

Von den Lichtteilchen zum Schlüssel

Wie aus Photonen Bits werden

Rathaus (Bob)				BA-CA (Alice)		
1	+/-	0	Alice und Bob speichern: *Nummer des Lichtteilchens (1,2,3...) *Basis, in der das Lichtteilchen gemessen wurde (+/- oder H/V) *Messwerte (0 oder 1)	1	+/-	0
2	H/V	0		2	H/V	0
3	H/V	0		3	+/-	0
4	H/V	0		4	+/-	0
5	+/-	0		5	+/-	0
6	+/-	1	Alice und Bob vergleichen öffentlich: *Nummer des Photons *Basis, in der es gemessen wurde. Sie vergleichen NICHT das Messresultat! Keine Gefahr!	6	H/V	1
7	H/V	1		7	+/-	1
8	+/-	0		8	H/V	0
9	H/V	1		9	H/V	1
10	+/-	0	Alice und Bob streichen jene Werte, deren Basis nicht übereinstimmt	10	+/-	0
11	+/-	1		11	H/V	1
12	+/-	1		12	+/-	1
13	H/V	1		13	H/V	1

Ergebnis: "gesiebter Schlüssel" (engl. Sifted key)

Wurde gelauscht?
Der öffentliche Vergleich eines Teils des Schlüssels ergibt die Fehlerrate. Ist diese über 11,4%, wurde abgehört;

Der Schlüssel
0001011...