A First Taste of Quantum Cryptography

Andreas Klappenecker

The Problem

Suppose that two parties (called Alice and Bob) want to share a common secret using public classical and quantum channels.

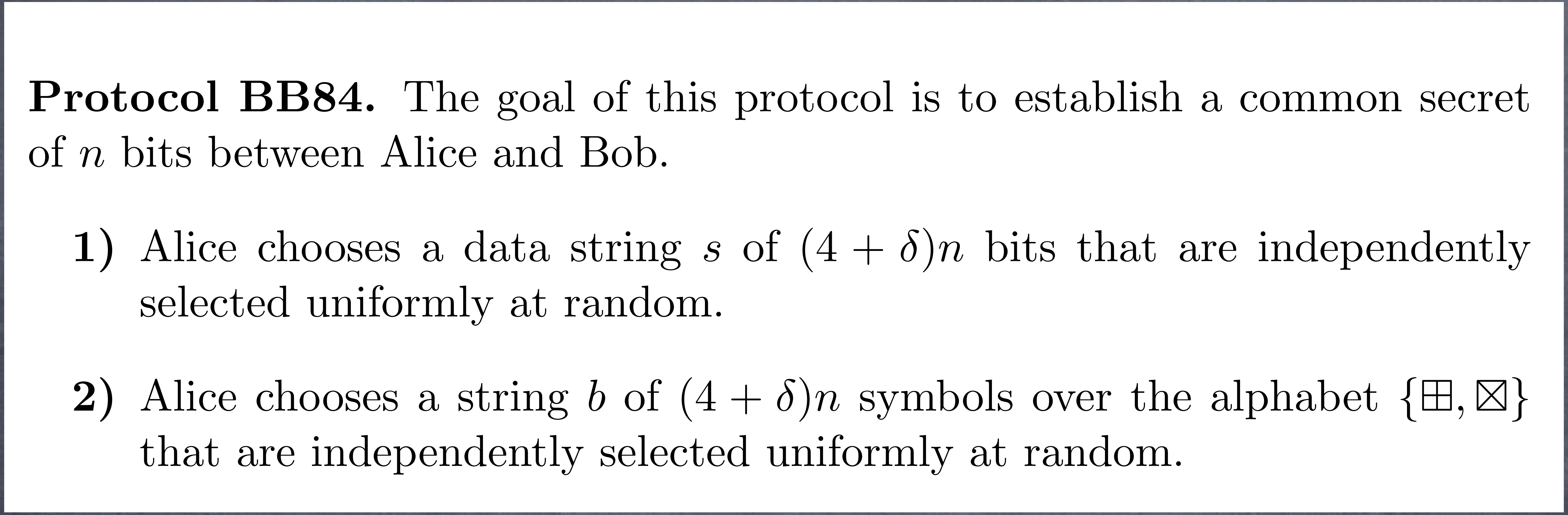
Can they accomplish this or find out whether someone is eavesdropping?

Setup

Alice ------------------photons----------------------> Bob

=============classical bidirectional channel===========

BB84 Protocol

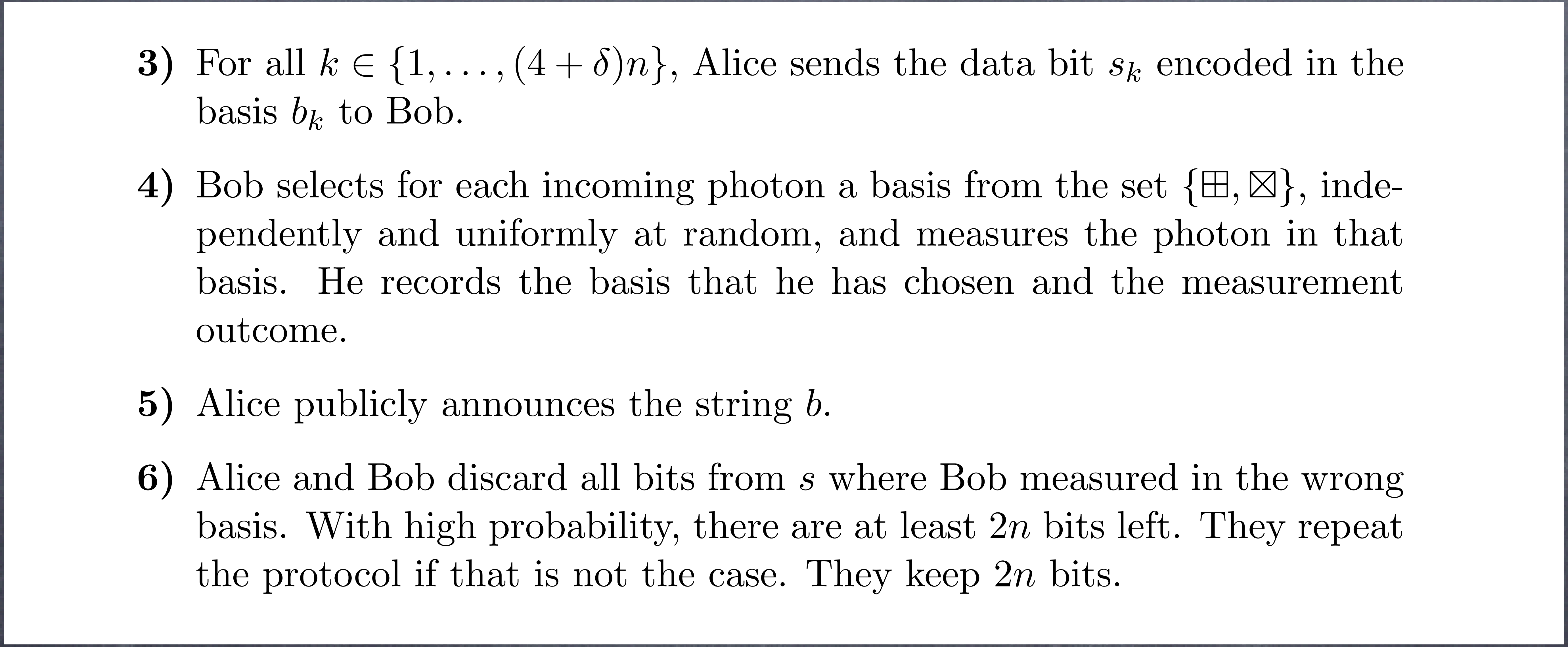


Protocol BB84. The goal of this protocol is to establish a common secret of n bits between Alice and Bob.

1) Alice chooses a data string s of $(4+\delta)n$ bits that are independently selected uniformly at random.

2) Alice chooses a string b of $(4+\delta)n$ symbols over the alphabet $\{\boxplus, \boxtimes\}$ that are independently selected uniformly at random.

BB84 Protocol



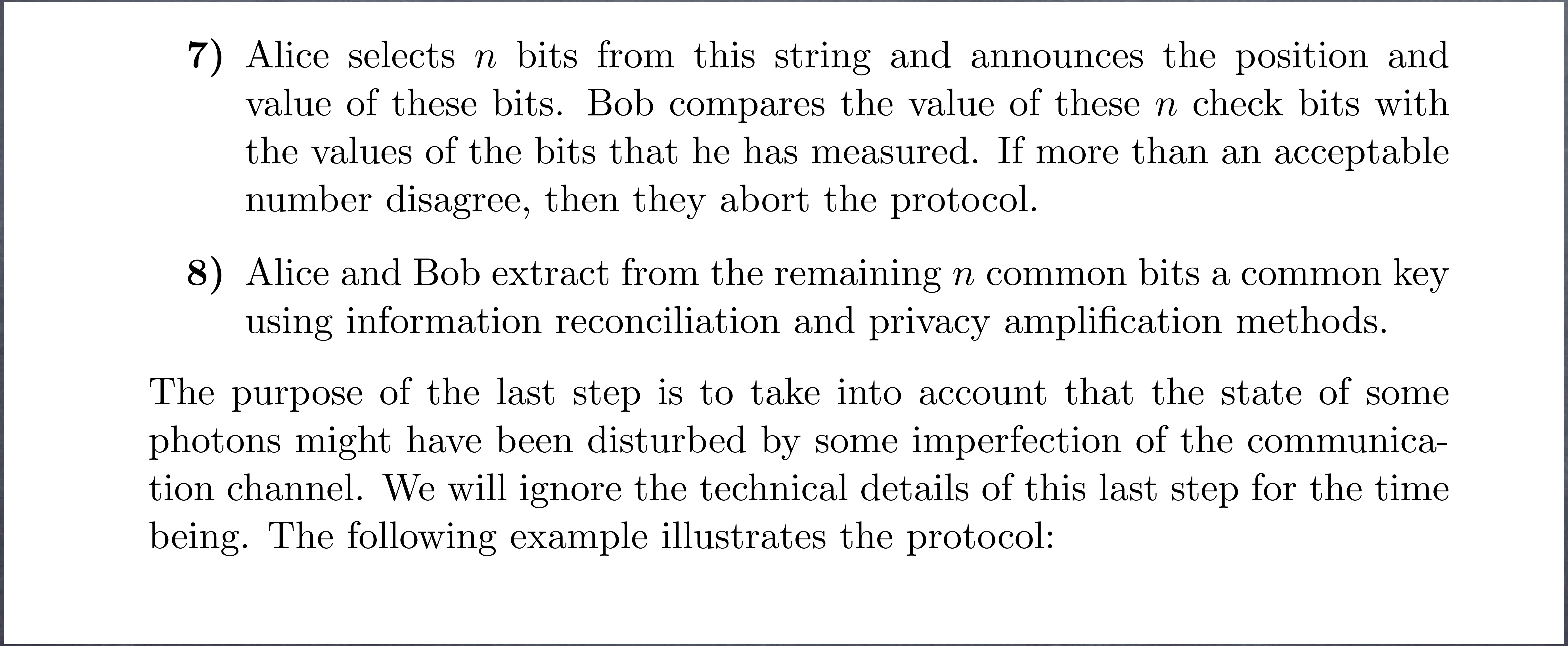
3) For all $k \in \{1, \dots, (4+\delta)n\}$, Alice sends the data bit s_k encoded in the basis b_k to Bob.

4) Bob selects for each incoming photon a basis from the set $\{\boxplus, \boxtimes\}$, independently and uniformly at random, and measures the photon in that basis. He records the basis that he has chosen and the measurement outcome.

5) Alice publicly announces the string b.

6) Alice and Bob discard all bits from s where Bob measured in the wrong basis. With high probability, there are at least $2n$ bits left. They repeat the protocol if that is not the case. They keep $2n$ bits.

BB84 Protocol

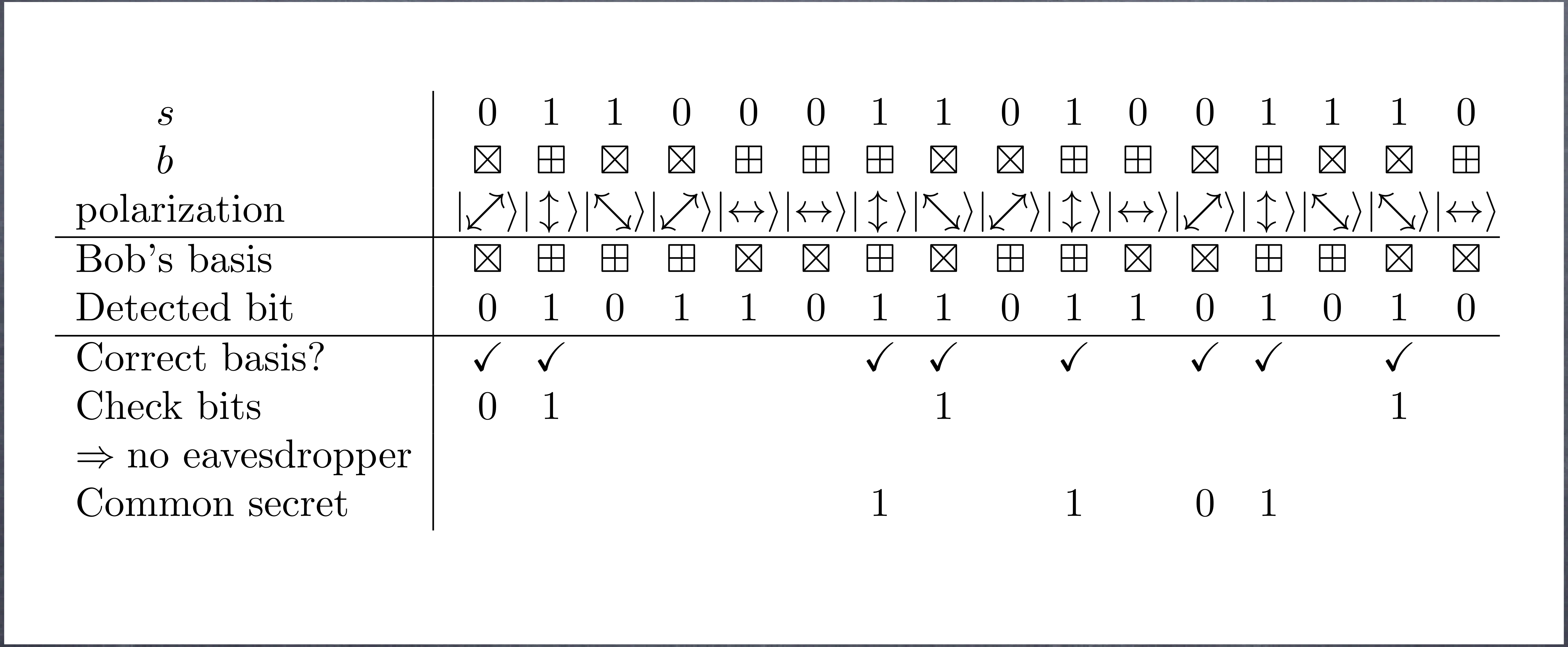


7) Alice selects n bits from this string and announces the position and value of these bits. Bob compares the value of these n check bits with the values of the bits that he has measured. If more than an acceptable number disagree, then they abort the protocol.

8) Alice and Bob extract from the remaining n common bits a common key using information reconciliation and privacy amplification methods.

The purpose of the last step is to take into account that the state of some photons might have been disturbed by some imperfection of the communication channel. We will ignore the technical details of this last step for the time being. The following example illustrates the protocol:

BB84 Protocol



s	0	1	1	0	0	0	1	1	0	1	0	0	1	1	1	0
b	⊠	⊞	⊠	⊠	⊞	⊞	⊞	⊠	⊠	⊞	⊞	⊠	⊞	⊠	⊠	⊞
polarization	|⤢⟩	|↕⟩	|⤡⟩	|⤢⟩	|↔⟩	|↔⟩	|↕⟩	|⤡⟩	|⤢⟩	|↕⟩	|↔⟩	|⤢⟩	|↕⟩	|⤡⟩	|⤡⟩	|↔⟩
Bob's basis	⊠	⊞	⊞	⊞	⊠	⊠	⊞	⊠	⊞	⊞	⊠	⊠	⊞	⊞	⊠	⊠
Detected bit	0	1	0	1	1	0	1	1	0	1	1	0	1	0	1	0
Correct basis?	✓	✓					✓	✓		✓		✓	✓		✓	
Check bits	0	1						1							1	
⇒ no eavesdropper																
Common secret							1			1		0	1			

Remarks

The proof that this protocol is secure (and the missing details of step 8) are beyond the scope of this introduction.

The protocol succeeds with high probability when no eavesdropper is present.