CIR
ENLIGHTENED ANALYSIS

CIR Market Report

CIR
ENLIGHTENED ANALYSIS

Quantum Encryption Systems Markets: A Technology and Business Opportunity Forecast – 2017 to 2026

June 2017

Chapter One: Introduction1.1 Background to this Report

Quantum encryption (a.k.a. quantum key distribution, QKD) is the first encryption process that is apparently unbreakable; a very strong use case in these days of (1) ubiquitous hacking and (2) imminent commercial quantum computers that can break standard public key encryption codes. QKD has been available since the 1980s, but the sudden urgency in the need for quantum encryption, will, CIR believes, spur the market for QKD systems in the next few years and certainly over the next decade.

We cannot, however, be sure just how big the market for QKD systems will ultimately be. QKD competes with an alternative breed of encryption that is also supposedly safe from attacks by quantum computers. This so-called post-quantum encryption is a "math solution" much like the current generation of public key encryption systems and so may have a familiarity to current end users that QKD (a "physics" solution) cannot bring. However, for now the post-quantum encryption discipline contains many suggestions for solutions, and we would consider it somewhat less mature than quantum encryption. On the other hand, rumors that quantum encryption has its own vulnerabilities refuse to go away.

1.1.1 The Addressable Market for QKD is About to Explode

Nonetheless, despite these uncertainties, we have every reason to believe that significant revenues will be generated by QKD in the near future. While in the past QKD use has been restricted to a few government, military and financial services users, we think the number of potential users are about to explode, specifically outside of the government/military sector.

Banks and financial services: Banks have been prominent as customers for QKD trials since the very beginning—the Bank of Austria was part of the first ever QKD trial, for example. However, we see the potential for QKD in the financial services sector to move well beyond trials to include a broad range of both large and smaller financial institutions.

As we see it, the largest potential for selling QKD systems into the banking/financial services sector will be where banks, etc., are making bulk transfers. Here the potential financial loss is so huge that almost any price paid for a QKD system could be worth it. Such bulk transfers occur where branches are communicating with head offices or sending to data storage facilities.

Bulk transfers are not the only use for encryption in the banking and financial services world and encryption is widely used in this sector. It is also mandated both internally by banking regulatory commissions in many cases, which suggests that—at the very least—there will be a budget of encryption systems and an openness to listening to firms marketing QKD systems.

Telecom networks: Telecom companies have also often been pioneers in QKD trials worldwide and CIR sees them as both utilizing more systems in the future as well as being actively involved in the development of them. Some of the large service providers that have become involved in the development of QKD transport include British Telecom, KPN, NTT and SK Telecom. Other firms that have traditionally been suppliers of telecom equipment are also involved to some extent in QKD. We note, in particular, that the Chinese telecom equipment firm, ZTE, has developed a QKD box for the optical transport network (OTN) infrastructure.

CIR believes that telephone companies represent a strong market for QKD suppliers going forward and we think that the specialist approach followed by ZTE might be the way to go; the market will be big enough to take this approach going forward. We are already seeing quantum networks being built by various providers. QKD will not be the only application that will be supported on this infrastructure, we also anticipate that they will support quantum computing and quantum sensing.

However, what is going to slow down the development of this part of the QKD market is the fact that there are inherent technical difficulties with long-distance transmission of QKD data. The point here is that traditional optical amplifiers can't be used in a quantum network because they break the no-cloning theorem in quantum information theory. New kinds of repeaters are emerging to solve this problem and some quantum networks are evolving to support long-haul quantum channels.

QKD, data centers and the enterprise: It is probably fair to say that there is hardly any QKD deployed the average business today, even in the largest ones. We think this is about to change for the reasons given at the beginning of this chapter—the growth in hacking and the growing vulnerability of public key encryption. From a purely marketing perspective what we are talking about here is the potential market for QKD systems growing from a few thousand locations to *potentially* hundreds of thousands or even millions.

This will put QKD on the map of enterprise technologies. Nonetheless, CIR believes that the penetration in enterprise/data center QKD will occur quite slowly, impacting the very largest firms and most vulnerable applications first. As far as the applications are concerned, what we think is the most likely initial use for QKD in the enterprise will be transfer of bulk data to specialized disaster recovery facilities, since there is typically a lot of important data involved and it is quite vulnerable.

But we also expect the penetration of QKD to move into other areas in business. For example, many businesses need to keep their design and development material, financial data and other documents in safety and security. The potential losses for customer organizations due to negligence can be devastating. And even where enhanced security is not mandated by law, it may be required by company policy.
But for QKD to take a significant bite into the enterprise market it will have to drop significantly in price. Given that at the component level QKD technology is not that different from other off-the-shelf photonics technologies, we believe that a significant

decline in QKD and related gear is to be expected based on volume shipments and experience curve impacts.

1.1.2 Funding QKD: From Governments to VCs

Much of the above tacitly implies that there will be significant amounts of money around to fund the development and marketing of QKD. There are several reasons to believe that money will not be a problem in this area.

Big support from government and military: This almost goes without saying. Government is a long-standing financial supporter for quantum technologies. For example, the U.K. has a quantum technology program valued at $337 million and the European Union has a similar program worth $1.08 billion to support pan-European R&D. Other governments that support quantum technologies at relatively high levels of funding include those of the U.S., China and Japan.

In addition, defense departments in major nations are providing funding for QKD projects separately from civil government funding. CIR believes that much of this is secret and we can only assume that the amounts are quite large. It is actually quite hard to find specific references to military uses of QKD, but they are no doubt hidden in plain sight, since many of the civilian QKD projects will no doubt have military spinoffs and applications.

The motivation for this funding is twofold. One aspect is that government, the military and intelligence services are simply funding the development of a technology they themselves use, which is natural enough. Another is that state actors want to support strategic superiority for their nations and blocs.

VCs entering this space: Relatively small amounts of venture capital have so far been invested in individual QKD firms, but it is by no means unusual for VC firms to make such investments. VCs are possibly even more interested in quantum computing firms than QKD ones, but we expect VCs to gradually think of “quantum” as a defined sector worth funding as QKD becomes further deployed and quantum computing becomes more of a reality. In other words, we expect VCs to see “quantum” as a good place to put venture money, with advances in quantum computing, QKD, quantum sensors and quantum networks, all supporting one another.

Big players with potential: While there are some interesting small and specialist firms in the QKD space—IDQ—perhaps most notably, the list of firms that are or have been involved in this space includes names such as HP, IBM, BT, Nokia, Toshiba and other tier one names. In some cases, these firms have been out of the QKD space for a while, but there are now good reasons for working in this space.

These reasons include the simple fact that QKD is expected to grow fast for all the reasons that we give above. However, many of these firms have particularized reasons for funding the development of QKD products and projects. For example, HP Enterprises is looking for spinoff products for the quantum computing program it operated until the breakup of the old HP and is also pursuing new opportunities in the data center field.

QKD products sound like a natural here. IBM does not have a QKD product but does have quantum computing programs and is active in the encryption space.

Of the large firms, however, the one with long-term leadership potential in this field is most likely Toshiba, which has pursued QKD opportunities for years now and has never wavered from the goal of making money in this space.

1.2 Goals and Scope of this Report

The primary goal of this report is to identify the main opportunities that will be available to both investors and direct players in the QKD market and to quantify them over the coming decade. As far as the latter is concerned, this report presents detailed ten-year forecasts for QKD systems and deployments over the coming decade.

With regard to the scope of the report, the focus is, of course, on QKD systems of all kinds, but our coverage includes related systems (e.g., photon counters). We include in our analysis all end-user segments of this market including military, civil government, intelligence and police services, banking and financial services, and general business applications, as well as niche applications.

The report includes an assessment of the latest R&D into QKD and how this impacts the commercial quantum encryption market and the development of QKD products. This assessment covers both work done at leading research institutes and at corporate labs. Finally, the report includes strategic profiles of all the leading firms supplying QKD and related systems or likely to do so. In these profiles we discuss how each firm regards the current state of the QKD market and how they are likely to participate in it.

Finally, in addition to our system forecasts, we also include forecasts of critical optical components and modules that are used in QKD systems.

1.3 Methodology of this Report

The methodology employed to construct this report involves both primary and secondary research. The primary research consists of interviews conducted primarily on the phone but also in person to some extent. The secondary research consisted of reviews of both technical and business articles related to quantum encryption.

The ten-year forecasts included in this report utilize a methodology that is described in Chapter Four.

1.4 Plan of this Report

Chapter Two of this report focuses on the evolution of QKD and looks especially at the critical problem of long-distance QKD and the impact of standards on the QKD market. Chapter Three examines the patterns of demand for QKD in many different markets, both traditional (e.g. military) and non-traditional (e.g. data centers).

Chapter Four contains the ten-year forecasts mentioned above, along with the methodology on which they were constructed. Finally, Chapter Five contains profiles of 19 companies that are active in the QKD space or likely to become so in the near future.