TRNGtech

Patent# US11341254

Uses **T**ruly **R**andom **N**umber **G**enerated key bits to Secure Data

ONCE SECURED BY TRNGTECH, ENCRYPTED DATA IS MATHEMATICALLY PROVEN INVULNERABLE TO ALL CRYPTOGRAPHIC ATTACK METHODS – INCLUDING "BRUTE FORCE" AND QUANTUM ASSAULTS

INVENTORS:

DANIEL ESBENSEN

STEVE OMOHUNDRO, PHD.

TRNGtech Hardware & Software: Benefits Summary

- Data is delivered 100% securely via physical media or networks without fear of hacking or data discovery.
- Data tunneled via TRNGtech using any network protocols can create a perfectly secure VPN.
- Provides invulnerable encryption during current and post-quantum environments
- Secured data is “future proof” and mathematically proven unbreakable, using any classic or quantum computing methods.

Problem: ***Encrypted data assumed safe is already compromised by researched quantum computing and AI technologies***

Researchers have developed a TECHNIQUE that quantum computers can use to crack 2,048-bit RSA encryption in just eight hours. This was previously estimated to take over 30 trillion years. (*Technology Review,* June 5, 2019)

"There is little to no margin of safety for beginning the migration to post-quantum cryptography (PQC)." (2020 RAND Corporation Report)

"Its problem-solving capacity will soon render all existing cryptography obsolete, jeopardizing communications, financial transactions, and even military defenses. " (Quantum News Briefs January 30, 2023)

TRNGtech: Use Cases For Unbreakable Security

- Mission-critical financial and medical data protection
- Protecting critical infrastructure
- Military point-to-point data gathering in hostile situations
- Paired device command and control, e.g., IOT (Internet of Things)
- Remote entry for cars, homes, smart buildings, etc.
- Controlling the time release of sensitive data
- Data transportation and long-term secured storage

The TRNGtech Implementation Steps

Create random key bit filled TRNG Disk pairs

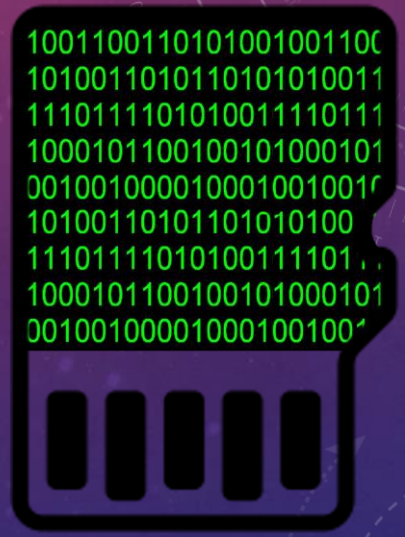
Within a secured environment, supply devices with TRNG Disks and software

Secure Network Communication

Secure Media Transportation

TRNG Disk

Cloned TRNG Disk



TRNGtech: Creating TRNG Disk Pairs of Key Bits

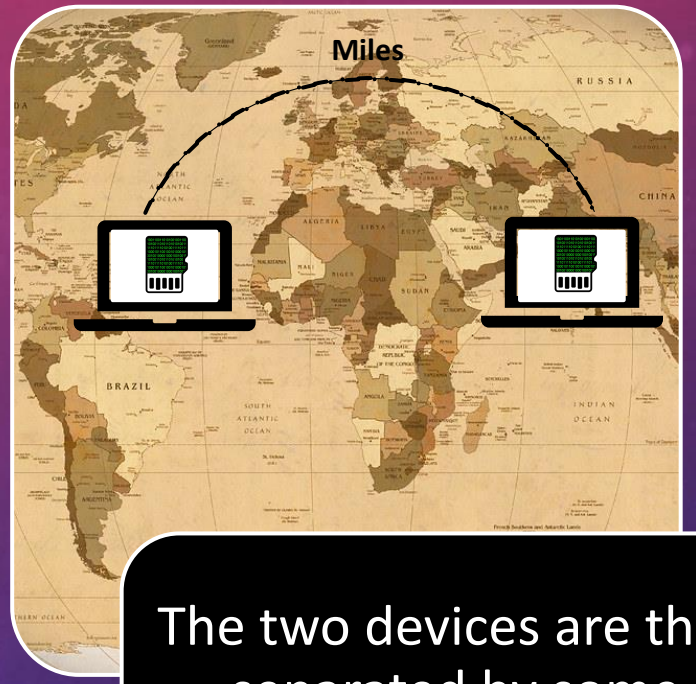
Use an existing **T**ruly **R**andom **N**umber **G**enerator to transfer random bits to disk media (**TRNG**)

Fill the disk media with the random bits and give the disk a Universally Unique Identifier (ID). This creates the TRNG Disk.

Clone the TRNG Disk. This creates the TRNG Clone and completes the TRNG Disk Pair.

TRNGtech: Deploying Point-to-Point Devices

Within a secured environment, a TRNG Disk and software is installed onto a device. Its TRNG Clone and software is installed onto another device.



The two devices are then separated by some distance for secured use. The devices can be computers, phones, servers, cameras, IOT, etc.

TRNGtech: Secured Network Transmission

The plaintext data to be transmitted is identified.

The plaintext is OTP-encrypted using a specific set of key bits from the TRNG Disk at a given bit offset.

The used TRNG Disk key bits are overwritten so they cannot be recovered.

The encrypted data, TRNG Disk ID, and the given bit offset are transmitted to the receiving device.

The receiving device uses its matching TRNG Clone and the received encrypted data and bit offset to extract the TRNG clone's key bits

The encrypted data is OTP decrypted back into the identified plaintext data.

TRNGtech: Secured Media Transportation

The plaintext data to be transported is identified.

The plaintext is OTP-encrypted using a specific set of key bits from TRNG Disk at a given bit offset.

The used TRNG Disk key bits are overwritten so they cannot be recovered.

The encrypted data, TRNG Disk ID, and the given offset are copied onto removable disk media.

The removable disk media is transported using a courier, FedEx, UPS, USPS, etc. to the location of the receiving device.

The receiving device uses its matching TRNG Clone and the received removable disk media's data to extract the encrypted data and its corresponding key bits.

The encrypted data is OTP decrypted back into identified plaintext data.

TRNGtech: Next Steps

We are looking to transfer the TRNGtech patent to a company that can take the patent and underlying technology and develop valuable marketable products/services for sale.

Contact Us

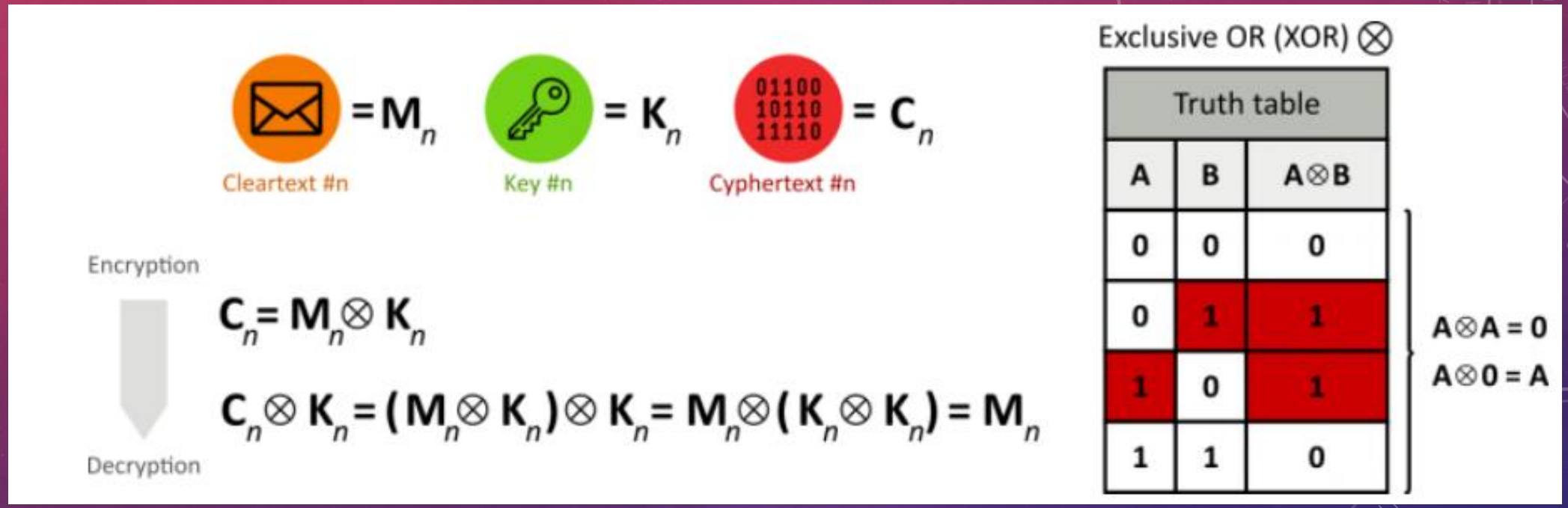
touchtechsupport@gmail.com
www.ttinet.com

TRNGtech: Deeper Dive

The following slide is for cryptography experts. It shows the mathematical proof underlying TRNGtech's patented methods. The proof is well known to cryptography experts and was discovered in 1949 through U.S. government research.

For more details, see our technology white paper at https://quantumproperties.ttinet.com/assets/files/Cryptography_Analysis.pdf

TRNGtech: OTP – Provides Unbreakable Security



One Time Pad key (OTP) is the only encryption method that when used correctly is mathematically proven to provide unbreakable security.

(See https://en.wikipedia.org/wiki/One-time_pad)