[secure PRF or not](http://crypto.stackexchange.com/questions/30767/secure-prf-or-not)

I am new in Cryptography and I saw this question in a note I solved it but I'm not sure about my answers.

Let F:{0,1}n×{0,1}n→{0,1}nF:{0,1}n×{0,1}n→{0,1}n be a secure PRF (i.e. a PRF where the key space, input space, and output space are all {0,1}n{0,1}n) and say n=128n=128. Which of the following is a secure PRF. In the following functions, + operation indicates the binary sum module 2n2nwhere an n-bit string is interpreted as number in Z2nZ2n and ≪≪ operation indicates left rotation.

1. F'(k1||k2),x)=F(k1,x)⊕F(k2,x)F′(k1||k2),x)=F(k1,x)⊕F(k2,x)
2. F'(k,x)=(x+k)⊕(x≪1)F′(k,x)=(x+k)⊕(x≪1)
3. F'(k,x)=(x+k)⊕(k≪1)F′(k,x)=(x+k)⊕(k≪1)
4. F'(k,x)=(x+k)⊕(k≪1)⊕(x≪1)F′(k,x)=(x+k)⊕(k≪1)⊕(x≪1)

I think number 1 is PRF because the input key of each F is different, and number 2, 3, 4 are PRF because x+kx+k term could be any string of {0,1}n{0,1}n. Is that correct?

[solution](http://crypto.stackexchange.com/questions/30767/secure-prf-or-not)

Here's a more elaborate proof for number 1. Given a distinguisher D′D′ for F′F′, we construct a distinguisher DD for FF as follows: we first pick a uniform k2k2 of length nn, and we run D′D′. When D′D′ asks to call its oracle on a string xx, we give it OD(x)⊕Fk2(x)OD(x)⊕Fk2(x) instead of OD′(x)OD′(x), where ODOD (resp. OD′OD′) is the oracle of DD (resp. D′D′). At the end, we output whatever D′D′ outputs.

If ODOD implements Fk1Fk1 for a uniform k1k1, OD(x)⊕Fk2(x)OD(x)⊕Fk2(x) will be distributed identically to F′k1||k2(x)Fk1||k2′(x) for a uniform k1||k2k1||k2, whereas if ODOD implements a uniform ff, it will be distributed identically to f(x)f(x) for a uniform ff. Those two cases can be distinguished by D′D′ by hypothesis, and thus DD can distinguish Fk1Fk1 from a uniform ff.