+44 20 8123 2220
info@marketpublishers.com

Post-Quantum Cryptography Market - A Global and Regional Analysis: Focus on Application, Product, and Regional and Country-Level Analysis - Analysis and Forecast, 2024-2034

https://marketpublishers.com/r/PD708E4CA75FEN.html
Date: November 2024
Pages: 0
Price: US$ 4,850.00 (Single User License)
ID: PD708E4CA75FEN

Abstracts

Hard copy option is available on any of the options above at an additional charge of $500. Please email us at order@marketpublishers.com with your request.

This report will be delivered in 7-10 working days.Post-Quantum Cryptography Market Overview

The post-quantum cryptography market was valued at $356.4 million in 2023 and is expected to grow at a CAGR of 41.47%, reaching $17,696.4 million by 2034. The market is driven by the rising need to secure digital infrastructure against quantum computing threats, leading to advancements in cryptographic algorithms. Enhanced R&D efforts, government funding, and collaborations have shaped this evolving post-quantum cryptography market, enabling the development of robust, quantum-resistant encryption protocols. Strategic alliances and a proactive regulatory landscape have been further propelling the market, emphasizing the importance of safeguarding sensitive data in critical industries. As cyber threats increase, the market focuses on innovation and security resilience to meet future cybersecurity demands.

Introduction of Post-Quantum Cryptography

The study conducted by BIS Research defines post-quantum cryptography as the development of encryption techniques designed to resist threats posed by quantum computing. Post-quantum cryptography focuses on creating algorithms capable of securing digital data even against quantum attacks, which have the potential to break traditional cryptographic systems. This field is critical for protecting sensitive information

+44 20 8123 2220
info@marketpublishers.com

in areas such as finance, healthcare, and national security. By leveraging new cryptographic algorithms, advanced mathematical theories, and continuous R&D efforts, post-quantum cryptography offers enhanced resilience for digital infrastructure, enabling organizations to safeguard their data and communications against the future risks of quantum-powered decryption.

Market Introduction

The post-quantum cryptography market has rapidly gained prominence due to the rising need to secure digital assets against the emerging threats posed by quantum computing. Post-quantum cryptography involves the development of advanced encryption algorithms that can withstand quantum-powered attacks, protecting critical sectors such as finance, healthcare, and government from potential data breaches. As organizations become increasingly aware of the future risks quantum computing poses to traditional encryption, governments and industries have been prioritizing investment in quantum-resistant solutions. The market encompasses a variety of approaches, including lattice-based, hash-based, and multivariate cryptography, all essential for ensuring data security and privacy in a quantum future. With the progression of quantum technology and a growing focus on robust cybersecurity, the post-quantum cryptography market is positioned for substantial growth, driven by ongoing innovation and the demand for secure, quantum-resistant systems.

Industrial Impact

The post-quantum cryptography market's industrial impact spans cybersecurity, data protection, and technological resilience. Advancements in quantum-resistant algorithms, such as lattice-based and hash-based cryptography, enhance the robustness of data security systems, safeguarding digital infrastructure against future quantum threats. This progress fosters collaborations among technology firms, governmental bodies, and cybersecurity agencies, elevating security standards and paving the way for resilient encryption methods. Additionally, the focus on quantum-resistant cryptographic solutions aligns with global priorities in privacy protection, digital trust, and secure communications, influencing practices across sectors that rely on encrypted data. As a result, the post-quantum cryptography market plays a critical role in strengthening cybersecurity frameworks, driving cryptographic innovation, and supporting a secure, quantum-ready digital future worldwide.

Market Segmentation:

+44 20 8123 2220
info@marketpublishers.com

Segmentation 1: by Security Application

Network Security

Application Security

Network Security Segment to Dominate the Post-Quantum Cryptography Market (by Security Application)

In the post-quantum cryptography market, network security remains the leading application, driven by the urgent need to protect critical infrastructure from evolving cyber threats, including those posed by quantum computing. Post-quantum cryptography is essential for securing network communications, as quantum-resistant encryption can safeguard sensitive data across sectors. As organizations recognize the limitations of traditional cryptographic methods against future quantum capabilities, they have been increasingly adopting advanced quantum-safe solutions for network protection. Government mandates on cybersecurity resilience and rising concerns over data privacy further drive the demand for network security solutions. With the escalation of cyber risks and advancements in post-quantum encryption, the demand for network security is expected to grow significantly, ensuring it remains a vital element in protecting data integrity and digital trust in the quantum era.

Segmentation 2: by End-Use Industry

BFSI

Government and Defense

IT and Telecommunications

Healthcare

Others

Government and Defense to Dominate the Post-Quantum Cryptography Market (by End-Use Industry)

+44 20 8123 2220
info@marketpublishers.com

In the post-quantum cryptography market, the government and defense sector has been leading the market due to its critical need for secure communications and data protection against quantum threats. This advanced encryption technology is essential for safeguarding national security, protecting sensitive information, and ensuring resilience in the face of emerging quantum risks. The growing recognition of potential vulnerabilities in traditional cryptographic methods has boosted the demand for post-quantum solutions within this sector. Additionally, heightened awareness of cybersecurity threats and the importance of robust encryption standards have been driving adoption. As the need for future-proof security measures intensifies, the use of post-quantum cryptography in government and defense is expected to grow significantly, solidifying its role as a crucial solution for national security and data integrity.

Segmentation 3: by Solution

- Lattice-Based Cryptography
- Code-Based Cryptography
- Multivariate Cryptography
- Hash-Based Cryptography
- Isogency-Based Cryptography
- Symmetric Key Quantum Resistance

Segmentation 4: by Product

- Hardware
- PQC Chips
- Quantum-Resistant Processors
- Cryptographic Accelerator
- Quantum-Resistant HSMs

+44 20 8123 2220
info@marketpublishers.com

Embedded Systems with PQC

Software

PQC Encryption Libraries

PQC Key Management Systems

Quantum Resistant VPNs

PQC-Integrated Security Software

PQC for Cloud Security

Segmentation 5: by Region

North America: U.S., Canada, and Mexico

Europe: Germany, France, Spain, Italy, U.K., and Rest-of-Europe

Asia-Pacific: China, Japan, India, Taiwan, South Korea and Rest-of-Asia-Pacific

Rest-of-the-World: Middle East and Africa and South America

The North America region is set to dominate the post-quantum cryptography market, driven by significant investments in cybersecurity, rapid advancements in quantum technology, and strong government initiatives to protect critical digital infrastructure. Countries such as the U.S. and Canada have been experiencing a notable rise in demand for quantum-resistant encryption solutions due to growing concerns over data privacy and national security. The region's advanced technology infrastructure and proactive policies addressing quantum-related cybersecurity threats have been accelerating the adoption of post-quantum cryptographic solutions. Government agencies and private enterprises have invested in R&D to strengthen encryption standards, boosting the demand for quantum-safe technologies. Additionally, North America's focus on pioneering innovations has been fostering the development of resilient encryption protocols to secure sensitive data and communications. As North

+44 20 8123 2220
info@marketpublishers.com

America continues to lead in cybersecurity advancements, it is expected to maintain its leadership position in the post-quantum cryptography market, significantly enhancing data protection and digital resilience against future quantum threats.

Recent Developments in the Post-Quantum Cryptography Market

In August 2024, the U.S. National Institute of Standards and Technology (NIST) officially published its first three post-quantum cryptography standards. Among these, two algorithms, i.e., ML-KEM (originally CRYSTALS-Kyber) and ML-DSA (originally CRYSTALS-Dilithium), were developed by IBM researchers in collaboration with industry and academic partners. Furthermore, a third algorithm, SLH-DSA (formerly SPHINCS+), was co-developed by a researcher who later joined IBM. In August 2024, the National Institute of Standards and Technology (NIST) published its first standardized post-quantum cryptographic (PQC) algorithms designed to secure data against both classical and quantum computer attacks. This milestone is part of NIST's ongoing efforts to develop quantum-resistant cryptographic standards, with final standards expected by 2024.

In February 2024, ETAS introduced ESCRYPT CycurHSM 3.x, the latest version of its cybersecurity firmware designed to protect modern E/E architectures in vehicles against cyberattacks and unauthorized access. This software stack for hardware security modules (HSMs) on automotive microcontrollers supports hardware acceleration and virtualization via hypervisor, addressing the growing cybersecurity requirements of future software-defined vehicles. ESCRYPT CycurHSM 3.x is compatible with AUTOSAR and non-AUTOSAR stacks and complies with ISO 26262 ASIL-D, Automotive SPICE, and ISO/SAE 21434 standards. It supports key security use cases, including secure lifecycle management, runtime tamper detection, secure data and key storage, and secure software updates, allowing OEMs to customize these features as needed.

Demand - Drivers, Limitations, and Opportunities

Market Demand Drivers: Rising Threat from Quantum Computing to Current Cryptographic Systems

The rise of quantum computing presents a significant challenge to the integrity of

+44 20 8123 2220
info@marketpublishers.com

current cryptographic systems, acting as a key driver for the post-quantum cryptography (PQC) market. As quantum computing technology advances, the ability of traditional encryption methods, such as RSA and elliptic curve cryptography (ECC), to protect sensitive data is increasingly called into question. The core issue lies in quantum computers' potential to exploit algorithms such as Shor's, which can efficiently factor large prime numbers, rendering conventional cryptographic methods vulnerable to decryption in a fraction of the time it would take classical computers. This rising threat has become one of the most prominent motivators for businesses, governments, and organizations to adopt quantum-resistant cryptographic techniques. Today, most encryption systems rely on the assumption that certain mathematical problems, such as factoring large integers or solving discrete logarithms, have been computationally infeasible for classical computers. However, quantum computers are expected to solve these problems exponentially faster, potentially breaking encryption that protects financial transactions, personal data, and state secrets.

Post-Quantum Cryptography Market Challenges: High Complexity and Cost of Implementing Post-Quantum Cryptography Solutions

The high complexity and cost of implementing post-quantum cryptography (PQC) solutions present a significant challenge for organizations navigating the transition to quantum-resistant security systems. While PQC is essential for protecting data from future quantum computing threats, the process of adopting these solutions involves considerable financial and technical burdens. This complexity and cost, in turn, slow down the widespread adoption of PQC in industries that need to future-proof their cybersecurity strategies.

The primary challenge stems from the inherent complexity of integrating PQC into existing systems. Current encryption infrastructure, built on classical algorithms such as RSA and ECC, is deeply embedded in enterprise IT architectures, cloud environments, and communication protocols. Transitioning to quantum-safe algorithms requires a comprehensive overhaul of these infrastructures, demanding new hardware and software and extensive testing and validation to ensure compatibility. The process of identifying cryptographic dependencies within complex systems can be time-consuming and resource-intensive. This represents a critical hurdle for many organizations, especially in highly regulated industries such as finance and healthcare.

Post-Quantum Cryptography Market Opportunities: Expansion of Post-Quantum Cryptography in Financial and Healthcare Sectors

+44 20 8123 2220
info@marketpublishers.com

The expansion of post-quantum cryptography (PQC) in the financial and healthcare sectors represents a significant growth opportunity for the post-quantum cryptography market. As quantum computing progresses, traditional encryption systems used by financial institutions and healthcare providers have been increasingly vulnerable to being compromised. The financial and healthcare sectors, which handle vast amounts of sensitive data, are particularly exposed to the security risks posed by future quantum technologies, making the implementation of PQC critical.

In the financial sector, the risk is particularly pronounced due to the reliance on current encryption protocols, such as RSA and ECC, which are susceptible to quantum attacks. Financial institutions manage large volumes of high-value data, including customer financial information, transaction records, and proprietary trading algorithms. The potential for quantum computers to break these encryptions in the coming years has driven the industry to explore quantum-safe alternatives proactively. By adopting PQC solutions, financial institutions can secure current data and future-proof systems against the computational power quantum technologies will bring. The demand for these solutions has been rapidly growing as the financial sector aims to ensure compliance with forthcoming regulations mandating quantum-safe encryption, such as the U.S. National Institute of Standards and Technology (NIST) standards.

How can this report add value to an organization?

This report can add value to an organization in several ways. Some of these are given here:

Product/Innovation Strategy: The product segment helps readers understand the various applications of post-quantum cryptography solutions based on use cases (such as network security, data storage, secure communications, and digital transactions). It covers different cryptographic approaches, including lattice-based, hash-based, and multivariate algorithms. With advancements in quantum-resistant encryption and increasing concerns over data security, the post-quantum cryptography market presents a high-growth, high-investment opportunity.

Growth/Marketing Strategy: The post-quantum cryptography market has been expanding rapidly, offering significant opportunities for both established and emerging players. Key strategies covered include R&D investments, partnerships, collaborations, and product development initiatives. Companies in post-quantum cryptography market have been focusing on developing robust, quantum-resistant solutions to secure a leading position and address evolving cybersecurity needs.

+44 20 8123 2220
info@marketpublishers.com

Competitive Strategy: The report profiles key players in the post-quantum cryptography market, including technology providers and cybersecurity firms. It offers a comprehensive view of the competitive landscape, covering alliances, joint ventures, and innovation strategies, enabling readers to identify new revenue opportunities and gain a competitive edge in this evolving market.

Research Methodology

Factors for Data Prediction and Modeling

The base currency considered for the market analysis is US$. Considering the average conversion rate for that particular year, currencies other than the US$ have been converted to the US$ for all statistical calculations.

The currency conversion rate has been taken from the historical exchange rate of the Oanda website.

Nearly all the recent developments from January 2021 to October 2024 have been considered in this research study.

The information rendered in the report results from in-depth primary interviews, surveys, and secondary analysis.

Where relevant information was not available, proxy indicators and extrapolation were employed.

Any economic downturn in the future has not been taken into consideration for the market estimation and forecast.

Technologies currently used are expected to persist through the forecast with no major technological breakthroughs.

Market Estimation and Forecast

This research study involves the usage of extensive secondary sources, such as certified publications, articles from recognized authors, white papers, annual reports of companies, directories, and major databases to collect useful and effective information

+44 20 8123 2220
info@marketpublishers.com

for an extensive, technical, market-oriented, and commercial study of the post-quantum cryptography market.

The market engineering process involves the calculation of the market statistics, market size estimation, market forecast, market crackdown, and data triangulation (the methodology for such quantitative data processes is explained in further sections). The primary research study has been undertaken to gather information and validate the market numbers for segmentation types and industry trends of the key players in the market.

Primary Research

The primary sources involve industry experts from the post-quantum cryptography market and various stakeholders in the ecosystem. Respondents such as CEOs, vice presidents, marketing directors, and technology and innovation directors have been interviewed to obtain and verify both qualitative and quantitative aspects of this research study.

The key data points taken from primary sources include:

validation and triangulation of all the numbers and graphs

validation of reports segmentation and key qualitative findings

understanding the competitive landscape

validation of the numbers of various markets for market type

percentage split of individual markets for geographical analysis

Secondary Research

This research study involves the usage of extensive secondary research, directories, company websites, and annual reports. It also uses databases, such as Hoovers, Bloomberg, Businessweek, and Factiva, to collect useful and effective information for an extensive, technical, market-oriented, and commercial study of the global market. In addition to the data sources, the study has been undertaken with the help of other data sources and websites, such as the Census Bureau, OICA, and ACEA.

+44 20 8123 2220
info@marketpublishers.com

Secondary research was done to obtain crucial information about the industry's value chain, revenue models, the market's monetary chain, the total pool of key players, and the current and potential use cases and applications.

The key data points taken from secondary research include:

- segmentations and percentage shares
- data for market value
- key industry trends of the top players of the market
- qualitative insights into various aspects of the market, key trends, and emerging areas of innovation
- quantitative data for mathematical and statistical calculations

Key Market Players and Competition Synopsis

The companies profiled in the post-quantum cryptography market have been selected based on inputs gathered from primary experts and analyzing company coverage, product portfolio, and post-quantum cryptography market penetration.

Some of the prominent names in post-quantum cryptography market are:

- IBM
- ID Quantique
- ETAS
- Infineon Technologies AG
- PQShield Ltd
- Qrypt

+44 20 8123 2220
info@marketpublishers.com

QuintessenceLabs

SandboxAQ

Thales

CryptoNext, inc.

Agnostiq

IonQ

D-Wave Quantum Inc.

Crypto Quantique

Quantinuum Ltd.

Atom Computing Inc.

PQ Solutions Limited

Toshiba Corporation

Microsoft

Fujitsu

Anhui Wentian Quantum Technology Co. Ltd.

Quantum Xchange

Quantum Blockchains

Companies that are not a part of the aforementioned pool have been well represented across different sections of the report (wherever applicable).

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

2 GLOBAL POST-QUANTUM CRYPTOGRAPHY MARKET (BY APPLICATION)

3 GLOBAL POST-QUANTUM CRYPTOGRAPHY MARKET (BY PRODUCT)

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

5 MARKETS - COMPETITIVE LANDSCAPED AND COMPANIES PROFILED

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

List Of Figures

LIST OF FIGURES

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

List Of Tables

LIST OF TABLES

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Post-Quantum Cryptography Market - A Global and Regional Analysis: Focus on Application, Product, and Regional and Country-Level Analysis - Analysis and Forecast, 2024-2034

Product link: https://marketpublishers.com/r/PD708E4CA75FEN.html

Price: US$ 4,850.00 (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/PD708E4CA75FEN.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

Custumer 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

+44 20 8123 2220
info@marketpublishers.com

and fax the completed form to +44 20 7900 3970