Extended Criterion for Absence of Fixed Points

Oleksandr Kazymyrov, Valentyna Kazymyrova

Selmer Center, Department of Informatics,
University of Bergen, Norway
Oleksandr.Kazymyrov@uib.no

CTCrypt 2013

Outline

Properties of Substitutions

Definition

Substitution boxes (S-boxes) map an n-bit input message to an m-bit output message.

- Minimum of Algebraic Degree
- Balancedness
- Nonlinearity
- Correlation Immunity
- δ-uniformity
- Cycle Structure
- Algebraic Immunity
- Absolute Indicator
- Absence of Fixed Points
- Propagation Criterion
- Sum-of-squares indicator
- ...

Properties of Substitutions

Definition

Substitution boxes (S-boxes) map an n-bit input message to an m-bit output message.

- Minimum of Algebraic Degree
- Balancedness
- Nonlinearity
- Correlation Immunity
- δ-uniformity
- Cycle Structure
- Algebraic Immunity
- Absolute Indicator
- Absence of Fixed Points
- Propagation Criterion
- Sum-of-squares indicator
- ...

Absence of Fixed Points

Proposition

A substitution must not have fixed point, i.e.

$$F(a) \neq a, \quad \forall a \in \mathbb{F}_2^n .$$

From the Specification of Rijndael

The constant has been chosen in such a way that the S-box has no fixed points (S-box$(a) = a$) and no 'opposite fixed points' (S-box$(a) = \overline{a}$).

Notations & Definitions

Proposition

Arbitrary S-box can be always associated with a vectorial Boolean function F in $\mathbb{F}_{2^n}[x]$.

Arbitrary substitution has representations

- algebraic normal form (ANF)
- function over field $\mathbb{F}_{2^n}$
- lookup table

Definition

For permutations A_1 of $\mathbb{F}_2^m$, A_2 of $\mathbb{F}_2^n$ and a linear L_3 from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ two functions $F, G : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ are called extended affine equivalent (EA-equivalent) if

$$F(x) = A_1 \circ G \circ A_2(x) + L_3(x). \quad (1)$$

Notations & Definitions

Definition

Two ciphers E_i and E_j are isomorphic to each other if there exist invertible maps $\phi : x^i \mapsto x^j$, $\psi : y^i \mapsto y^j$ and $\chi : k^i \mapsto k^j$ such that $y^i = E_i(x^i, k^i)$ and $y^j = E_j(x^j, k^j)$ are equal for all x^i, k^i, x^j and k^j.

Definition

A mixing key procedure of a block cipher is an algorithm which injects a round key into an encryption procedure.

Notations & Definitions

$$E_K(M) = PW_{k_{r+1}} \circ \prod_{i=2}^{r} (R_{k_i}) \circ IW_{k_1}(M)$$

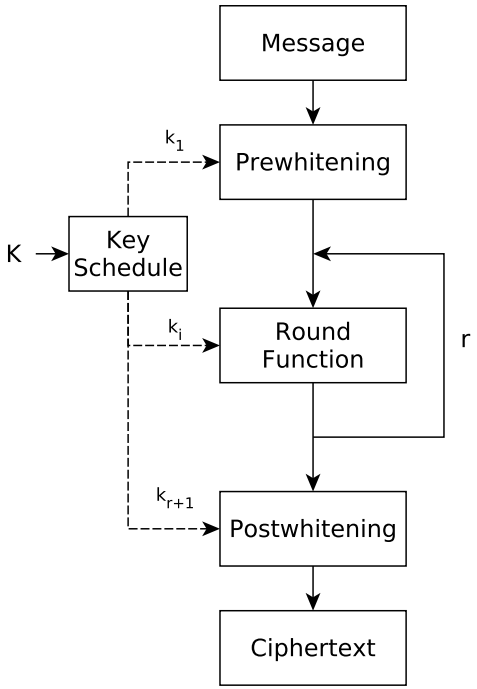


Figure : General Structure of an Iterative Block Cipher

Basic Functions of the AES

The round function consists of four functions

- AddroundKey (σ_k)
- SubBytes (γ)
- ShiftRows (π)
- MixColumns (θ)

$$E_K(M) = \sigma_{k_{r+1}} \circ \pi \circ \gamma \circ \prod_{i=2}^{r} (\sigma_{k_i} \circ \theta \circ \pi \circ \gamma) \circ \sigma_{k_1}(M).$$

Basic Functions of the AES

The round function consists of four functions

- AddroundKey (σ_k)
- SubBytes (γ)
- ShiftRows (π)
- MixColumns (θ)

$$E_K(M) = \sigma_{k_{r+1}} \circ \pi \circ \gamma \circ \prod_{i=2}^{r} (\sigma_{k_i} \circ \theta \circ \pi \circ \gamma) \circ \sigma_{k_1}(M).$$

Both MixColumns and ShiftRows are linear transformations with respect to XOR

$$\theta(x + y) = \theta(y) + \theta(y);$$
$$\pi(x + y) = \pi(y) + \pi(y).$$

Encryption Algorithm

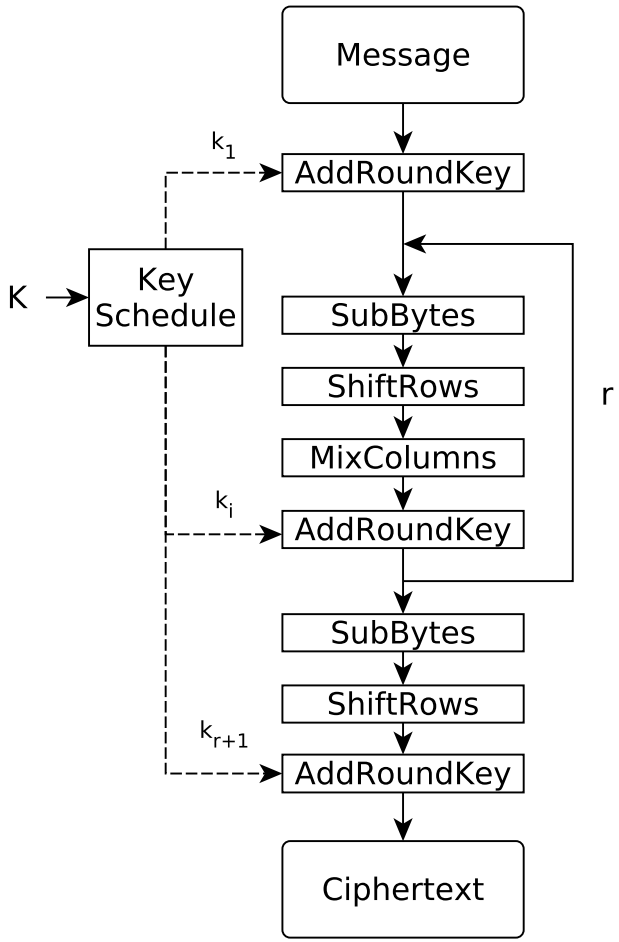


Figure : Encryption Algorithm of AES

Fast Decryption Algorithm

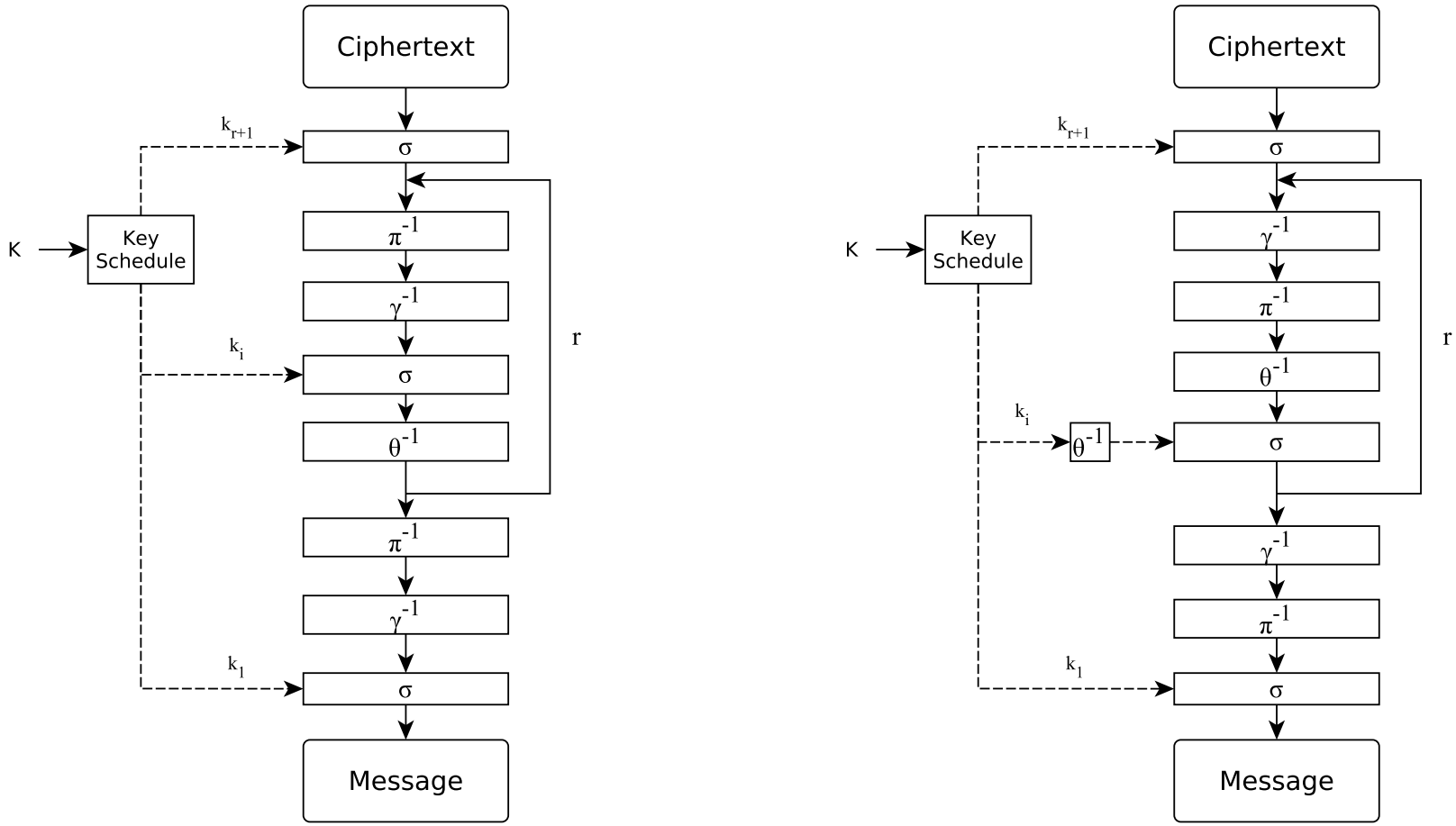
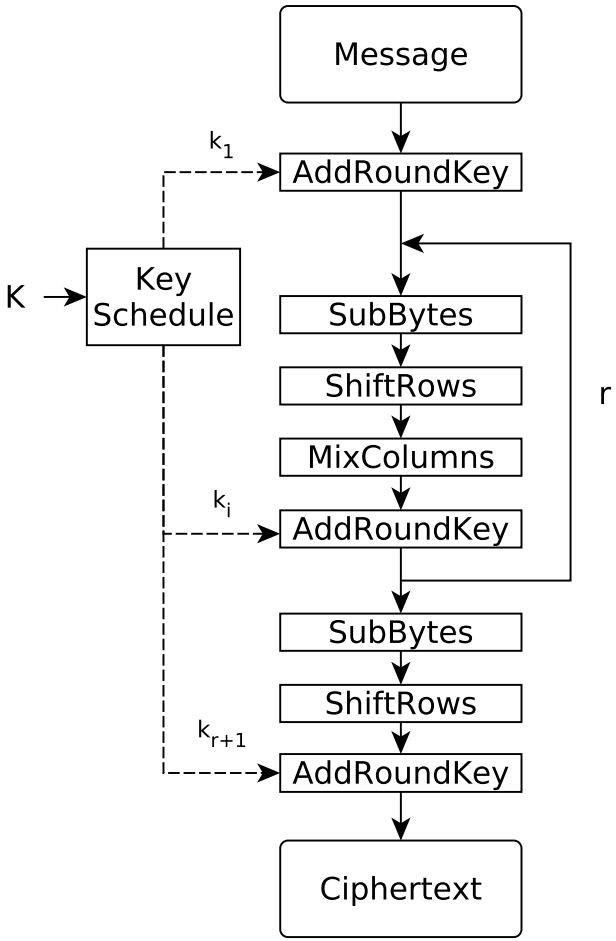


Figure : Decryption Algorithm of AES

Isomorphic Algorithm to the AES



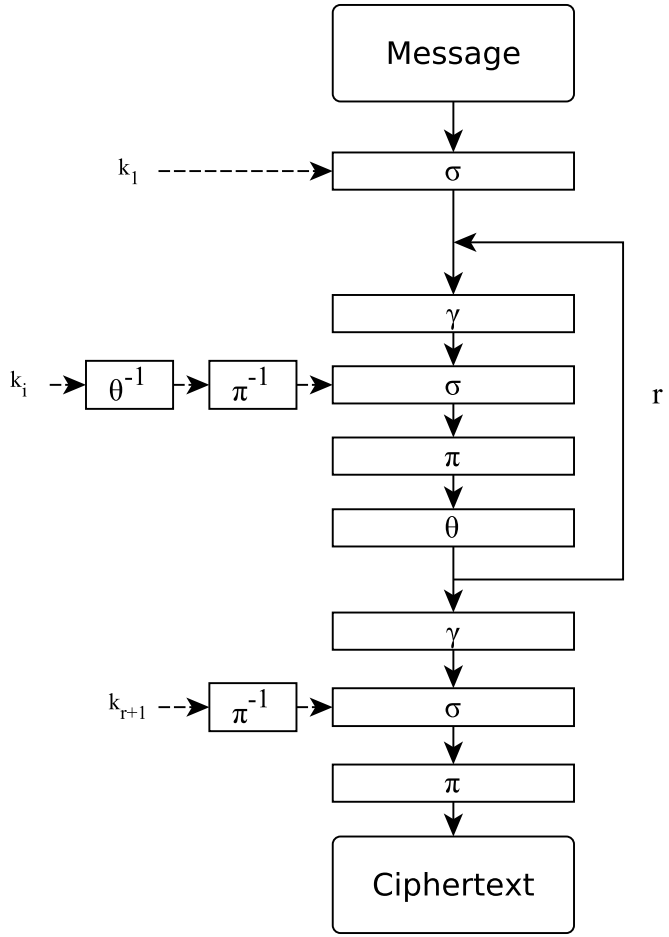


Figure : Encryption Algorithm

Generation of Substitutions

From the Specification of Rijndael

1. Taking the multiplicative inverse in $\mathbb{F}_{2^8}$ (00 is mapped onto itself).
2. Applying an affine transformation.

Affine equivalence in terms of vectorial Boolean functions

$$F(x) = A_1(x^{-1}) = L_1(x^{-1}) + c_1 = M_1 \cdot x^{-1} + C_1.$$

Definition

Let ξ be a function in which the constant c_1 is XORed with all bytes of a state and k_i' be the round keys of the form

$$\pi^{-1} \circ \theta^{-1} \circ \xi(k_i).$$

Isomorphic Algorithm to AES

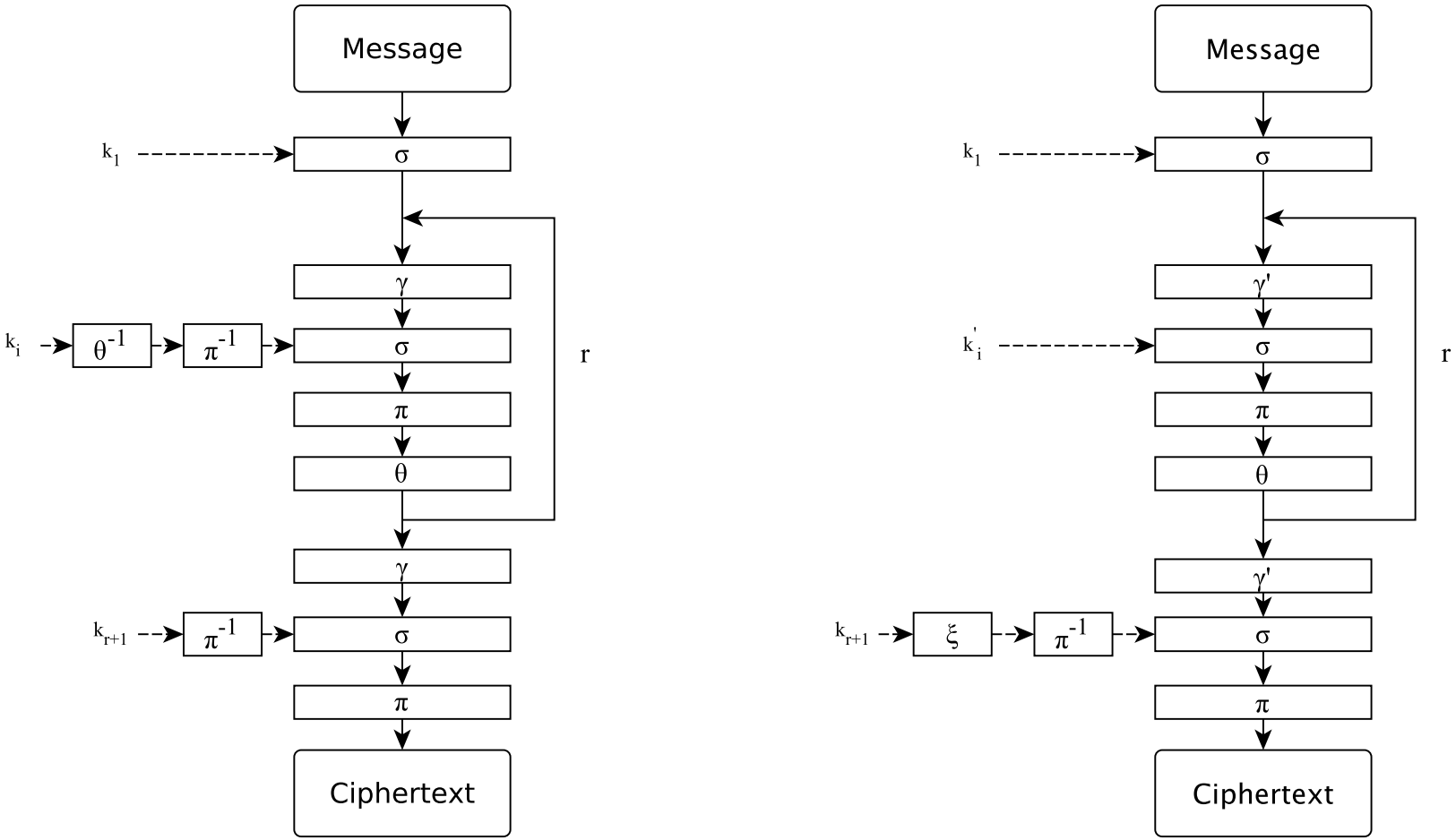
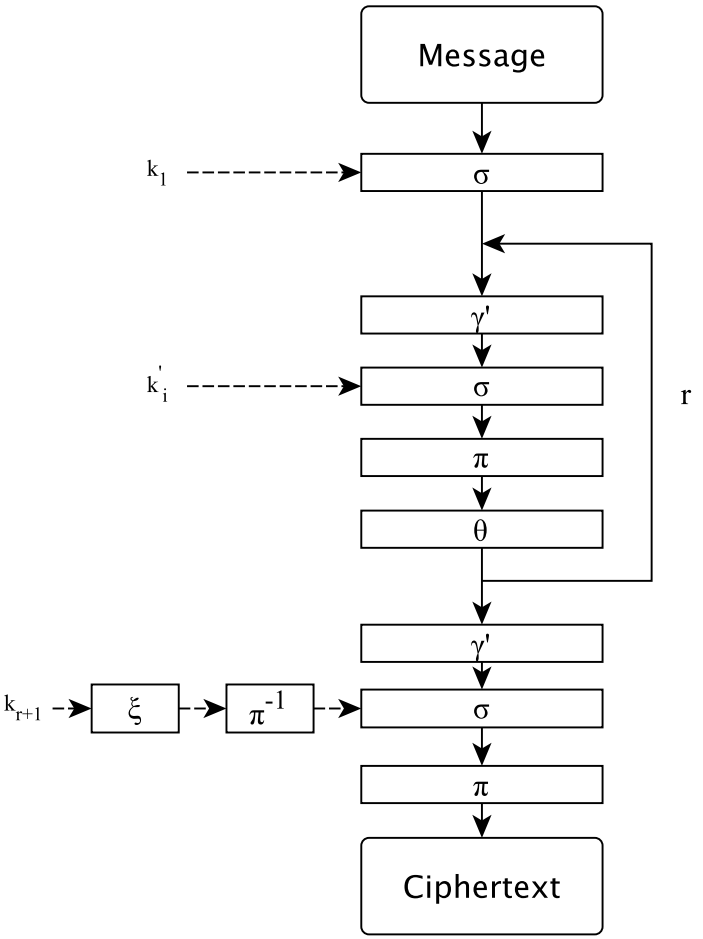


Figure : Encryption Algorithm

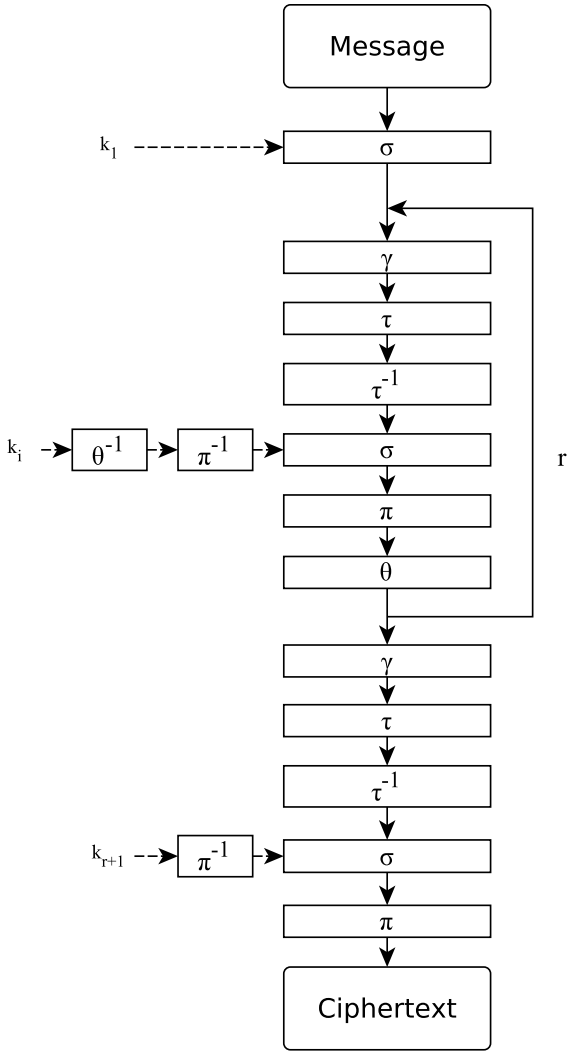
Overview of the Isomorphic Cipher

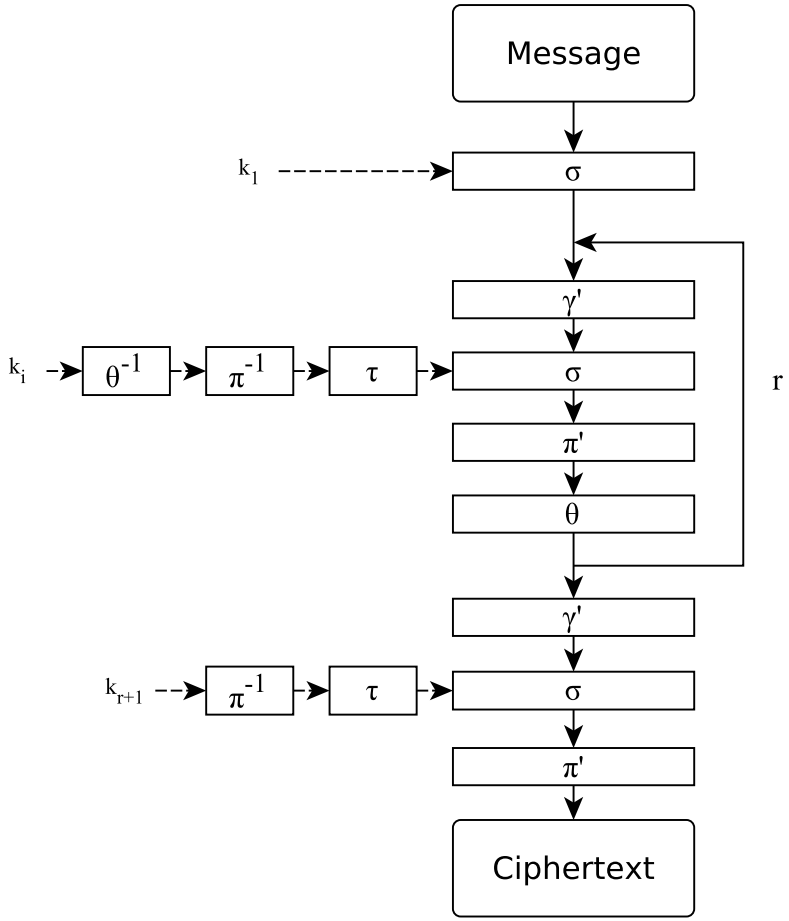
- Last π function does not increase security.
- Permutation has fixed point $(x = 0)$

$$F(x) = L_1(x^{-1}) = M_1 \cdot x^{-1}$$



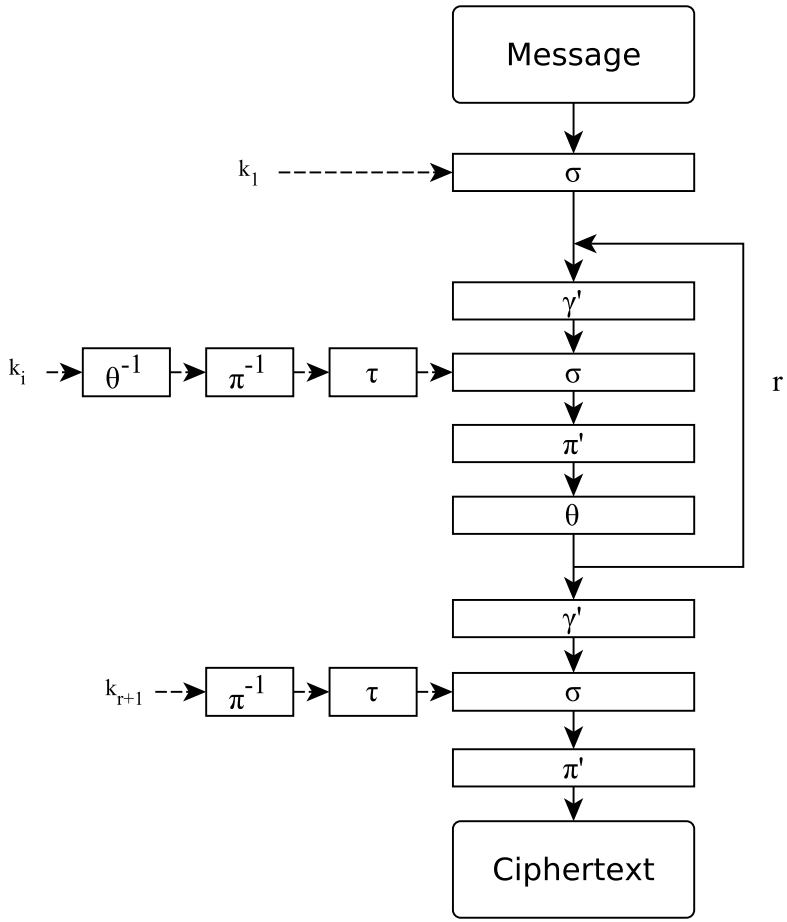
Isomorphic Cipher with a Linear Function





Overview of the Isomorphic Cipher

- Modification of τ leads to changes in cyclic properties of S-box.
- Such isomorphisms work with respect to XOR mixing key function.



Conclusions

Isomorphic ciphers allow to

- Show redundancy of the last ShiftRow operation of the AES.
- Prove/disprove necessity of some characteristics of substitutions.
- Introduce new criterion for several substitutions.
- Show advantages of addition modulo 2^n in comparison with XOR operation.

Conclusions

Isomorphic ciphers allow to

- Show redundancy of the last ShiftRow operation of the AES.
- Prove/disprove necessity of some characteristics of substitutions.
- Introduce new criterion for several substitutions.
- Show advantages of addition modulo 2^n in comparison with XOR operation.

Proposition

At least absence of fixed points criterion should be reviewed with other components of ciphers.