Special Soundness of Fiat-Shamir sigma-protocol

Number : 199606131115

Our aim is to retrieve the secret key used in a eavesdropped Fiat-Shamir protocol. We have got several runs of the protocol and sometimes the random value sent to the verifier, R, is the same. Our first task is so to find which runs give the same value of R.
For that, we just add two for loops to compare all the R values of each run together. When we have couple of R values equal, we can stop, there is no need to have two couples as one couple is sufficient to retrieve the secret key.
As we know that c can take the value 0 or 1, we put the value of s when c = 0 in variable sc0 and the value of s when c = 1 in sc1.
We now have two different values of s, sc0 = $R^{1/2}*x^0$ (mod N) and sc1 = $R^{1/2}*x^1$ (mod N). To compute the secret key, we just have to compute the modular inverse of sc0, so we have $(R^{1/2})^{-1}$ (mod N) as x^0 is equal to 1, then we multiply sc1 with $(R^{1/2})^{-1}$ (mod N) so we obtain x^1 (mod N). We compute x^1 (mod N) and we obtain x^1 or x. The message is decrypted with this key.

Decoded text: A common mistake that people make when trying to design something completely foolproof is to underestimate the ingenuity of complete fools. - Douglas Adams