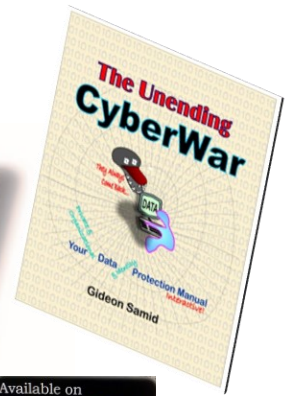
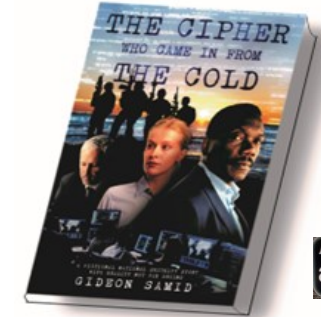


Quantum computers: - The Next Threat to National Security and What to Do About It



Available on  
amazonkindle

# QSEC

*Trans-Vernam Cryptography TVC*

BitMint AI-Powered  
Cyber-Innovation Hub

$\Phi$  BitMint

Quantum, Randomness, Paradigm Shift

February 2023


Amnon Samid  
+972544200400  
amnon@BitMint.com



“Nothing is more powerful than an idea whose time has come.”



— Victor Hugo

The idea of One-Time-Pad as the ONLY mathematical proven cryptography was first invented by Gilbert S. Vernam  104 years ago, and was later proven by Claude Shannon to be unbreakable.

**The time for deploying it is NOW.**

With **QSEC** we revived the equivocation defense of Vernam cipher, with a new generation of Trans Vernam Ciphers (TVC). They are fast, convenient, and open the door to a host of new cryptographic use cases.

---

The Vernam cipher per se is old and not very fitting for modern use. But its underlying principle does not age.

All that we had to do then was to apply modern cryptographic methodology to the underlying Vernam principle, and come forth with a slew of **Trans-Vernam ciphers (TVC)** that share the mathematical proof of invincibility, but are built to fit into modern cyberspace.

# The challenge:

On Aug. 24, 2022 the Cybersecurity and Infrastructure Security Agency (CISA) raised the red flag regarding the quantum computing threat



Critical infrastructure systems rely on digital communications to transmit data.

To secure the data in transit, cryptographic technologies are used to authenticate the source and protect the confidentiality and integrity of communicated and stored information.

As quantum computing advances over the next decade, it is increasing risk to certain widely used encryption methods.

# The solution:

BitMint addresses threats posed by quantum computing, to support critical infrastructure and government network owners and operators



Recognizing Randomness as Cyber Oil

Building the new security universe  
for the fourth industrial revolution

*Developing the Fundamental  
Quantum-Grade Technology*

for

**Peace in Cyber Space**

# Prelude



Everything in cryptography today moves in one direction: the complexity defense; guarding our secrets with a computational workload to keep our adversary busy long enough.

Alas, a smarter adversary and faster computers will overcome the complexity defense.

## It is time to look for an alternative strategy:

Using our adversary's computing power against it. We release a ciphertext that when cryptanalyzed by our smart attacker, it points to several conflicting messages, each of them could have been encrypted to the same ciphertext.

The ciphertext itself does not point to the plain message that actually generated it, so no smart mathematician and no powerful computer will be able to hammer out of the ciphertext the message they are after.

**We generate this equivocation with the power of randomness.**

We build on the legacy of Gilbert S. Vernam who filed his unbreakable cipher in 1917. Vernam cipher was proven as mathematically secure by Claude Shannon a quarter of a century later, and a quarter of century after that Joseph Stalin used it to steal the Atomic secrets from Los Alamos.

A full century after the Vernam patent, a bouquet of patents revived this equivocation defense with a new generation of ciphers. They are fast, convenient, and they open the door to a host of new cryptographic use cases. And much like the cipher they descended from, these **Trans-Vernam Ciphers (TVC)** use the sling of a mathematical proof, to beat the Goliath of quantum computers.

# Cyber Security Paradigm Shift



*from:*  
***Mathematical Complexity***

+

***Limited Randomness***

*to:*  
***Abundant Randomness***

+

***Limited Math Complexity***



**Randomness: The Fix  
for Today's Broken Security**

# Data Security Today



*We place our data under a cryptographic lock.  
Hackers smash the lock...*

*We Build a bigger crypto-lock.  
Hackers build a bigger hammer...*

Mathematical Wisdom is defeated  
by Greater Mathematical Wisdom

*The Age of Weaponized Math*

# The Future

- Quantum Randomness withstands Quantum Computing
- Quantum Randomness Restores Citizens' Privacy
- Quantum Randomness Prevents Massive Harmful Database Breaches
- Quantum Randomness Mints Durable Efficient Convenient Digital Money
- Quantum Randomness Provides Safe Haven to Evil Doers.

*The Evil Doers are Already on It, and We Should Catch Up!*

# The need

*Washington, D.C.* — April 18, 2022: As the capability of quantum computing advances, Representatives Ro Khanna (D- CA-17), Gerry Connolly (D-VA-11), and Nancy Mace (R-SC-1) are introducing the bipartisan Quantum Computing Cybersecurity Preparedness Act to ensure that encryption used by the federal government to keep our systems and valuable data safe are quantum proof and establish Congress' oversight role in the process.

---

- ➡ Quantum computers pose a fundamental threat to cyber security today, all based on Turing machines.
- ➡ It is not clear how powerful, sophisticated and when the quantum attack will be.
- ➡ It is an inherent risk calling for immediate deployment of defensive cryptographic tools to ensure a baseline of secure communication under even the most severe quantum attack.
- ➡ Such tools are available and should be deployed right away.





“The transition to post-quantum encryption algorithms is as much dependent on the development of such algorithms as it is on their adoption. While the former is already ongoing, planning for the latter remains in its infancy. **We must prepare for it now to protect the confidentiality of data that already exists today and remains sensitive in the future.**”  
- **U.S. Secretary of Homeland Security, Alejandro Mayorkas**, <https://www.dhs.gov/quantum>



# The need [cont.]

There is a race to build a fully capable quantum computer that would be so powerful, it could break encryption and allow adversaries to steal valuable information. It is believed that adversaries are conducting a practice called “[steal now, decrypt later](#)” where they collect data to store for years until they possess a powerful enough quantum computer to decrypt it.

---

-  The main risk in the situation in question is silent compromise of the nominal ciphers.
-  Our starting point is that adversaries are already recording traffic today  
*harvest now, decrypt later*
-  It is not certain that we will know when they have an effective ability to decipher the encrypted information.
-  Our solution protocol calls for applying *QSEC* to transmit any long-life secret, which the adversary can harvest now and breach later.

# One by one NIST "post quantum ciphers" are breached.

New ones in the same direction are put forth, likely to be breached much the same.

It is time to go back to the fundamentals and apply a new thinking and new solutions.

The screenshot shows a web browser window with the URL <https://www.securityweek.com/ai-helps-crack-a-nist-recommended-post-quantum-encryption-algorithm/>. The page features the SecurityWeek logo and a navigation menu with categories like Malware & Threats, Security Operations, Security Architecture, Risk Management, CISO Strategy, ICS/OT, and Funding/M&A. The main content area is under the 'DATA PROTECTION' category and displays the article title 'AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm'. The article's subtitle reads: 'The CRYSTALS-Kyber public-key encryption and key encapsulation mechanism recommended by NIST for post-quantum cryptography has been broken using AI combined with side channel attacks.' The author is identified as Kevin Townsend, with a publication date of February 21, 2023. Social media sharing icons for Facebook, Twitter, LinkedIn, and others are visible. The browser's taskbar at the bottom shows the time as 13:36 on 23/02/2023 and various application icons.

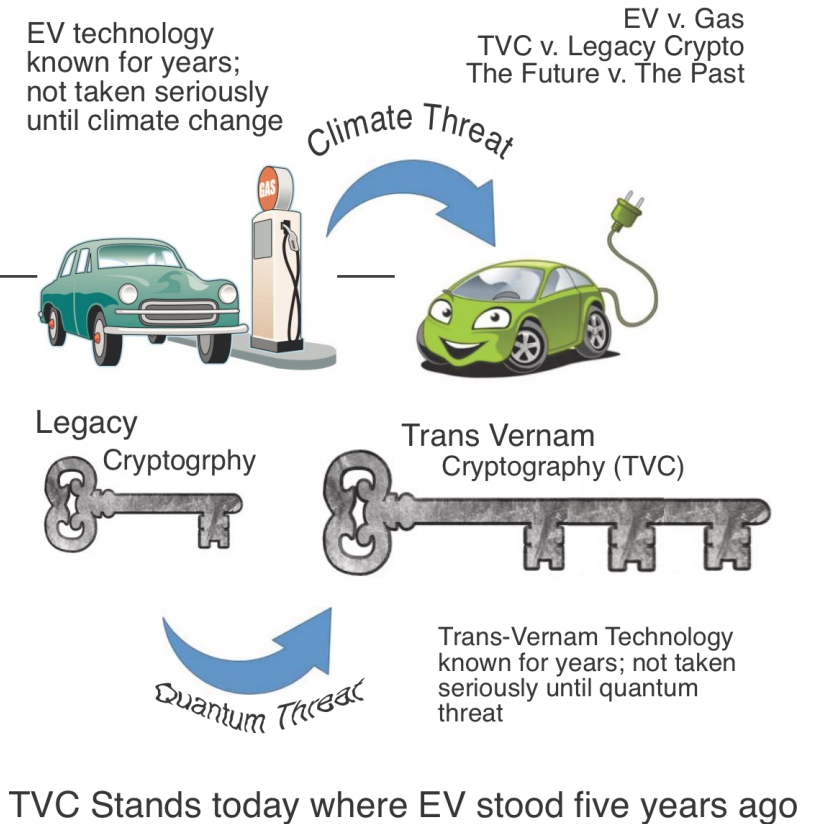
# What is the alternative?

Several smarter ciphers were developed -- Claude Shannon proof shields them from quantum attack. It even shields them from attackers much smarter than we are.

And it so happens that they have assorted advantages: they hide the size of the message, they hide the pattern of the communication, and the key can be safeguarded off the digital grid -- in a newly patented BitMint nanotechnology chip where the data is written with chemistry.

The security of Vernam, and **the new Trans-Vernam ciphers (TVC)** is based on the simple fact that they are pattern devoid.

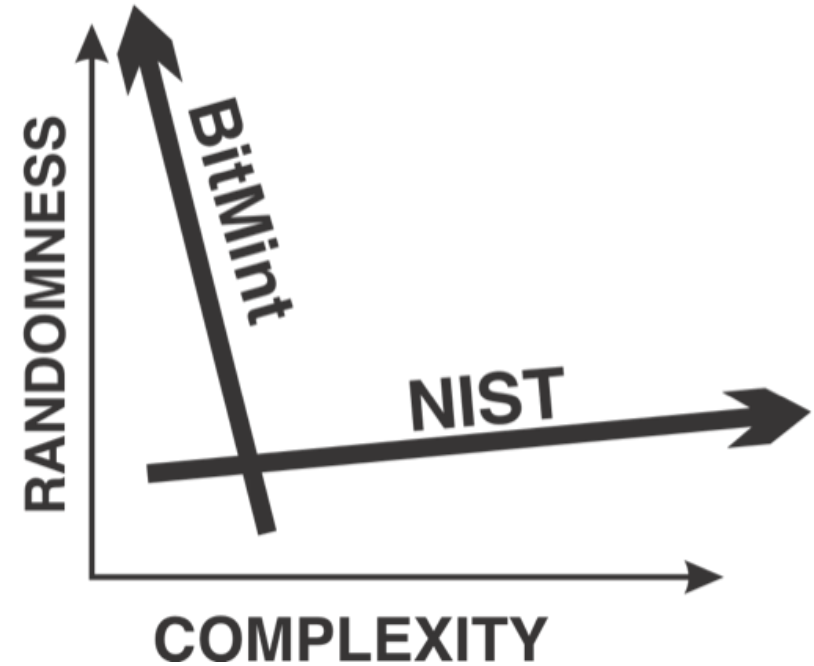
Cryptanalysis is based on pattern detection and exploitation. Trans-Vernam ciphers have no pattern to be detected, no vulnerability to exploit.



Hereafter two products  
from our basket of **TVC** solutions  
based on two of our 39 granted patents



## Two Quantum Security Strategies



**QSEC & BITFLIP**

# QSEC

QSEC is a cryptographic premise where intensive computation is avoided, and security is achieved via non-complex processing of at-will size keys.

---

The approach is to increase the role of randomness, and to build ciphers that can handle any size key without choking on computation.

Orthodox cryptography seeks to create a thorough mix between key bits and message bits, resulting in heavy-duty computation.

QSEC is a simple, fast cipher that allow their user to adjust the security of the ciphertext by determining how much randomness to use.

It is a mathematically proven quantum resistant solution.

It is based on ciphertexts that do not commit to their generating plaintext, thereby making it impossible to identify the generating plaintext out of the myriad of different plaintexts that with proper keys would generate the same ciphertext.

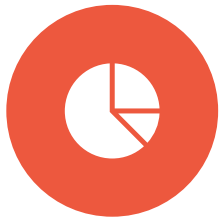
Without having the key there is no mathematical way to cryptanalyze the ciphertext, which makes it irrelevant how powerful the attacker is.

QSEC operates with a large secret size key and a large as desired ciphertext, confounding the attacker, without confusing the intended recipient holding the proper key.

# QSEC ADDED VALUE



Quantum Randomness



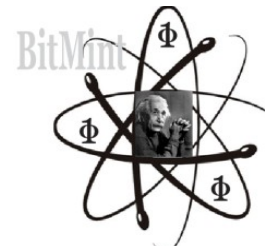
MATHEMATICAL PROOF  
OF EFFICACY.



ALLOWING THE  
TRANSMITTER TO  
DECIDE HOW MUCH  
SECURITY TO PROJECT



It may be used to  
exchange messages that  
contain long-term  
secrets, which the  
adversary may capture  
now and crack later when  
quantum computing  
becomes available



IT MAY BE USED TO  
CONCEAL PATTERN OF  
COMMUNICATION



It may be used in  
"Lifeboat on the  
Titanic" mode --  
as a backup plan  
in case the  
adopted NIST  
ciphers fail.

**QSEC** inherent resilience is based on the **BitMap** attribute of passing to the transmitter of the information the power to decide how much security to project.

In none of the prevailing ciphers can the user control the projected security beyond selecting among three key sizes (e.g., AES). In BitMap, it is a continuous application of security projection. A new powerful concept of resilience. The transmitter decides. The transmitter is the best judge of how much security his message requires -- and project security to match.

**Q** that was asked by a national security official **& A**

***Q: Some attack scenarios suggest to use Quantum Machine Learning (QML) as a tool to break common mitigate techniques. How can QSEC provide answer to this threat?***

**A:** This threat is exactly what QSEC is designed for. QML is very efficient in detecting and learning well concealed patterns. And thus it presents a serious risk to pattern-based (complexity based) ciphers.

BitMap replaces pattern with non-algorithmic randomness, which is pattern-devoid. The BitMap user expects its attacker to apply most powerful pattern -detecting algorithms, and it fights back by feeding the attacker with larger amount of random data to chew on and to hopelessly look for pattern therein. The attacker always assumes a hidden pattern and spins its wheels looking for it.

The BitMap user is in control. He decides how much randomness to use, how much wasted attack computation to cause. Yes BitMap is ready for quantum machine learning, very much so.

# BitFlip

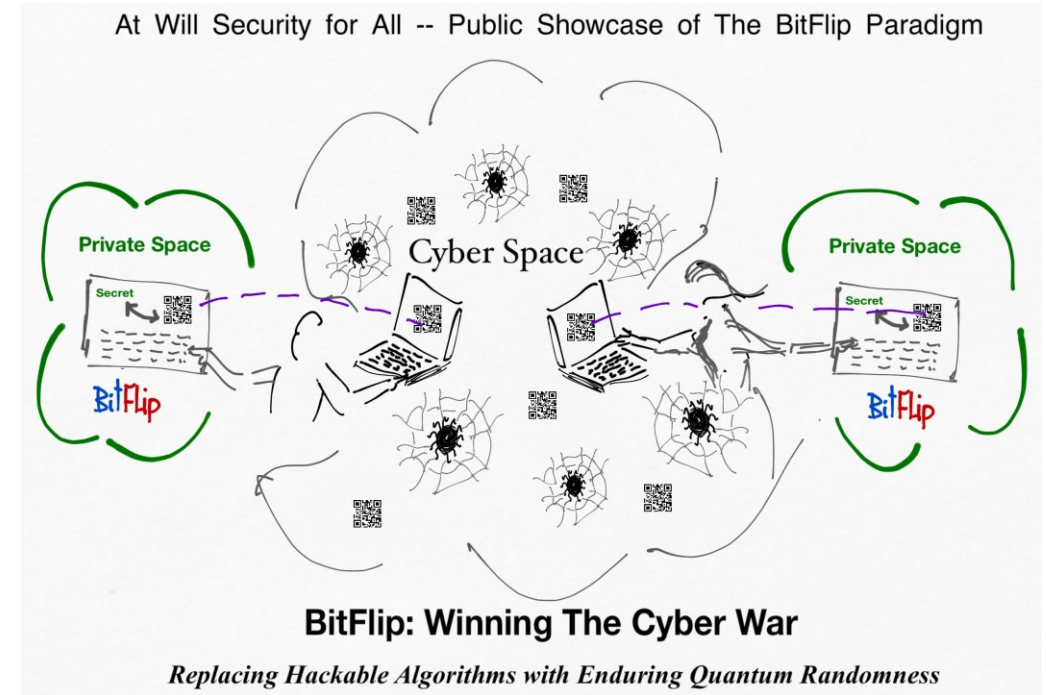
Quantum Security

**BitFlip** is a quantum-resistant communication security technology



BitFlip was independently evaluated by TÜV Informationstechnik GmbH – Evaluation Body for IT Security

TÜV evaluated the suitability of BitFlip and its augmentations as a new kind of crypto technology for high-end **financial** security, and the burgeoning **Internet-of-Things** market is a highly credible proposition,



BitFlip was evaluated by the global concern Giesecke+Devrient

BitFlip doesn't use any kind of classical number-obfuscation approach like AES, but uses equivocation to provide very high (provable) security, and its augmentations as a new kind of crypto technology for high-end financial security.



**BitFlip: Harassment-Resistant Cipher:**  
*Cyber Privacy,*  
*Finally*

**BitFlip**

**Protects your communications**  
**against any smart attacker!**



## David against Goliath

Quantum computers and super computers are like a gigantic Goliath armed with huge computing power. These Goliath can break most encrypted messages used by consumers and institutions nowadays.

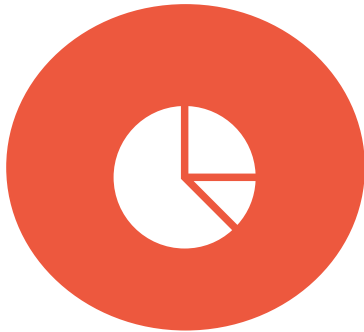
The simplicity of Bitflip is like a David using the power and simplicity of mathematics to protect secret messages against an army of Goliath!



# *BitFlip*

is a comprehensive solution to protect your data

---



QUANTUM  
RESISTANT



MATHEMATICALLY  
PROVEN.



PEER-REVIEWED  
AND PATENTED.



Certified by  
Institute of  
Standards  
[TÜV]



# BitMint AI-Powered Cyber-Innovation Hub

# The BitMint Edge

- Deploying State of the Art Innovation Productivity Tools
- Recognizing the Strategic factors ahead
- Exploiting the rich technological and security background of its founders
- Laser focused on Technology Development, seeking partners for its implementation

# BitMint Innovation Tools

- **Innovation<sup>SP</sup>** an innovation protocol for mapping the relevant knowledge in a formal order pointing to the best direction for further exploration.
- **Applying the Cost Estimation Credibility Principle:**  
Innovation is guided so as to maximize the credibility of the estimate of cost-to-complete and time-to-finish the research and development project.

# Recognizing the Strategic Factors Ahead

- Cyber Security is a race of imagination
- Cyber Space Identities are inherently unreliable
- Quantum Computing stands to upend Cyber Space
- Firewalls, fences, filters succumb to smarter attackers
- Digital Money is the most consequential development in cyber space

# Brief about BitMint

BitMint is a technology hub pioneering novel thematic innovation through the methodology of Artificial Intelligence Assisted Innovation (AIAI).

Innovation spans from material sciences to computer sciences.

We focus our new technology on exploitation of non-algorithmic randomness based on BitMint's US Patent: 11,394,530 ("RandoSol: Randomness Solutions"), and on various commercially available providers.

BitMint mission with respect to secure communication is to contribute to societal wellbeing in cyberspace by offering tools for identity management, and privacy preservation.

In this deck we focus on the effective use of non-algorithmic randomness as the critical ingredient for a suite of security tools, which put users in the driver's seat, allowing them to deploy sufficient randomness to defend against any and all cyber-attacks.

BitMint also innovated comprehensive cyber recovery tools, to bounce back following a security breach.

Our technology is documented in our library of US patents (39 awarded patents, many more pending).

More is found in various peer-reviewed articles published by BitMint's Chief Technology Officer, Prof. Gideon Samid, PhD. Eng., who is also a prolific author of **technology books**: "The Innovation Turing Machine", "The UnEnding CyberWar", "Tethered Money", "The Dawn of Digital Currency", "Computer-Organized Cost Engineering", while the underlying idea of these products is also highlighted in a recently published thriller: "The Cipher Who Came in from the Cold".

# Technology Development

- BitMint charted a technology development course with a vision to help bring about Cyber Peace by smart deployment of quantum-grade randomness and through handling cyber security as a reverse research and development effort.
- BitMint strategy is to focus on developing these technologies and concepts together with its initiative for artificial-intelligence assisted innovation (AIAI),
- while granting its mature IP and know-how of relevant technologies to successful implementers .





# Trans Vernam Ciphers

US Patents

11,290,253 11,159,317 11,212,097 11,539,519 11,336,447

11,038,668 10,790,997 10,965,460 11,394,530

10,541,954 10,673,822 10,911,215

10,728,028 10,523,642

10,608,814 10,798,065 10,541,808

10,728,028

6,823,068

Vernam

CIPHER

US Patent 1,310,719

# Thank You!

# BitMint

Quantum Safe Technology

<https://www.bitmintalk.com/qsec>

[amnon@BitMintMail.com](mailto:amnon@BitMintMail.com)