

The Outlook of German Companies on IT-Security and Their Readiness for Quantum Computing

Paulina Schindler

Friedrich Schiller University Jena, Germany

Abstract

Quantum computers are currently in development. As soon as they are available for widespread use, they can offer great benefits for companies. However, they can also pose dangers to information security. Because of this, protection measures are needed. To gain an insight into the outlook and knowledge of companies on quantum computing and their internal decision processes when establishing new technologies, qualitative interviews were conducted. Because not all companies know about quantum computing, the questions were designed without necessary previous knowledge in mind. Additionally, an employee of the German Federal Office for Information Security (BSI) was asked for their opinions. Many of the interviewed companies were not well informed about quantum computing and some lacked preparation of their general IT security. However, they had ideas how they could utilize such a much more powerful computer in the future. To gauge how quantum-secure measures could be implemented among companies, the companies were asked about their decision criteria when deciding on implementing a new technology. Their answers often included price and distribution, functions of the technology and external influences like other companies or guidelines from the government. To support the transition to quantum computer-safe cryptography in companies, different areas of action are examined. Supporting the availability of relevant use cases, market incubation and standards, collaboration between companies and education among them can help in pushing the spread of post-quantum security in companies in the future.

Keywords: post-quantum cryptography, decision criteria, interview