Quantum Security – Preparing for the next era

Dong-Hi SIM, Head of Global Standards at ICT R&D Center, SK Telecom

It is no surprise at all to emphasize the security threats in terms of computing power, hacking and massive eavesdropping especially nowadays. We all notice that the news articles related to these almost every day.

In particular, optical fiber hacking could happen even though you are not an expert in this area.
You can easily buy the simple equipment to hack into optical fiber network.

From cryptography perspective, there are also major threats as public key cryptography is based on mathematical problems which can be broken by future technology. And this also means that the increase in computing power makes it easier to break public key cryptography.
And finally the most important one is quantum computing as it can solve certain mathematical problems - exponentially faster than classical computing as it relies on quantum physics.

Basically any crypto-system based on mathematical complexities is vulnerable to quantum attack. So we need to have a much better solution to distribute secret keys between distant parties. And the answer is Quantum Key Distribution(QKD). Quantum cryptography allows us the key exchange between two remote parties with absolute security as this is guaranteed by the fundamental laws of physics.

Ensuring forward-secrecy for the most sensitive information, QKD works on the intrinsic and proven principles of quantum physics – i.e. that the generation of the quantum key is truly random, and that any interruption or eavesdropping of the data will perturb the system and can thus be detected. Each quantum key is independent and uncorrelated, and automatically updated every minute. Unlike classical encryption based on mathematical algorithms, QKD will not be compromised by mathematical progress or the continued increase in computing power and it is not vulnerable to fibre tapping. Such attacks are potentially the most dangerous as they are most often not even detected and compromise a large volume of data. QKD is a quantum-safe technology available and deployed today in production environment.

SK telecom has been making efforts for aiming to develop a secure infrastructure as well as detecting and blocking eavesdropping in the network.

This presentation will attempt to give the benefits of QKD and the commercialization efforts from SK Telecom in South Korea.