UDC 004.056.55

Quantum cryptanalysis of ciphers based on generalized Feistel and Lai-Massey schemes

Andrii Fesenko[1]

[1]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Physics and Technology*

Abstract

This paper investigates generalizations of the Lai-Massey scheme, including unified constructions combining it with the Feistel scheme (MD GLM, UFLM, L-Feistel, and quasi-Feistel). New reductions to the quasi-Feistel scheme are provided. Known efficient quantum attacks are analyzed, including chosen-plaintext attacks on 3 rounds and chosen-ciphertext attacks on 4 rounds for a special case of the quasi-Feistel cipher using Simon's algorithm. It is demonstrated that restrictions in that work led to the degeneration of the quasi-Feistel scheme into the standard Feistel scheme, replicating known quantum attacks on the Feistel scheme. New two-round distinguishing attacks are presented for the L-Feistel and MD-1 GLM schemes, enabling round key recovery.

Keywords: La-Massey scheme, quasi-Feistel cipher, L-Feistel scheme, quantum cryptanalysis

Introduction

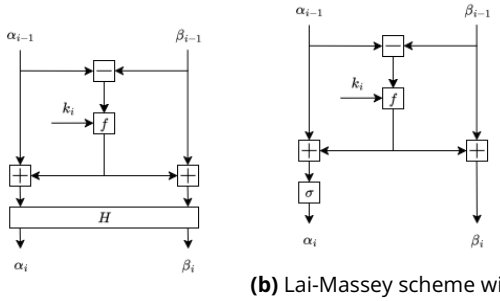
The Lai-Massey scheme is a cryptographic construction for building block ciphers that serves as an alternative to the more popular Feistel scheme. It was first proposed in 1990 for the PES cipher (Proposed Encryption Standard) by Xuejia Lai with contributions from James Massey [1]. After vulnerabilities to differential cryptanalysis were discovered in PES, the cipher was modified and renamed IDEA. Serge Vaudenay formalized the construction of the IDEA cipher, identified the need for an additional transformation to prevent a distinguishing attack, and named it the "Lai-Massey scheme" [2]. Since then, modifications and generalizations of the Lai-Massey scheme have emerged, though their applications in cipher design are far fewer than those of the Feistel scheme. Ciphers such as FOX (IDEA-NXT), WIDEA, Akelarre, BISON, and iSCREAM are built on schemes similar to Lai-Massey. These constructions are used not only as the global iterative round structure but also locally — for nonlinear components. For example, the S-boxes in MESH have a similar design, as do the S-boxes in Littlun of the FLY cipher. The Lai-Massey scheme remains less popular than Feistel or SPN schemes due to certain weaknesses (e.g., invariant subspaces), but it is valued for its fast diffusion property. Additionally, the encryption and decryption schemes are identical up to the key schedule, and the round function does not need to be invertible.

Given the modern use of modified and generalized Lai-Massey schemes, the question of quantum cryptanalysis and obtaining corresponding security estimates for such schemes is relevant, particularly unified approaches that combine Lai-Massey and Feistel schemes.

1. The Lai-Massey Scheme and Its Generalizations

Let $(G, +)$ be a finite abelian group, and σ a mapping of the form $G \to G$. If the mappings σ and $x \mapsto \sigma(x) - x$ are permutations on the set G, then the mapping σ is called an *orthomorphic permutation* or *orthomorphism*. In particular, if $G = \{0,1\}^n$ and the group operation is component-wise addition modulo 2 (i.e., $\oplus$), then an orthomorphic permutation $\sigma\colon \{0,1\}^n \to \{0,1\}^n$ is called a *linear orthomorphic permutation*.

The Lai-Massey scheme, shown in Fig. 1a, is an abstraction of the IDEA block cipher. Let $(G, +)$ be a finite abelian group, and subtrac-



(a) Lai-Massey scheme

(b) Lai-Massey scheme with orthomorphism

Figure 1: i-th round of the Lai-Massey scheme

tion $-$ defined as addition with the inverse element. For given r functions $f_1, \ldots, f_r \colon G \to G$ and mapping $H \colon G \times G \to G \times G$, the r-round Lai-Massey scheme LM_r is a permutation on the set G^2, defined as follows. The inputs to the i-th round, $i \in \{1, \ldots, r\}$, are the pair $(\alpha_{i-1}, \beta_{i-1})$, where $\alpha_{i-1}, \beta_{i-1} \in G$. The outputs of the i-th round are the pair (α_i, β_i), such that

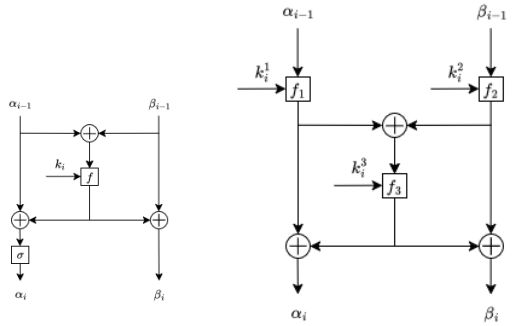
$$\alpha_i = H\big(\alpha_{i-1} + f_i(\alpha_{i-1} - \beta_{i-1})\big),$$
$$\beta_i = \beta_{i-1} + f_i(\alpha_{i-1} - \beta_{i-1}).$$

Usually, the functions $f_1, \ldots, f_r$ are parameterized by round key values, so one can assume that $f_i = f(k_i, \cdot)$ for any value $i \in \{1, \ldots, r\}$. The half-round transformation H prevents the appearance of an invariant $(\alpha_i - \beta_i)$ and the corresponding distinguishing attack. In general, the transformation H may depend on the key, but in most cases it does not, so the application of the mapping H is omitted in the last r-th round. Moreover, typically the half-round transformation H for the Lai-Massey scheme has the form $H(\alpha, \beta) = (\sigma(\alpha), \beta)$ for some orthomorphic permutation σ, as shown in Fig. 1b.

Initially, the Lai-Massey scheme was defined over an arbitrary abelian group $(G, +)$, for which the subtraction operation is naturally defined. Using an orthomorphic permutation σ, the round transformation has the form

$$(\alpha, \beta) \mapsto (\sigma(\alpha + f(\alpha - \beta)), \beta + f(\alpha - \beta)).$$

The structural properties of the iterative block cipher construction usually do not depend on the specific implementation of the abelian group, so often, without loss of generality, for such analysis it is assumed that $(G, +) = (\{0,1\}^{2n}, \oplus)$ for some natural number n. This does not mean that all implementations over other groups are equivalent in terms of security to this choice of group, but this substitution is important for theoretical analysis of the scheme itself. Accordingly, the Lai-Massey scheme is also referred to as the scheme shown in Fig. 2a.



(a) Lai-Massey $\oplus$ scheme

(b) MD GLM scheme

Figure 2: i-th round of the Lai-Massey scheme

2. Unified Generalizations

The simplest generalizations of the Lai-Massey scheme could involve replacing the addition and subtraction operations with three different operations with corresponding properties, as well as using the experience of generalizing the Feistel scheme to construct a multi-branch Lai-Massey scheme. More interesting is the approach to constructing a generalization of the Lai-Massey scheme that combines it with the Feistel scheme, as this allows, first, for a more flexible construction, second, to compare different construction schemes, and third, to try to leverage the advantages of each scheme to build more secure ciphers.

Mirzaee-Dehnavi Generalized Lai-Massey Scheme

The term generalized Lai-Massey scheme or GLM (from generalized Lai-Massey scheme) is used for several constructions, so it is necessary to specify which generalized construction is being considered.

One variant of generalizing the Lai-Massey scheme is the schemes proposed by Mirzaee Shamsabad and Dehnavi in the work [3] in 2020. Inspired by the features of the S-box construction in Littlun of the FLY cipher, they proposed a new generalized Lai-Massey scheme that uses multiple parts of the round key and is shown in Fig. 2b. We will refer to this scheme as the

Mirzaee-Dehnavi generalized Lai-Massey scheme or abbreviated as the MD GLM scheme.

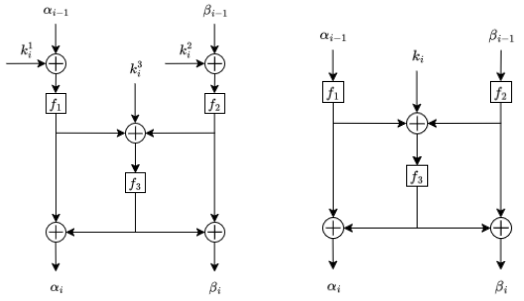
Since round keys are often added using component-wise addition modulo 2, the work [3] also proposed modifications of the MD GLM scheme, in which this operation is highlighted, shown in Fig. 3a and Fig. 3b. We will refer to these schemes as MD-3 GLM and MD-1 GLM, respectively.

Thus, for arbitrary inputs to the i-th round $(\alpha_{i-1}, \beta_{i-1})$, i-th round key $(k_i^1, k_i^2, k_i^3) \in (\{0,1\}^n)^3$, and arbitrary round functions $f_1, f_2, f_3 \colon \{0,1\}^n \to \{0,1\}^n$ (where functions f_1 and f_2 are bijective), the round transformation of the MD GLM scheme has the form

$$F_{MD}(\alpha_{i-1}, \beta_{i-1}) = \\ = (f_1(k_i^1, \alpha_{i-1}) \oplus \Delta, f_2(k_i^2, \beta_{i-1}) \oplus \Delta), \\ \Delta = f_3(k_i^3, f_1(k_i^1, \alpha_{i-1}) \oplus f_2(k_i^2, \beta_{i-1})).$$

And, for arbitrary inputs to the i-th round $(\alpha_{i-1}, \beta_{i-1} \in \{0,1\}^n)$, i-th round key $(k_i^1, k_i^2, k_i^3) \in (\{0,1\}^n)^3$ or $k_i \in \{0,1\}^n$, and arbitrary functions $f_1, f_2, f_3 \colon \{0,1\}^n \to \{0,1\}^n$ (where functions f_1 and f_2 are bijective), the round transformations of the MD-3 GLM and MD-1 GLM schemes have the form

$$F_{MD\text{-}3}(\alpha_{i-1}, \beta_{i-1}) = \\ = (f_1(k_i^1 \oplus \alpha_{i-1}) \oplus \Delta_3, f_2(k_i^2 \oplus \beta_{i-1}) \oplus \Delta_3), \\ \Delta_3 = f_3(k_i^3 \oplus f_1(k_i^1 \oplus \alpha_{i-1}) \oplus f_2(k_i^2 \oplus \beta_{i-1})); \\ F_{MD\text{-}1}(\alpha_{i-1}, \beta_{i-1}) = \\ = (f_1(\alpha_{i-1}) \oplus \Delta_1, f_2(\beta_{i-1}) \oplus \Delta_1), \\ \Delta_1 = f_3(k_i^3 \oplus f_1(\alpha_{i-1}) \oplus f_2(\beta_{i-1})).$$



(a) MD-3 GLM scheme **(b)** MD-1 GLM scheme

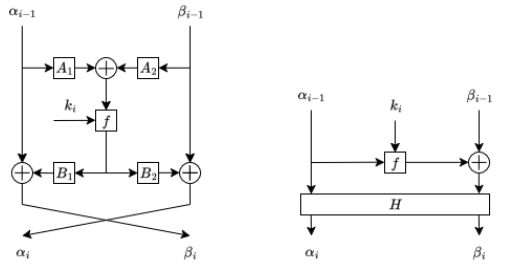
Figure 3: i-th round of the Lai-Massey scheme

L-Feistel Scheme

In the work [4] in 2022, Jiajie Liu, Bing Sun, and Chao Li proposed a new two-branch iterative block cipher construction, named by the authors as the L-Feistel scheme (likely, the name comes from the word linear). This scheme generalizes the two-branch Feistel and Lai-Massey schemes, is self-inverse, and is shown in Fig. 4a.

$\mathbb{F}_2^n$ is an n-dimensional vector field over the binary field $\mathbb{F}_2$, $n \in \mathbb{N}_{\geq 1}$. Let the square matrices $A_1, A_2, B_1, B_2 \in \mathbb{F}_2^{n \times n}$ be such that $A_1 B_1 \oplus A_2 B_2 = 0$ (ensures the involutivity of one round and identical encryption and decryption procedures), and the rank of the matrices $\begin{bmatrix} A_1 & A_2 \\ A_2 & A_1 \end{bmatrix}$ and $\begin{bmatrix} B_1^T & B_2^T \\ B_2^T & B_1^T \end{bmatrix}$ equals $2n$ (from which follows the non-degeneracy of the matrix $A_1 B_2 \oplus A_2 B_1$). For arbitrary inputs to the i-th round $\alpha_{i-1}, \beta_{i-1} \in \{0,1\}^n$, i-th round key $k_i \in \{0,1\}^n$, arbitrary linear mapping $\varphi \colon \{0,1\}^{2n} \to \{0,1\}^{2n}$, and arbitrary round function $f \colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, the round transformation of the L-Feistel scheme (with swapping the left and right parts) has the form

$$F_L(\alpha_{i-1}, \beta_{i-1}) = (\beta_{i-1} \oplus B_2 \Delta, \alpha_{i-1} \oplus B_1 \Delta), \\ \Delta = f(k_i, A_1 \alpha_{i-1} \oplus A_2 \beta_{i-1}).$$



(a) L-Feistel scheme **(b)** UFLM scheme

Figure 4: i-th round of the Lai-Massey scheme

UFLM Scheme

In the work [5] in 2024, Zhengyi Dai, Chao Li, and Chun Guo proposed the unified UFLM scheme, which covers both the two-branch Feistel scheme and the two-branch Lai-Massey scheme as special cases. They showed that the differences between these two schemes with similar encryption and decryption procedures reduce to different applications of a part

permutation of order 2 and an orthomorphic permutation whose order is at least 3.

For arbitrary inputs to the i-th round $\alpha_{i-1}, \beta_{i-1} \in \{0,1\}^n$, i-th round key $k_i \in \{0,1\}^n$, arbitrary linear mapping $\varphi\colon \{0,1\}^{2n} \to \{0,1\}^{2n}$, and arbitrary round function $f\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, the round transformation of the UFLM scheme has the form

$$F_L \begin{bmatrix} \alpha_{i-1} \\ \beta_{i-1} \end{bmatrix} = \varphi \begin{bmatrix} \alpha_{i-1} \\ \beta_{i-1} \oplus f(k_i, \alpha_{i-1}) \end{bmatrix},$$

and is shown in Fig. 4b.

Quasi-Feistel Scheme

Aaram Yun, Je Hong Park, and Jooyoung Lee in the works [6] in 2007 and [7] proposed a quasi-Feistel scheme construction for iterative block ciphers, which is a generalization of Feistel-like schemes and the Lai-Massey scheme.

Definition 1 ([6]). *A combiner function for a pair of sets (X, Y) is a function $\Gamma\colon X \times X \times Y \to X$ such that for arbitrary elements $x \in X$ and $y \in Y$, the mappings $v \mapsto \Gamma(v, x, y)$ and $w \mapsto \Gamma(x, w, y)$ are permutations on the set X.*

For an arbitrary integer $b > 1$, combiner functions for the pair of sets (X, X^{b-1}) are called b-combiners over the set X.

Definition 2 ([6]). *For an arbitrary non-empty set X, let $b > 1$ and $r \geq 1$ be some fixed integers, $P, Q\colon X^b \to X^b$ arbitrary permutations, and Γ an arbitrary b-combiner over the set X. For given r functions $f_1, \ldots, f_r\colon X^{b-1} \to X$, the b-branch r-round quasi-Feistel cipher for round functions $f_1, \ldots, f_r$ relative to (P, Q, Γ) is the mapping*

$$\Psi = \Psi_{b,r}^{P,Q}(f_1, \ldots, f_r)\colon X^b \to X^b,$$

defined using the quasi-Feistel scheme: for an arbitrary value $x = (x_1, \ldots, x_b) \in X^b$, compute $y = \Psi(x)$ according to the rules:

1) $(z_0, z_1, \ldots, z_{b-1}) = P(x)$,

2) $z_{i+b-1} = \Gamma\big(z_{i-1}, f_i(z_i, \ldots, z_{i+b-2}), (z_i, \ldots, z_{i+b-2})\big)$ *for* $i \in \{1, \ldots, r\}$,

3) $y = Q^{-1}(z_r, z_{r+1}, \ldots, z_{r+b-1})$.

The set X is called the underlying set, the permutation P the pre-processing permutation, and the permutation Q the post-processing permutation.

For an arbitrary combiner function Γ for a pair of sets (X, Y), fix an arbitrary value $y \in Y$, then the algebraic structure (X, Γ_y) is a quasigroup, where $\Gamma_y\colon X \times X \to X$, $\Gamma_y(v, x) = \Gamma(v, x, y)$ for arbitrary elements $v, x \in X$. Thus, an arbitrary combiner function Γ can be viewed as a parameterized family $\{\Gamma_y\}_{y \in Y}$ of quasigroups, which gave the name to the scheme proposed in the work [6].

All round functions $f_1, \ldots, f_r$ can also be defined using a binary function with an additional argument being the round key value. A quasi-Feistel cipher (scheme) is balanced if $b = 2$, and unbalanced when $b > 2$. Obviously, any quasi-Feistel cipher is a permutation on the set X^b.

Claim 1 ([6]). *The (unbalanced) Feistel scheme is a special case of the quasi-Feistel scheme with the combiner function $\Gamma(v, x, y) = v \oplus x$.*

Claim 2 ([6]). *The Lai-Massey scheme is a special case of the quasi-Feistel scheme with the combiner function $\Gamma(v, x, y) = y + \tau(y - v + x + \tau^{-1}(y - v))$, where $\tau(x) = \sigma(x) - x$, and the underlying set is a finite abelian group G.*

3. Reductions of Schemes

Obviously, the Lai-Massey scheme with addition modulo 2 (Fig. 2a) is a special case of the Lai-Massey scheme with orthomorphic permutation (Fig. 1b), which, in turn, is a special case of the general Lai-Massey scheme (Fig. 1a).

Also, it is clear that the MD-1 GLM scheme (Fig. 3b) is a special case of the MD-3 GLM scheme (Fig. 3a), which, in turn, is a special case of the MD GLM scheme (Fig. 2b). Using transformations in the MD GLM scheme that depend on parts of the round key does not allow exploiting the structural features of the scheme, and it can be described using a quasi-Feistel scheme with the combiner function $\Gamma(v, x, y) = x$, i.e., considering the entire round as one key-dependent transformation.

The round of the UFLM scheme also looks like one key-dependent transformation. But when reducing the L-Feistel scheme to the quasi-Feistel scheme, one can use the constructive features of building one round.

Claim 3. *The L-Feistel scheme is a special case of the quasi-Feistel scheme with the combiner function* $\Gamma(v,x,y) = v \oplus (A_1B_2 \oplus A_2B_1)x$.

Proof. Let the square matrices $A_1, A_2, B_1, B_2 \in \mathbb{F}_2^{n\times n}$ be such that $A_1B_1 \oplus A_2B_2 = 0$, for the L-Feistel scheme. Denote the inputs to the i-th round as $\alpha_{i-1}, \beta_{i-1} \in \{0,1\}^n$, and the i-th round function as $f_i\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$, $i \in \{1,\ldots,r\}$. Denote the ciphertext values through (α_r, β_r).

If $(\alpha_{i-1}, \beta_{i-1})$ is the input to the i-th round, $i \in \{1,\ldots,r\}$, then according to the definition of the round transformation we have:

$$(\alpha_i, \beta_i) = (\beta_{i-1} \oplus B_2\Delta, \alpha_{i-1} \oplus B_1\Delta),$$
$$\Delta = f(k_i, A_1\alpha_{i-1} \oplus A_2\beta_{i-1}).$$

From this, it follows that the identity holds for all values $i \in \{1,\ldots,r\}$

$$\begin{aligned} &A_2\alpha_i \oplus A_1\beta_i = A_2\beta_{i-1} \oplus A_2B_2\Delta \oplus \\ &\oplus A_1\alpha_{i-1} \oplus A_1B_1\Delta = A_1\alpha_{i-1} \oplus A_2\beta_{i-1}. \end{aligned} \quad (1)$$

Define the underlying set of the combiner function as the set $\mathbb{F}_2^n$, and the combiner function itself as $\Gamma\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\Gamma(v,x,y) = v \oplus (A_1B_2 \oplus A_2B_1)x$ for arbitrary values $v, x, y \in \mathbb{F}_2^n$. Let $z_0 = A_2\alpha_0 \oplus A_1\beta_0$ and $z_1 = A_1\alpha_0 \oplus A_2\beta_0$. According to the quasi-Feistel scheme using the given combiner function, we have

$$\begin{aligned} z_{i+1} &= \Gamma(z_{i-1}, f_i(z_i), z_i) = \\ &= z_{i-1} \oplus (A_1B_2 \oplus A_2B_1)f_i(z_i). \end{aligned}$$

We prove by induction that the identity $z_i = A_2\alpha_i \oplus A_1\beta_i$ holds for all values $i \in \{1,\ldots,r\}$. For $i = 1$, this holds directly by the definition of z_1. Assume the statement holds for all values i, $1 \le i \le t < r$.

Using the round transformation and identity (1), we have

$$\begin{aligned} z_{t+1} =& z_{t-1} \oplus (A_1B_2 \oplus A_2B_1)f_t(z_t) = \\ =& A_2\alpha_{t-1} \oplus A_1\beta_{t-1} \oplus \\ &\oplus (A_1B_2 \oplus A_2B_1)f_t(A_2\alpha_t \oplus A_1\beta_t) = \\ =& A_2\alpha_{t-1} \oplus A_1\beta_{t-1} \oplus \\ &\oplus (A_1B_2 \oplus A_2B_1)f_t(A_1\alpha_{t-1} \oplus A_2\beta_{t-1}) = \\ =& A_1(\beta_{t-1} \oplus B_2f_t(A_1\alpha_{t-1} \oplus A_2\beta_{t-1})) \oplus \\ &\oplus A_2(\alpha_{t-1} \oplus B_1f_t(A_1\alpha_{t-1} \oplus A_2\beta_{t-1})) = \\ =& A_1\alpha_t \oplus A_2\beta_t = A_2\alpha_{t+1} \oplus A_1\beta_{t+1}, \end{aligned}$$

which by induction proves the identity $z_i = A_2\alpha_i \oplus A_1\beta_i$ for all values $i \in \{1,\ldots,r\}$.

From the system of equations regarding the values α_i and β_i, $i \in \{1,\ldots,r\}$,

$$\begin{aligned} z_i &= A_2\alpha_i \oplus A_1\beta_i \\ z_{i+1} &= A_2\alpha_{i+1} \oplus A_1\beta_{i+1} = \\ &= A_1\alpha_i \oplus A_2\beta_i \end{aligned}$$

we have

$$\alpha_i = (A_1^{-1}A_2 \oplus A_2^{-1}A_1)^{-1}(A_1^{-1}z_i \oplus A_2^{-1}z_{i+1})$$
$$\beta_i = (A_2^{-1}A_1 \oplus A_1^{-1}A_2)^{-1}(A_2^{-1}z_i \oplus A_1^{-1}z_{i+1}).$$

That is, from the intermediate (α_i, β_i), $i \in \{1,\ldots,r\}$, one can efficiently compute the corresponding value z_i, and conversely — from the values z_i and z_{i+1}, one can efficiently compute the corresponding value (α_i, β_i). From this, it follows that the L-Feistel scheme is a special case of the quasi-Feistel scheme with the combiner function $\Gamma(v,x,y) = v \oplus (A_1B_2 \oplus A_2B_1)x$, and permutations P, Q such that

$$P(\alpha_0, \beta_0) = (A_2\alpha_0 \oplus A_1\beta_0, A_1\alpha_0 \oplus A_2\beta_0),$$

and the permutation Q returns the pair of values (α_r, β_r) from the values z_r and z_{r+1} according to the solution of the previous system of equations. □

4. Quantum Cryptanalysis

In the work [2], Vaudenay proved that 3-round and 4-round Lai-Massey schemes are secure in the classical computing model against chosen-plaintext attacks and chosen-ciphertext attacks, respectively. In the work [8], it was proven that 3 rounds (4 rounds) is a necessary and sufficient condition for CPA-security (CCA-security) of the Lai-Massey scheme in the classical computing model.

But in the quantum computing model, in the work [9], it was proven that the 3-round Lai-Massey scheme is resistant to attacks using Simon's quantum algorithm, which distinguishes it from the Feistel scheme. On the other hand, it is sometimes noted that in the 2022 work [10] by Shuping Mao, Tingting Guo, Peng Wang, and Lei Hu, efficient quantum chosen-plaintext attacks on 3 rounds and chosen-ciphertext attacks on 4 rounds of the quasi-Feistel cipher were constructed using Simon's algorithm. Since the quasi-Feistel cipher is a unified scheme for Feistel and Lai-Massey schemes, and is a gen-

eralization of the Lai-Massey scheme, such a result may appear contradictory to the result in [9]. However, in [10], these attacks are constructed under an extremely strong restriction on the combiner function — only one specific function $\Gamma(v,x,y) = L_1(v) \oplus L_2(x) \oplus L_3(y)$ is considered, where the mapping L_1 is linear (Fig. 5 from [10]), which is very convenient for analysis.

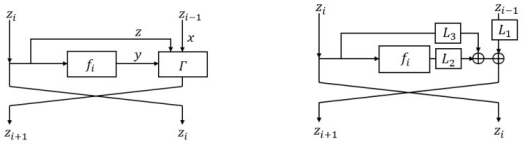


Figure 5: i-th round of the Lai-Massey scheme

Claim 4. *The scheme shown in Fig. 5 with the linear combiner function $\Gamma(v,x,y) = L_1(v) \oplus L_2(x) \oplus L_3(y)$ is equivalent to the standard Feistel scheme with different round functions.*

Proof. According to the scheme shown in Fig. 5, we have the round transformation for both parts $\alpha_i, \beta_i \in \{0,1\}^n$ of the i-th round, $i \in \{0,\dots,r-1\}$:

$$\alpha_{i+1} = L_1(\beta_i) \oplus L_3(\alpha_i) \oplus L_2(f_i(\alpha_i))$$
$$\beta_{i+1} = \alpha_i.$$

From this, it follows that for $i \in \{0,\dots,r-2\}$

$$\beta_{i+2} = L_1(\beta_i) \oplus L_3(\beta_{i+1}) \oplus L_2(f_i(\beta_{i+1})),$$

or

$$\beta_{i+2} = L_1(\beta_i) \oplus f_i^{'}(\beta_{i+1}),$$

since the transformations L_2 and L_3 can be included in the round functions:

$$f_i^{'}(\beta_{i+1}) = L_3(\beta_{i+1}) \oplus L_2(f_i(\beta_{i+1})).$$

For correct decryption, the transformation L_1 must be invertible, meaning an additional modification of the round functions will reduce the round transformation to this form:

$$\beta_{i+2} = \beta_i \oplus f_i^{''}(\beta_{i+1}),$$

where for all $i \in \{2,\dots,r-1\}$

$$f_i^{''}(\beta_{i+1}) = L_1^{-1}(f_i(L_1(\beta_{i+1}))),$$
$$f_1^{''}(\beta_2) = L_1^{-1}(f_1(\beta_2)),$$
$$f_r^{''}(\beta_{r+1}) = f_1(L_1(\beta_{r+1})).$$

This leads to the scheme shown in Fig. 5 being equivalent to the standard Feistel scheme with additional use of a linear transformation to one part of the ciphertext. □

Thus, there are no contradictions with the results of the work [9], since in the work [10] the standard Feistel scheme was investigated, and the obtained results are already known, starting from the work [11], and more complex attacks on a larger number of rounds are already known.

Moreover, it appears that even a distinguishing attack on one round of the quasi-Feistel scheme in the quantum computing model cannot be effective in the general case. The same applies to the general form of the MD GLM and UFLM schemes. It may be possible to construct attacks for specific partial cases.

Claim 5. *There exists an efficient chosen-plaintext distinguishing attack on two rounds of the L-Feistel scheme.*

Proof. We use property (1) for the first two rounds of the L-Feistel scheme, where (α_0,β_0), (α_1,β_1) and (α_2,β_2) are the plaintext and the outputs after the first and second rounds, respectively

$$A_1\alpha_0 \oplus A_2\beta_0 = A_2\alpha_1 \oplus A_1\beta_1,$$
$$A_1\alpha_1 \oplus A_2\beta_1 = A_2\alpha_2 \oplus A_1\beta_2.$$

When constructing the attack on two rounds, the values (α_0,β_0) and (α_2,β_2) are known, so we solve this system for α_1,β_1:

$$\alpha_1 = \big(A_1 \oplus A_2A_1^{-1}A_2\big)^{-1}\Big(A_2\alpha_2 \oplus A_1\beta_2 \oplus$$
$$\oplus A_2A_1^{-1}(A_1\alpha_0 \oplus A_2\beta_0)\Big),$$
$$\beta_1 = \big(A_2 \oplus A_1A_2^{-1}A_1\big)^{-1}\Big(A_1\alpha_0 \oplus A_2\beta_0 \oplus$$
$$\oplus A_1A_2^{-1}(A_2\alpha_2 \oplus A_1\beta_2)\Big).$$

This allows computing the value of the first round function from the value $A_1\alpha_0 \oplus A_2\beta_0$, so when constructing the attack, we use only such plaintexts for which this value is fixed, while for a random permutation this value is random, allowing the construction of an efficient distinguisher. □

The constructed attack even allows recovering the values of two round keys in the sense of recovering the round function value for a given argument.

Claim 6. *If there exists a quantum algorithm for solving the equation $f_1(x) \oplus f_2(x) = c$, then there exists an efficient chosen-plaintext distinguishing attack on two rounds of the MD-1 GLM scheme.*

Proof. The idea is very similar to the construction of the previous attack, but using the property of the MD-1 GLM scheme:

$$\alpha_{i+1} \oplus \beta_{i+1} = f_1(\alpha_i) \oplus f_2(\beta_i).$$

We use this property for the first two rounds, where (α_0, β_0), (α_1, β_1) and (α_2, β_2) are the plaintext and the outputs after the first and second rounds, respectively

$$\alpha_1 \oplus \beta_1 = f_1(\alpha_0) \oplus f_2(\beta_0),$$
$$\alpha_2 \oplus \beta_2 = f_1(\alpha_1) \oplus f_2(\beta_1).$$

If we take values α_0 and β_0 such that $f_1(\alpha_0) = f_2(\beta_0)$, then it follows that $\alpha_1 = \beta_1$, and this value can be recovered by solving the equation $\alpha_2 \oplus \beta_2 = f_1(\alpha_1) \oplus f_2(\alpha_1)$, since α_2 and β_2 are known, which will distinguish the cipher from a random permutation. □

This attack also allows recovering the values of the round keys and can be performed given a quantum algorithm for solving the equation $f_1(x) \oplus f_2(x \oplus d) = c$ for known values c, d.

Conclusions

In this work, various generalizations of the Lai-Massey scheme are considered, including unified schemes that combine Lai-Massey and Feistel schemes: MD GLM, MD GLM-1, MD GLM-3, UFLM, L-Feistel scheme, and quasi-Feistel scheme. Reductions of the MD GLM, UFLM, and L-Feistel schemes to the quasi-Feistel scheme are constructed. Efficient quantum attacks from the work by Shuping Mao et al. are examined: chosen-plaintext on 3 rounds and chosen-ciphertext on 4 rounds for a special case of the quasi-Feistel cipher using Simon's algorithm. It is proven that the restrictions on the quasi-Feistel cipher in that work led to the degeneration of the quasi-Feistel scheme into the standard Feistel scheme, thus their results replicate known results of quantum attacks on the Feistel scheme. It does not seem possible in the quantum computing model to even construct an efficient distinguishing attack on one round of the quasi-Feistel scheme in the general case. Additionally, efficient distinguishing attacks on two rounds of the L-Feistel scheme and the MD-1 GLM scheme are constructed (assuming the existence of an efficient quantum algorithm for solving an equation of a certain form), which also allow recovering the values of the corresponding round keys.

References

[1] X. Lai and J. L. Massey, *A Proposal for a New Block Encryption Standard*, pp. 389–404. Springer Berlin Heidelberg, 1991.

[2] S. Vaudenay, *On the Lai-Massey Scheme*, pp. 8–19. Springer Berlin Heidelberg, 1999.

[3] M. R. M. Shamsabad and S. M. Dehnavi, "Lai-Massey Scheme Revisited." Cryptology ePrint Archive, Paper 2020/005, Jan. 2020.

[4] J. Liu, B. Sun, and C. Li, "Design and cryptanalysis of a new iterative structure," *IET Information Security*, vol. 17, pp. 335–346, Nov. 2022.

[5] Z. Dai, C. Guo, and C. Li, *UFLM: A Unified Framework for Feistel Structure and Lai-Massey Structure*, pp. 117–142. Springer Nature Switzerland, Dec. 2024.

[6] A. Yun, J. H. Park, and J. Lee, "Lai-Massey Scheme and Quasi-Feistel Networks." Cryptology ePrint Archive, Paper 2007/347, Sept. 2007.

[7] A. Yun, J. H. Park, and J. Lee, "On Lai-Massey and quasi-Feistel ciphers," *Designs, Codes and Cryptography*, vol. 58, pp. 45–72, Mar. 2010.

[8] Y. Luo, X. Lai, and Z. Gong, "Pseudorandomness analysis of the (extended) lai-massey scheme," *Information Processing Letters*, vol. 111, pp. 90–96, Dec. 2010.

[9] Y.-Y. Luo, H.-L. Yan, L. Wang, H.-G. Hu, and X.-J. Lai, "Study on block cipher structures against Simon's quantum algorithm (in chinese)," *Journal of Cryptologic Research*, vol. 6(5), pp. 561–573, 2019.

[10] S. Mao, T. Guo, P. Wang, and L. Hu, *Quantum Attacks on Lai-Massey Structure*, pp. 205–229. Springer International Publishing, Aug. 2022.

[11] H. Kuwakado and M. Morii, "Quantum distinguisher between the 3-round Feistel cipher and the random permutation," in *2010 IEEE International Symposium on Information Theory*, IEEE, June 2010.