GUESS AGAIN: UNCONDITIONALLY SECURE PUBLIC-KEY ENCRYPTION (WITH POSSIBLE DECRYPTION ERRORS)

Possible attacks

As we have shown in the proposal narrative, our protocol is IND-CCA2 secure against any passive adversary, even computationally unbounded one. Here we discuss a couple of other standard attacks.

1. KNOWN (OR CHOSEN) PLAINTEXT ATTACK

Security against a computationally unbounded adversary using the KPA or CPA attack is established along the same lines as IND-CCA2 security is established in Proposition 3 in the proposal narrative since in both cases, we allow the adversary to have arbitrarily many (plaintext, ciphertext) pairs.

Suppose the adversary, Eve, has a ciphertext for the "1" bit. That is, Eve has $R = 2000$ pairs (a_i, B_i), together with labels of the intervals $\{x < a_i\}$ by bits, that represent an encryption of 1.

Now suppose Eve sees another 2,000 pairs (a_i, B_i) with the same a_i and the same corresponding B_i, together with the same labeling of intervals as before. What is the probability that this is again an encryption of 1? We claim that this probability is $\frac{1}{2}$. To see this, let us look at a particular pair (a, B). According to the protocol, Alice's choice of labeling the interval $\{x < a\}$ was done with probability $\frac{1}{2}$, determined by the choice between the number of steps (either $f(n)$ or $g(n)$) in her random walk and between the conditions $A > B$ and $A < B$, both choices with probability $\frac{1}{2}$. Thus, for any particular a, labeling the interval $\{x < a\}$ with the "0" bit or with the "1" bit is equally likely, from Eve's perspective. To see why this does not mean that the probability for Alice to transmit her bit correctly is also $\frac{1}{2}$, see Section 3.3 in the narrative part of the proposal.

The same argument applies if Eve has not one but many ciphertexts for the "1" (or "0") bit.

2. IMPERSONATION ATTACKS

Any public-key encryption scheme is vulnerable to impersonation attacks, where the adversary impersonates one of the parties (typically, the receiver). This is why a public-key encryption scheme is usually accompanied by an authentication protocol to authenticate the receiver.

We do not contribute anything new as far as authentication procedures are concerned, which may or may not be considered a weakness of our scheme. In most real-life applications though, authenticity of the receiver (such as an online bank or an online retailer) is not a concern since a sender typically initiates an exchange herself by connecting to a trusted website. Thus, impersonating the receiver is problematic for an adversary in this scenario. On the other hand, impersonating the sender usually has no benefits for the adversary.