QRET

Quantum Resistant Encryption Technology (QRET)

QRET is a highly robust encryption technology capable of resisting the emerging quantum computing decryption technology and capable of protecting data in motion from today and tomorrow's threats.

The Problem:

As we move closer to quantum computing getting in the hands of enemy states and even homeland eavesdropping entities, the need for a more secure method of conveying messages becomes increasingly necessary. Perceived future advancements over the next 3 -10 years indicate that quantum computing decryption is at our doorstep.

Google claimed in October of 2019, to have calculated a mathematical equation that would have taken existing supercomputers over 10,000 years to complete, in a matter of 3 minutes and 20 seconds. IBM has disputed their claim, and taken it a step further, arguing that it could be theoretically be run on a current computer in less than two and a half days. In either case, the time to protect better, is now.

Deployment of a cryptographic algorithm across national security systems are currently estimated to take 20 years to fully deploy. It is incredibly important that action be taken now to prevent possible and probable attacks to our nation's security interest.

The Solution

TIMMES, Inc. QRET is a non-fixed key length encryption method that employs a reversible hash and initialization vector (key), to securely encode any computer data in such a way that it becomes impossible to recover the data with the key used to decrypt it. The encryption and signature generation algorithms are extremely lightweight, while being as powerful as AES-256, but without the key-space limitations of AES-256. After deployment, a key size can be chosen and changed at will, according to the needs of the sender or receiver. By employing key-lengths that can exceed the length of the clear-text, without increasing the size of the cipher-text beyond the size of the clear-text. Without the key, which can be of indeterminate length, the true meaning of the clear-text cannot be garnered.

QRET can also be used to increase cryptographic strength by being used as an external wrapper for pre-encrypted packages or messages adding to the difficulty of divulging their secrets, without fear of reducing the cryptographic strength of existing strategies

About Timmes We are changing the way data is secured and moved with our innovative SALT approach: Sea, Air & Land Technology.
We have been providing revolutionary, patent-driven compression and encryption products for over 15 years.

TIMMES USA
Clearwater - Florida
+1 (727) 712-0190

TIMMES Dubai
United Arab Emirates

TIMMES Pakistan
Lahore - Pakistan

QRET Benefits

QRET offers the US Government quantum resistant encryption of all electronic data with the ability to protect critical national infrastructure from foreign and domestic data exfiltration or modification.

QRET is impervious to Shor's algorithm due to its use of a non-fixed key space and that the key space is not limited to numbers exhibiting primality.

Secondly, it is impervious to power analysis due to the decryption not using complex math and due to each member of the key space exhibiting the same computational timeframe.

Also, it is impervious to trial division for the same reasons shown for Shor's algorithm. Lastly, it is impervious to Deutsch–Jozsa algorithm, because more than one correct answer can be correctly devised from a single cipher-text.

Because of this; it is likewise impervious to Bernstein–Vazirani, and other black box problem solving routines, not the least of which are Quantum least-squares, Simon's, and quantum approximate optimization.

$6 Trillion

ANNUAL ESTIMATED COST OF CYBERCRIME. THIS FIGURE HAS NEARLY DOUBLED IN THE LAST FIVE YEARS ALONE.

DATA BREACHES BY THE NUMBERS

> 440+ **US Govt. entities breached between** 2014 **and** 2019.
> 95.1**M records exposed in Washington DC during that time.**
> 237.2**M Government records exposed in merely** 35 **breaches.**
> 66% **of breaches in** 2014 **involved paper data.**
> 240 **digit encryption key cracked in** 2019 **by French scientists.**

The Time for Action

In 2016, thirteen minutes after the Pentagon challenged people to attempt hacking their website, it was accomplished by a teenager on a laptop.

The use of quantum computing is getting closer to reality in commercial and business applications. There is too much at stake for this question to be unanswered for as long as it has.

The time for action is yesterday and the answer is QRET.

> QRET stands to be a best solution to mitigate the perceived deleterious impacts of the assessed technological advancements of quantum computing.
> TIMMES proprietary quantum resistant technology does not suffer the surface exposure that a fixed key length encryption method does.
> Fundamentally, security is intended to keep honest people on the good side of the law. Excellent security, on the other hand, is intended to make it more trouble than it is possibly worth to get in.
> Access to QRET is available to security and intelligence agencies, government systems, defense and special users. ITAR restricted with CONUS upon approvals.
> Our solution is available immediately, and can be used to supplement existing encryption methods where they are needed most without requiring agencies lower in triage to adapt to a new standard right away.
> QRET is available to the government for testing right away. TIMMES requests the opportunity to demonstrate QRET encryption to the appropriate government agencies for test and exploitation resistance using quantum computing devices.

QRET Applications

Unmanned & Manned Vehicles;
Warfighters;
Satellites;
Surveillance;
Telemedicine;
Smart Weapons;
Loitering weapons.

About Timmes We are changing the way data is secured and moved with our innovative SALT approach: Sea, Air & Land Technology. We have been providing revolutionary, patent-driven compression and encryption products for over 15 years.

TIMMES USA
Clearwater - Florida
+1 (727) 712-0190

TIMMES Dubai
United Arab Emirates

TIMMES Pakistan
Lahore - Pakistan