

Quantum Cryptography - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

<https://marketpublishers.com/r/QE8032B38697EN.html>

Date: July 2024

Pages: 135

Price: US\$ 4,750.00 (Single User License)

ID: QE8032B38697EN

Abstracts

The Quantum Cryptography Market size is estimated at USD 0.58 billion in 2024, and is expected to reach USD 2.09 billion by 2029, growing at a CAGR of 29.19% during the forecast period (2024-2029).

The key drivers contributing to the increase in the adoption of data-intensive approaches and decisions with the growth, including the rise in the number of cyber-attacks globally with the growing digitalization, have the potential to damage the internet-linked digital infrastructure of various government or private sector enterprises, thereby significantly driving the market's growth rate.

Key Highlights

The need for cybersecurity majors in enterprises and government entities of various countries increased in the post-pandemic period due to the trend of online and data-driven businesses, fueling the implementation of quantum cryptography solutions by encrypting sensitive information through quantum mechanics.

With the growing dependence on technology and digitalization, BFSI players such as banks, investment banks, and insurance firms have increased their use of best safety solutions over recent years. Further, as indicated in the graph, the attacks in the BFSI sector have been significant, thereby contributing to the market's growth rate. Quantum cryptography has become a major point of view, given the scale of exposure to cyberspace. As indicated in the graph, there have been several malware, network, and application policy violations, among other attacks.

The increasing risk of cyberattacks based on quantum technology is emerging in the market, which can create threats to the network and data platform of the end users using traditional cryptography-based cyber security measures and can drive the demand for quantum cryptography cyber security solutions in the market.

Quantum cryptography has emerged as the optimal choice for securing communication and data storage, given its unique features, including high security and cyber detection. However, this comes with high installation, maintenance, and supporting infrastructure costs, limiting the market's growth.

The pandemic has raised the demand for cyber solutions to protect businesses and countries from malicious cyber-attacks supported by increasing digitalization. Additionally, the Bank for International Settlements stated that, during the COVID-19 pandemic, financial institutions faced an increasing risk of cyberattacks, which were accelerated by remote working conditions.

Quantum Cryptography Market Trends

BFSI Sector to Witness Major Growth

The emergence of digital banking services and the development of Fintech ecosystems worldwide have raised the number of electronic financial data about banks and their customers, which are vulnerable to cybercrime incidents. These drive the adoption of quantum cryptography solutions in data management among the banks due to their applications in protecting the bank's network, applications, and data from quantum computing-based cyberattacks.

The volume of digital payment users is increasing exponentially, especially since the COVID-19 pandemic. According to the RBI, around 114 digital payments were made in India in FY 2023. The growth of digital payments in line with the trend of a cashless society is raising the demand for the quantum cryptography market in banks because electronic payments rely on encryption to protect customers and businesses from cyberattacks. This can be further secured by upgrading traditional encryption to quantum encryption in processing the payment data, which would support the market's growth in the future.

For instance, in July 2023, HSBC was the first bank to join BT and Toshiba's quantum-secured metro network, connecting two UK sites using Quantum Key Distribution (QKD) to prepare its global operations against future cyber threats. Using an AWS Snowball

Edge device, this technology would be trialed in multiple scenarios, including financial transactions, secure video communications, one-time pad encryption, and AWS edge computing capabilities, showing the increasing demand for quantum cryptography solutions in the BFSI sector in the future.

By geography, the Asia-Pacific region is expected to contribute significantly to the growth of the market in the BFSI sector, supported by the growth in the digital payment and online banking landscape in the Asian and Southeast Asian countries during the forecast period.

The increasing awareness of quantum computing-based solutions in the banking sector for secured information transfer would support the market's growth by creating an opportunity for quantum cryptography solutions in the BFSI sector.

Asia-Pacific Is Expected to Register the Fastest Growth

With the increasing incidence of cyber threats, organizations in the Asia-Pacific region are prioritizing cybersecurity measures to protect their sensitive data and communications. Quantum cryptography offers advanced security by leveraging the principles of quantum mechanics, making it a solution for those organizations looking to enhance their cybersecurity posture.

Further, advances in quantum technology are making quantum cryptography more practical and accessible in Asia. Also, regional researchers and companies are investing significantly in developing quantum key distribution (QKD) systems, quantum random number generators (QRNGs), and other quantum-enhanced security solutions.

For instance, in August 2023, SKY Perfect JSAT Corporation announced the launch of a Quantum Cryptography Optical Communication Device with built-in satellite-based Quantum Key Distribution (QKD) and Cryptography Technology. The development was implemented as part of the research and development of quantum encryption technology regarding satellite communications.

Again, in March 2023, Chinese research institutes announced that the country is working to build a quantum communications network utilizing satellites in low and medium-to-high Earth orbits. Under this, China has used aspects of quantum mechanics to encrypt and secure the transmission of information. The mission executed

experiments in quantum key distribution (QKD), quantum entanglement distribution, and quantum teleportation.

Moreover, the demand for quantum cryptography in the IT and telecom sector in the Asia-Pacific region is rising rapidly. The IT and telecom sectors handle vast volumes of sensitive data, including personal information, financial transactions, and other business data. With the increasing frequency and threat of cyberattacks, organizations in these sectors are focusing on their data security measures with the adoption of quantum cryptography, as it offers advanced security by using the principles of quantum mechanics to secure communications and protect data against such cyber threats.

Quantum Cryptography Industry Overview

The quantum cryptography market is fragmented, with the presence of major players like QuintessenceLabs Pty Ltd, Crypta Labs Limited, ID Quantique SA, MagiQ Technologies Inc., and Nucrypt LLC. Market players are implementing strategies such as partnerships, innovations, and acquisitions to improve their product offerings and gain sustainable competitive advantage.

October 2023: 1touch.io announced a strategic Independent Software Vendor (ISV) partnership with QuintessenceLabs to strengthen enterprise defenses against the cryptographic threats posed by quantum computing. The company's collaboration with QuintessenceLabs provides enterprises with a comprehensive view of their entire cryptographic landscape, enabling them to pinpoint vulnerabilities and take targeted action.

October 2023: Crypta Labs partnered with Blueshift Memory to create a cybersecurity memory solution capable of countering threats from quantum computing. Also, Blueshift Memory will integrate the QOM into its Cambridge Architecture FPGA module to establish a cybersecurity memory solution resistant to threats, even those from quantum computing.

Additional Benefits:

The market estimate (ME) sheet in Excel format

3 months of analyst support

Contents

1 INTRODUCTION

- 1.1 Study Assumptions and Market Definition
- 1.2 Scope of the Study

2 RESEARCH METHODOLOGY

3 EXECUTIVE SUMMARY

4 MARKET INSIGHTS

- 4.1 Market Overview
- 4.2 Industry Attractiveness - Porter's Five Forces Analysis
 - 4.2.1 Bargaining Power of Suppliers
 - 4.2.2 Bargaining Power of Buyers
 - 4.2.3 Threat of New Entrants
 - 4.2.4 Threat of Substitute Products and Services
 - 4.2.5 Degree of Competition
- 4.3 Industry Value Chain Analysis
- 4.4 Impact of COVID-19 on the Industry

5 MARKET DYNAMICS

- 5.1 Market Drivers
 - 5.1.1 Rising Number of Cyberattacks
 - 5.1.2 Growing Need for Next Generation Security Solutions for Cloud and IoT Technologies
 - 5.1.3 Evolution of Wireless Network Technologies
- 5.2 Market Restraints
 - 5.2.1 High Implementation and Installation Costs
 - 5.2.2 Absence of Skilled Expertise and Technological Challenges

6 MARKET SEGMENTATION

- 6.1 By Component
 - 6.1.1 Solutions
 - 6.1.2 Services

6.2 By Application

6.2.1 Network Security

6.2.2 Application Security

6.2.3 Database Security

6.3 By End Users

6.3.1 IT and Telecommunication

6.3.2 BFSI

6.3.3 Government and Defence

6.3.4 Healthcare

6.3.5 Other End Users

6.4 By Geography

6.4.1 North America

6.4.2 Europe

6.4.3 Asia-Pacific

6.4.4 South America

6.4.5 Middle East and Africa

7 COMPETITIVE LANDSCAPE

7.1 Company Profiles*

7.1.1 QuintessenceLabs Pty Ltd

7.1.2 Crypta Labs Limited

7.1.3 ID Quantique SA

7.1.4 MagiQ Technologies, Inc.

7.1.5 Nucrypt Llc

7.1.6 PQ Solutions Limited

7.1.7 ISARA Corporation

7.1.8 QuantumCTek Co. Ltd

7.1.9 Quantum Xchange Inc.

7.1.10 QuNu Labs Pvt Ltd

7.1.11 Qutools GmbH

7.1.12 AUREA Technology

7.1.13 Infineon Technologies AG

7.1.14 Toshiba Corporation

7.1.15 Kets Quantum Security Ltd

7.1.16 IBM Corporation

7.1.17 Qrypt Inc.

8 INVESTMENT ANALYSIS

9 FUTURE OF THE MARKET

I would like to order

Product name: Quantum Cryptography - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts (2024 - 2029)

Product link: <https://marketpublishers.com/r/QE8032B38697EN.html>

Price: US\$ 4,750.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/QE8032B38697EN.html>