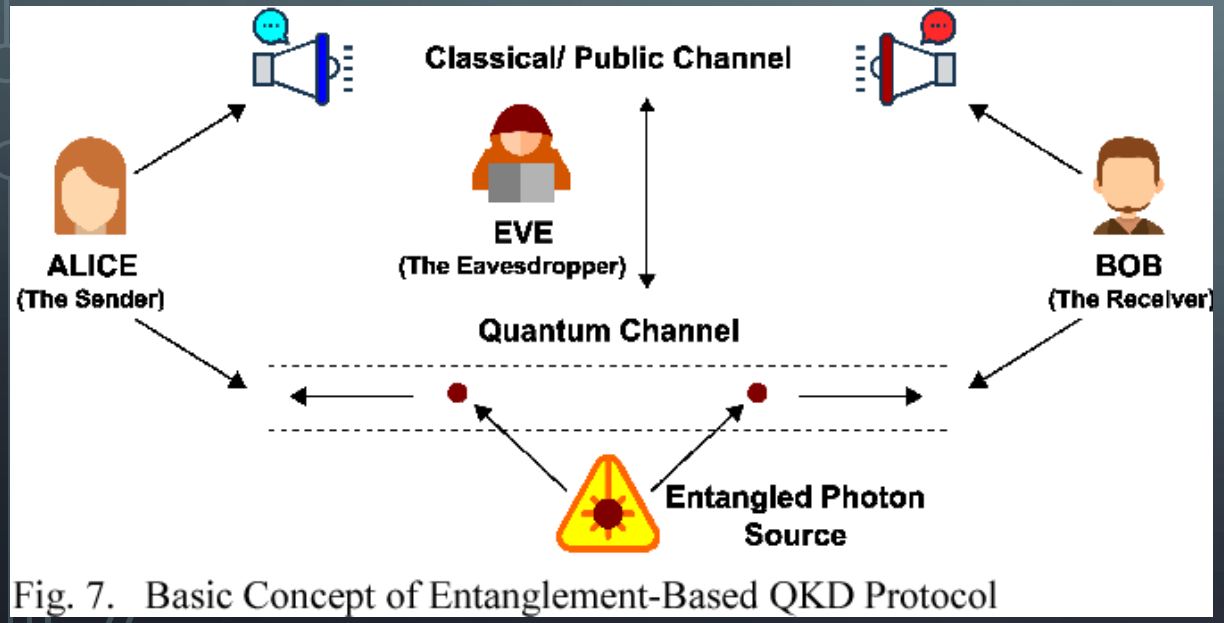


Fig. 7. Basic Concept of Entanglement-Based QKD Protocol

OTPK encryption integrated with network eavesdrop detection (such as QKD)

Produces unbreakable secure network data communication

One-Time Pad Key (OTPK) Encryption:

- Mathematically proven impossible to break, even applying quantum computing methods
- Consequently, a SECnet-secured network cannot be broken either

Network eavesdrop detection – such as Quantum Key Distribution (QKD):

- Established quantum technologies that detect if a network transmission has been eavesdropped
- Continually evolving to become faster and cheaper

The SECnet Solution Implementation

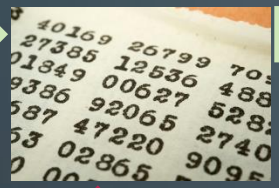
A perfectly secured hardware network transmission system that:

- Receives and assesses the Source Data to be encrypted
- Generates random encryption keys the same size of the Source Data (One-Time Pad Keys)
- Applies the OTPKs to the Source Data, producing the Encrypted Data
- Uses network eavesdrop detection techniques to help secure data while in transit throughout a network

SECnet Process Flow Overview

Data to Send

1 Generate One-Time Pad Key (OTPK)

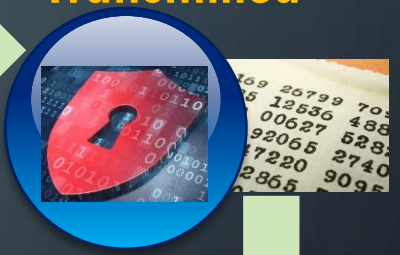


2 Eavesdrop detection (QKD or other methods)

3 Eavesdrop?

NO

4 Data Encrypted using OTPK & Transmitted



YES

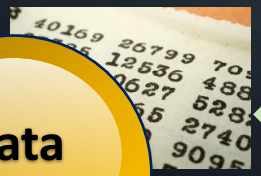
5 Eavesdrop detection (QKD or other methods)

6 Eavesdrop?

YES

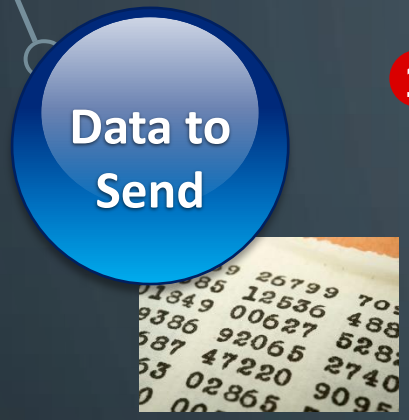
NO

7 Data Decrypted using OTPK



Data Received

SECnet Process Flow Details



1. SECnet generates an OTPK the same length as the source data using random bits from a PRNG (Pseudo Random Number Generator) or a TRNG (Truly Random Number Generator).

2. SECnet transmits the OTPK across the network using an eavesdrop detection method such as QKD.

3. If eavesdropped, SECnet generates a new OTPK and transmits it to the receiver.

4. SECnet efficiently encrypts the source data using the generated OTPK via an XOR operation. Encryption is achieved in less than one millisecond (regardless of source size) via parallelized CPUs, GPUs, or hardware logic circuits.

5. SECnet transmits the OTPK encrypted data across the network using an eavesdrop detection method such as QKD.

6. If eavesdropped, SECnet restarts the entire process with a new OTPK.

7. The SECnet receiver, in possession of both the OTPK and encrypted data, transmits an acknowledgement of data receipt to the sender and then rapidly decrypts the encrypted data using the previously received OTPK.

SECnet Solution: Targeted Best Use

SECnet's target is situations where the security of the data is so important that using twice the storage and bandwidth pales in comparison with the benefits of the absolute mathematical certainty of cryptographic security.

For important military, intelligence, and governmental data, mathematically eliminating these risks is worth the extra communication overhead. With SECnet, the overhead is only a factor of two for the simplest implementation.

SECnet – Next Steps

We are looking to transfer the SECnet patent to a company that can take the patent and underlying technology and run with it.

Contact Us

touchtechsupport@gmail.com

www.ttinet.com

QUESTIONS?

CONTACT US

touchtechsupport@gmail.com

www.ttinet.com