Quantum Cryptography: An introduction to and comparison of the BB84 and SARG04 Protocols

Jacob Norman

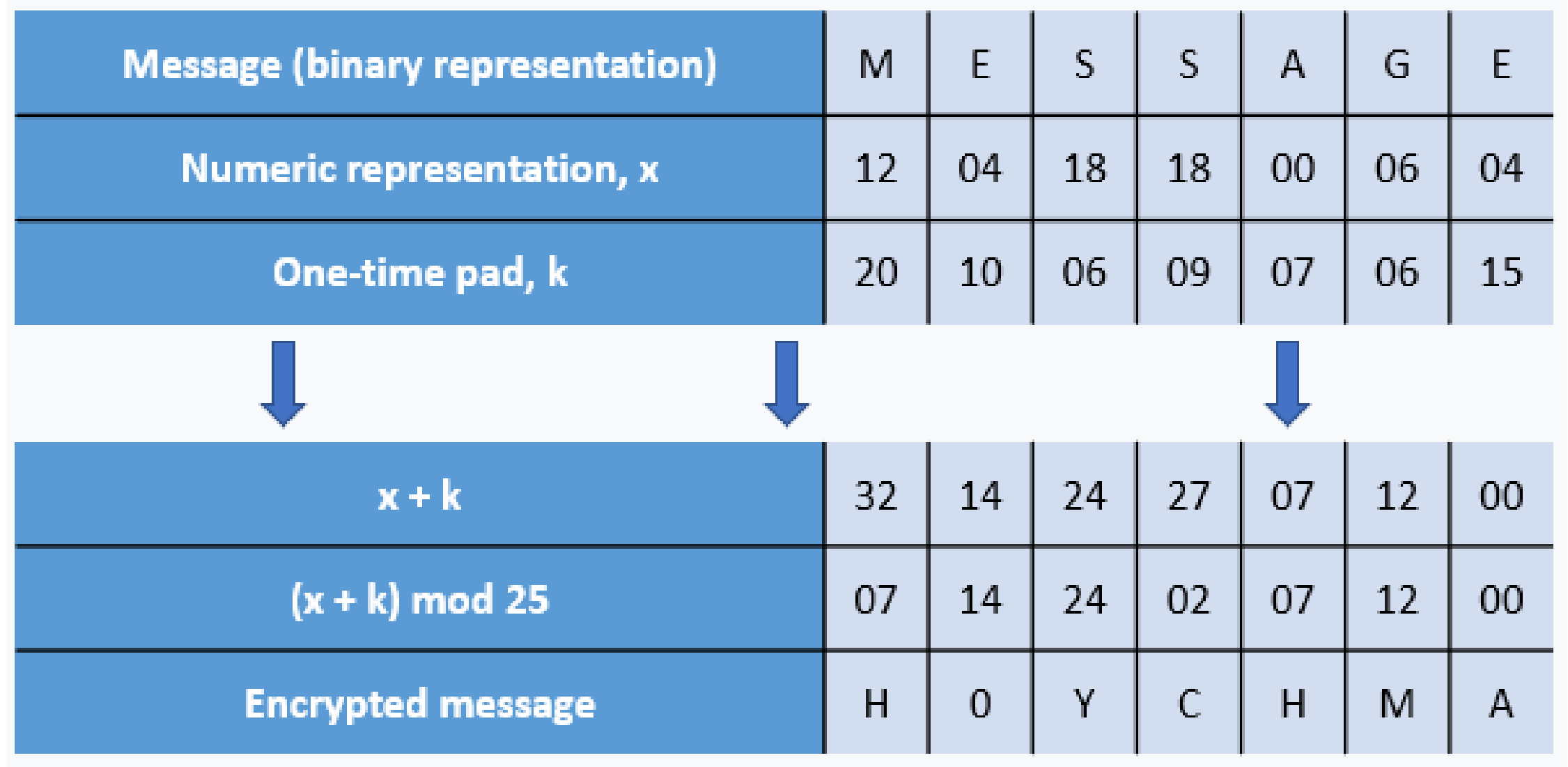
School of Physics and Astronomy, University of Birmingham

Background

The aim of cryptography is to develop techniques to send information securely. There are two general types of encryption:

- **symmetric encryption**, where one key is used to encrypt and decrypt the message, and
- **asymmetric encryption**, where one key is used to encrypt the message and, another is used to decrypt the message.

Since 1949 [4], we have known about a simple but provably secure symmetric-key encryption method, called *one-time pad encryption.* A private key consisting of random numbers is added to the message and thus the encrypted information is uncorrelated with the original message.



Message (binary representation)	M	E	S	S	A	G	E
Numeric representation, x	12	04	18	18	00	06	04
One-time pad, k	20	10	06	09	07	06	15
x + k	32	14	24	27	07	12	00
(x + k) mod 25	07	14	24	02	07	12	00
Encrypted message	H	O	Y	C	H	M	A

Figure 1: An example of a one-time pad encryption

The drawback to symmetric key encryption is that both parties must share the symmetric key. Classically, sharing a one-time pad securely is at least as hard as sending the message securely, since the one-time pad must be at least as long as the message.

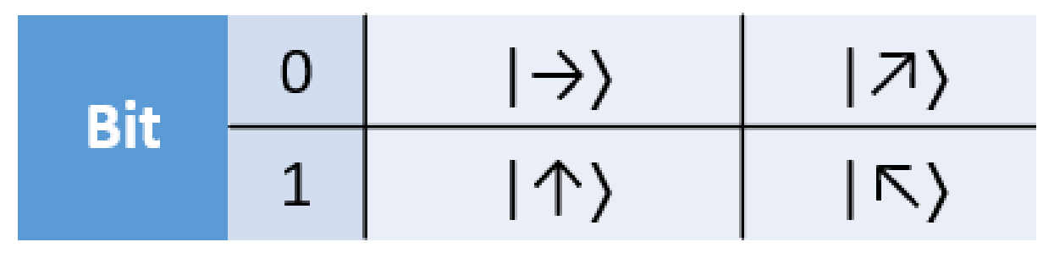
For this reason, most modern encryption techniques instead use asymmetric key encryption. However, these methods usually rely on the assumption that factorizing large numbers is computationally difficult. Given enough time or computation power, such methods can be broken. In addition, quantum computers may be able to factorize large numbers exponentially faster than current computers [5], rendering current encryption methods useless.

Quantum mechanics provide an elegant method for sending a key, such as a one-time pad, so that the sender and receiver can know for sure whether the key was intercepted by an eavesdropper. This process is called *quantum key distribution (QKD).* The first QKD protocol was the BB84 protocol, proposed by Bennet and Brasser in 1984 [3]. Since then, there have been experimental realizations of the protocol, as well as the development of many other protocols. This poster discusses the BB84 and SARG04 protocols.

BB84

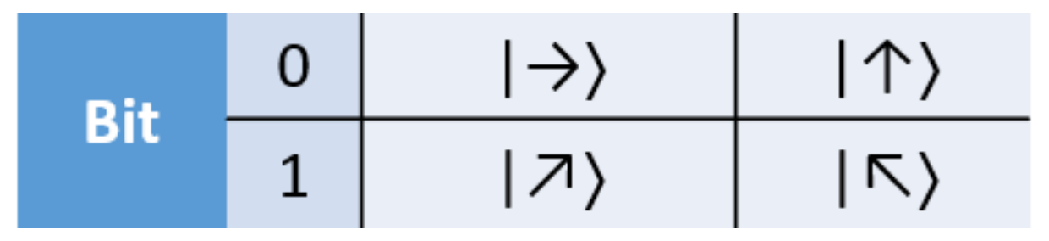
Initial Setup:

- Alice (sender) and Bob (receiver) use two communication channels: a classical channel and a quantum channel.
- The classical channel can be intercepted, but not modified, by Eve (an eavesdropper).
- Any quantum object can be used for the quantum channel, along with any two non-orthogonal bases.
- Here, the BB84 protocol is described using polarized photons measured in a rectilinear or diagonal (rotated 45 degrees) basis. One state from each basis is chosen to represent 0 and the other 1 (shown in Figure 2).



Bit			
	0	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
	1	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

Figure 2: The coding scheme used in the BB84 protocol

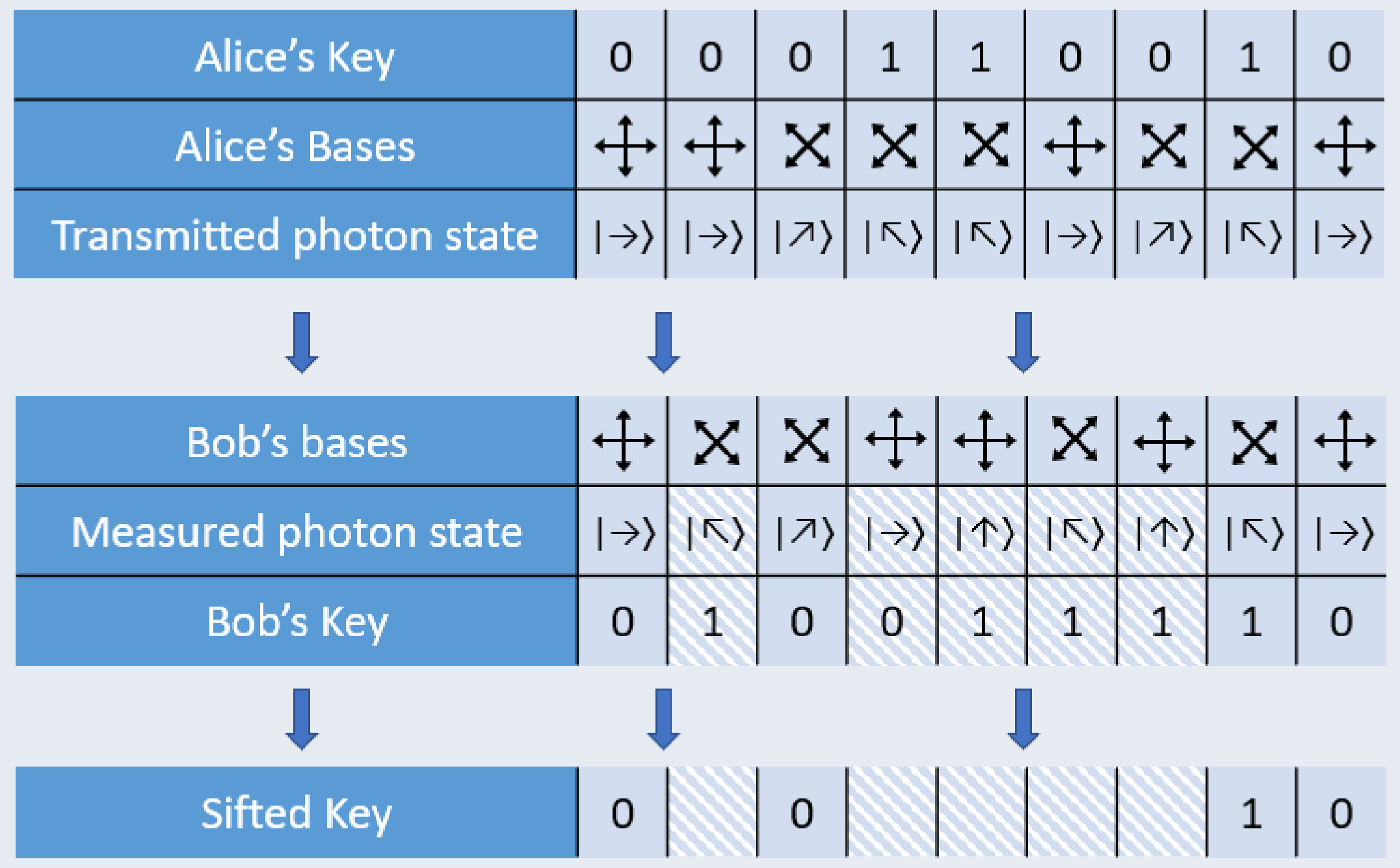


Bit			
	0	$\|\rightarrow\rangle$	$\|\uparrow\rangle$
	1	$\|\nearrow\rangle$	$\|\nwarrow\rangle$

Figure 3: The coding scheme for the SARG04 QKD protocol

BB84 Protocol

1. Alice generates a one-time pad (binary representation) and randomly chooses a basis for each bit. She transmits the corresponding polarized photons through the quantum channel.
2. Bob randomly chooses a basis to measure each photon sent by Alice.
3. Alice and Bob use the classical channel to share which bases were used for each photon.
4. Alice and Bob discard all measurements where they did not use the same basis since measurements of the photon in different bases are not correlated. Alice and Bob now possess the same string called the sifted key.
5. Alice and Bob compare a subset of the sifted key to ensure they match. If a match occurs, the remainder of the sifted key can be used as a one-time pad and Alice and Bob can be sure the key was not intercepted.



Alice's Key	0	0	0	1	1	0	0	1	0
Alice's Bases	+	+	×	×	×	+	×	×	+
Transmitted photon state	$\|\rightarrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	$\|\nwarrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	$\|\rightarrow\rangle$
Bob's bases	+	×	×	+	+	×	+	×	+
Measured photon state	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$	$\|\rightarrow\rangle$
Bob's Key	0	1	0	0	1	1	1	1	0
Sifted Key	0	▨	0	▨	▨	▨	▨	1	0

Figure 4: An example implementation of BB84

BB84 Security

Comparing a subset of the sifted key protects against intercept-resend attack. For an undetected attack on each bit of the key, Eve must either randomly

- choose the same basis as Alice and Bob (50% chance), or
- choose the other basis but Alice and Bob's measurements agree (25% chance).

In the latter case, Eve's measurement is random and provides her no information. Therefore, if Alice and Bob's n-bit sifted keys are the same, the probability that Eve is successful in intercepting and resending the key is

$$p(\text{successful attack}) = 1 - \left(\frac{3}{4}\right)^n .$$

When considering the robustness of QKD protocols, it is necessary to consider weaknesses introduced by imperfections in the physical realization. One such weakness is that photon sources for BB84 are usually attenuated laser pulses and the pulses produced are not exclusively single photons. This makes the protocol susceptible to a photon-number splitting attack (PNS). In a PNS attack, Eve removes a photon from pulses containing more than one photon. Then, when the bases are revealed in step 3, she measures the photon in the correct basis.

SARG04

The SARG04 protocol [2] was introduced as a modification to the BB84 protocol that was less susceptible to a PNS attack. One of the reasons BB84 is not robust against this attack is that the bases are revealed publicly, allowing Eve to measure the intercepted photon in the correct basis. Therefore, steps 1 and 2 are unchanged in the SARG04 protocol, but the sifting phase is modified so that the bases remain secret. The coding scheme used is shown in Figure 3.

SARG04 Protocol

1. Alice generates a one-time pad (binary representation) and randomly chooses a basis for each bit. She transmits the corresponding polarized photons through the quantum channel.
2. Bob randomly chooses a basis to measure each photon sent by Alice.
3. Over the classical channel, Alice discloses a pair of non-orthogonal states. One of these is the state of the photon she sent to Bob. 25% of the time, this is enough information for Bob to deduce the photon Alice sent.
4. If Bob cannot determine the state of the photon, the measurement is discarded. The resulting sifted key is a quarter of the length of the raw key.

Note on step 3: Let the pair of non-orthogonal states Alice announces be $\{|x\rangle, |y\rangle\}$, measured in the X and Y basis respectively. If Alice sent a photon in state $|x\rangle$, Bob is only able to deduce the state of Alice's photon when he chooses the Y basis but does not measure $|y\rangle$. For a concrete example, see Figure 5.

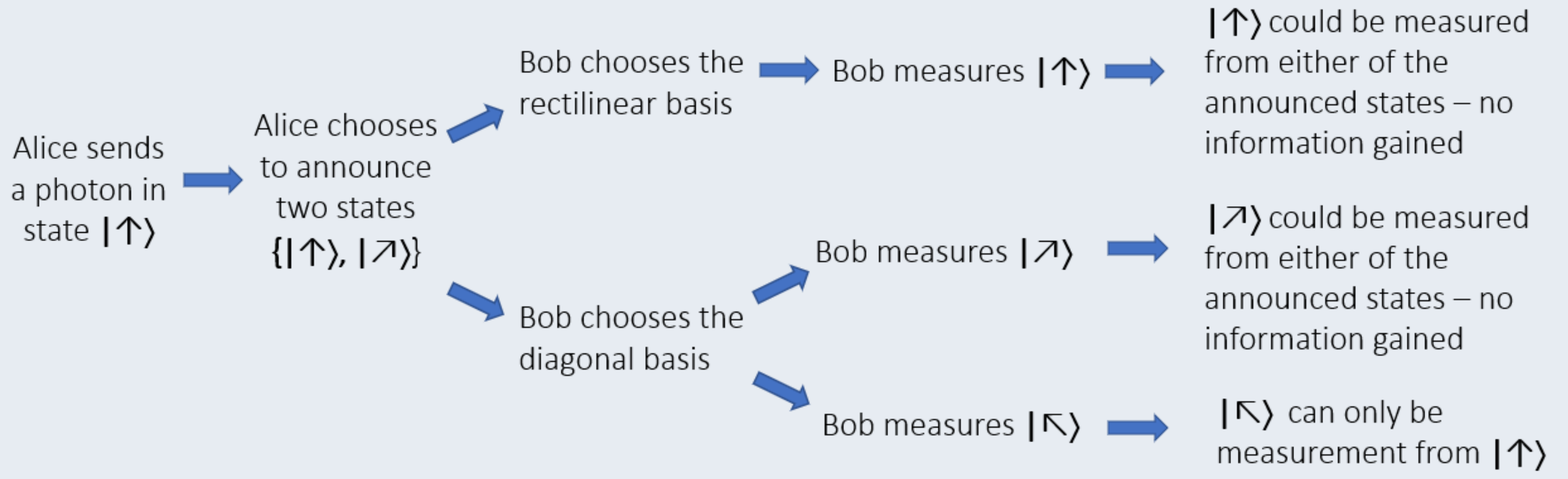

Alice sends a photon in state |↑⟩
Alice chooses to announce two states {|↑⟩, |↗⟩}
Bob chooses the rectilinear basis
Bob measures |↑⟩
|↑⟩ could be measured from either of the announced states – no information gained
Bob chooses the diagonal basis
Bob measures |↗⟩
|↗⟩ could be measured from either of the announced states – no information gained
Bob measures |↖⟩
|↖⟩ can only be measurement from |↑⟩

Figure 5: An example of the sifting process for one bit in SARG04

Conclusion

- Two QKD methods were discussed. Both protocols are computationally secure; an improvement compared to classical encryption techniques such as RSA encryption.
- SARG04 uses the same quantum states as BB84 but a different sifting protocol. The result is far more robust again PNS attacks and hence has a significant advantage when using apparatus that cannot reliably send single photon pulses.
- Experiments have shown these protocols can be implemented successfully.
- Other types of attacks are possible; a variety of other protocols have been devised to be more robust against these attacks [1].

References

[1] S. Pirandola et al. "Advances in Quantum Cryptography". In: *arXiv* (2020).

[2] V. Scarani et al. "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". In: *Physical review letters* 92 (Mar. 2004), p. 057901.

[3] H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* 175 (1984).

[4] C. E. Shannon. "Communication theory of secrecy systems". In: *The Bell System Technical Journal* 28.4 (1949), pp. 656–715.

[5] P. W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. ISSN: 1095-7111.