

Alice

Unsifted key: 0x **E199 (1a)**
 0b 1110 0001 1001 1001

Basis choice: 0x **279D (1b)**
 0b 0010 0111 1001 1101

Bob's basis choice: 0x **E269 (2)**
 0b 1110 0010 0110 1001

Matched basis: 0x **3A0B (MB)**
 0b 0011 1010 0000 1011

Matched Key Bits:
 0b ~~1~~~~1~~10 ~~0~~~~0~~~~1~~~~1~~101

Sifted Key Bits:
 0b ~~1~~~~1~~~~0~~~~0~~~~1~~~~1~~1001

Secure Key: 0x **45 (5)**
 7 bits

Public Channel

Step 1: Bob shares his basis choices

Basis choice: 0x **E269 (1b)**

Step 2: Alice shares the matched basis

Matched basis : 0x **3A0B (MB)**

Step 3: Establish secure key

Bob

Measurement result: 0x **644D (1a)**
 0b 0110 0100 0100 1101

Basis choice: 0x **E269 (1b)**
 0b 1110 0010 0110 1001

Matched basis: 0x **3A0B (MB)**
 0b 0011 1010 0000 1011

Matched Key Bits:
 0b ~~0~~~~1~~10 ~~0~~~~0~~~~1~~~~1~~101

Sifted Key Bits:
 0b ~~0~~~~1~~~~0~~~~0~~~~1~~~~1~~1001

Secure Key: 0x **45 (5)**
 7 bits

1. First, Alice copies the unsifted key (1a) and basis choice (1b) from computer. She needs to translate from hex to binary as well.

2a. Alice receives Bob's basis choice from public channel (2), and compares the basis choices (1b) and (2) to obtain the matched basis:

(1b)	(2)	(MB)
0	0	1
0	1	0
1	0	0
1	1	1

2b. Alice then sends the matched basis (MB) to Alice (in hex) through the public channel.

3. From the matched basis (MB), Alice selects the measurement result according to table on the right.

4. After the sifting process, move all the matched bits to the right. Ignore all the non-matching bits.

5. Translate from binary to hex, and count how many bits you have. Finally, you get the key!

1. First, Bob copies the measurement result(1a) and basis choice (1b) from computer. He needs to translate from hex to binary as well.

2. Bob writes his basis choice (1b) on the public channel (in hex), and sends the paper to Alice.

3. After receiving the matched basis (MB) from Alice, Bob selects the measurement result accordingly:

(1a)	(MB)	(3)
0	0	X (removed)
0	1	X (removed)
1	0	0
1	1	1

4. After the sifting process, move all the matched bits to the right. Ignore all the non-matching bits.

5. Translate from binary to hex, and count how many bits you have. Finally, you get the key!