Minimalism in Cryptography: The Even-Mansour Scheme Revisited

Orr Dunkelman, Nathan Keller, and Adi Shamir

Haifa University, Bar-Ilan University, and The Weizmann Institute

April 17-th 2012

Minimal Constructions

- A construction is minimal if it cannot be simplified by eliminating any one of its components

Minimalism is a Very Popular Topic in Cryptography:

There are many papers on:

- Minimal cryptographic assumptions
- Minimal key sizes
- Minimal # rounds in Feistel structures
- Minimal # of honest parties in Protocols
- .....

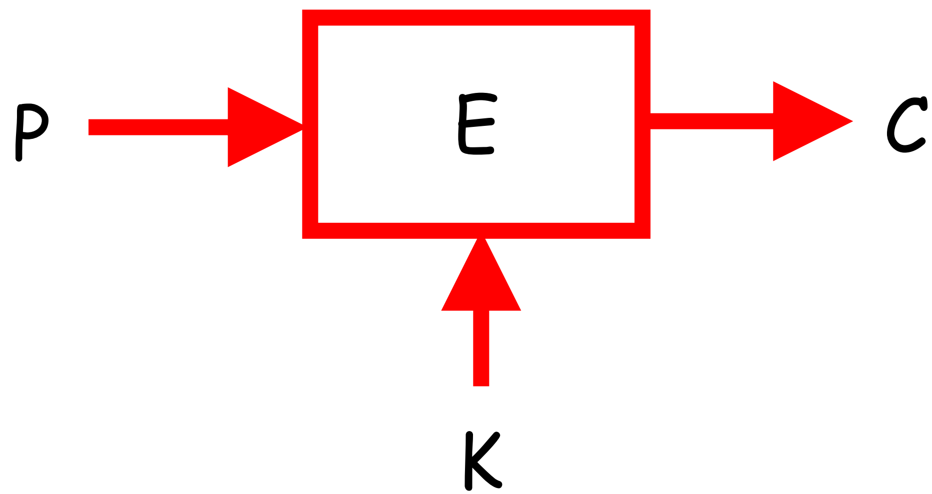
Minimal Provably Secure Stream Ciphers:

- The one time pad:

Ciphertext = Plaintext + Key

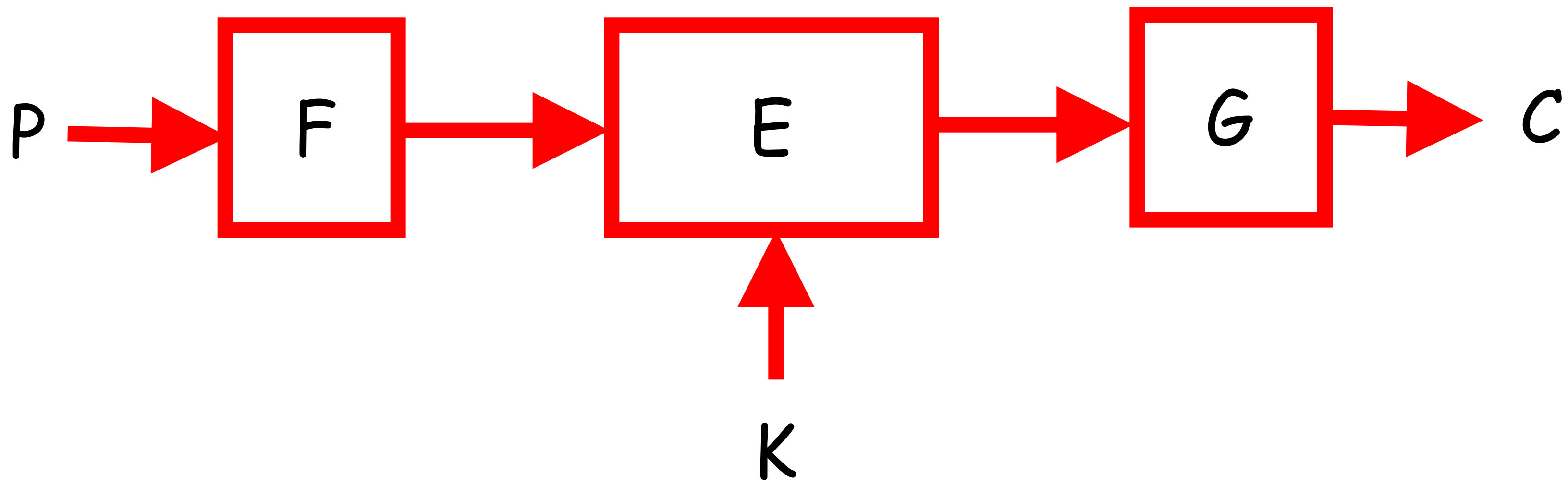
Minimal Provably Secure Block Ciphers:

- At Asiacrypt 91, Even and Mansour tried to construct the simplest possible block cipher which has a formal proof of security:



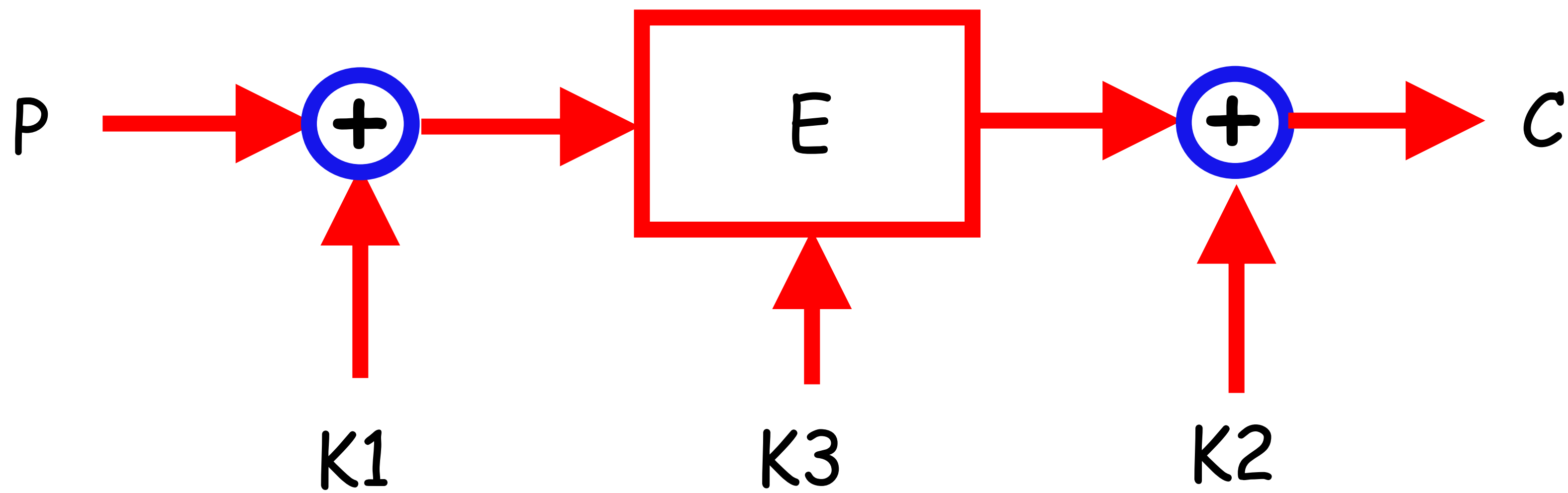
Minimal Block Ciphers:

- In a minimal construction, there should be no key-independent invertible operations F and G which are applied to the plaintext or ciphertext



Minimal Block Ciphers

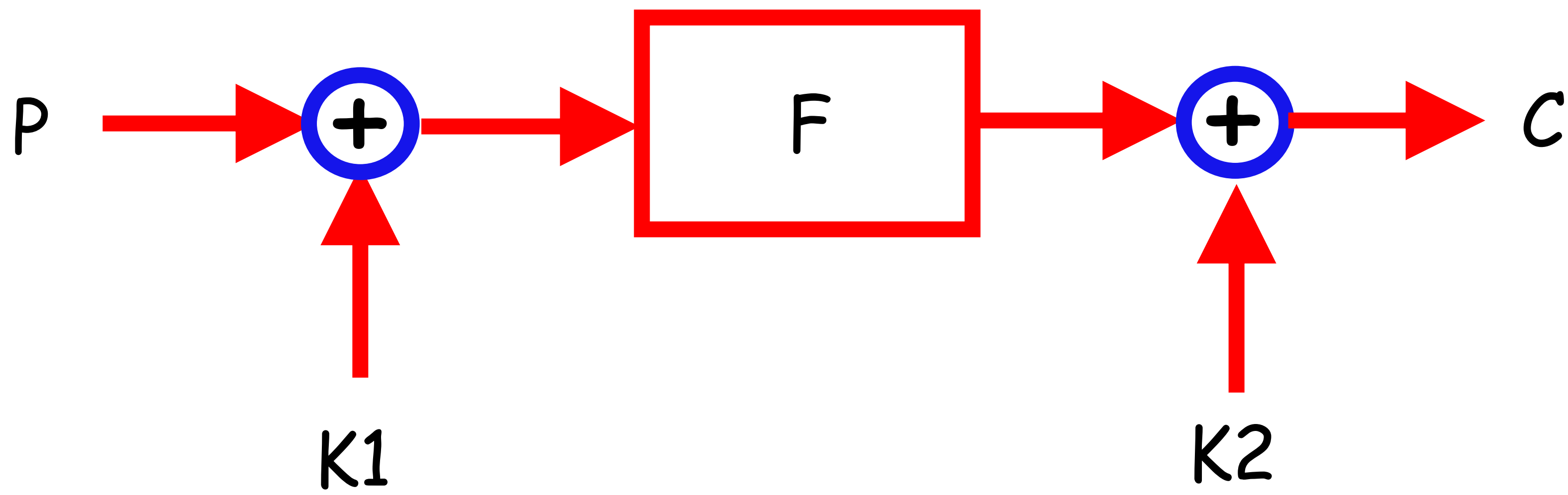
- The simplest way to process the plaintext and ciphertext in a key dependent way is to XOR to them a prewhitening key K1 and a postwhitening key K2:



The Even-Mansour Scheme:

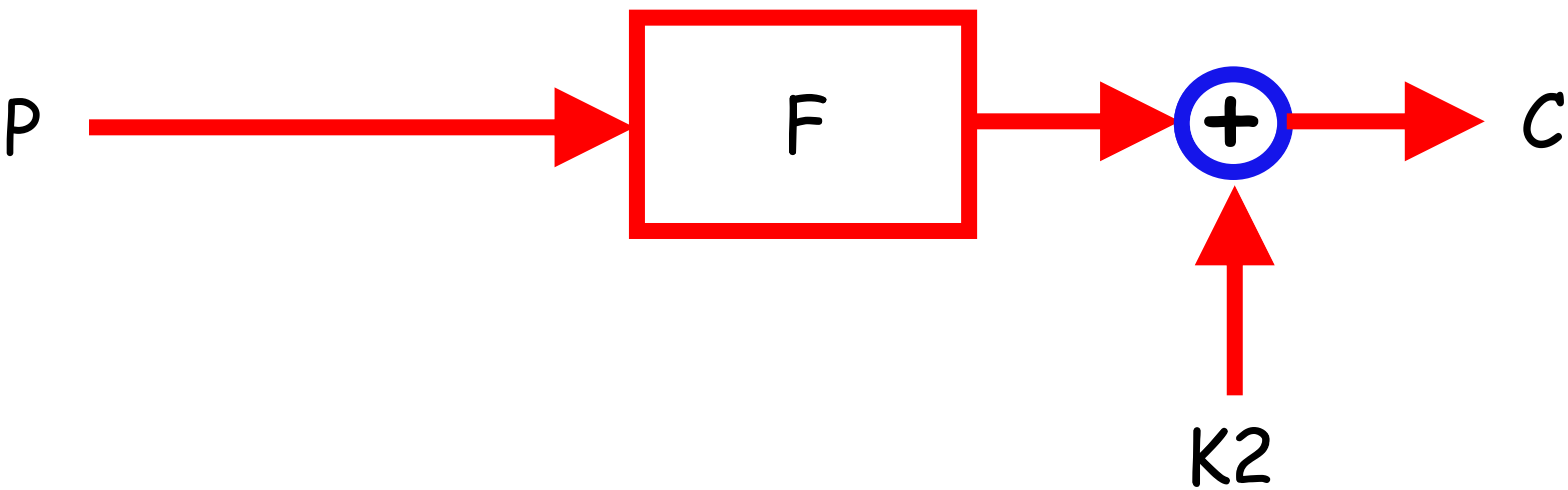
- Replace the middle part by a single, publicly known, randomly selected, keyless permutation F:

|state|=n bits |key|=2n bits



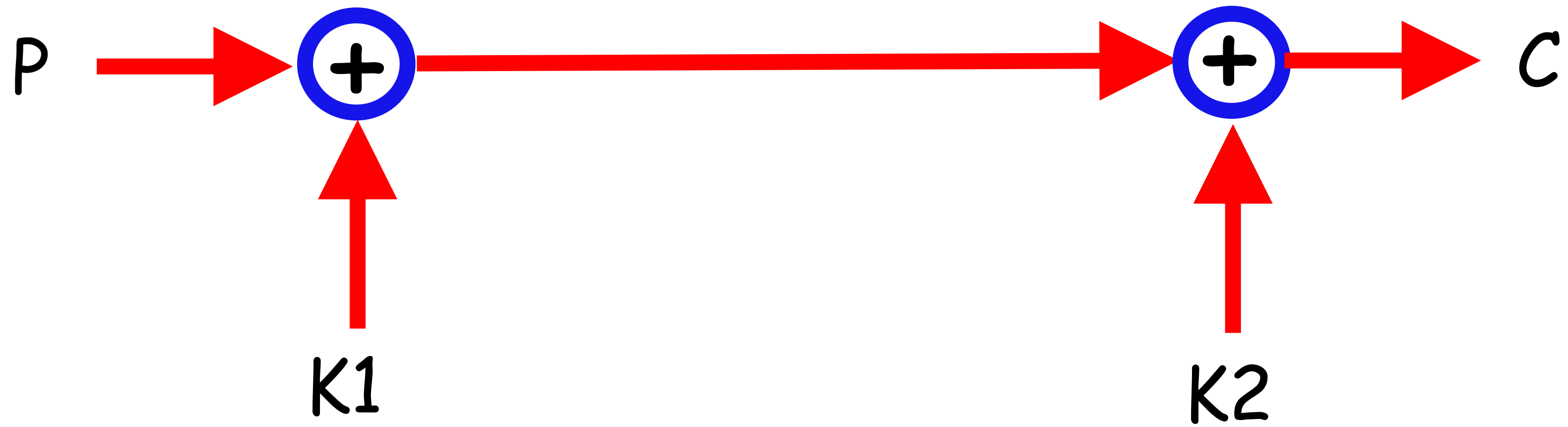
The Minimality of the Even-Mansour Scheme:

- Eliminating either K1 or K2 makes the scheme easily breakable since F is known



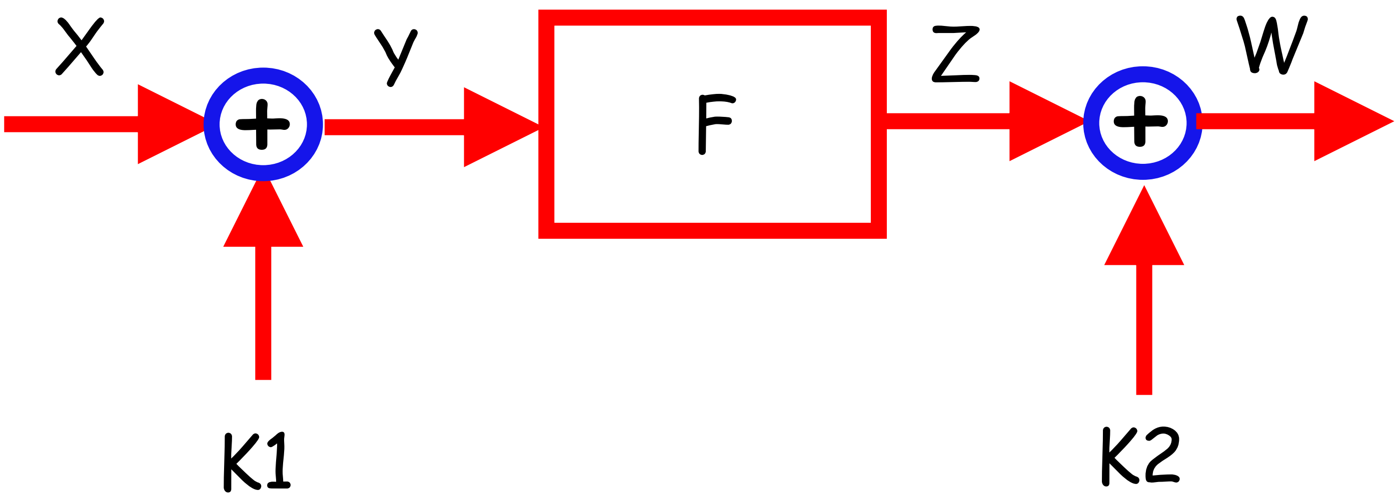
The Minimality of the Even-Mansour Scheme:

- Eliminating F makes the scheme linear



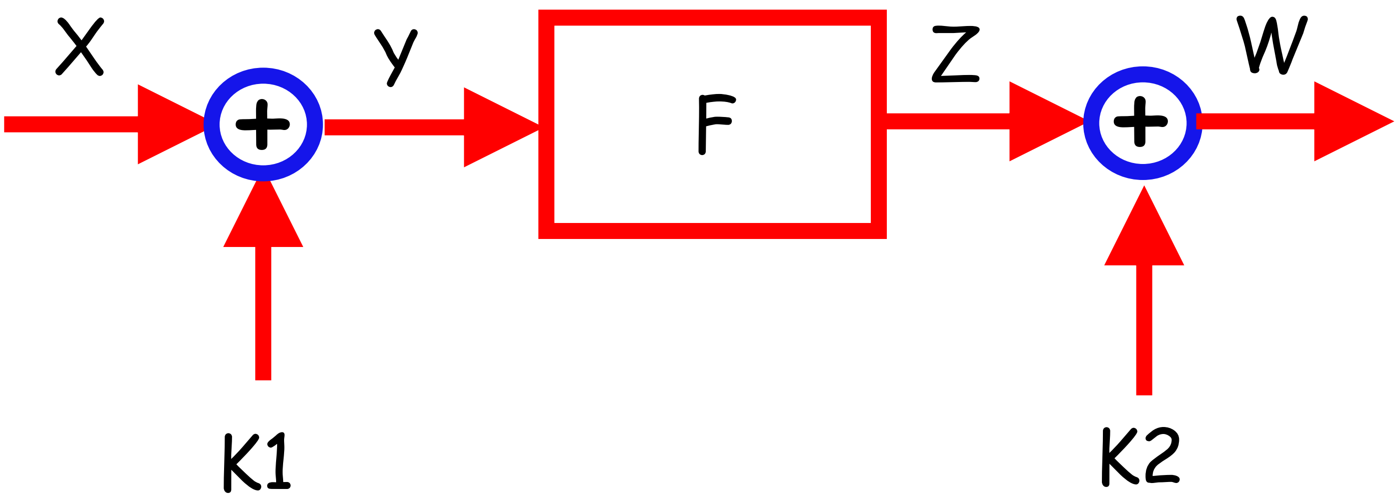
To Study the Exact Security of EM, We Have to Formalize an Attack Model:

- Consider the following 4-tuple of values in each encryption E(x)=w



To Study the Security of EM, We Have to Formalize an Attack Model:

- The attacker is allowed to ask for D pairs of known or chosen (X,W) values (D stands for data)
- The attacker is allowed to evaluate (by himself) T pairs of (Y,Z) values (T stands for time)



Important Remarks:

- We are old fashioned cryptanalysts here: A successful attack means complete key recovery

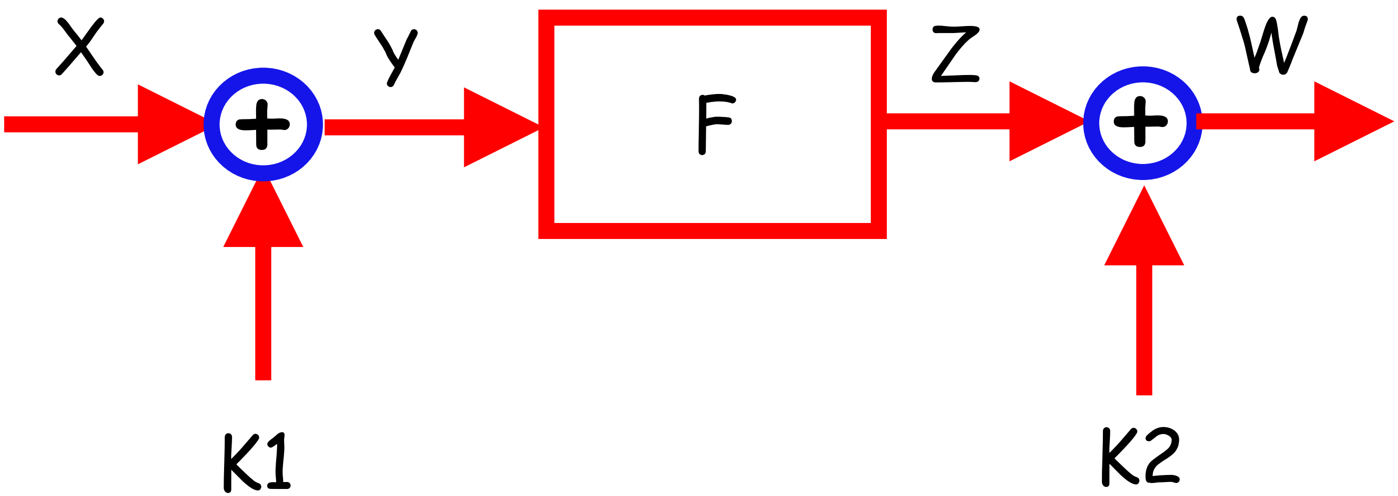
- We distinguish between cheap queries to F and expensive queries to E

Is the Even-Mansour Scheme Secure?

- In their original paper, Even and Mansour formally proved that any attack must satisfy $DT > \Omega(2^n)$
- The lower bound proof is information theoretic, and is applicable both to known plaintext attacks and to chosen plaintext attacks

The EM Proof of Security (Simplified)

- Initially there are 2^{2n} possible keys (K1,K2)
- Given D pairs of (X,W) values of E and T pairs of (Y,Z) values of F, we can combine them in DT possible ways into a 4-tuple of values (X,Y,Z,W)

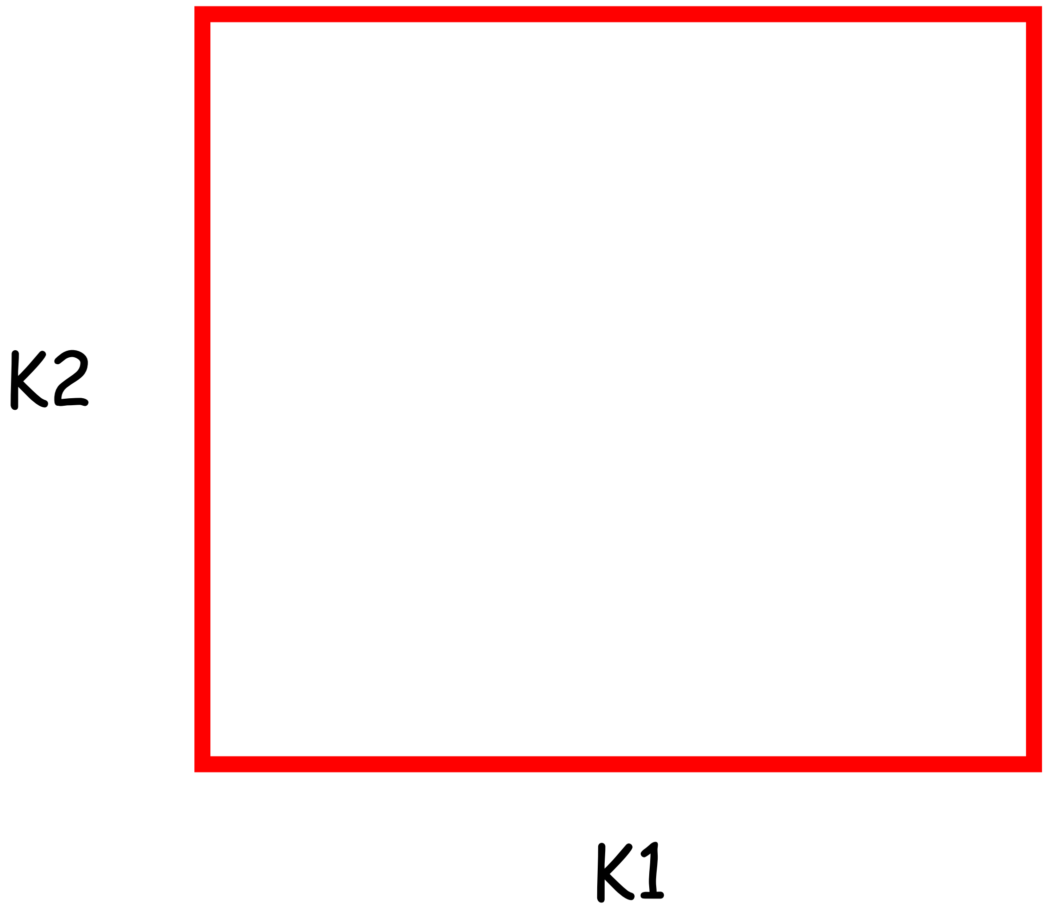


The EM Proof of Security (Simplified)

- Each 4-tuple suggests a unique value for the two keys via K1=X+Y and K2=Z+W
- We cannot say that these values are correct. However, we can say that for each K1 all the other values of K2 are certainly incorrect
- Similarly, for each K2 all the other values of K1 are certainly incorrect

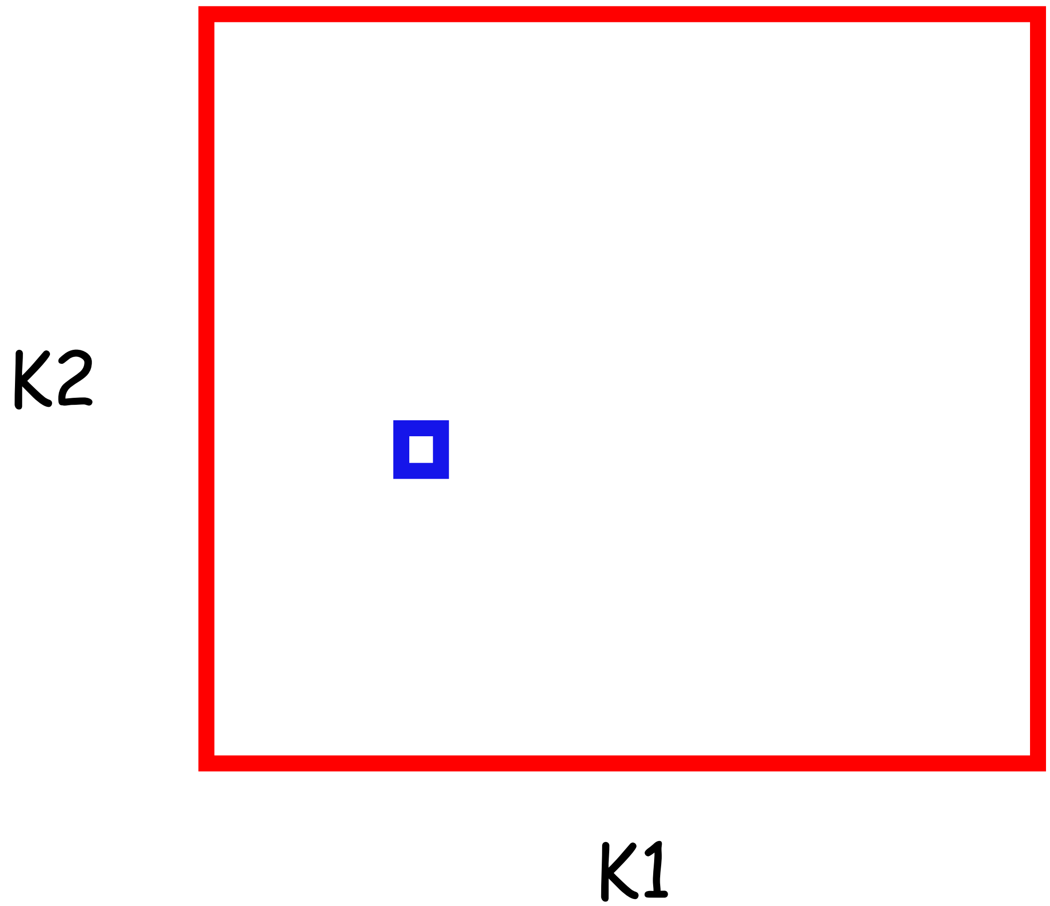
The EM Proof of Security (Simplified)

The 2^{2n} key combinations:



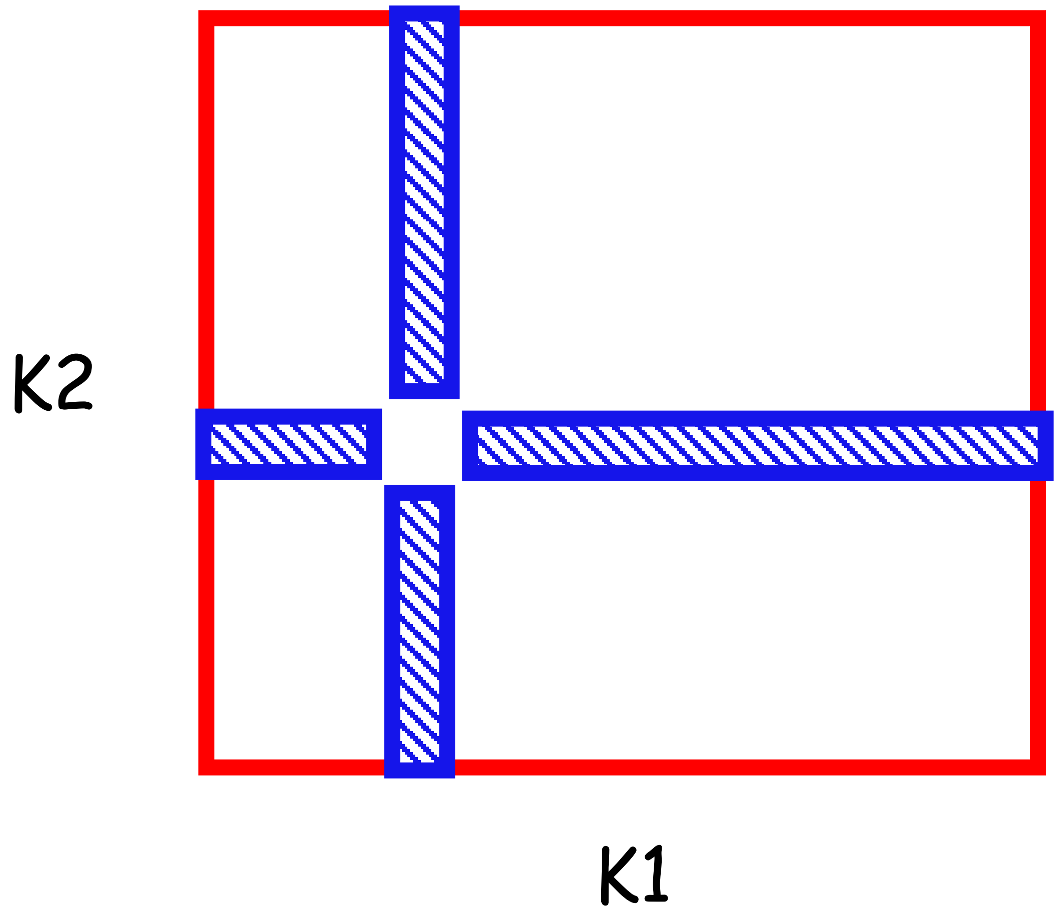
The EM Proof of Security (Simplified)

Each 4-tuple defines a unique suggestion for the keys:



The EM Proof of Security (Simplified)

We can thus erase the following keys as impossible:



The EM Proof of Security (Simplified)

- Each one of the DT possible 4-tuples can eliminate at most $2(2^n-1)$ key pairs (K1,K2)
- To eliminate all the $2^{2n}-1$ wrong key pairs, the number of 4-tuples DT must be at least $(1/2)2^n$

An Interesting Comment:

- The proof is actually quite subtle, and formalizing it requires great care.
- To demonstrate the subtlety, consider the special case in which the random permutation F is a random involution (i.e. for all X, $F(F(X))=X$)
- The only way this affects the simplified proof given above is that whenever we query F and learn that $F(X)=Y$, we get another value of F (namely, that $F(Y)=X$) for free, so this can at most halve the number of required queries to F

In This Involutional Variant of EM:

- We can actually find K1 XOR K2 (and thus eliminate the vast majority of the wrong keys) by:
  - asking only $D=2^{n/2}$ queries of E
  - asking $T=0$ queries of F

- which seems to contradict the lower bound proof that $DT > 2^n$

Going Back to Random Permutations, Can We Find Matching Upper Bounds?

- It is easy to find attacks with:
  - $D=2$, $T=2^n$
  - $T=2$, $D=2^n$

- Can we connect these extreme cases with a known plaintext attack that matches the lower bound curve $DT = O(2^n)$ for any combination of D and T?

Previously Published Attacks:

- At Asiacrypt 1991, Joan Daemen described a simple differential attack with any T and D satisfying $DT = O(2^n)$, which matches the lower bound curve, but requires chosen plaintexts

- At Eurocrypt 2000, Biryukov and Wagner described an advanced slide attack against Even-Mansour, which uses known plaintexts, but matches the lower bound curve only at one point: $D=2^{n/2}$ and $T=2^{n/2}$

Daemen's Chosen Plaintext Attack:

- Consider the differential properties of F.
- Since it is a random permutation, we expect each combination of a particular input difference and a particular output difference of F to be generated from a single pair of input values and a single pair of output values.

Daemen's Chosen Plaintext Attack:

- Notice that the XOR'ing of keys to the inputs and outputs in the Even-Mansour scheme does not change the input/output differences of F!

- The main problem is that going back from differences to values is a difficult task

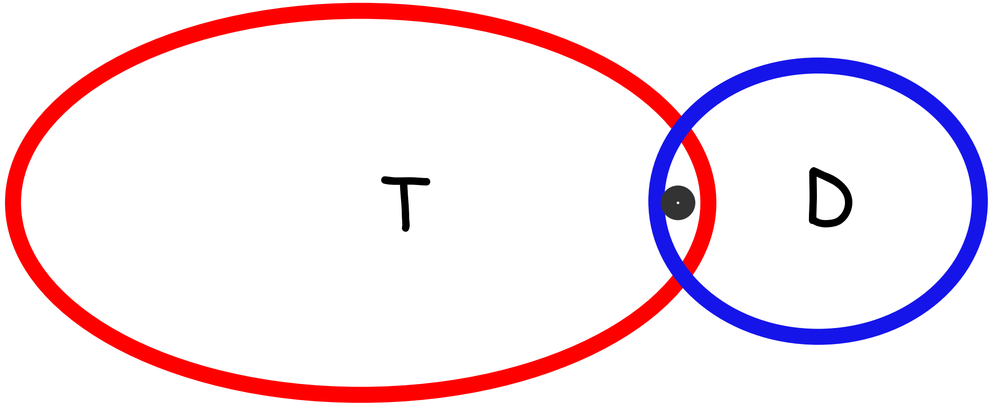
Daemen's Simple Solution:

- Prepare D pairs of chosen plaintexts with a fixed non-zero input difference d, ask to see their encryptions through E, and compute their output differences

- Prepare another set of T pairs of chosen values with the same input difference d, and compute by yourself through F their output values (and thus their output differences)

Daemen's Simple Solution:

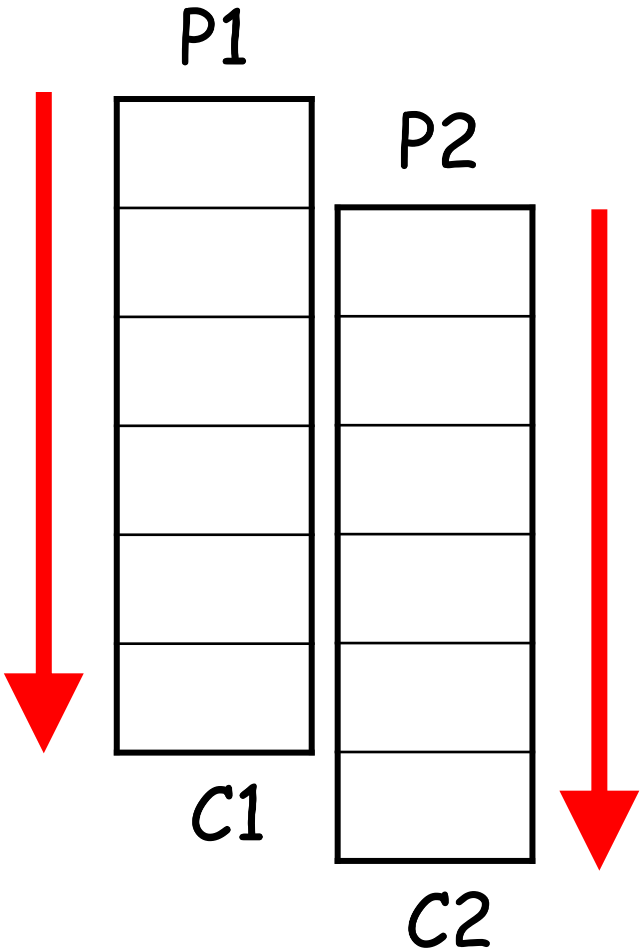
- By the birthday paradox, when $DT > 2^n$ we expect to find some common output difference in the two sets of difference values
- Since the actual input/output values in T are known, we can find the (Y,Z) values in an actual encryption in D. By combining these (Y,Z) values with (X,W) values, we can easily recover both K1 and K2



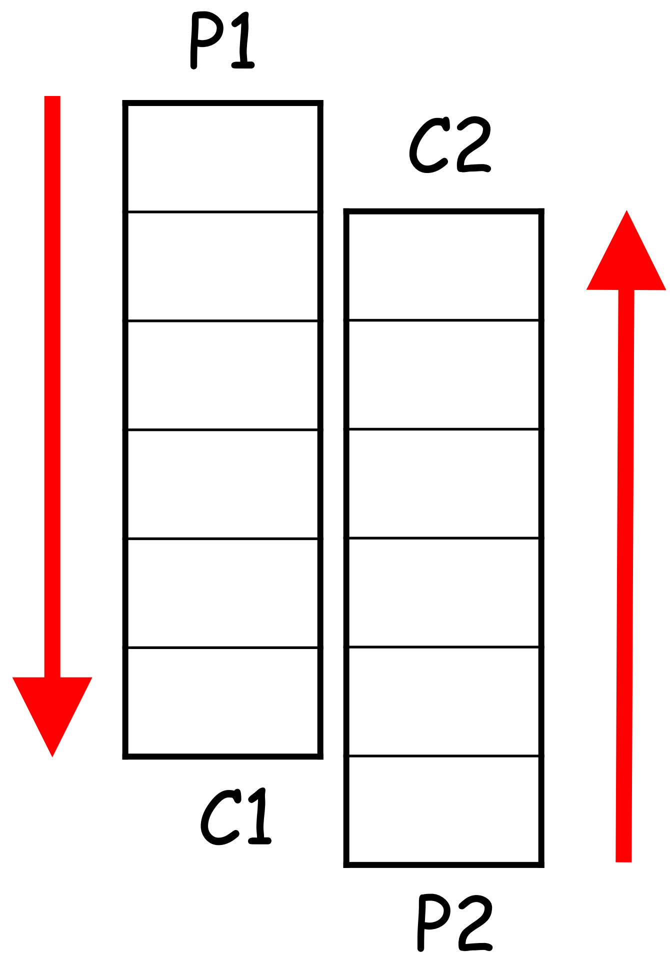
Ten Years Later, Biryukov and Wagner Finally Developed a Known Plaintext Attack:

- Their attack is an advanced version of a slide attack
- Slide attacks are usually applied to iterated cryptosystems with a lot of self similarity under shifts
- This is surprising, since the Even-Mansour scheme is not an iterated cryptosystem and does not seem to have any self similarity

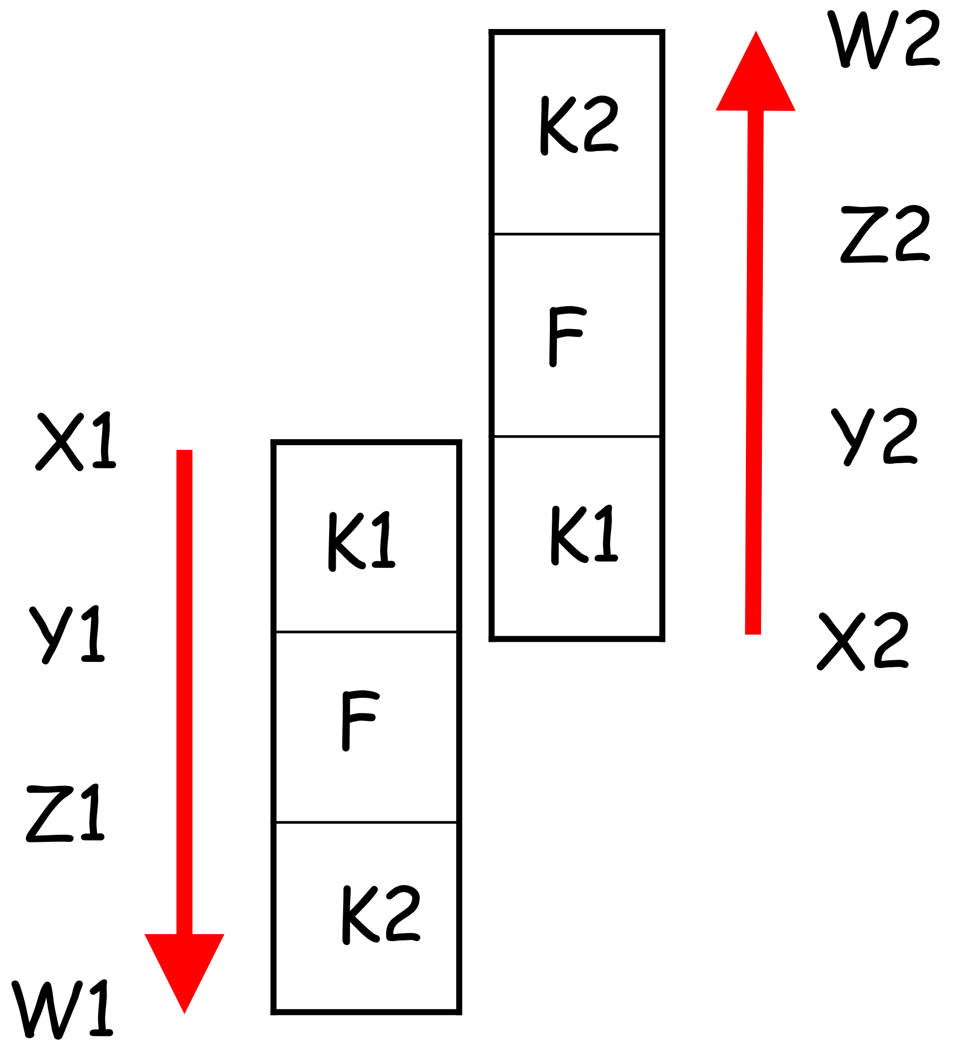
Standard slide attacks try to identify and use shifted versions of the encryption process:



A Slide with a Twist attack uses shifted versions of an encryption and a decryption process:



In this advanced form, Even-Mansour has a very minimal form of self similarity:



The Biryukov and Wagner Known Plaintext Attack on Even-Mansour:

- Given at least $D=2^{n/2}$ known plaintext/ciphertext pairs, we expect to find such a slid pair among them, in which X in one encryption happens to be equal to Y in another encryption

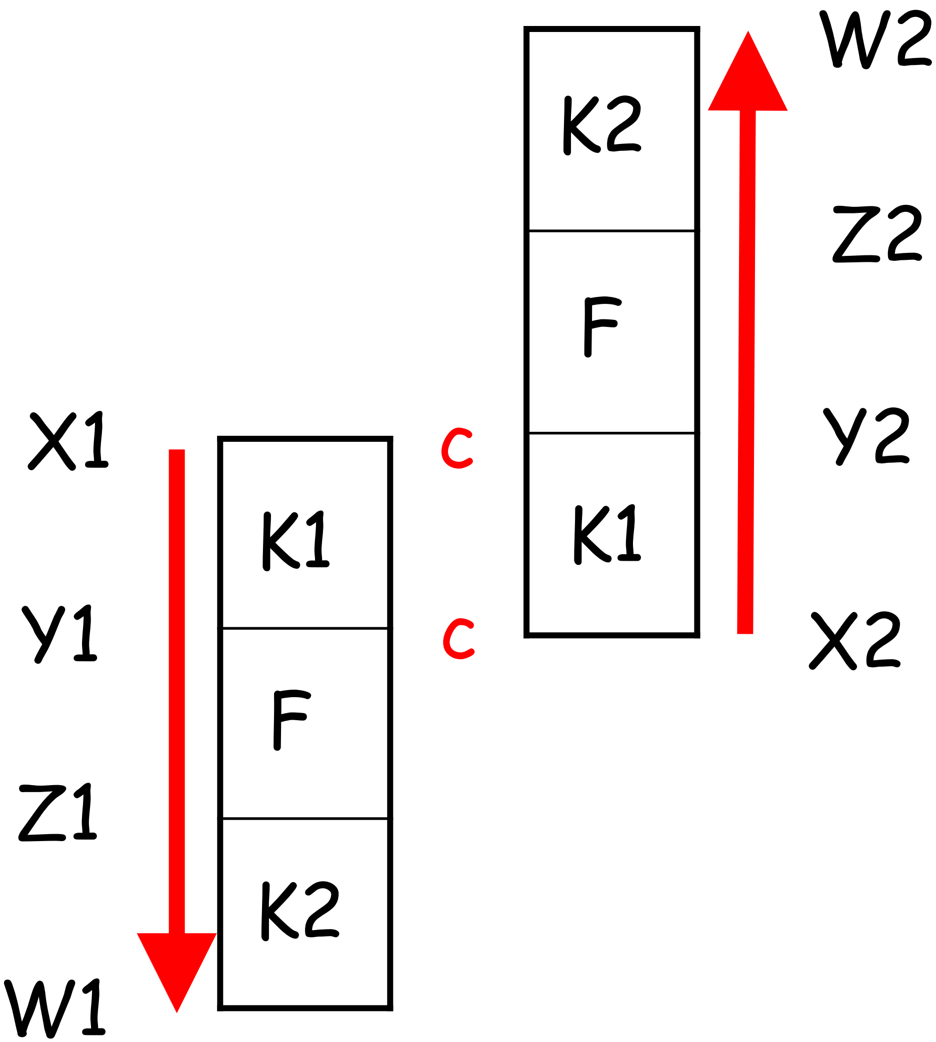
- Slid pairs can be efficiently recognized, and once they are found they can be used to recover the key by solving the resultant equation

Can you exploit a smaller number of known plaintext/ciphertext pairs?

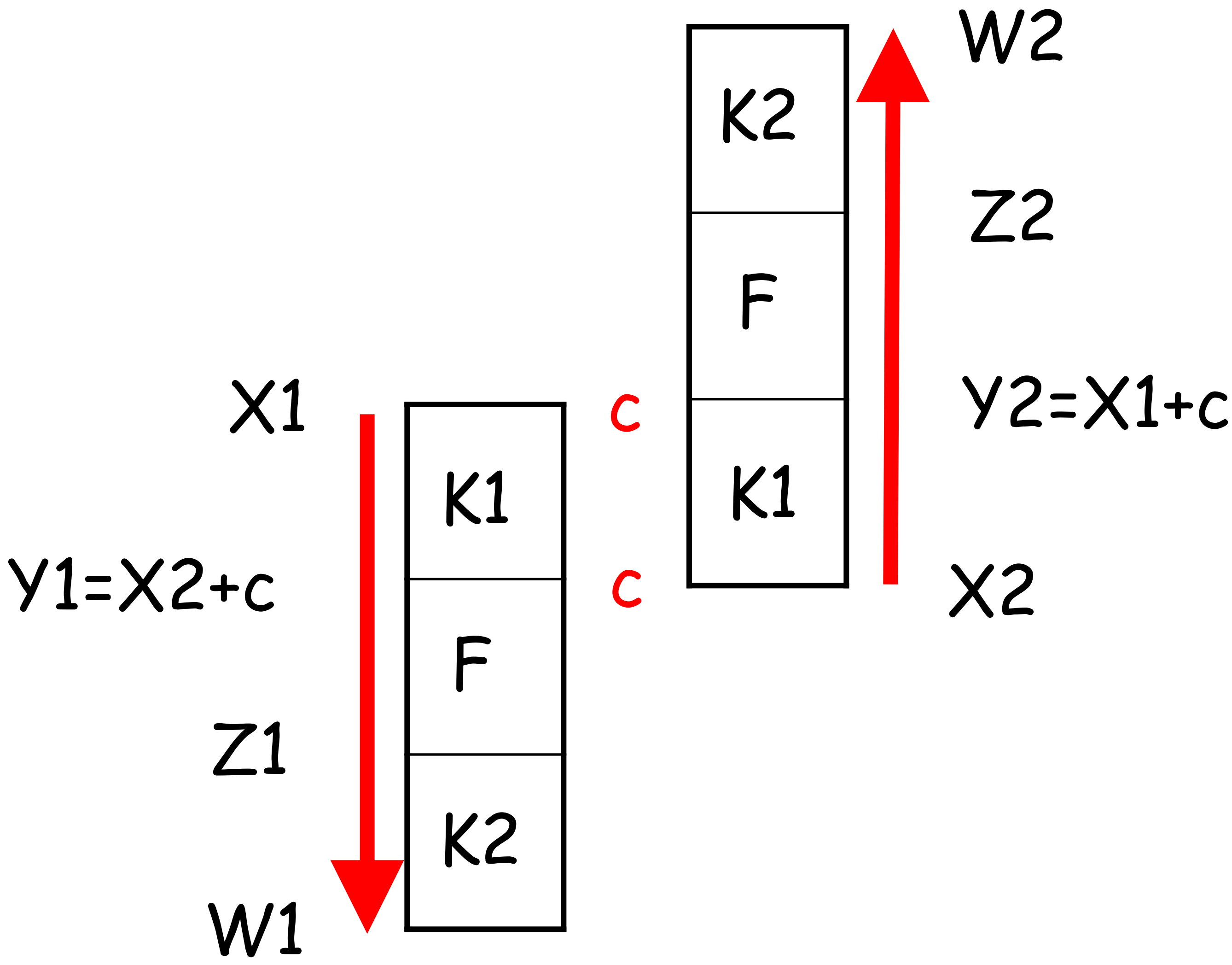
- Since data is much harder to get than time, $D=T=2^{n/2}$ is not the ideal point on the tradeoff curve $DT = 2^n$

- Slide attacks (like many other cryptanalytic techniques, including differential attacks) can not effectively exploit a small number of known plaintexts, since they have to wait for some lucky event to happen by chance, and only then start the attack

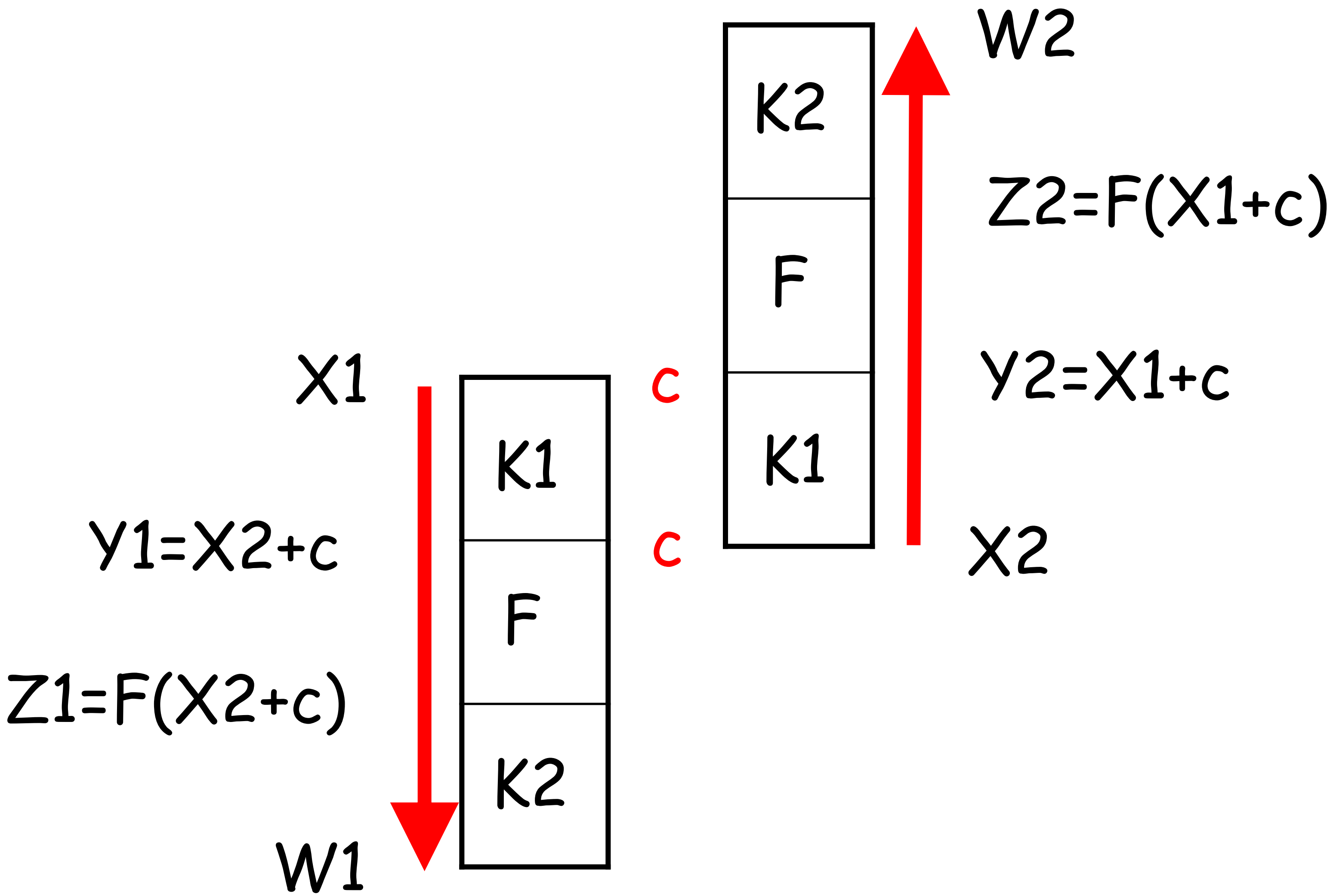
Our New SLIDEX Cryptanalytic Technique: A Slide Plus a Twist Plus a Difference



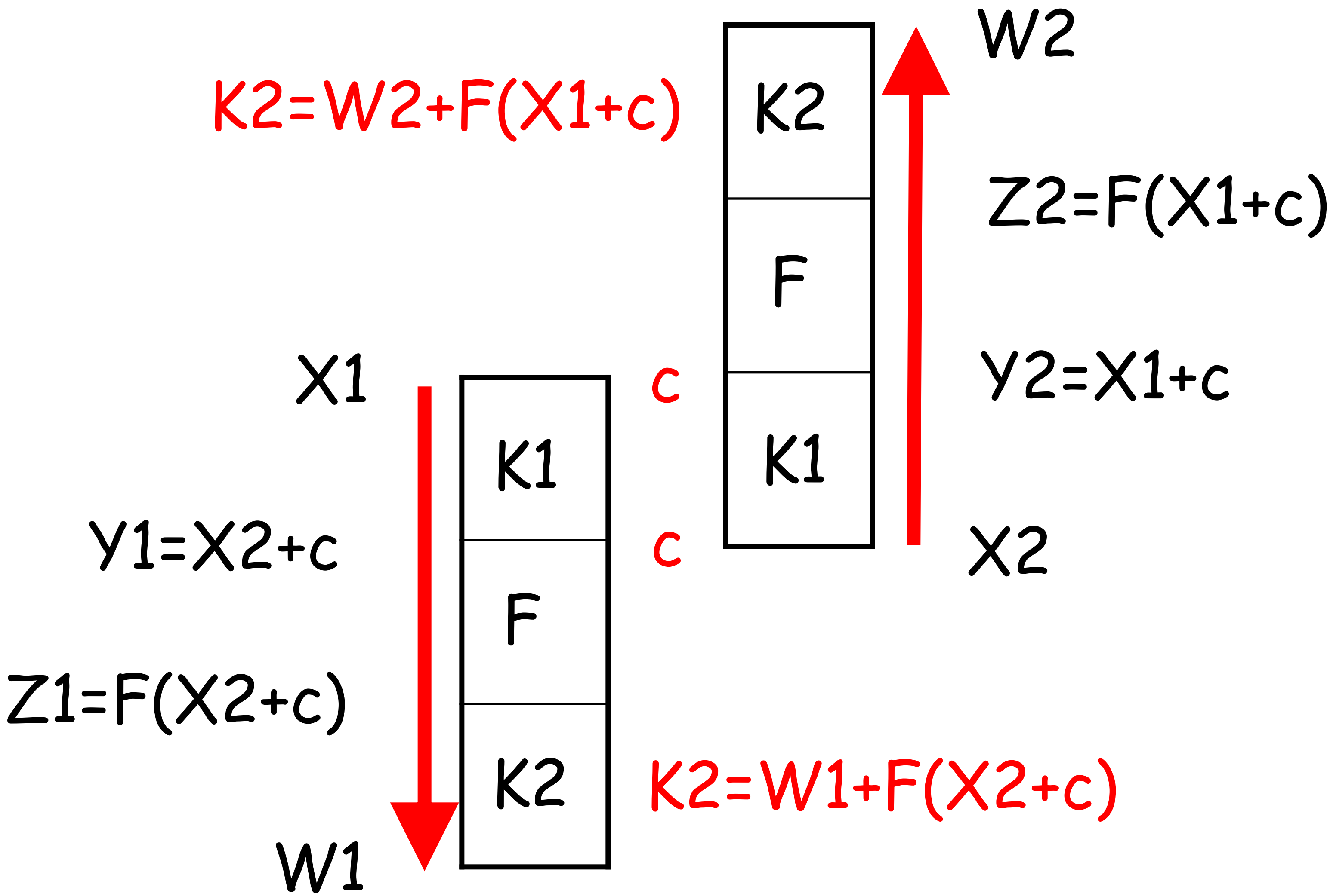
Our New SLIDEX Cryptanalytic Technique: A Slide Plus a Twist Plus a Difference



Our New SLIDEX Cryptanalytic Technique: A Slide Plus a Twist Plus a Difference



Our New SLIDEX Cryptanalytic Technique: A Slide Plus a Twist Plus a Difference



Applying the New SLIDEX Attack:

- Given any number D of known pairs (X_i, W_i), search for a triplet c, X_1, X_2 satisfying:

$$W_1+F(X_1+c)=W_2+F(X_2+c)$$

- The number of random values c you have to try is expected to be about $2^n/D^2$, since for these many D's the total number of possible triplets is 2^n, and each triplet satisfies the equation with probability of 2^{-n}

Our New Attack (Continued):

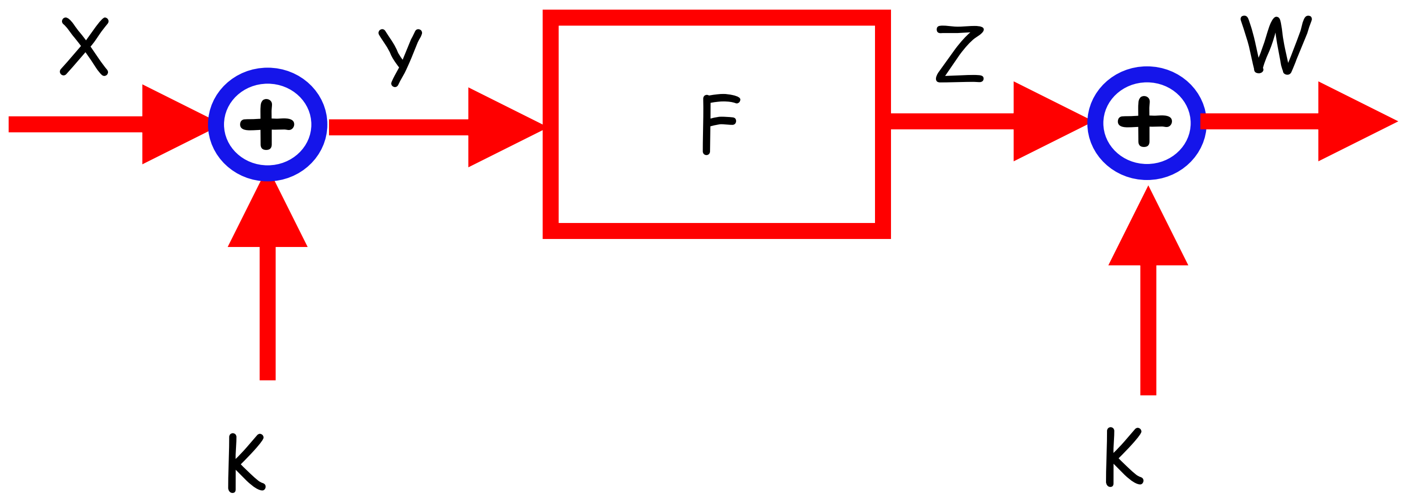
- For each c we prepare a list of values of $W+F(X+c)$ for all the D known plaintexts

- Look for a repetition in each list separately, from which it is easy to recover the two keys

- The total running time is thus $T=(2^n/D^2)xD=2^n/D$, so D and T satisfy $DT=2^n$

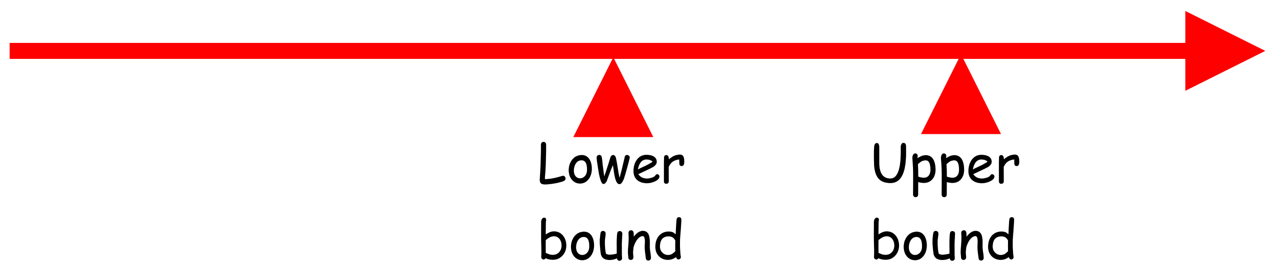
Let Us Reconsider Now the Basic Question: Is Even-Mansour Minimal?

- Consider an even simpler variant of the Even-Mansour block cipher, in which K1=K2. Such simplifications had been suggested before, but do they provide exactly the same security?

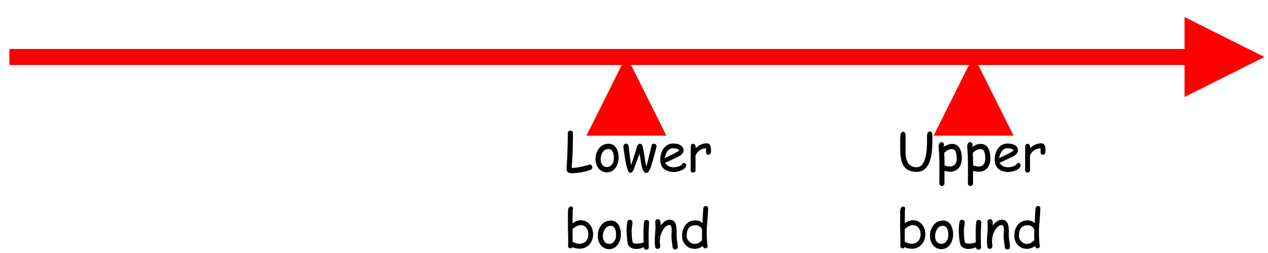


The Importance of Having Tight Bounds

Security bounds for cryptosystem A:

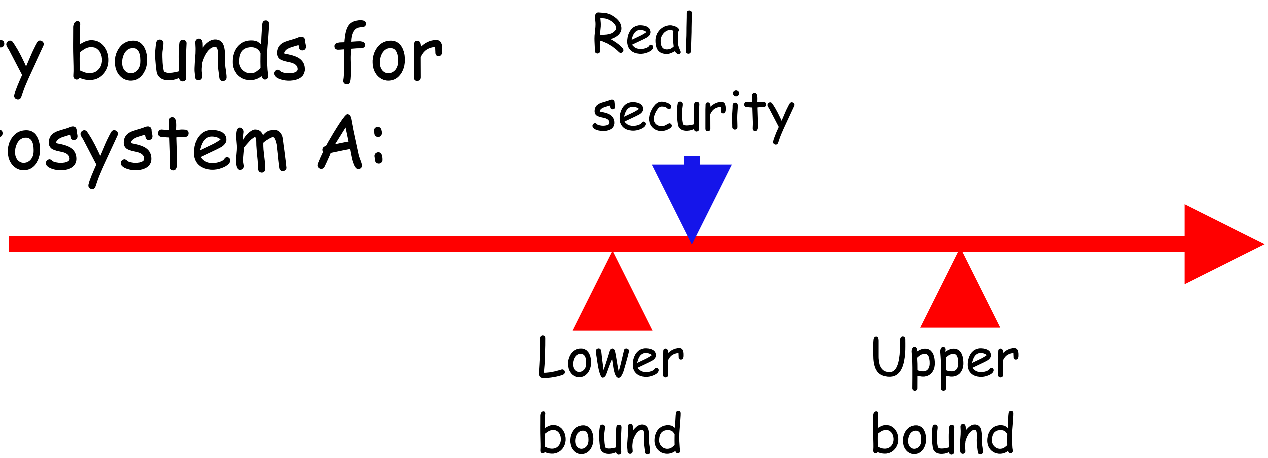


Security bounds for cryptosystem B:

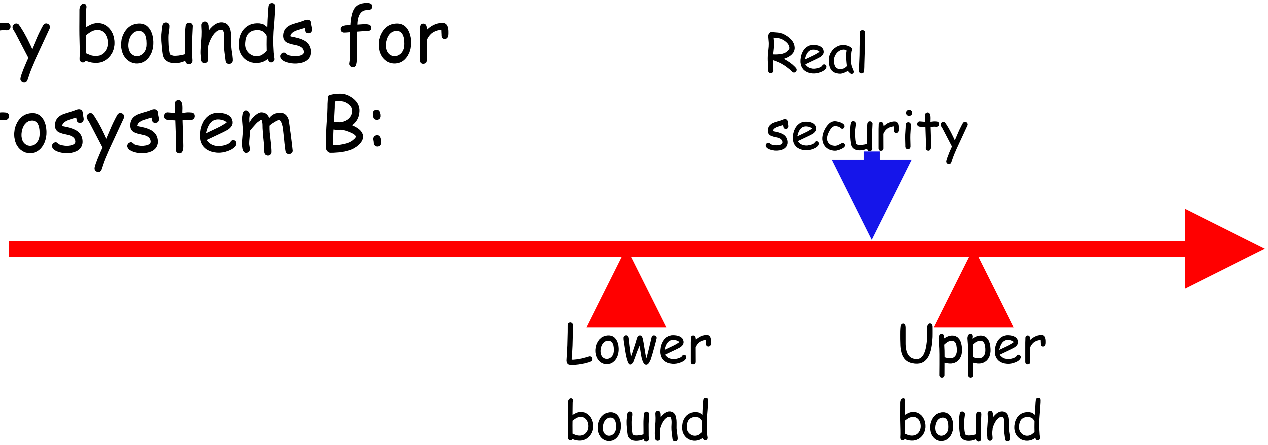


The Importance of Having Tight Bounds

Security bounds for cryptosystem A:

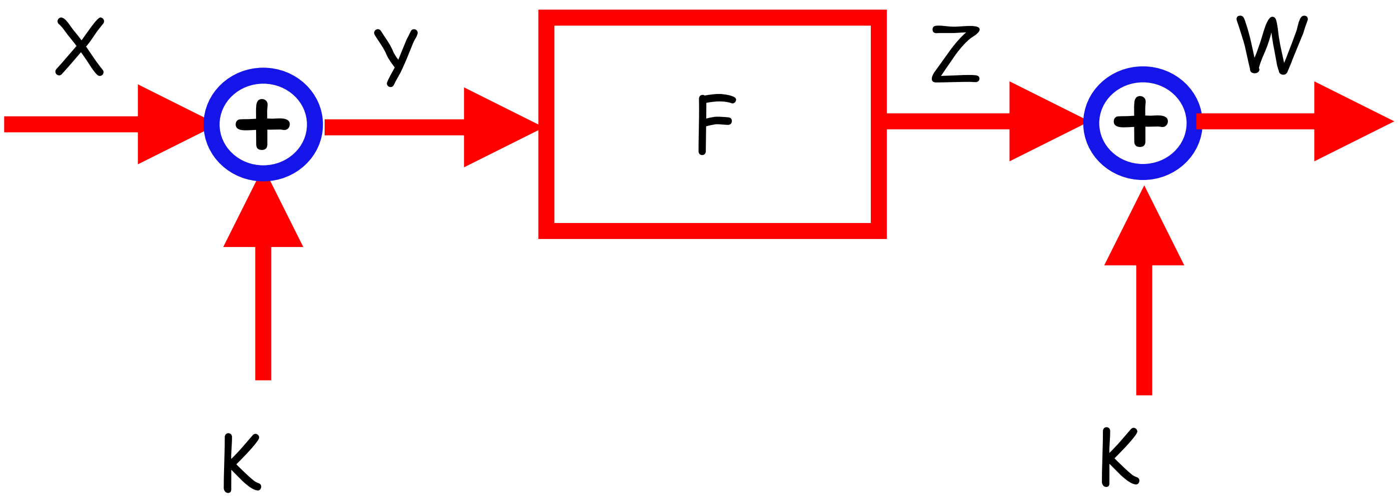


Security bounds for cryptosystem B:



The Equivalence of the Single-Key and Double-Key Even-Mansour Schemes

- By carefully examining the lower bound proof, we can show that the same lower bound $DT > \Omega(2^n)$ is also applicable here:



Let Us Reconsider Now the Basic Question: Is Even-Mansour Minimal?

- Clearly, any attack on the two-key variant of EM also breaks its single key variant
- Consequently, Even-Mansour is not minimal, and can be further simplified by using a single key without losing any security!
- The resulting block cipher is extremely simple: To encrypt a plaintext, XOR a key, apply a fixed known permutation, and XOR the same key again

Concluding Remarks:

- The SLIDEX attack is a new known plaintext attack which overcomes the main limitation of slide attacks: We no longer have to wait beyond the birthday bound for the lucky event to happen by chance - we force it to happen by guessing c

- This attack solves the 20-year old open problem of the exact security of the EM scheme, and makes it possible to further simplify the scheme by using a single key variant without any loss of security