KETS

How KETS' solutions remove key barriers to adoption for quantum encryption technologies

The 2016 NCSC Quantum Key Distribution (QKD) Whitepaper succinctly summarised a number of key issues previously identified in the quantum research community which require addressing before the technology becomes widespread and delivers on its full promise. Crucially, KETS' solutions are specifically designed to address the most important of these issues.

KETS's approach removes several practical limitations of quantum encryption technology. KETS' first devices are capable of multi-protocol operation. This already enables a certain amount of remote patching – if a vulnerability is found in the implementation of one protocol the device can switch to another one. Further redundancy will be built into future devices, removing the automatic need to recall equipment to the vendor. This is facilitated by the integrated platform where the increase in footprint for redundant optical circuits on-chip is negligible as compared to fibre optic and bulk implementations.

KETS' integrated chip technology greatly increases the feasibility and affordability of large multi-device, multi-path network topologies. Banks of integrated QKD transceivers, each with their own optical channel and potential routing, can be incorporated into a single system. This removes the limitations of the original QKD protocols which were initially point-to-point algorithms. We enable a very flexible, optical network architecture capable of many different network topologies and routing paths which can crucially be reconfigured when an attack is detected. This ability to switch to a safe alternative route leverages the same approach contemporary technologies use to thwart denial-of-service attacks. KETS Founders are some of the original pioneers of these concepts in the Software Defined Networking (SDN) setting. Finally, our multi-protocol operation also allows our devices to be reconfigured in real-time for optimal network operation as different operating conditions are detected.

KETS takes a modern, systems level approach to designing new cryptosystems. Modern cryptosystems go far beyond basic public key/asymmetric cryptography algorithms to include functions in secure identification, data integrity, trust, and certificate authorities. KETS knows that full solutions are complex and will utilise the most appropriate tools for each task, including quantum encryption, post-quantum cryptography algorithms, and future certificate authorities. Additionally, solutions might utilise designs such as trusted nodes to extend distances and provide lawful interception where required. Security must always be designed for at a systems level, whether quantum or classical, to make sure no vulnerabilities are inadvertently opened.

KETS' world-leading integrated quantum photonics approach drives down costs, facilitates scalability, and enables many new applications. Previous bulk and fibre optic implementations were not only expensive, big, and power hungry, but their form-factor prevented a large number of critical applications from being addressed (e.g. satellites and aerospace platforms, easy incorporation into larger systems, and deployment into nuclear power station sensor networks). KETS' system is uniquely built on an integrated quantum photonics platform enabling low-SWaP (size, weight, and power) applications today and eventual integration *at the chip level* tomorrow. KETS aims to reduce the cost of its quantum encryption solutions by orders of magnitude.

Unit DX, St Philips Central Albert Road, Bristol, BS2 OXJ
www.kets-quantum.com
Company No: 10297688

Chris Erven, CEO
+44 (0) 791 469 0411
chris.erven@kets-quantum.com

KETS places a premium on the security assurance of its devices. Any real-world QKD system will be built from several different components. We are working closely with NPL through the ISCF AQuaSeC and upcoming AQRNGs grants on the certification of our devices and sub-systems to guarantee their proper operation, as well as to accurately assess, quantify, and validate the security of our devices. We are also supporting cutting-edge chip-based quantum hacking work at the University of Bristol with some of the world's leading "Quantum Hackers". Quantum encryption is no different than any other encryption technology and our devices will be subjected to rigorous analysis and penetration testing before release. Just as with classical cryptography algorithms such as SHA-1 and GCHQ's recently rescinded post-quantum cryptography algorithm Soliloquy; if any weaknesses are discovered in KETS' devices, they will quickly be patched. Finally, KETS is engaging with ETSI's and ITU-T's critical quantum encryption standardisation push through our partnership on the Quantum Communications Hub.

KETS recognises the key requirement of crypto-agility as we secure our information systems from quantum computers. Launched in 2015, new NIST post-quantum standards are expected in 2022-23. As vendors prepare for a very costly migration to new crypto standards now is the time to consider all quantum-safe alternatives including quantum encryption technologies. Many of the post-quantum cryptography algorithms have drawbacks including massive memory and processing requirements as well as limitations on speed, not to mention that their security promise is the conjecture that *to the best of our knowledge, this algorithm is not susceptible to an attack by a quantum computer or other device.* Crypto-agility, the ability of an information system to switch to alternative cryptographic primitives and algorithms without making significant changes to the system's infrastructure, is now the name of the game to ensure we have the most robust and update-to-date cryptographic protection. Moreover, we need to ensure the new technologies we migrate to are backwards compatible. KETS is committed to designing our systems to allow the highest degree of crypto-agility as they are incorporated into secure systems.

Applications need to be evaluated on a case-by-case basis. Limited range is cited as a concern; however, many mission critical data back-up and cloud storage applications are routinely performed to sites within 40 miles of each other while distances in smart-city applications are reachable with quantum encryption technologies. Further, we can optimise our solutions when specific operating conditions are identified. Integrating quantum security with the internet-of-things (IoT) is seen as another challenging area. However, the security of cheap IoT devices would benefit from an affordable, integrated QRNG partnered with post-quantum algorithms. While industrial IoT devices which have a higher value, complexity, and risk, could benefit from a full quantum solution. For securing the control plane of the UK's next generation telecommunications network, full QKD coupled with a strong key management system could be crucial to maintaining its security. And efficiently distributing secure quantum keys globally with satellites will only be possible with a chip-based approach. Finally, new applications – such as mapping your genome for your future health – will require radically new security guarantees and business models.

In summary, we believe that quantum technologies have a key role to play in addressing the future of information security. The key is to take a systems approach, applying the right hardware, software, and operational security at each point. KETS' low cost, robust, scalable technology will enable the use of quantum technology in practical next generation solutions.

Unit DX, St Philips Central Albert Road, Bristol, BS2 OXJ
www.kets-quantum.com
Company No: 10297688

Chris Erven, CEO
+44 (0) 791 469 0411
chris.erven@kets-quantum.com