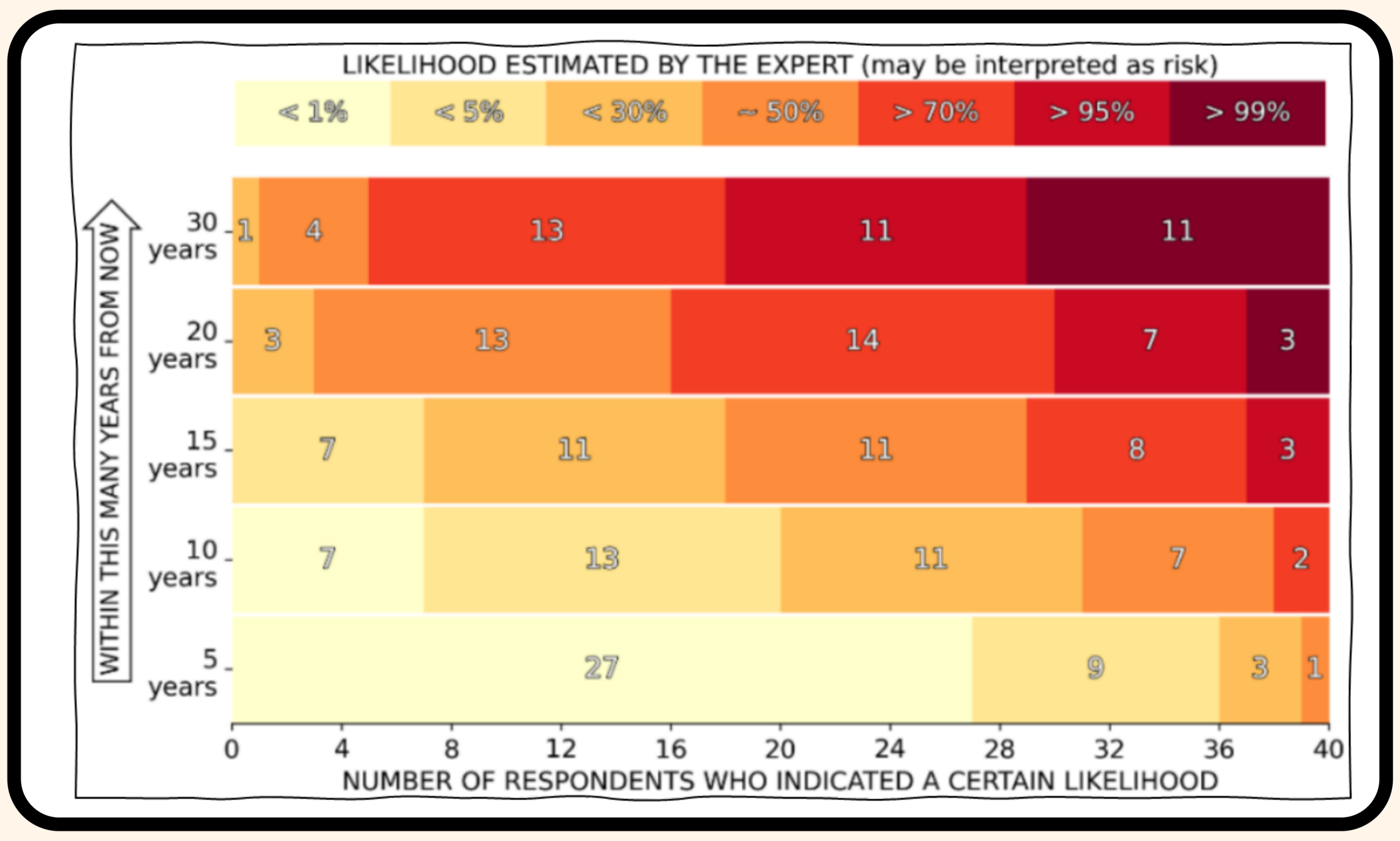
POST-QUANTUM NON-INTERATIVE KEY EXCHANGE

INDERJEET GILL
LEAD SUPERVISOR: FRANCOIS DUPRESSOIR

INDERJEET.GILL@BRISTOL.AC.UK
F.DUPRESSOIR@BRISTOL.AC.UK

INTRODUCTION

1976: DIFFE-HELLMAN REVOLUTIONISED CRYPTOGRAPHY WITH THE ADVENT OF PUBLIC-KEY CRYPTOGRAPHY, WHICH IS RELIED ON FOR MANY APPLICATIONS INCLUDING **TLS** AND THE **SIGNAL PROTOCOL** (USED BY **WHATSAPP**).
QUANTUM COMPUTERS **THREATEN** THIS AND THE **SECURITY OF MODERN CRYPTOSYSTEMS**, AND **POST-QUANTUM CRYPTOGRAPHY** SEEKS TO SOLVE THIS PROBLEM. ONE OF THE THREATENED PROTOCOLS IS **NON-INTERACTIVE KEY EXCHANGE (NIKE)**. I WILL BE WORKING ON OPEN PROBLEMS IN A NEW POST-QUANTUM NIKE CANDIDATE, **SWOOSH.**

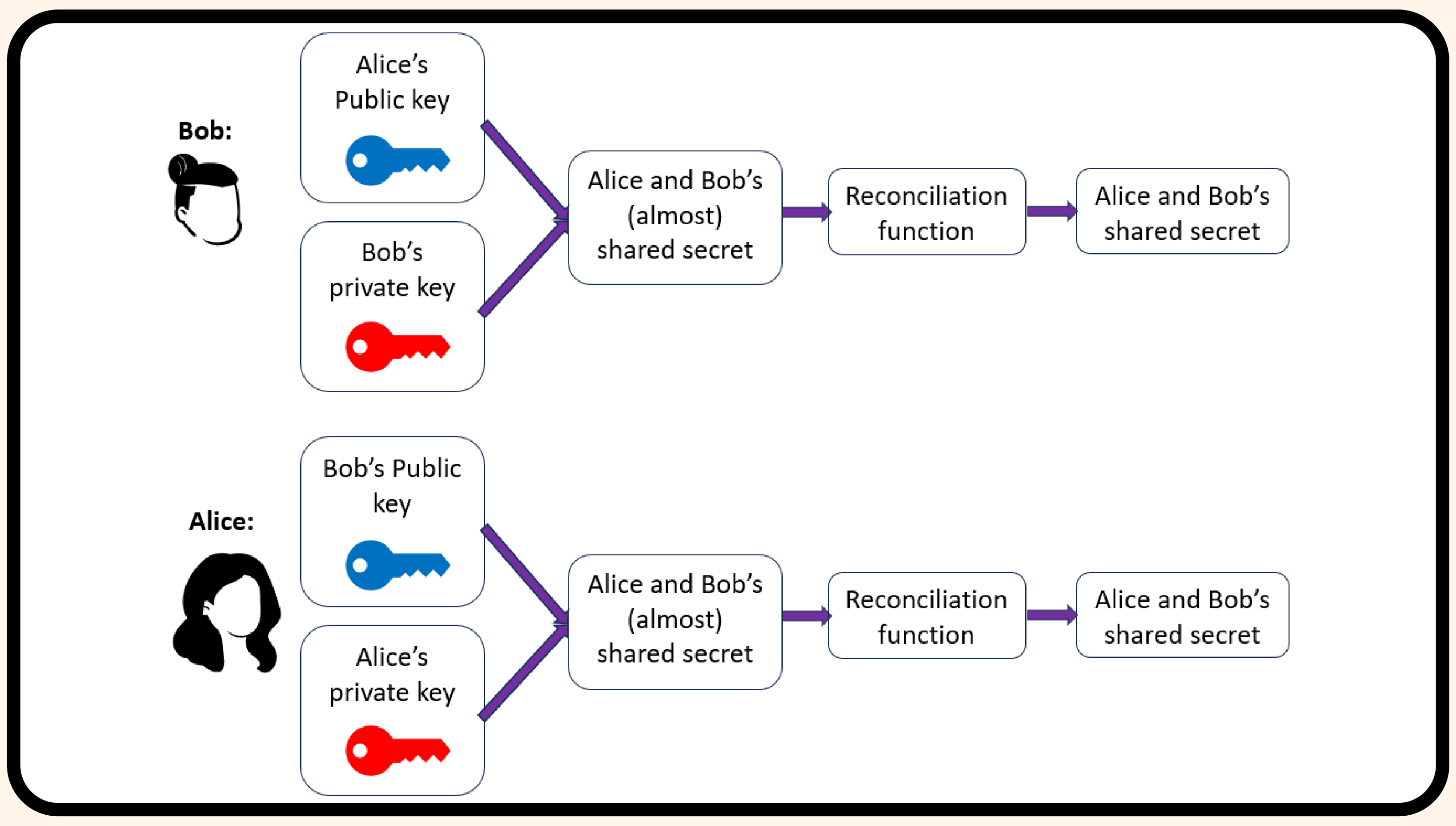


QUANTUM THREAT

BY UTILISING **SHOR'S ALGORITHM**, A SCALABLE QUANTUM COMPUTER WILL BE ABLE TO **BREAK MODERN PUBLIC-KEY CRYPTOSYSTEMS**. THIS WILL MAKE PROTOCOLS SUCH AS **DIFFE-HELLMAN**, THAT WE RELY ON, **OBSOLETE**. WE THEREFORE NEED SUITABLE **QUANTUM-RESISTANT REPLACEMENTS**.

NIKE

SYMMETRIC ENCRYPTION REQUIRES BOTH PARTIES TO HAVE THE **SAME SECRET KEY**. EXCHANGING THE SECRET KEY **WITHOUT INTERACTION** (NIKE) HAS MANY BENEFITS AND IS **REQUIRED** BY THE SIGNAL PROTOCOL, NOISE PROTOCOL FRAMEWORK, WIREGUARD VPN AND MORE. HOWEVER, THERE IS **CURRENTLY NO FULLY IMPLEMENTABLE** PRACTICAL POST-QUANTUM LATTICE-BASED NIKE.


Bob:
Alice's Public key
Bob's private key
Alice and Bob's (almost) shared secret
Reconciliation function
Alice and Bob's shared secret
Alice:
Bob's Public key
Alice's private key
Alice and Bob's (almost) shared secret
Reconciliation function
Alice and Bob's shared secret

SWOOSH

SWOOSH IS A **PRACTICAL LATTICE-BASED NIKE**, WHOSE SECURITY IS BASED ON THE HARDNESS OF THE **MODULE LEARNING WITH ERRORS** PROBLEM. THE ONLY OTHER PLAUSIBLE POST-QUANTUM NIKE IS THE ISOGENY-BASED **CSIDH**. HOWEVER, IT IS DIFFICULT TO COMPARE BOTH AS THERE IS CURRENTLY NO FULL IMPLEMENTATION OF SWOOSH. THERE ARE ALSO FURTHER UNKNOWNS REGARDING DETAILS OF THE SWOOSH PROTOCOL, WHICH WE WILL BE INVESTIGATING.

METHODOLOGY

I WILL EMPLOY A **CROSS-DISCIPLINARY APPROACH** INCLUDING CRYPTANALYSIS, PROVABLE SECURITY, CRYPTOGRAPHIC PRIMITIVE DESIGN, QUANTUM ALGORITHMS AND CRYPTOGRAPHIC ENGINEERING TO ADDRESS THE PROBLEMS IDENTIFIED. THESE INCLUDE: ANALYSING THE FLEXIBILITY OF **CONSTRUCTION'S CONDITIONS**, POSSIBLE **ATTACKS**, AND IF THE **NON-INTERACTIVE ZERO-KNOWLEDGE PROOF** USED IS ACHIEVABLE OR EVEN REQUIRED.

REFERENCES

- MOSER, M. 2022 QUANTUM THREAT TIMELINE REPORT, GLOBAL RISK INSTITUTE
- P. GAJLAND, B. KOCK, M. QUARESMA, G. MALAOVOLTA AND P. SCHWABE (2023), "SWOOSH: PRACTICAL LATTICE-BASED NON-INTERACTIVE KEY EXCHANGE"