Minimum Blockcipher Calls for Block cipher based Designs

Mridul Nandi

Indian Statistical Institute, Kolkata

mridul@isical.ac.in

30th Sept, ASK-2015, NTU, Singapore

Distinguishing Game

Distinguishing a real keyed construction from an ideal object.

1. PRF or Pseudorandom function.
2. PRP or Pseudorandom permutation.
3. SPRP or Strong Pseudorandom permutation.
4. ...

Differential Distinguisher Event

1. Make some queries x_i and obtain responses y_i, $1 \leq i \leq q$.
2. Finally makes two queries X and X', obtain corresponding responses Y, Y'.
3. Distinguisher Event:
   1. $\Delta Y := Y \oplus Y' = \mu$ (some constant). It is n bit equations.
   2. A more general event look like $L(\Delta Y) = b$ where L is a binary equation and b is a bit.

Notation

$\Delta X := X \oplus X'$

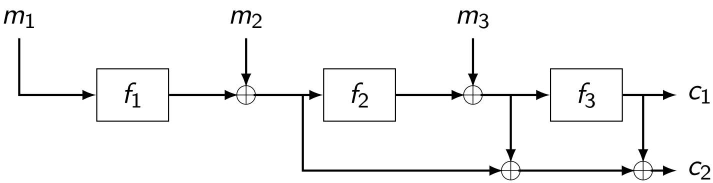
Block cipher based constructions

1. No field multiplication.
2. All lightweight operations - linear functions
3. Only Non-linear Operations - block cipher (modeled PRP), keyed non-compressing function (PRF)
4. multiple independent keys can be used.
5. Masking (again, linear operation) by random keys

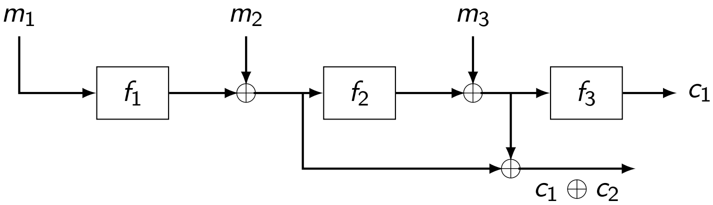
Examples

1. PRF: Counter-based Stream cipher.
2. (S)PRP: Luby-Rackoff, Feistel Structure, CMC, EME, AEZ, FMix etc.

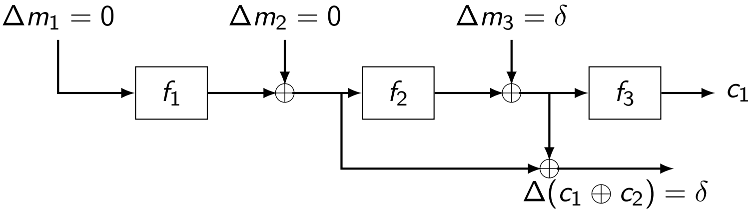
Is It Pseudorandom Function?



Is It Pseudorandom Function?



Is It Pseudorandom Function?



Differential Distinguisher

$\Delta(c_1 \oplus c_2) = \delta$.
So, it is not PRF.

Is It Pseudorandom Function?

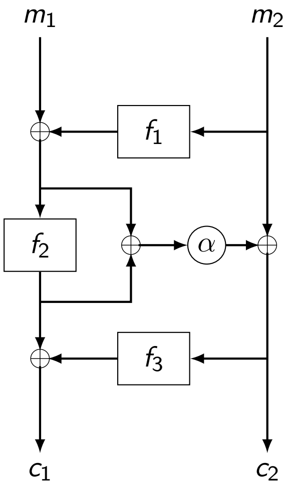
- We know that 2 round balanced Fiestel for 2 blocks is not PRF.
- What about Unbalanced Fiestel Structure with different rounds?

1. Initially blocks $X = (X_1, \ldots, X_\ell)$ is set to be the message.
2. For round $i = 1$ to $2\ell - 2$, updates ℓ blocks $X = (X_1, \ldots, X_\ell)$ as $X \leftarrow Lin(X, f(X_1))$. [1]
3. returns X;

Is it secure?

[1] Here the linear function *Lin* and the non-linear function *f* can be different at each round. *Lin* should be chosen so that invertible property maintains (in case of PRP construction).

Is It Strong Pseudorandom Permutation?

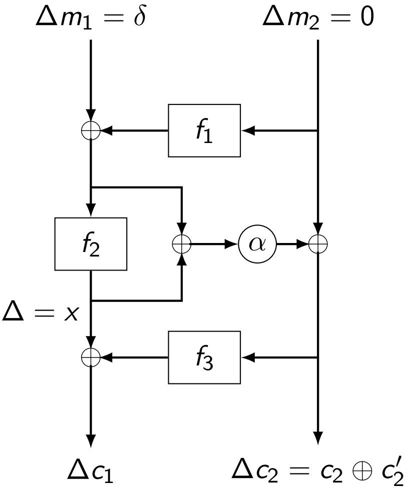


Is It Strong Pseudorandom Permutation?

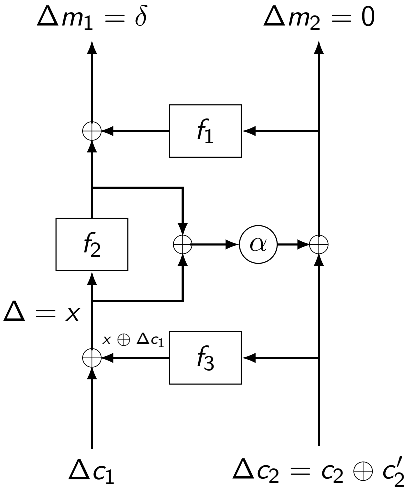
solve for x as follows:

1. $\alpha \cdot (x \oplus \delta) = \delta c_2$
2. $x = \alpha^{-1}(\Delta c_2) \oplus \delta$.

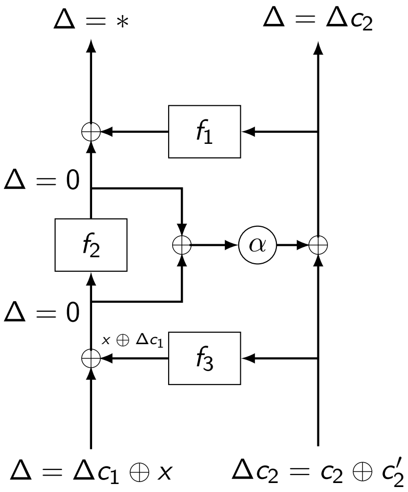
So,
$f(c_2) \oplus f(c_2') = x \oplus \Delta c_1$.



Is It Strong Pseudorandom Permutation?

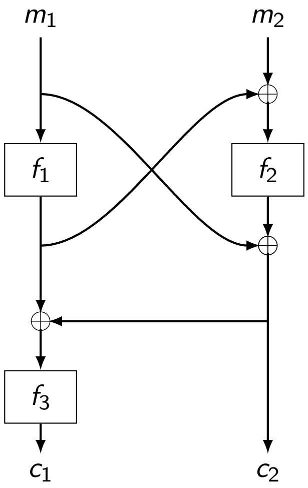


Is It Strong Pseudorandom Permutation?



So It is not.

Is It Strong Pseudorandom Permutation?



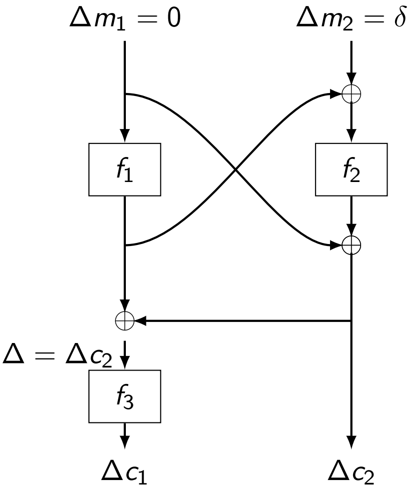
(construction is proposed due to Lear Bahack)

Is It Strong Pseudorandom Permutation?

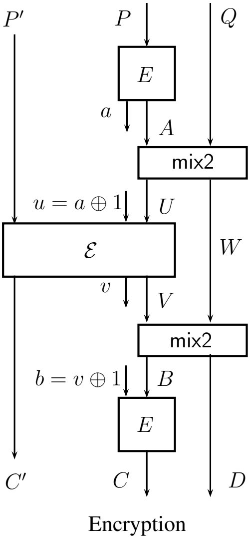
1. It is not again SPRP.
2. We find the difference of inputs for f_3 and so we make two decryption queries with same Δc_2.

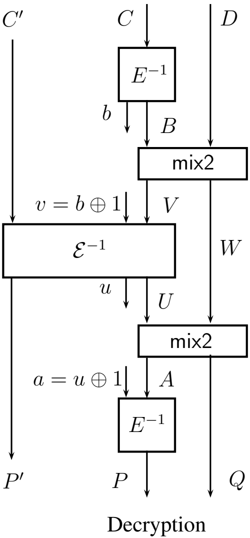
Decryption order

This example is different from other examples. The decryption order is $3 \to 1 \to 2$.
Usual decryption order
$3 \to 2 \to 1$.



or XLS?

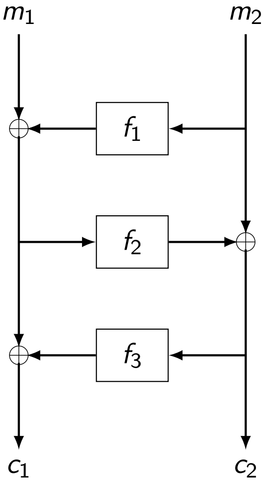




We know that XLS is not SPRP.

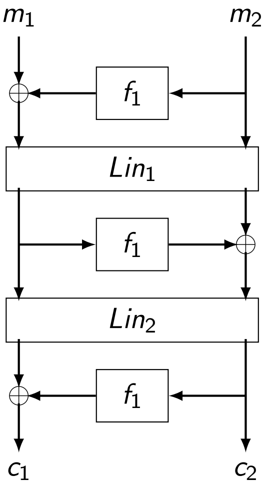
Inverse-free Single Key Pseudorandom Permutation

1. We know that three round LR is PRP but not SPRP, whereas 4 round is SPRP.
2. Nandi in Indocrypt 2010 showed that LR with $r \geq 3$ rounds is not isecure if and only if key-assignment is palindorme.



Inverse-free Single Key Pseudorandom Permutation

1. We know that three round LR is PRP but not SPRP, whereas 4 round is SPRP.
2. Nandi in Indocrypt 2010 showed that LR with $r \geq 3$ rounds is not isecure if and only if key-assignment is palindorme.
3. One can use some linear mixing layers.

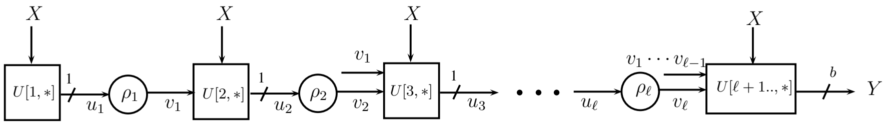


Inverse-free Single Key Pseudorandom Permutation

1. Can we have PRP for 3 rounds?
2. Nandi showed that an PRP attack on 3 rounds. So single key inverse free PRP construction requires 4 rounds.
3. What about general constructions of Fiestel? Surprisingly we see that inverse free single key PRP and SPRP have same cost.

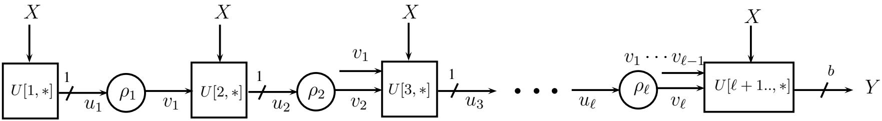
Affine Mode

1. We need to formally define ALL block cipher based constructions.
2. We consider affine mode for this.

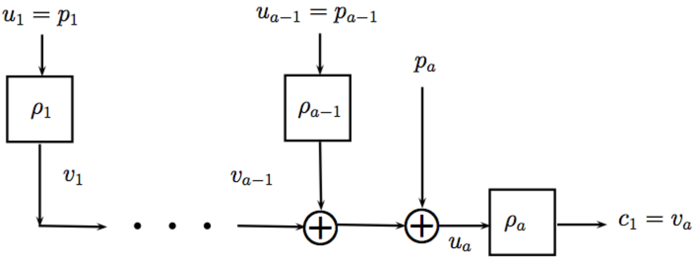


ρ_i non linear functions, $U[i,]$ are linear or affine functions.

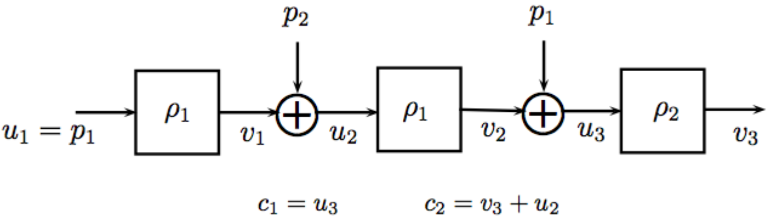
Examples of Affine Mode



PMAC: Examples of Affine Mode



What is this affine mode ???



CMC : Examples - SPRP

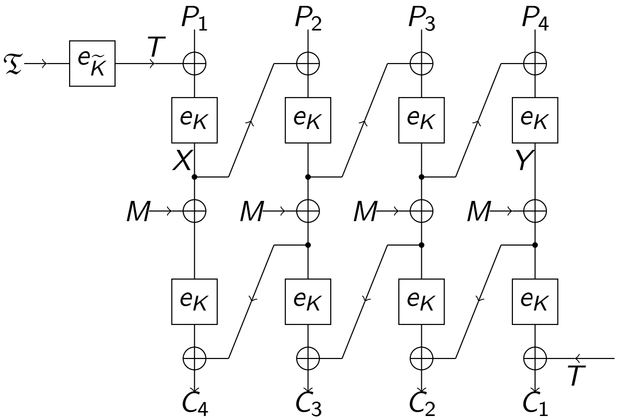
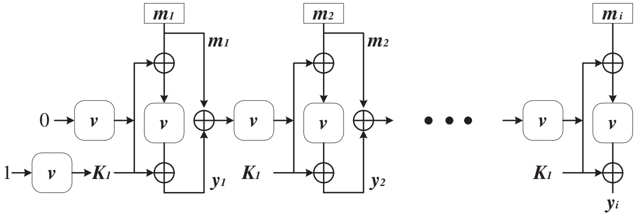


Figure : CMC for four blocks, with tweak $\mathfrak{T}$ and $M = 2(X \oplus Y)$. Here 2 represents a primitive element of a finite field over $\{0,1\}^n$.

MCBC : Examples - online-SPRP



OLEF : Examples - online-SPRP

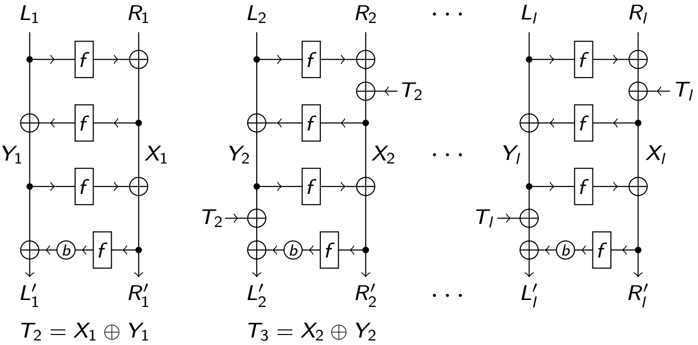
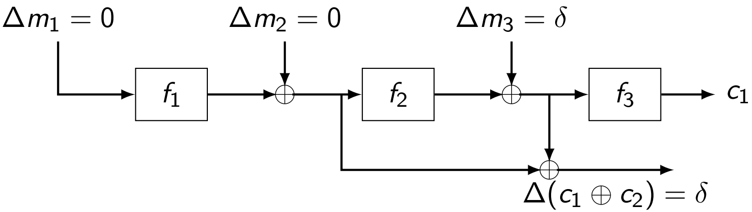


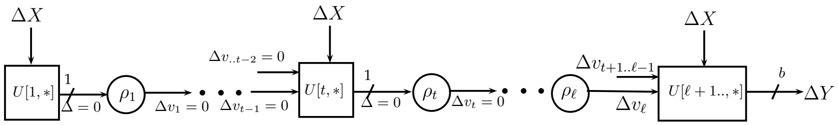
Figure : OleF for l Complete Diblocks

PRF/PRP Distinguisher

Recall PRF attack of our first example.



PRF/PRP Distinguisher



1. we try to equate inputs for two messages as much as possible.
2. then after observing the outputs we try to obtain all other internal input output differences.
3. if the number of blocks of unknown differences is less than the number of output blocks then we have redundancy.

Minimum Number of non-linear Calls

- **PRP** for a blocks - $2a-1$ calls. LR with 3 rounds. CMC without one of the middle blockcipher call is PRP.
- **PRF** from a blocks to b blocks - $a+b-1$ calls. PMAC, PMAC with counter mode.
- **SPRP** for a blocks - $2a$ calls. CMC, LR with 4 rounds, FMix.
- **Online** over a blocks - $2a$ calls for both PRP and SPRP. MCBC, OLEF, TC3 etc.
- **IV-PRP** For inverse-free single key PRP over a blocks - $2a$ calls. However, we see if we are allowed to mask by a key then $2a-1$ is sufficient.

PRP Distinguisher for a block message $2a-2$ calls

1. **step-1** find a difference in a pair of plaintext queries such that the first a inputs are same.
2. **step-2** make the queries m, m' with the difference Δm obtained in step-1. Let

   $$u_1, v_1, \ldots, u_{2a-2}, v_{2a-2}, \text{ and } u'_1, v'_1, \ldots, u'_{2a-2}, v'_{2a-2}$$

   denote the intermediate inputs outputs for the two queries respectively. We have $1 \leq i \leq a-1$, $u_i = u'_i, v_i = v'_i$.
3. **step-3** find a relation on a blocks output difference depends linearly on $a-1$ blocks unknown output difference.

SPRP Distinguisher for a block message $2a-1$ calls

step-1 Make two queries with a certain difference, same as PRP distinguisher. Let $u_1, v_1, \ldots, u_{2a-1}, v_{2a-1}$ and $u'_1, v'_1, \ldots, u'_{2a-1}, v'_{2a-1}$ denote the intermediate inputs outputs for the two queries respectively. We have $1 \le i \le a-1$, $u_i = u'_i, v_i = v'_i$.

step-2 solve for Δu, Δv using the invertible property.

step-3 find a difference for the final decryption query. Now we find a non zero difference d' for ciphertext such that a block inputs will be same.

step-4 So again we find a relation on a block output difference which is defined on $a-1$ blocks unknown output differences.

PRP Distinguisher for inverse-free single keyed

step-1 Make two queries with a certain difference, same as PRP distinguisher. Let $u_1, v_1, \ldots, u_{2a-1}, v_{2a-1}$ and $u'_1, v'_1, \ldots, u'_{2a-1}, v'_{2a-1}$ denote the intermediate inputs outputs for the two queries respectively. We have $1 \leq i \leq a-1$, $u_i = u'_i, v_i = v'_i$.

step-2 solve for Δu, Δv using the invertible property.

step-3 We can not make decryption query .. However, we can find the last input blcoks (due to invertiblity). So we can make two encryption queries such that

1. the first block inputs for two queries are same as the last block inputs for the previous queries.
2. the next $a-1$ block inputs are same.

step-4 So again we make output difference for the first a blocks known and so find a relation on a block output difference which is defined on $a-1$ blocks unknown output differences.

inverse free single nonlinear function PRP

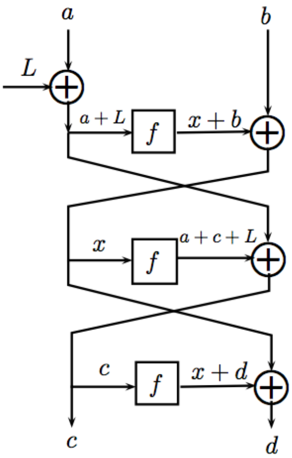


Figure : with a presence of masking key we can have three rounds inverse free single function keyed PRP.

Conclusion

1. Introduce Affine Mode.
2. Lower bounds on the number of calls for symmetric key primitives.
3. Tight by showing some constructions achieving bounds.

Thank You