Question

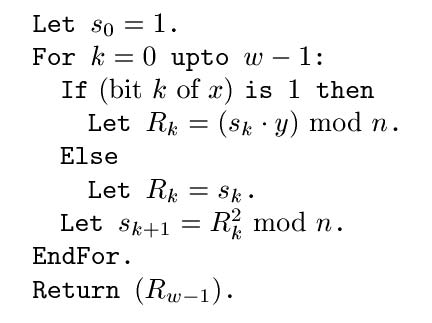
1. What kind of information that leaked from Cryptographic Devices can be utilized to apply side-channel attack?(list at least 3)
2. In what situation you would choose SPA to attack? And how about DPA?
3. Take the AES-128 algorithm as an example, the key size is 128bit(16bytes Ki,i=1~16)

Then use DPA to attack AES-128, how many tests do you need for per Ki? And what’s the total number of tests to recover the whole 128bit key?

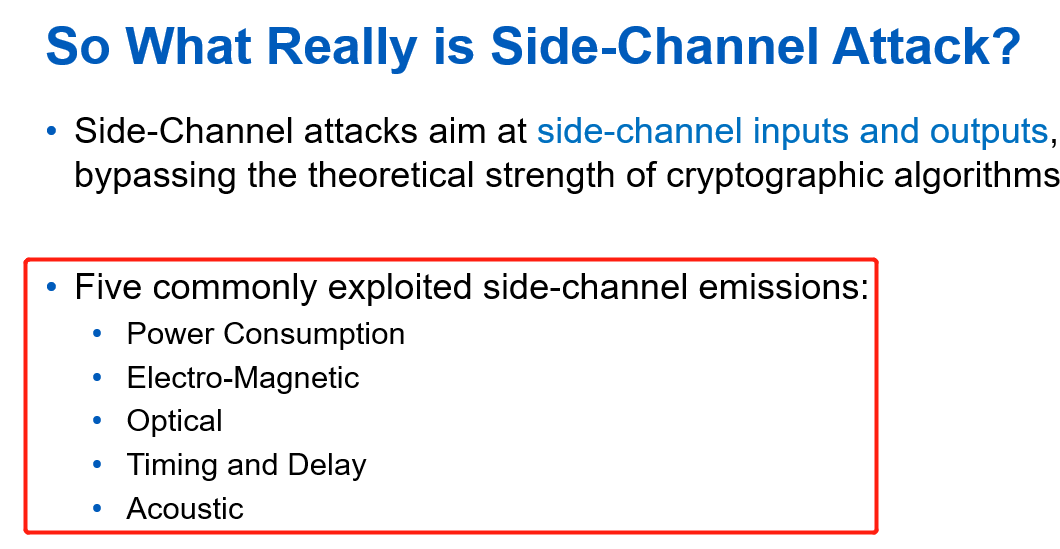
1. Assume that there is a 5-bit key in RSA. The computation of the RSA decryption is shown below.

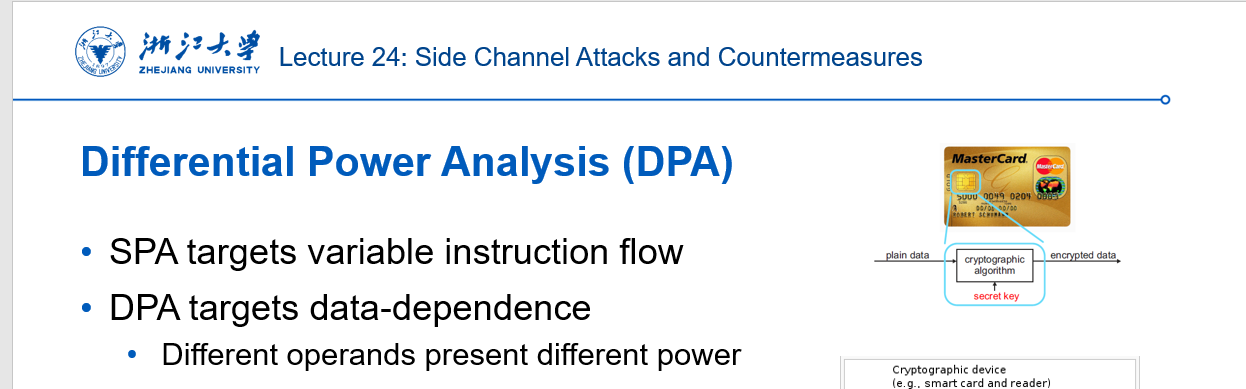
Assume that the power consumption model of “multiply and mod” is M, and the consumption model of assignment is A.

Now we observe one power consumption trace and it shows model sequence like: MAAMAMAA. So what’s the predicted key do you think is corresponding to this power consumption?

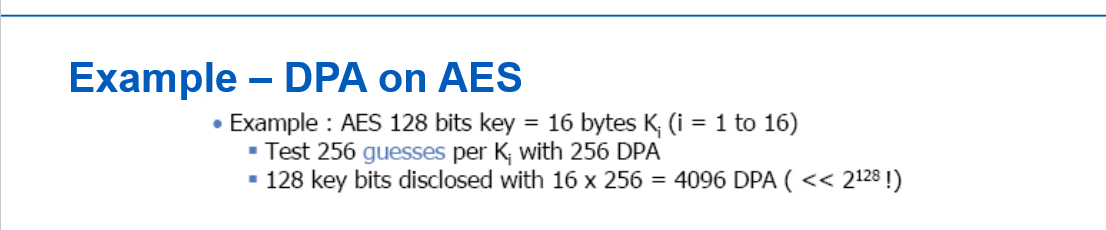


Answer:

1. page15
2. page35



1. page48



4.10110