

Quantum Cryptography (QC) Market by Solution (Quantum Key Distribution (QKD), Quantum Random Number Generators (QRNG), Quantum-safe Cryptography)), Service (Professional, Managed), Security Type (Network, Application, Cloud) - Global Forecast to 2030

<https://marketpublishers.com/r/QBCD9296B913EN.html>

Date: October 2024

Pages: 386

Price: US\$ 4,950.00 (Single User License)

ID: QBCD9296B913EN

Abstracts

The global quantum cryptography (QC) market size is estimated to grow from USD 1.15 billion in 2024 to USD 7.59 billion by 2030 at a Compound Annual Growth Rate (CAGR) of 36.8% during the forecast period. The drivers for the quantum cryptography market are the rising levels of cybersecurity attacks and threats, improved approaches related to the progression of quantum computing, investments from government and military setups, the need for regulatory compliance, and integration with emerging technologies like IoT and AI. Main challenges-from both high deployment costs, largely QKD systems as well as technical complexity associated with the technology (requiring 'specialized knowledge' for deployment and possibly becoming complex to integrate into already existing IT infrastructures) -are said to be the biggest barriers to entry for the market, more so among SMEs. Low awareness of the benefits of quantum cryptography is another reason for which many organizations depend on conventional measures of security. Indefinite clarity about the maturity of the market and the intense competition by established solutions with encryption also prevents its widespread adoption. Overcoming these challenges is crucial to the quantum cryptography's extensive usage.

By Solution Segment, Quantum Key Distribution (QKD) solutions account for a larger market share during the forecast period

Quantum Key Distribution is an essential product in the quantum cryptography market,

as it offers security that can never be faked with any other technology. It detects attempts at interception using principles of quantum mechanics. With the ability to survive against the rising threats from quantum computers, encryption is secured in the long term; hence, there is an increasing need to adopt QKD as new cybersecurity threats are on the rise. QKD can easily be applied to the existing infrastructures.

Progress toward security improvement, scalability, and cost-effectiveness are ongoing developments in quantum cryptography. CV-QKD uses the light waves inherent in quantum states for scalable, secure key distribution, making it more deployable and compatible with existing telecom infrastructures. The measurement device-independent QKD further increases security by removing the two-state detection vulnerabilities; this enhances protection from all sidechannel attacks. Chip-based QKD systems based on integrated photonic circuits present compact and cost-effective solutions that really improve the scalability. The emergence of QKD as a Service (QKDaaS) brings quantum-safe communications to even more citizens. National initiatives like the National Quantum-Safe Network Plus of Singapore aim to integrate QKD in national infrastructure, foster industry collaborations between government agencies and private sector players, and position QKD as a fast-growing cybersecurity solutions.

By region, North America accounts for the highest market size during the forecast period.

The quantum cryptography market, being the fastest growing in North America, is driven primarily by the surge in cyber-attacks and the added focus on improving data security. Growth drivers of this market include a mature technological infrastructure, intensified government investment in cybersecurity, and landmark data protection regulations like HIPAA and GDPR, compelling organizations to promote advanced encryption solutions. Early adoption of digital transformation across the region increases demand for quantum-safe encryption as technologies such as cloud computing and IoT only expand the attack surface. A strong presence of market giants that deal in leading quantum cryptography companies and government initiatives such as the National Quantum Initiative Act also helps develop market growth. Gradually, quantum cryptography has emerged as necessary in the sectors involved in finance, healthcare, and cloud services to protect sensitive data, thus emphasizing the importance of countering evolving cyber threats.

Breakdown of primaries

The study contains insights from various industry experts, from component suppliers to

Tier 1 companies and OEMs. The break-up of the primaries is as follows:

By Company Type: Tier 1 – 40%, Tier 2 – 35%, and Tier 3 – 25%

By Designation: C-level Executives – 45%, Directors – 35%, and Managers– 20%

By Region: North America – 35%, Asia Pacific – 30%, Europe – 25%, Middle East & Africa– 5%, and Latin America – 5%

Major vendors in the PQC market include Toshiba (Japan), NXP Semiconductor (Netherlands), Thales (France), IDEMIA (France), Palo Alto Networks (US), DigiCert (US), Quintessence Labs (Australia), QuantumCtek (China), ISARA (Canada), IBM (US), ID Quantique (Switzerland), MagiQ Technologies (US), Crypto Labs (South Korea), Qasky (China), Qubitekk (US), Nucrypt (US), Quantum Xchange (US).

The study includes an in-depth competitive analysis of the key players in the PQC market, their company profiles, recent developments, and key market strategies.

Research Coverage

The report segments the QC market by solution, service, security type, transmission medium, deployment mode, organization size, vertical, and region. It forecasts its size by Solution (Quantum Key Distribution, Quantum Random Number Generator, Quantum-Safe Cryptography, Quantum Key Management), By Service (Professional Services, Managed Services), By Security Type (Network Security, Application Security, Cloud Security), By Transmission Medium (Fibre-Optic Cable Transmission, Satellite-Based Transmission), By Deployment (On-Premises, Cloud) By Organization Size (SME's and Large Enterprises), By Vertical (BFSI, government and Defense, Healthcare, IT & ITeS, Automotive, Energy and Utilities and Other Verticals), By Region (North America, Europe, Asia Pacific, Rest of the World).

The study also includes an in-depth competitive analysis of the market's key players, their company profiles, key observations related to product and business offerings, recent developments, and key market strategies.

Key Benefits of Buying the Report

The report will help the market leaders/new entrants with information on the closest approximations of the revenue numbers for the overall quantum cryptography market and the subsegments. This report will help stakeholders understand the competitive landscape and gain more insights to position their businesses better and plan suitable go-to-market strategies. The report also helps stakeholders understand the market pulse and provides information on key market drivers, restraints, challenges, and opportunities.

The report provides insights on the following pointers:

Analysis of key drivers such as (Rising cyberattacks in the digitalization era, Rising investments in Research and Development (R&D), Rising demand for next-generation security solutions for cloud and IoT technologies, Growing demand for advanced encryption techniques in real-world applications, Growing advancements in Quantum Computing); Restraints (High Implementation Costs, Rising technical complexities, Lack of expertise); Opportunities (Spur in demand for security solutions across industry verticals, Increasing need for integrated solutions, Strategic Collaborations Accelerating Innovation in Quantum Cryptography) and Challenges (Commercialization of quantum cryptography, Technological implementation challenges, Integration of Quantum Cryptography with existing system, scalability issues to meet high volume data transmission).

Product Development/Innovation: Detailed insights on upcoming technologies, research development activities, new products, and service launches in the QC market.

Market Development: Comprehensive information about lucrative markets – the report analyses the QC market across varied regions.

Market Diversification: Exhaustive information about new products and services, untapped geographies, recent developments, and investments in the QC market.

Competitive Assessment: In-depth assessment of market shares, growth strategies, and service offerings of leading players Toshiba (Japan), NXP Semiconductor (Netherlands), Thales (France), IDEMIA (France), Palo Alto Networks (US), DigiCert (US), Quintessence Labs (Australia), QuantumCtek (China), ISARA (Canada), IBM (US), ID Quantique (Switzerland), MagiQ Technologies (US), Crypta Labs (UK), Qasky (China), Qubitekk (US), Nucrypt

(US), Quantum Xchange (US) among others, in the QC market strategies.

Contents

1 INTRODUCTION

- 1.1 STUDY OBJECTIVES
- 1.2 MARKET DEFINITION
 - 1.2.1 INCLUSIONS AND EXCLUSIONS
- 1.3 STUDY SCOPE
 - 1.3.1 MARKETS COVERED
 - 1.3.2 YEARS CONSIDERED
- 1.4 CURRENCY CONSIDERED
- 1.5 STAKEHOLDERS
- 1.6 SUMMARY OF CHANGES

2 RESEARCH METHODOLOGY

- 2.1 RESEARCH DATA
 - 2.1.1 SECONDARY DATA
 - 2.1.2 PRIMARY DATA
 - 2.1.2.1 Breakup of primaries
 - 2.1.2.2 Key industry insights
- 2.2 MARKET BREAKUP AND DATA TRIANGULATION
- 2.3 MARKET SIZE ESTIMATION
 - 2.3.1 TOP-DOWN APPROACH
 - 2.3.2 BOTTOM-UP APPROACH
- 2.4 MARKET FORECAST
- 2.5 RESEARCH ASSUMPTIONS
- 2.6 RESEARCH LIMITATIONS

3 EXECUTIVE SUMMARY

4 PREMIUM INSIGHTS

- 4.1 ATTRACTIVE OPPORTUNITIES FOR KEY MARKET PLAYERS
- 4.2 QUANTUM CRYPTOGRAPHY MARKET, BY SOLUTION
- 4.3 QUANTUM CRYPTOGRAPHY MARKET FOR QUANTUM KEY DISTRIBUTION (QKD)
- 4.4 QUANTUM CRYPTOGRAPHY MARKET FOR QUANTUM RANDOM NUMBER GENERATORS (QRNG)

- 4.5 QUANTUM CRYPTOGRAPHY MARKET, BY SERVICE
- 4.6 QUANTUM CRYPTOGRAPHY MARKET, BY PROFESSIONAL SERVICE
- 4.7 QUANTUM CRYPTOGRAPHY MARKET, BY TRANSMISSION MEDIUM
- 4.8 QUANTUM CRYPTOGRAPHY MARKET, BY SECURITY TYPE
- 4.9 QUANTUM CRYPTOGRAPHY MARKET, BY ORGANIZATION SIZE
- 4.10 QUANTUM CRYPTOGRAPHY MARKET, BY VERTICAL
- 4.11 MARKET INVESTMENT SCENARIO

5 MARKET OVERVIEW AND INDUSTRY TRENDS

5.1 INTRODUCTION

5.2 MARKET DYNAMICS

5.2.1 DRIVERS

5.2.1.1 Rising number of cyberattacks

5.2.1.2 Increasing investments in research and development

5.2.1.3 Growing demand for next-generation security solutions for cloud and IoT technologies

5.2.1.4 Rising need for advanced encryption techniques in real world applications

5.2.1.5 Advancements in quantum computing

5.2.2 RESTRAINTS

5.2.2.1 High implementation costs

5.2.2.2 Rising technical complexities

5.2.2.3 Lack of expertise among users

5.2.3 OPPORTUNITIES

5.2.3.1 Growing requirement for sophisticated security solutions across sectors

5.2.3.2 Increasing need for integrated solutions

5.2.3.3 Strategic collaborations for technological innovation

5.2.4 CHALLENGES

5.2.4.1 Slow commercialization of quantum cryptography

5.2.4.2 Integration with existing systems

5.2.4.3 Scalability issues related to high-volume data transmission

5.3 EVOLUTION OF QUANTUM CRYPTOGRAPHY MARKET

5.4 IMPACT OF GENERATIVE AI/AI ON QUANTUM CRYPTOGRAPHY MARKET

5.4.1 TOP USE CASES & MARKET POTENTIAL

5.4.1.1 Key use cases

5.4.2 IMPACT OF GEN AI ON INTERCONNECTED AND ADJACENT ECOSYSTEMS

5.4.2.1 Quantum computing

5.4.2.2 Quantum key distribution (QKD)

5.4.2.3 Blockchain technology

5.4.2.4 Cloud security

5.4.2.5 Post-quantum cryptography

5.4.2.6 Artificial intelligence (AI) & machine learning (ML)

5.5 CASE STUDY ANALYSIS

5.5.1 CASE STUDY 1: HITACHI ENERGY AND ID QUANTIQUE DELIVER HIGHLY SECURE END-TO-END ENCRYPTION FOR CRITICAL INFRASTRUCTURE NETWORKS

5.5.2 CASE STUDY 2: QUINTESSENCELABS' CRYPTO GATEWAY SOLUTION ENABLES HIGH SECURITY AND LOW-COST CLOUD STORAGE FOR FINANCIAL INSTITUTION

5.5.3 CASE STUDY 3: SK BROADBAND AND IDQ IMPLEMENT END-TO-END QUANTUM CRYPTOGRAPHY SOLUTION FOR SOUTH KOREAN GOVERNMENT

5.5.4 CASE STUDY 4: QUANTUM SECURE SYSTEMS ENHANCES SECURITY OF FINANCIAL TRANSACTIONS WITH QKD SOLUTION

5.5.5 CASE STUDY 5: PQSHIELD'S PQPLATFORM-COPRO TECHNOLOGY INTEGRATES WITH SIFIVE'S ESSENTIAL RISC-V FOR IMPROVED QUANTUM SAFETY

5.6 VALUE CHAIN ANALYSIS

5.6.1 TECHNOLOGY INFRASTRUCTURE PROVIDERS

5.6.2 QUANTUM CRYPTOGRAPHY PROVIDERS

5.6.3 APPLICATION DEVELOPERS

5.6.4 SYSTEM INTEGRATORS

5.6.5 END USERS

5.7 ECOSYSTEM ANALYSIS

5.8 PORTER'S FIVE FORCES MODEL ANALYSIS

5.8.1 THREAT OF NEW ENTRANTS

5.8.2 THREAT OF SUBSTITUTES

5.8.3 BARGAINING POWER OF SUPPLIERS

5.8.4 BARGAINING POWER OF BUYERS

5.8.5 INTENSITY OF COMPETITIVE RIVALRY

5.9 PRICING ANALYSIS

5.9.1 PRICING ANALYSIS OF SOLUTION BY KEY PLAYERS

5.10 TECHNOLOGY ANALYSIS

5.10.1 KEY TECHNOLOGIES

5.10.1.1 Quantum key distribution (QKD)

5.10.1.2 Quantum random number generators (QRNG)

5.10.1.3 Quantum entanglement

5.10.1.4 Quantum digital signatures (QDS)

5.10.2 COMPLEMENTARY TECHNOLOGIES

- 5.10.2.1 Blockchain technology
- 5.10.2.2 Public key infrastructure (PKI)
- 5.10.2.3 Transport layer security (TLS)
- 5.10.3 ADJACENT TECHNOLOGIES
 - 5.10.3.1 Quantum computing
 - 5.10.3.2 Quantum communication
 - 5.10.3.3 AI/ML
 - 5.10.3.4 Cloud computing
- 5.11 PATENT ANALYSIS
 - 5.11.1 METHODOLOGY
- 5.12 TRADE ANALYSIS
 - 5.12.1 IMPORT DATA
 - 5.12.2 EXPORT DATA
- 5.13 TARIFF & REGULATORY LANDSCAPE
 - 5.13.1 TARIFFS RELATED TO QUANTUM CRYPTOGRAPHY PRODUCTS
 - 5.13.2 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)
 - 5.13.3 EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI)
 - 5.13.4 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)
 - 5.13.5 INTERNATIONAL TELECOMMUNICATION UNION (ITU)
 - 5.13.6 INTERNET ENGINEERING TASK FORCE (IETF)
 - 5.13.7 CLOUD SECURITY ALLIANCE (CSA)
 - 5.13.8 GLOBAL FORUM ON CYBER EXPERTISE (GFCE)
 - 5.13.9 WORLD ECONOMIC FORUM (WEF)
 - 5.13.10 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)
 - 5.13.11 INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH (IACR)
 - 5.13.12 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS
- 5.14 KEY STAKEHOLDERS AND BUYING CRITERIA
 - 5.14.1 KEY STAKEHOLDERS IN BUYING PROCESS
 - 5.14.2 BUYING CRITERIA
- 5.15 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS
- 5.16 KEY CONFERENCES & EVENTS, 2024–2025
- 5.17 BUSINESS MODEL ANALYSIS
 - 5.17.1 QUANTUM KEY DISTRIBUTION AS A SERVICE (QKDAAS)
 - 5.17.2 LICENSING OF QUANTUM CRYPTOGRAPHIC TECHNOLOGY
 - 5.17.3 HARDWARE AND SOFTWARE SALES
 - 5.17.4 QUANTUM CRYPTOGRAPHY AS A SERVICE (QCAAS)
 - 5.17.5 INTEGRATED SECURITY SOLUTIONS

- 5.17.6 CONSULTING AND ADVISORY SERVICES
- 5.17.7 CLOUD-BASED QUANTUM CRYPTOGRAPHY SOLUTIONS
- 5.17.8 RESEARCH AND DEVELOPMENT PARTNERSHIPS
- 5.17.9 GOVERNMENT CONTRACTS
- 5.18 INVESTMENT AND FUNDING SCENARIO

6 QUANTUM CRYPTOGRAPHY MARKET, BY SOLUTION

6.1 INTRODUCTION

- 6.1.1 SOLUTIONS: QUANTUM CRYPTOGRAPHY MARKET DRIVERS

6.2 QUANTUM KEY DISTRIBUTION (QKD)

- 6.2.1 ABILITY TO PROVIDE UNCONDITIONAL SECURITY TO DRIVE MARKET
- 6.2.2 DISCRETE VARIABLE QKD (DV-QKD)
- 6.2.3 CONTINUOUS VARIABLE QKD (CV-QKD)

6.3 QUANTUM-RANDOM NUMBER GENERATORS (QRNG)

- 6.3.1 PROVISION OF HIGH LEVELS OF RANDOMNESS TO DRIVE DEMAND
- 6.3.2 QRNG CHIPS
- 6.3.3 QRNG USB DEVICES
- 6.3.4 PCIE CARDS
- 6.3.5 HARDWARE SECURITY MODULES (HSM)

6.4 QUANTUM-SAFE CRYPTOGRAPHY

- 6.4.1 ABILITY TO RESIST CLASSICAL AND QUANTUM ATTACKS TO BOOST MARKET

6.5 QUANTUM KEY MANAGEMENT

- 6.5.1 GROWING DEMAND TO PROTECT SENSITIVE CLIENT DATA TO FUEL MARKET

7 QUANTUM CRYPTOGRAPHY MARKET, BY SERVICE

7.1 INTRODUCTION

- 7.1.1 SERVICES: QUANTUM CRYPTOGRAPHY MARKET DRIVERS

7.2 PROFESSIONAL SERVICES

- 7.2.1 DEMAND FROM COMPANIES TRANSITIONING TO QUANTUM-SAFE TECHNOLOGIES TO DRIVE MARKET
- 7.2.2 CONSULTING
- 7.2.3 DEPLOYMENT & INTEGRATION
- 7.2.4 SUPPORT & MAINTENANCE

7.3 MANAGED SERVICES

- 7.3.1 RISING DEMAND DUE TO INCREASING RISK OF CYBERATTACKS TO

BOOST MARKET

8 QUANTUM CRYPTOGRAPHY MARKET, BY SECURITY TYPE

8.1 INTRODUCTION

8.2 NETWORK SECURITY

8.2.1 RISING VIRTUALIZATION OF SERVERS AND USE OF CLOUD SERVICES TO DRIVE DEMAND

8.3 APPLICATION SECURITY

8.3.1 INCREASING NEED FOR PROTECTION AGAINST HIGH-RISK ATTACKS TO BOOST MARKET

8.4 CLOUD SECURITY

8.4.1 URGENT NEED TO FUTURE-PROOF CLOUD ENVIRONMENTS TO FUEL MARKET

9 QUANTUM CRYPTOGRAPHY MARKET, BY TRANSMISSION MEDIUM

9.1 INTRODUCTION

9.1.1 TRANSMISSION MEDIUMS: QUANTUM KEY DISTRIBUTION MARKET DRIVERS

9.2 FIBER-OPTIC CABLE TRANSMISSION

9.2.1 HIGH SECURITY LEVELS AND SCALABILITY TO DRIVE DEMAND

9.3 SATELLITE-BASED TRANSMISSION

9.3.1 SUITABILITY TO GLOBAL-SCALE APPLICATIONS TO FUEL MARKET

10 QUANTUM CRYPTOGRAPHY MARKET, BY DEPLOYMENT MODE

10.1 INTRODUCTION

10.1.1 DEPLOYMENT MODES: QUANTUM CRYPTOGRAPHY MARKET DRIVERS
10.2 ON-PREMISES

10.2.1 NEED FOR COMPLETE OVERSIGHT OF ENCRYPTION PROCESSES TO DRIVE DEMAND

10.3 CLOUD

10.3.1 COST-EFFECTIVENESS AND SCALABILITY TO BOOST MARKET

11 QUANTUM CRYPTOGRAPHY MARKET, BY ORGANIZATION SIZE

11.1 INTRODUCTION

11.1.1 ORGANIZATION SIZES: QUANTUM CRYPTOGRAPHY MARKET DRIVERS

11.2 SMES

11.2.1 INCREASING ADOPTION OF CUSTOMIZED CLOUD-BASED SOLUTIONS TO DRIVE MARKET

11.3 LARGE ENTERPRISES

11.3.1 RISING NEED TO SAFEGUARD SENSITIVE DATA TO FUEL DEMAND

12 QUANTUM CRYPTOGRAPHY MARKET, BY VERTICAL

12.1 INTRODUCTION

12.1.1 VERTICALS: QUANTUM CRYPTOGRAPHY MARKET DRIVERS

12.2 BANKING, FINANCIAL SERVICES, AND INSURANCE (BFSI)

12.2.1 NEED TO PROTECT SENSITIVE AND PROPRIETARY INFORMATION TO DRIVE DEMAND

12.3 GOVERNMENT & DEFENSE

12.3.1 RISING REQUIREMENT TO SAFEGUARD CRITICAL INFORMATION TO FUEL MARKET

12.4 HEALTHCARE

12.4.1 GROWING DEMAND TO SECURE PATIENT INFORMATION TO BOOST MARKET

12.5 IT & ITES

12.5.1 INCREASING USE OF CLOUD SERVICES TO PROPEL MARKET

12.6 ENERGY & UTILITIES

12.6.1 GROWING ADOPTION OF IOT IN ENERGY SYSTEMS TO FUEL DEMAND

12.7 OTHER VERTICALS

13 QUANTUM CRYPTOGRAPHY MARKET, BY REGION

13.1 INTRODUCTION

13.2 NORTH AMERICA

13.2.1 NORTH AMERICA: QUANTUM CRYPTOGRAPHY MARKET DRIVERS

13.2.2 NORTH AMERICA: MACROECONOMIC OUTLOOK

13.2.3 US

13.2.3.1 Rising research and development initiatives to drive market

13.2.4 CANADA

13.2.4.1 Government and private sector investments to boost market

13.3 EUROPE

13.3.1 EUROPE: QUANTUM CRYPTOGRAPHY MARKET DRIVERS

13.3.2 EUROPE: MACROECONOMIC OUTLOOK

13.3.3 UK

- 13.3.3.1 Increasing research in quantum technology to boost market
- 13.3.4 GERMANY
 - 13.3.4.1 Increased government investments to fuel market
- 13.3.5 FRANCE
 - 13.3.5.1 Rising investments and innovation to bolster market
- 13.3.6 ITALY
 - 13.3.6.1 Strong technological base to drive innovation in market
- 13.3.7 REST OF EUROPE
- 13.4 ASIA PACIFIC
 - 13.4.1 ASIA PACIFIC: QUANTUM CRYPTOGRAPHY MARKET DRIVERS
 - 13.4.2 ASIA PACIFIC: MACROECONOMIC OUTLOOK
 - 13.4.3 CHINA
 - 13.4.3.1 Extensive research activities to strengthen market
 - 13.4.4 JAPAN
 - 13.4.4.1 Strategic collaborations to propel market
 - 13.4.5 INDIA
 - 13.4.5.1 Significant government investments to bolster market
 - 13.4.6 REST OF ASIA PACIFIC
- 13.5 MIDDLE EAST & AFRICA
 - 13.5.1 MIDDLE EAST & AFRICA: QUANTUM CRYPTOGRAPHY MARKET DRIVERS
 - 13.5.2 MIDDLE EAST & AFRICA: MACROECONOMIC OUTLOOK
 - 13.5.3 GCC COUNTRIES
 - 13.5.3.1 Government initiatives and advancements in technologies to drive market
 - 13.5.3.2 KSA
 - 13.5.3.2.1 Collaborative efforts and investments to fuel market
 - 13.5.3.3 UAE
 - 13.5.3.3.1 Rising cybersecurity concerns to drive demand
 - 13.5.3.4 Rest of GCC Countries
 - 13.5.4 SOUTH AFRICA
 - 13.5.4.1 Growing government initiatives and research activities to bolster market
 - 13.5.5 REST OF MIDDLE EAST & AFRICA
- 13.6 LATIN AMERICA
 - 13.6.1 LATIN AMERICA: QUANTUM CRYPTOGRAPHY MARKET DRIVERS
 - 13.6.2 LATIN AMERICA: MACROECONOMIC OUTLOOK
 - 13.6.3 BRAZIL
 - 13.6.3.1 Increasing need to safeguard sensitive data to drive demand
 - 13.6.4 MEXICO
 - 13.6.4.1 Digital transformation in industries to fuel market
 - 13.6.5 REST OF LATIN AMERICA

14 COMPETITIVE LANDSCAPE

- 14.1 KEY PLAYER STRATEGIES/RIGHT TO WIN
- 14.2 REVENUE ANALYSIS
- 14.3 MARKET SHARE ANALYSIS
- 14.4 BRAND COMPARISON
- 14.5 COMPANY VALUATION AND FINANCIAL METRICS
 - 14.5.1 COMPANY VALUATION
 - 14.5.2 FINANCIAL METRICS
- 14.6 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2023
 - 14.6.1 STARS
 - 14.6.2 EMERGING LEADERS
 - 14.6.3 PERVASIVE PLAYERS
 - 14.6.4 PARTICIPANTS
 - 14.6.5 COMPANY FOOTPRINT: KEY PLAYERS, 2023
 - 14.6.5.1 Company footprint
 - 14.6.5.2 Solution footprint
 - 14.6.5.3 Service footprint
 - 14.6.5.4 Vertical footprint
 - 14.6.5.5 Region footprint
- 14.7 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2023
 - 14.7.1 PROGRESSIVE COMPANIES
 - 14.7.2 RESPONSIVE COMPANIES
 - 14.7.3 DYNAMIC COMPANIES
 - 14.7.4 STARTING BLOCKS
 - 14.7.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2023
 - 14.7.5.1 Detailed list of key startups/SMEs
 - 14.7.5.2 Competitive benchmarking of key startups/SMEs
- 14.8 COMPETITIVE SCENARIO
 - 14.8.1 PRODUCT LAUNCHES
 - 14.8.2 DEALS

15 COMPANY PROFILES

- 15.1 KEY PLAYERS
 - 15.1.1 TOSHIBA
 - 15.1.1.1 Business overview
 - 15.1.1.2 Products/Solutions/Services offered

- 15.1.1.3 Recent developments
- 15.1.1.4 MnM view
 - 15.1.1.4.1 Key strengths
 - 15.1.1.4.2 Strategic choices
 - 15.1.1.4.3 Weaknesses and competitive threats
- 15.1.2 NXP SEMICONDUCTORS
 - 15.1.2.1 Business overview
 - 15.1.2.2 Products/Solutions/Services offered
 - 15.1.2.3 Recent developments
 - 15.1.2.4 MnM view
 - 15.1.2.4.1 Key strengths
 - 15.1.2.4.2 Strategic choices
 - 15.1.2.4.3 Weaknesses and competitive threats
- 15.1.3 THALES
 - 15.1.3.1 Business overview
 - 15.1.3.2 Products/Solutions/Services offered
 - 15.1.3.3 Recent developments
 - 15.1.3.4 MnM view
 - 15.1.3.4.1 Key strengths
 - 15.1.3.4.2 Strategic choices
 - 15.1.3.4.3 Weaknesses and competitive threats
- 15.1.4 IDEMIA
 - 15.1.4.1 Business overview
 - 15.1.4.2 Products/Solutions/Services offered
 - 15.1.4.3 Recent developments
 - 15.1.4.4 MnM view
 - 15.1.4.4.1 Key strengths
 - 15.1.4.4.2 Strategic choices
 - 15.1.4.4.3 Weaknesses and competitive threats
- 15.1.5 PALO ALTO NETWORKS
 - 15.1.5.1 Business overview
 - 15.1.5.2 Products/Solutions/Services offered
 - 15.1.5.3 Recent developments
 - 15.1.5.4 MnM view
 - 15.1.5.4.1 Key strengths
 - 15.1.5.4.2 Strategic choices
 - 15.1.5.4.3 Weaknesses and competitive threats
- 15.1.6 DIGICERT
 - 15.1.6.1 Business overview

- 15.1.6.2 Products/Solutions/Services offered
- 15.1.6.3 Recent developments
- 15.1.7 QUINTESSENCELABS
 - 15.1.7.1 Business overview
 - 15.1.7.2 Products/Solutions/Services offered
 - 15.1.7.3 Recent developments
- 15.1.8 QUANTUMCTEK
 - 15.1.8.1 Business overview
 - 15.1.8.2 Products/Solutions/Services offered
- 15.1.9 ISARA
 - 15.1.9.1 Business overview
 - 15.1.9.2 Products/Solutions/Services offered
 - 15.1.9.3 Recent developments
- 15.1.10 IBM
 - 15.1.10.1 Business overview
 - 15.1.10.2 Products/Solutions/Services offered
 - 15.1.10.3 Recent developments
- 15.1.11 ID QUANTIQUE
 - 15.1.11.1 Business overview
 - 15.1.11.2 Products/Solutions/Services offered
 - 15.1.11.3 Recent developments
- 15.1.12 MAGIQ TECHNOLOGIES
 - 15.1.12.1 Business overview
 - 15.1.12.2 Products/Solutions/Services offered
- 15.1.13 CRYPTA LABS
 - 15.1.13.1 Business overview
 - 15.1.13.2 Products/Solutions/Services offered
- 15.1.14 QASKY
 - 15.1.14.1 Business overview
 - 15.1.14.2 Products/Solutions/Services offered
 - 15.1.14.3 Recent developments
- 15.1.15 QUBITEKK
 - 15.1.15.1 Business overview
 - 15.1.15.2 Products/Solutions/Services offered
 - 15.1.15.3 Recent developments
- 15.1.16 NUCRYPT
 - 15.1.16.1 Business overview
 - 15.1.16.2 Products/Solutions/Services offered
- 15.1.17 QUANTUM XCHANGE

- 15.1.17.1 Business overview
- 15.1.17.2 Products/Solutions/Services offered
- 15.1.17.3 Recent developments

15.2 OTHER PLAYERS

- 15.2.1 QUTOOLS
- 15.2.2 QNU LABS
- 15.2.3 POST QUANTUM
- 15.2.4 HPE
- 15.2.5 NEC
- 15.2.6 CRYPTO QUANTIQUÉ
- 15.2.7 QRYPT
- 15.2.8 KETS QUANTUM SECURITY
- 15.2.9 PQ SHIELD
- 15.2.10 QUBALT
- 15.2.11 VERIQLOUD
- 15.2.12 SSH COMMUNICATIONS SECURITY
- 15.2.13 HEQA SECURITY (FORMERLY QUANTLR)
- 15.2.14 QUSECURE

16 ADJACENT MARKETS

- 16.1 INTRODUCTION
- 16.2 LIMITATIONS
- 16.3 POST-QUANTUM CRYPTOGRAPHY MARKET
- 16.4 QUANTUM COMPUTING MARKET
 - 16.4.1 QUANTUM COMPUTING MARKET, BY OFFERING
- 16.5 ENCRYPTION SOFTWARE MARKET
 - 16.5.1 ENCRYPTION SOFTWARE, BY DEPLOYMENT MODE

17 APPENDIX

- 17.1 DISCUSSION GUIDE
- 17.2 KNOWLEDGESTORE: MARKETSandMARKETS' SUBSCRIPTION PORTAL
- 17.3 CUSTOMIZATION OPTIONS
- 17.4 RELATED REPORTS
- 17.5 AUTHOR DETAILS

I would like to order

Product name: Quantum Cryptography (QC) Market by Solution (Quantum Key Distribution (QKD), Quantum Random Number Generators (QRNG), Quantum-safe Cryptography)), Service (Professional, Managed), Security Type (Network, Application, Cloud) - Global Forecast to 2030

Product link: <https://marketpublishers.com/r/QBCD9296B913EN.html>

Price: US\$ 4,950.00 (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/QBCD9296B913EN.html>

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:
Last name:
Email:
Company:
Address:
City:
Zip code:
Country:
Tel:
Fax:
Your message:

****All fields are required**

Customer signature _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at <https://marketpublishers.com/docs/terms.html>

To place an order via fax simply print this form, fill in the information below
and fax the completed form to +44 20 7900 3970