

# Post-Quantum Cryptography (PQC) Market by Solution (Quantum-safe Hardware, Quantum-resistant Encryption Products, Cryptographic Libraries, VPN, Authentication), Service (Migration Services, Quantum Risk Assessment) - Global Forecast to 2029

<https://marketpublishers.com/r/P542B0D1B64FEN.html>

Date: September 2024

Pages: 250

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

ID: P542B0D1B64FEN

## Abstracts

The Post-Quantum Cryptography (PQC) market size is estimated to grow from USD 302.5 million in 2024 to USD 1,887.9 million by 2029 at a Compound Annual Growth Rate (CAGR) of 44.2% during the forecast period.

The main reason for implementing PQC is a direct threat from quantum computing, which can break encryption methods such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic curve cryptography) exponentially faster than classical computers. Requiring quantum-resistant cryptographic solutions to be implemented is considered a provision for compliance with developing regulatory requirements, such as requirements from the US National Institute of Standards and Technology.

In addition, organizations need to secure long-term fiscal and healthcare-related data from quantum decryption in the future. Very early adoption of PQC can bring competitive military advantages associated with commitment to information security and privacy. Further, technology partner relationships can help ease an organization's migration to quantum-safe cryptography through technology collaborations. For all these reasons, there has been an increasing need for PQC to be used in sensitive data protection to stay compliant.

'By Region, BFSI accounts for a larger market share.'

The BFSI sector is significantly different from others in the PQC market for several

reasons. Stringent regulations like GDPR compel the use of advanced encryption to protect sensitive data and ensure compliance as one such reason. BFSI organizations must rely on PQC because financial data is the most valuable and has become very attractive to cybercriminals, making it a must-guarded item to retain customer trust.

Quantum Safe Hardware accounts for a larger market share by Solutions Segment.

Quantum-safe hardware is estimated to hold the largest market share in the PQC market. As quantum computing progresses, traditional cryptographic methods like RSA and ECC become vulnerable to quantum attacks. Quantum-safe hardware provides the foundational infrastructure needed to implement PQC algorithms effectively, making it indispensable for organizations looking to protect their data against future quantum threats. Hardware such as HSM (Hardware security modules) and TPM (Trusted Platform Module) Play a significant role in securing communication channels using QKD (Quantum Key Distribution) systems and QRNG (Quantum random number generators). Quantum-safe hardware is needed across multiple industries, including BFSI, healthcare, defense, and IT. This broad applicability ensures that quantum-safe hardware will be a central focus of PQC solutions, driving significant demand and market share.

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

North America, particularly the US, is leading in adopting PQC due to significant government initiatives and investments. US Agencies like the National Institute of Standards and Technology (NIST) have been at the forefront of standardizing PQC algorithms, driven by concerns over future quantum computing threats. The US & Canada government support accelerates regional research, development, and deployment. North American companies and research institutions are investing substantially in PQC research and development to stay ahead of emerging quantum threats. North America's robust technology ecosystem, including major tech firms and universities, fosters innovation in PQC, accelerating market growth and development.

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 – 35%, Tier 2 – 45%, and Tier 3 – 20%

By Designation: C-level – 40% and Managerial and Other Levels – 60%

By Region: North America – 50%, Europe – 25%, Asia Pacific – 20%, and Rest of the World – 5%

Major vendors in the PQC market include NXP Semiconductor (Netherlands), Thales (France), AWS (US), IDEMIA (France), Palo Alto Networks (US), DigiCert (US), Kloch (US), Post-Quantum (UK), PQ Shield (US), Entrust (US), IBM (US), Utimaco (Germany), Crypto Quantique (US), Crypto4A (Canada), CryptoNext (France), Qnu Labs (India), Qrypt (US), Enquantum (Israel), Xiphera (Finland), Sixscape (Singapore), Keyfactor (US), ResQuant (Poland), Rambus (US), Archon (British Virgin Island), Riscure (Netherlands).

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 PQC market by solution, service, organization size, vertical, and region. It forecasts its size by Solution (Quantum-safe hardware, Quantum-resistant algorithms, Quantum-safe cryptographic libraries, Quantum-safe VPN, email service, messaging systems, Quantum-safe blockchain solutions, Quantum-safe authentication solutions, Quantum-resistant encryption products), By Service (consulting services, Migration services, Quantum risk assessment), By Organization Size (SME's and Large Enterprises), By Vertical (BFSI, government and Defense, Healthcare, IT & ITES, Retail and E-commerce, 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 PQC 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 (Integration of Innovative Cryptographic algorithms, Hybrid PQC Mechanisms, Growing awareness of Cybersecurity and Data Privacy, Driving awareness toward Quantum Computing Threats); Restraints (High Implementation Costs in Solutions, Lack of Standardized algorithms); Opportunities (Early development of new products and service provides a competitive edge, Government and Defense Contracts, Migration to post-quantum cryptography) and Challenges (Significantly sizeable key size and implications on performance, Implementation Challenges, Difficulty in Encryption and Scalability, Vulnerabilities Due to Advancements in Quantum Technology).

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

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

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

**Competitive Assessment:** In-depth assessment of market shares, growth strategies, and service offerings of leading players NXP Semiconductor (Netherlands), Thales (France), AWS (US), IDEMIA (France), Palo Alto Networks (US), DigiCert (US), Klocx (US), Post-Quantum (UK), PQ Shield (US), Entrust (US), IBM (US), Utimaco (Germany), Crypto Quantique (US), Crypto4A (Canada), CryptoNext (France), Qnu Labs (India), Qrypt (US), Enquantum (Israel), Xiphera (Finland), Sixscape (Singapore), Keyfactor (US), ResQuant (Poland), Rambus (US), Archon (British Virgin Island), Riscure (Netherlands) among others, in the PQC market strategies.

## Contents

### 1 INTRODUCTION

- 1.1 STUDY OBJECTIVES
- 1.2 MARKET DEFINITION
  - 1.2.1 INCLUSIONS AND EXCLUSIONS
- 1.3 MARKET SCOPE
  - 1.3.1 MARKET SEGMENTATION
  - 1.3.2 YEARS CONSIDERED
- 1.4 CURRENCY CONSIDERED
- 1.5 STAKEHOLDERS

### 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 STUDY LIMITATIONS

### 3 EXECUTIVE SUMMARY

### 4 PREMIUM INSIGHTS

- 4.1 ATTRACTIVE OPPORTUNITIES FOR KEY MARKET PLAYERS
- 4.2 POST-QUANTUM CRYPTOGRAPHY MARKET, BY SOLUTION
- 4.3 POST-QUANTUM CRYPTOGRAPHY MARKET, BY SERVICE
- 4.4 POST-QUANTUM CRYPTOGRAPHY MARKET, BY ORGANIZATION SIZE
- 4.5 POST-QUANTUM CRYPTOGRAPHY MARKET: TOP 3 VERTICALS AND REGIONS
- 4.6 MARKET INVESTMENT SCENARIO

## **5 MARKET OVERVIEW AND INDUSTRY TRENDS**

### **5.1 INTRODUCTION**

### **5.2 MARKET DYNAMICS**

#### **5.2.1 DRIVERS**

- 5.2.1.1 Integration of innovative cryptographic algorithms
- 5.2.1.2 Hybrid PQC mechanisms
- 5.2.1.3 Growing awareness of cybersecurity and data privacy
- 5.2.1.4 Driving awareness toward quantum computing threat

#### **5.2.2 RESTRAINTS**

- 5.2.2.1 High implementation costs in post-quantum cryptography market
- 5.2.2.2 Lack of standardized algorithms

#### **5.2.3 OPPORTUNITIES**

- 5.2.3.1 Early development of new products and services to provide competitive edge
- 5.2.3.2 Government and defense contracts
- 5.2.3.3 Migration to post-quantum cryptography

#### **5.2.4 CHALLENGES**

- 5.2.4.1 Significantly large key size and implications on performance
- 5.2.4.2 Implementation challenges
- 5.2.4.3 Difficulty in encryption and scalability
- 5.2.4.4 Vulnerabilities due to advancements in quantum technology

### **5.3 IMPACT OF GENERATIVE AI ON POST-QUANTUM CRYPTOGRAPHY MARKET**

#### **5.3.1 TOP USE CASES AND MARKET POTENTIAL**

- 5.3.1.1 Key use cases

#### **5.3.2 IMPACT OF GEN AI ON INTERCONNECTED AND ADJACENT ECOSYSTEMS**

- 5.3.2.1 Quantum Computing
- 5.3.2.2 Quantum Key Distribution (QKD)
- 5.3.2.3 Hardware Security Modules (HSMs)
- 5.3.2.4 Cloud Security
- 5.3.2.5 Digital Signatures
- 5.3.2.6 Identity and Access Management (IAM)

### **5.4 CASE STUDY ANALYSIS**

#### **5.4.1 POST-QUANTUM CRYPTOGRAPHY FOR DEFENSE AND GOVERNMENT APPLICATIONS**

#### **5.4.2 ADOPTION OF BIO-KEY'S IDENTITY-BOUND BIOMETRICS SOLUTION AS PART OF PASSWORDLESS AUTHENTICATION STRATEGY**

#### **5.4.3 NAVIGATING QUANTUM LEAP: ROADMAP FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY**

## 5.5 VALUE CHAIN ANALYSIS

- 5.5.1 TECHNOLOGY INFRASTRUCTURE PROVIDERS
- 5.5.2 POST-QUANTUM CRYPTOGRAPHY PROVIDERS
- 5.5.3 APPLICATION DEVELOPERS
- 5.5.4 SYSTEM INTEGRATORS
- 5.5.5 END USERS

## 5.6 ECOSYSTEM ANALYSIS

## 5.7 PORTER'S FIVE FORCES MODEL ANALYSIS

- 5.7.1 THREAT OF NEW ENTRANTS
- 5.7.2 THREAT OF SUBSTITUTES
- 5.7.3 BARGAINING POWER OF SUPPLIERS
- 5.7.4 BARGAINING POWER OF BUYERS
- 5.7.5 INTENSITY OF COMPETITIVE RIVALRY

## 5.8 PRICING MODEL ANALYSIS

- 5.8.1 INDICATIVE PRICING ANALYSIS, BY OFFERING

## 5.9 TECHNOLOGY ANALYSIS

### 5.9.1 KEY TECHNOLOGIES

- 5.9.1.1 Lattice-based Cryptography
- 5.9.1.2 Code-based Cryptography
- 5.9.1.3 Hash-based Cryptography
- 5.9.1.4 Multivariate Cryptography
- 5.9.1.5 Symmetric Key Quantum Resistance
- 5.9.1.6 Isogeny-based Cryptography

### 5.9.2 COMPLEMENTARY TECHNOLOGIES

- 5.9.2.1 Quantum-resistant Hardware Accelerators
- 5.9.2.2 Cloud-based PQC

### 5.9.3 ADJACENT TECHNOLOGIES

- 5.9.3.1 Quantum Computing
- 5.9.3.2 Post-quantum Cybersecurity
- 5.9.3.3 Blockchain

## 5.10 PATENT ANALYSIS

### 5.10.1 METHODOLOGY

## 5.11 TRADE ANALYSIS

## 5.12 TARIFF & REGULATORY LANDSCAPE

- 5.12.1 TARIFF RELATED TO PQC PRODUCTS
- 5.12.2 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)
- 5.12.3 EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI)
- 5.12.4 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)
- 5.12.5 INTERNATIONAL TELECOMMUNICATION UNION (ITU)



- 5.12.6 INTERNET ENGINEERING TASK FORCE (IETF)
- 5.12.7 CLOUD SECURITY ALLIANCE (CSA)
- 5.12.8 GLOBAL FORUM ON CYBER EXPERTISE (GFCE)
- 5.12.9 WORLD ECONOMIC FORUM (WEF)
- 5.12.10 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)
- 5.12.11 INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH (IACR)
- 5.12.12 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS
- 5.13 KEY STAKEHOLDERS AND BUYING CRITERIA
  - 5.13.1 KEY STAKEHOLDERS IN BUYING PROCESS
  - 5.13.2 BUYING CRITERIA
- 5.14 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS
- 5.15 KEY CONFERENCES & EVENTS
- 5.16 BUSINESS MODEL ANALYSIS
  - 5.16.1 ALGORITHM DEVELOPMENT AND LICENSING IN POST-QUANTUM CRYPTOGRAPHY
  - 5.16.2 CONSULTING SERVICES
  - 5.16.3 HARDWARE SOLUTIONS
  - 5.16.4 SOFTWARE SOLUTIONS
  - 5.16.5 CLOUD-BASED SERVICES MODEL
  - 5.16.6 SPECIALIZED SECURITY SOLUTIONS
  - 5.16.7 SUBSCRIPTION-BASED MODEL
  - 5.16.8 EDUCATION AND TRAINING IN POST-QUANTUM CRYPTOGRAPHY MARKET
- 5.17 INVESTMENT AND FUNDING SCENARIO

## **6 POST-QUANTUM CRYPTOGRAPHY MARKET, BY SOLUTION**

- 6.1 INTRODUCTION
  - 6.1.1 SOLUTION: POST-QUANTUM CRYPTOGRAPHY MARKET DRIVERS
- 6.2 QUANTUM-SAFE HARDWARE
  - 6.2.1 SECURE HARDWARE FOR QUANTUM-COMPUTING AGE
- 6.3 QUANTUM-RESISTANT ALGORITHMS
  - 6.3.1 FORTIFY AGAINST QUANTUM THREATS WITH ADVANCED CRYPTOGRAPHIC ALGORITHMS
- 6.4 QUANTUM-SAFE CRYPTOGRAPHIC LIBRARIES
  - 6.4.1 EMPOWER DEVELOPERS WITH READY-TO-USE QUANTUM-SAFE ENCRYPTION



## 6.5 QUANTUM-SAFE VPN, EMAIL SERVICE, AND MESSAGING SYSTEMS

### 6.5.1 ENSURE SECURE COMMUNICATIONS EVEN IN QUANTUM WORLD

## 6.6 QUANTUM-SAFE BLOCKCHAIN SOLUTIONS

### 6.6.1 BLOCKCHAINS SECURED AGAINST QUANTUM THREATS, ENSURING TRUST

## 6.7 QUANTUM-SAFE AUTHENTICATION SOLUTIONS

### 6.7.1 PROTECT DIGITAL IDENTITIES WITH QUANTUM-RESISTANT AUTHENTICATION

## 6.8 QUANTUM-RESISTANT ENCRYPTION SOLUTIONS

### 6.8.1 HELPS ENCRYPT DATA AND SAFEGUARD AGAINST FUTURE QUANTUM RISK

## **7 POST-QUANTUM CRYPTOGRAPHY MARKET, BY SERVICE**

### 7.1 INTRODUCTION

#### 7.1.1 SERVICE: POST-QUANTUM CRYPTOGRAPHY MARKET DRIVERS

### 7.2 DESIGN, IMPLEMENTATION, AND CONSULTING

#### 7.2.1 TAILORED QUANTUM-SAFE SOLUTIONS FOR ROBUST SECURITY

### 7.3 MIGRATION SERVICES

#### 7.3.1 ENABLES SEAMLESS UPGRADE TO QUANTUM-RESISTANT ENCRYPTION

### 7.4 QUANTUM RISK ASSESSMENT

#### 7.4.1 ENABLES TO IDENTIFY AND MITIGATE FUTURE QUANTUM THREATS

## **8 POST-QUANTUM CRYPTOGRAPHY MARKET, BY ORGANIZATION SIZE**

### 8.1 INTRODUCTION

#### 8.1.1 ORGANIZATION SIZE: POST-QUANTUM CRYPTOGRAPHY MARKET DRIVERS

### 8.2 SMALL & MEDIUM-SIZED ENTERPRISES

#### 8.2.1 COST-EFFECTIVE, SCALABLE PQC FOR SMALL BUSINESSES

### 8.3 LARGE ENTERPRISES

#### 8.3.1 ENTERPRISE-GRADE PQC FOR ROBUST, HIGH-VALUE PROTECTION

## **9 POST-QUANTUM CRYPTOGRAPHY MARKET, BY VERTICAL**

### 9.1 INTRODUCTION

#### 9.1.1 VERTICAL: POST-QUANTUM CRYPTOGRAPHY MARKET DRIVERS

### 9.2 BANKING, FINANCIAL SERVICES, AND INSURANCE (BFSI)

#### 9.2.1 ENHANCING FINANCIAL DATA SECURITY WITH PQC

### 9.3 GOVERNMENT & DEFENSE

#### 9.3.1 FORTIFYING NATIONAL SECURITY THROUGH PQC

### 9.4 HEALTHCARE

#### 9.4.1 SECURING PATIENT DATA WITH QUANTUM-RESISTANT METHOD

### 9.5 IT & ITES

#### 9.5.1 STRENGTHENING IT INFRASTRUCTURE WITH PQC

### 9.6 RETAIL & E-COMMERCE

#### 9.6.1 PROTECTING E-COMMERCE TRANSACTIONS WITH PQC

### 9.7 OTHER VERTICALS

## **10 POST-QUANTUM CRYPTOGRAPHY MARKET, BY REGION**

### 10.1 INTRODUCTION

### 10.2 NORTH AMERICA

#### 10.2.1 NORTH AMERICA: MARKET DRIVERS

#### 10.2.2 NORTH AMERICA: MACROECONOMIC OUTLOOK

#### 10.2.3 US

10.2.3.1 Rapid development of quantum computing technology poses significant threat to existing cryptographic algorithms

#### 10.2.4 CANADA

10.2.4.1 Partnerships between universities and tech companies to foster innovation in post-quantum cryptography

### 10.3 EUROPE

#### 10.3.1 EUROPE: MARKET DRIVERS

#### 10.3.2 EUROPE: MACROECONOMIC OUTLOOK

#### 10.3.3 UK

10.3.3.1 UK National Cyber Security Centre (NCSC) to promote transition to quantum-safe technologies

#### 10.3.4 FRANCE

10.3.4.1 French startups and research institutions at forefront of innovation and creating solutions that can be integrated into existing system

### 10.4 ASIA PACIFIC

#### 10.4.1 ASIA PACIFIC: MARKET DRIVERS

#### 10.4.2 ASIA PACIFIC: MACROECONOMIC OUTLOOK

#### 10.4.3 CHINA

10.4.3.1 Increasing demand for post-quantum cryptography in various sectors

#### 10.4.4 JAPAN

10.4.4.1 Contribution of top technology companies and semiconductor manufacturers to development of advanced post-quantum cryptographic solutions to drive market

## 10.5 REST OF THE WORLD (ROW)

### 10.5.1 REST OF THE WORLD (ROW): MARKET DRIVERS

### 10.5.2 REST OF THE WORLD (ROW): MACROECONOMIC OUTLOOK

## 11 COMPETITIVE LANDSCAPE

### 11.1 KEY PLAYER STRATEGIES/RIGHT TO WIN

### 11.2 REVENUE ANALYSIS

### 11.3 MARKET SHARE ANALYSIS

### 11.4 BRAND COMPARISON

### 11.5 COMPANY VALUATION AND FINANCIAL METRICS

#### 11.5.1 COMPANY VALUATION

#### 11.5.2 FINANCIAL METRICS USING EV/EBITDA

### 11.6 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2023

#### 11.6.1 STARS

#### 11.6.2 EMERGING LEADERS

#### 11.6.3 PERVASIVE PLAYERS

#### 11.6.4 PARTICIPANTS

#### 11.6.5 COMPANY FOOTPRINT: KEY PLAYERS, 2024

##### 11.6.5.1 Company footprint

##### 11.6.5.2 Region footprint

##### 11.6.5.3 Solution footprint

##### 11.6.5.4 Service footprint

##### 11.6.5.5 Vertical footprint

### 11.7 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2023

#### 11.7.1 PROGRESSIVE COMPANIES

#### 11.7.2 RESPONSIVE COMPANIES

#### 11.7.3 DYNAMIC COMPANIES

#### 11.7.4 STARTING BLOCKS

#### 11.7.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2023

##### 11.7.5.1 Detailed list of key startups/SMEs

##### 11.7.5.2 Competitive benchmarking of key startups/SMEs

### 11.8 COMPETITIVE SCENARIO

#### 11.8.1 PRODUCT LAUNCHES

#### 11.8.2 DEALS

## 12 COMPANY PROFILES

### 12.1 KEY PLAYERS

## 12.1.1 NXP SEMICONDUCTORS

- 12.1.1.1 Business overview
- 12.1.1.2 Products/Solutions/Services offered
- 12.1.1.3 Recent developments
- 12.1.1.4 MnM view
  - 12.1.1.4.1 Key strengths
  - 12.1.1.4.2 Strategic choices
  - 12.1.1.4.3 Weaknesses and competitive threats

## 12.1.2 THALES

- 12.1.2.1 Business overview
- 12.1.2.2 Products/Solutions/Services offered
- 12.1.2.3 Recent developments
- 12.1.2.4 MnM view
  - 12.1.2.4.1 Key strengths
  - 12.1.2.4.2 Strategic choices
  - 12.1.2.4.3 Weaknesses and competitive threats

## 12.1.3 AWS

- 12.1.3.1 Business overview
- 12.1.3.2 Products/Solutions/Services offered
- 12.1.3.3 Recent developments
- 12.1.3.4 MnM view
  - 12.1.3.4.1 Key strengths
  - 12.1.3.4.2 Strategic choices
  - 12.1.3.4.3 Weaknesses and competitive threats

## 12.1.4 IDEMIA

- 12.1.4.1 Business overview
- 12.1.4.2 Products/Solutions/Services offered
- 12.1.4.3 Recent developments

## 12.1.5 PALO ALTO NETWORKS

- 12.1.5.1 Business overview
- 12.1.5.2 Products/Solutions/Services offered
- 12.1.5.3 Recent developments
- 12.1.5.4 MnM view
  - 12.1.5.4.1 Key strengths
  - 12.1.5.4.2 Strategic choices
  - 12.1.5.4.3 Weaknesses and competitive threats

## 12.1.6 DIGICERT

- 12.1.6.1 Business overview
- 12.1.6.2 Products/Solutions/Services offered

12.1.6.3 Recent developments

#### 12.1.7 KLOCH

12.1.7.1 Business overview

12.1.7.2 Products/Solutions/Services offered

#### 12.1.8 POST-QUANTUM

12.1.8.1 Business overview

12.1.8.2 Products/Solutions/Services offered

#### 12.1.9 PQSHIELD

12.1.9.1 Business overview

12.1.9.2 Products/Solutions/Services offered

12.1.9.3 Recent developments

#### 12.1.10 ENTRUST

12.1.10.1 Business overview

12.1.10.2 Products/Solutions/Services offered

12.1.10.3 Recent developments

#### 12.1.11 IBM

12.1.11.1 Business overview

12.1.11.2 Products/Solutions/Services offered

12.1.11.3 Recent developments

### 12.2 OTHER PLAYERS

#### 12.2.1 UTIMACO

#### 12.2.2 CRYPTO QUANTIQUÉ

#### 12.2.3 CRYPTO4A

#### 12.2.4 CRYPTONEXT

#### 12.2.5 QNU LABS

#### 12.2.6 QRYPT

#### 12.2.7 ENQUANTUM

#### 12.2.8 XIPHERA

#### 12.2.9 SIXSCAPE

#### 12.2.10 KEYFACTOR

#### 12.2.11 RESQUANT

#### 12.2.12 RAMBUS

#### 12.2.13 ARCHON

#### 12.2.14 RISCURE

## 13 ADJACENT MARKETS

### 13.1 INTRODUCTION

### 13.2 LIMITATIONS

### 13.3 QUANTUM CRYPTOGRAPHY MARKET

#### 13.3.1 QUANTUM CRYPTOGRAPHY MARKET, BY OFFERING

### 13.4 ENCRYPTION SOFTWARE MARKET

#### 13.4.1 ENCRYPTION SOFTWARE, BY DEPLOYMENT MODE

## **14 APPENDIX**

### 14.1 DISCUSSION GUIDE

### 14.2 KNOWLEDGESTORE: MARKETSandMARKETS' SUBSCRIPTION PORTAL

### 14.3 CUSTOMIZATION OPTIONS

### 14.4 RELATED REPORTS

### 14.5 AUTHOR DETAILS

## I would like to order

Product name: Post-Quantum Cryptography (PQC) Market by Solution (Quantum-safe Hardware, Quantum-resistant Encryption Products, Cryptographic Libraries, VPN, Authentication), Service (Migration Services, Quantum Risk Assessment) - Global Forecast to 2029

Product link: <https://marketpublishers.com/r/P542B0D1B64FEN.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](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/P542B0D1B64FEN.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