

# Secure Channels Unveils Encryption Fix For IoT Leveraging ID Quantique's Quantum Technology

*Solution Provides Answers to Weak Encryption Keys Common to IoT Devices*

IRVINE, CA, UNITED STATES, January 7, 2020 /EINPresswire.com/ -- Resource-constrained IoT devices are notorious for their inability to host robust encryption with sufficient entropy. [Secure Channels](#)'s quantum-resilient, embedded symmetric encryption solution leverages ID Quantique's (IDQ) quantum technology giving IoT manufacturers a powerful new tool to deliver protected network devices. The new solution particularly adapted for drones will be displayed at the CES 2020 conference Jan. 7 to 10 in Las Vegas.

A recent report by cybersecurity firm Keyfactor emphasizes IoT devices' lack of adequate entropy sources, leading to serious cybersecurity shortcomings. Entropy provides the integrated cipher with the randomness required in order to generate strong keys that are difficult for adversaries to break. IoT devices like sensors, IP cameras and connected consumer devices are primarily designed for optimal performance, cost and battery life. These considerations leave little space or resources for sound encryption technology. Manufacturers that manage to include encryption into their products gravitate toward common asymmetric ciphers like RSA. However, device architecture often prohibits the inclusion of an entropy source the cryptosystem can leverage. The keys generated in these deployments, therefore, lack the degree of randomness that can keep adversaries from cracking the encryption and accessing the device.

Further diluting IoT device security is the possible weakness of the RSA cipher itself. RSA was determined to be breakable through quantum computing a quarter century ago, giving the cipher an impending shelf life. However, teams in France recently cracked the largest RSA keys to date with shocking speed using classical computers. Although the size of the cracked key (795 bits) is still very very far from the currently used keys (2048 bits), the accomplishment highlights the dangers of asymmetric cryptosystems centered around presumed unsolvable math and suggests RSA's whole failure may occur earlier than estimated.

Secure Channels's encryption aims to address IoT's cybersecurity gaps. Secure Channels' [XOTIC Core](#) cryptosystem delivers efficient post-quantum encryption at speeds that exceed those of popular stream ciphers. XOTIC Core's unique one-time pad element draws entropy from the IDQ's Quantis QRNG chip to rapidly create scalable, symmetric encryption keys ranging from 512



to 8,192 bits. The Quantis QRNG chip is a compact, durable quantum random number generator that can be integrated into small, low-power products. XOTIC Core is ultra-lightweight with only 72KB of code providing a highly efficient, post-quantum strength cryptosystem, allowing easy integration into any resource-constrained device.

The solution affords IoT manufacturers a flexible, new option for protecting their devices from evolving threats. It addresses the cybersecurity gap in an exploding IoT market. By 2025, a forecast 76 billion devices will have been deployed — devices that are predominantly the weakest network links. Their “trusted status” on a network can extend the reach of an adversary successful in compromising a single encryption key. One exploited device can net adversaries free reign over network endpoints to access sensitive data, manipulate machinery or deluge websites with traffic. This first solution represents the foundation of a future collaboration between Secure Channels and ID Quantique.

Secure Channels CEO Richard Blech feels that this solution can eliminate potentially tragic cyberattack scenarios in the consumer electronics market and beyond. “The rampant expansion of IoT and IIoT has been aided by a grossly misplaced trust in weak onboard encryption. It’s created a precarious situation now that these devices are tasked with transmitting sensitive personal data, monitoring embedded health devices and operating machinery at the heart of critical infrastructure. Strong future-proof encryption may be the deciding factor that averts ruined livelihoods, health crises or widespread catastrophe. I’m confident manufacturers of these devices and equipment appreciate their responsibility to protect end users with entropy-backed, dependably secure products”

Learn more about Secure Channels’ XOTIC Core at [www.securechannels.com/xotic](http://www.securechannels.com/xotic).  
Learn more about ID Quantique’s Quantis QRNG chip at [www.idquantique.com/random-number-generation/products/quantis-qrng-chip/](http://www.idquantique.com/random-number-generation/products/quantis-qrng-chip/)

#### About Secure Channels

Secure Channels is a cybersecurity solutions development company based in Irvine, Calif. Our experts engineer and develop high-performance, cost-effective cybersecurity technologies as platform-agnostic software and hardware-ready solutions to protect against present and emerging threats. Our award-winning, cryptanalyst-celebrated solutions include advanced data protection, future-ready encryption, authentication and enterprise confidentiality solutions. Learn more at [www.securechannels.com](http://www.securechannels.com).

#### Contact

Secure Channels Inc.

+1 949-679-5777

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

---

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases. © 1995-2020 IPD Group, Inc. All Right Reserved.