In theory, so-called quantum cryptography provides a totally secure way of sending information. In practice, maybe not.

Suppose Alice wants to send Bob a secret message. In ordinary cryptography, she can convert the message to binary numbers—i.e., a string of 0s and 1s—and then scramble it by combining it mathematically with another string of random 0s and 1s, which serves as the key.

Quantum cryptography introduces a twist—literally. Alice passes Bob the key by encoding it in single photons, which can be polarized horizontally to signal a 0 or vertically to signal a 1. If this were all there were to it, then Eve the eavesdropper could also read the key and then pass the photons to Bob. But Alice can also randomly rotate her transmitter to send photons polarized diagonally at plus or minus 45° some of the time. When her transmitter isn't aligned with Bob's receiver, the key transmission becomes ambiguous: For example, if Alice sends a photon polarized at 45° and Bob has his detector set to the horizontal-or-vertical orientation, then according to the rules of quantum mechanics, Bob will register a horizontal click with 50% probability or a vertical click with 50% probability. That's no problem, as after the transmission of stream of photons, Alice and Bob can tell each other for which photons their devices were aligned and use only those to define the key.

All this twisting shuts Eve out. Eve doesn’t know which orientations Alice and Bob are using, and if she guesses wrong she'll disturb the photons in a detectable way.

However, in 2010, an international team of researchers showed that Eve could hack the system by exploiting a weakness in the so-called avalanche photodiodes (APDs) used to detect the individual photons. The problem is that APDs react differently to intense pulses of light than they do to single photons, so that the energy of the pulse must exceed a threshold to register a hit.

If she guessed right and measured the photons with her apparatus in the same orientation as Alice and Bob's, then Bob's apparatus would interpret the bright pulse just like a single photon. But if she guessed wrong, so that she sent Bob a bright pulse whose polarization was off-kilter relative to the orientation of his apparatus, then Bob's apparatus would actually split it into two dim pulses. Neither of these would be strong enough to make Bob's detectors fire.