

Comprehensive Report on Project Leap Presentation

Analysis by Angela Dupont

Presentation at BIS, Basel, Switzerland



Author's Note

This report is a personal account of the presentation by Angela Dupont, as interpreted and compiled by Olivier Atangana. It reflects my understanding and perspective on the topics discussed during the event.

Introduction

Angela Dupont presented Project Leap at the BIS in Basel, focusing on addressing the emerging threats posed by quantum computing to financial

stability through advanced cryptographic solutions. This project symbolizes a significant step towards quantum-resistant cryptography, essential for safeguarding financial infrastructures.

1 Quantum Computing Threat

Quantum computers present a substantial threat to current cryptographic systems, potentially destabilizing the financial sector. Dupont emphasizes the urgency of addressing these vulnerabilities.

2 Quantum-Resistant Cryptography

Project Leap is at the forefront of developing quantum-resistant cryptographic solutions. This proactive measure, overseen by entities like NIST, is crucial for future-proofing financial systems.

3 Collaborative Efforts with Major Banks

The project exemplifies collaboration, particularly with Banque de France and Bundesbank, to implement secure solutions in diverse IT environments, ranging from private to public clouds.

4 Implementation of Hybrid VPNs

A key achievement of Project Leap is the successful implementation of hybrid VPNs, integrating quantum-resistant and traditional cryptography, adhering to European regulatory guidelines.

5 Deployment Challenges

Dupont outlines the challenges in deployment, especially in identifying current usage of vulnerable cryptography and the necessity of extensive training for cybersecurity experts.

6 Cryptographic Agility

Project Leap highlights the importance of cryptographic agility – the ability to seamlessly transition between algorithms in response to evolving threats.

7 Performance vs. Security

A critical observation made is the trade-off between performance and security, particularly when integrating new algorithms into existing systems.

8 Future Prospects - LEAP 2.0

Looking ahead, Project Leap aims to broaden its scope in LEAP 2.0, focusing on securing payment systems and engaging more central banks in the initiative.

9 Insights and Strategic Focus

Dupont stresses the importance of preparation over immediate implementation, advocating for a comprehensive approach encompassing inventory management, training, and risk assessment.

10 The Imperative of Collaboration

The project underscores the necessity of collaboration over competition, especially in the context of global financial security.

11 Coexistence of Quantum and Classical Cryptography

Dupont envisions a gradual transition from classical to quantum cryptography, necessitating a shift in mindset towards crypto-agility.

12 Questions and Answers

12.1 Migration Plan and Timeline

Addressing the timeline for the migration plan, Dupont emphasizes the need for strategic preparation well in advance of implementation.

12.2 Impact on Secure Communication Architecture

With the advent of quantum computing, Dupont acknowledges the inevitable changes in the architecture of secure communication, highlighting the need for adaptability.

12.3 Global Cooperation and Risks

Dupont calls for global cooperation, considering the interconnected nature of financial systems and the risks posed by uneven cybersecurity frameworks across nations.

12.4 Quantum Mechanical Key Exchanges

The presentation touched on the potential of quantum mechanical key exchanges, acknowledging the technical challenges and the need for pragmatic solutions.

Concluding Remarks

Angela Dupont's presentation on Project Leap provides insightful perspectives on the challenges and strategies for securing financial systems against quantum threats. The emphasis on collaboration, preparation, and agility sets the tone for future developments in this critical field.

13 Legal Notices

13.1 Copyright

© 2023 Olivier Atangana. All rights reserved. This report is the intellectual property of Olivier Atangana.

13.2 Terms of Use

This report may be cited with proper attribution, but may not be reproduced in its entirety without permission.

13.3 Disclaimer

The opinions expressed in this report are those of Olivier Atangana and do not necessarily reflect the views of any associated organizations.

13.4 Contact Information

For inquiries or additional permissions, please contact Olivier Atangana at olivier.atangana@fime.com.