Open letter to the security community:

on **Recommendations for Quantum Entropy Sources**

Washington, December 6th, 2018
At the Hudson Institute

In full awareness of the urgent need to act, we, the undersigned – representing fourteen organisations from six countries – call on the security community to establish recommendations applicable to quantum entropy sources.

Quantum physics is peculiarly suited to implement noise sources with an entropy that can be estimated based on information theory. However, there are not yet any existing recommendations that explicitly distinguish between noise sources based on quantum physics and ones based on classical physics. This recommendation is an add-on to existing noise or entropy source recommendations that allow specification of whether the noise source under evaluation is based on quantum physics or not.

Therefore, this recommendation defines: a generic architecture of a quantum entropy source, a common method to estimate and validate the entropy of a noise source under evaluation, and a common method to specify randomness extractors when they are part of the implemented system.

We, the undersigned, support this initiative as a starting point for work items within study groups and will continue to liaise with international standards bodies such as ITU, ISO and ETSI.

Appendix A (Quantum Entropy Source Recommendations)

Signed,

Armafex Partners LLC

Harris Corporation

QuantumXchange

Bra-ket Science

Hudson Institute

SK Telecom

Cambridge Quantum Computing

IDQuantique

SPAWAR Systems Center Pacific

Ciena

Qubitekk

University of Warsaw

Florida Atlantic University

QuintessenceLabs

Signed,

MagiQ Technologies

Rivada Networks

Institute for National Defense & Security Research

BrightApps LLC

Open letter to the security community:

on **Foundational Recommendations for Quantum Key Distribution (QKD)-secured systems**

Washington, December 6th, 2018
At the Hudson Institute

In full awareness of the urgent need to act, we, the undersigned – representing fourteen organisations from six countries – call on the security community to establish foundational recommendations on Quantum Key Distribution (QKD)-secured systems.

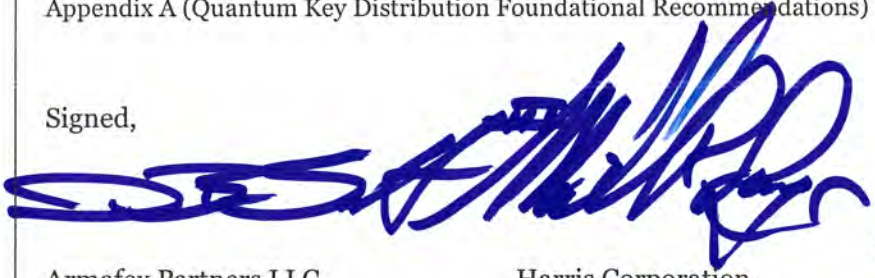
There is presently a strong interest from potential users for Quantum Key Distribution (QKD) technologies. This interest is driven by the benefits of cryptographic key generation and distribution that does not require any computational assumptions and can resist quantum computing attacks. However, there is no existing certification that permits keys provided by QKD to be approved for cryptographic applications. An intensive standardization effort is ongoing at ETSI to fill this gap. In the meantime, recommendations based on existing standards for cryptographic systems should be proposed to facilitate and accelerate the deployment of QKD systems at a larger scale.

The present recommendation aims to add specifications for QKD to existing cryptographic standards to make QKD systems approvable. This recommendation focuses on making the keys generated and distributed by a QKD system approvable based on these existing standards.

We, the undersigned, support this initiative as a starting point for work items within study groups and will continue to liaise with international standards bodies such as ITU, ISO and ETSI.

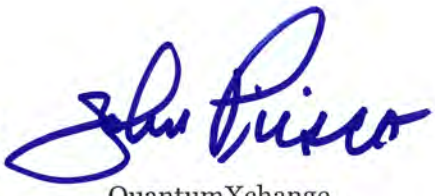
Appendix A (Quantum Key Distribution Foundational Recommendations)

Signed,

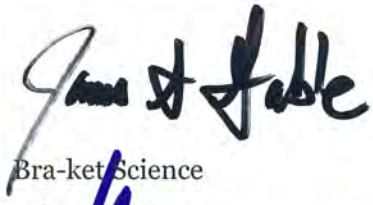


Armafex Partners LLC

Harris Corporation

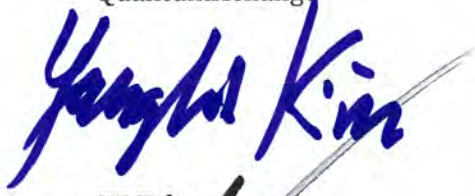


QuantumXchange



Bra-ket Science

Hudson Institute



SK Telecom

Cambridge Quantum Computing

IDQuantique

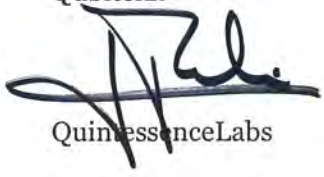
SPAWAR Systems Center Pacific

Ciena

Qubitekk

University of Warsaw

Florida Atlantic University



QuintessenceLabs

Signed,

MagiQ Technologies

Rivada Networks

Institute for National Defense & Security Research

BrightApps LLC