International Journal of Mathematics and Statistics (IJMS)

DOI: 10.5281/zenodo.21461266 | ISSN: 3141-6438 | Volume: 1 | Issue: 2 | 2026

Free Inverse Semigroups: Scheiblich and Wagner Constructions, Universal Properties, and Algebraic Applications

Udoaka, O. G.

Department of Mathematics, Akwa Ibom State University, Nigeria
Corresponding Author: otobongawasi@aksu.edu.ng

Abstract

This paper presents a rigorous and unified account of the construction of free inverse semigroups, with emphasis on the classical approaches associated with Scheiblich and Wagner. Beginning with the algebraic foundations of regular and inverse semigroups, the paper formulates the universal property that characterizes a free inverse semigroup on a nonempty set. It then describes two complementary constructions: a representation through isomorphisms between principal ideals of a semilattice and a quotient construction arising from the free semigroup with involution. The relationship between these models is clarified by showing that both satisfy the same universal mapping property and are therefore uniquely isomorphic. The discussion also includes the natural partial order, idempotent semilattices, the Wagner–Preston representation theorem, and the role of Munn-type representations. A small worked example illustrates how words, formal inverses, and commuting idempotents interact in the free inverse setting. Finally, the paper highlights connections with transformation semigroups, homomorphism problems, group-theoretic cryptography, and modern algebraic security models. The resulting treatment converts the classical constructions into a coherent reference suitable for further work in semigroup theory, computational algebra, and algebraic cryptography.

Keywords: inverse semigroup; free inverse semigroup; involution; Scheiblich construction; Wagner construction; universal property; idempotent semilattice; transformation semigroup.
MSC 2020: 20M18, 20M05, 20M30, 20F10.

1. Introduction

Inverse semigroups occupy a natural position between group theory and general semigroup theory. A group models global symmetry: each element acts everywhere and has a two-sided inverse. An inverse semigroup models partial symmetry: an element may act only on part of a space, but it still has a uniquely determined inverse on its domain. This viewpoint explains why inverse semigroups occur in the study of partial bijections, automata, symbolic dynamics, operator algebras, geometric group theory, and the algebra of computation.

The existence of free objects in varieties follows abstractly from universal algebra. Such an existence theorem, however, does not by itself reveal the internal structure of the free inverse semigroup. The classical constructions of Scheiblich, Wagner, Preston, and Munn provide concrete models. Scheiblich's method realizes the free inverse semigroup through isomorphisms between principal ideals of a semilattice, while the Wagner-style method begins with freely generated words equipped with a formal involution and factors by the identities needed for regularity and commuting idempotents. Preston's canonical forms, Munn's representation theory, and later comparative accounts clarify the geometry, order structure, and representation theory of the resulting object [18, 20, 19, 13, 10, 4]. Presentations and relations for semigroups and inverse semigroups supply a complementary algebraic viewpoint [2], while the contrast between groups and semigroups places these constructions in a wider structural setting [12].

Recent algebraic work also demonstrates that semigroup and group structures remain relevant to cryptographic design. Nilpotent and solvable groups, conjugacy classes, quaternion-group homomorphisms, transformation semigroups, and elliptic-curve groups have all been studied as algebraic platforms or structural tools in security-oriented research [7, 9, 6, 8, 16, 14]. These works do not construct free inverse semigroups directly, but they motivate the broader study of algebraic objects with effective normal forms, homomorphism theory, and computable partial symmetries.

2. Preliminaries

Definition 2.1. A *semigroup* is a nonempty set S equipped with an associative binary operation. A *monoid* is a semigroup possessing an identity element.

Definition 2.2. An element $y \in S$ is an *inverse* of $x \in S$ if

$$xyx = x \qquad \text{and} \qquad yxy = y.$$

A semigroup is *regular* if every element has at least one inverse. It is an *inverse semigroup* if every element has a unique inverse, denoted x^{-1}.

Lemma 2.3. *If S is an inverse semigroup and $x \in S$, then xx^{-1} and $x^{-1}x$ are idempotents.*

Proof. Using $xx^{-1}x = x$ and associativity,

$$(xx^{-1})^2 = xx^{-1}xx^{-1} = xx^{-1}.$$

Similarly,

$$(x^{-1}x)^2 = x^{-1}xx^{-1}x = x^{-1}x.$$

□

The set of idempotents of S is denoted by

$$\mathrm{E}(S) = \{e \in S : e^2 = e\}.$$

Theorem 2.4. *A regular semigroup is inverse if and only if its idempotents commute.*

Proof. This is the standard characterization of inverse semigroups among regular semigroups. If the idempotents commute, two inverses y and z of an element x satisfy

$$y = yxy = y(xz) = (yx)z = (zx)y = z(xy) = zxy = z,$$

so the inverse is unique. Conversely, uniqueness of inverses forces the idempotents of a regular semigroup to commute. A complete classical proof is given in Howie [5] and Lawson [10]. □

Definition 2.5. An *involution* on a semigroup S is a map $* : S \to S$ satisfying

$$(st)^* = t^* s^*, \qquad (s^*)^* = s$$

for all $s, t \in S$. In an inverse semigroup, the map $s \mapsto s^{-1}$ is an involution.

2.1. Natural partial order

Every inverse semigroup carries a canonical partial order.

Definition 2.6. For $s, t \in S$, define $s \leq t$ if there exists $e \in \mathrm{E}(S)$ such that $s = te$.

Proposition 2.7. *For an inverse semigroup S and $s, t \in S$, the following are equivalent:*

(i) $s \leq t$;
(ii) $s = te$ *for some* $e \in \mathrm{E}(S)$;
(iii) $s = ft$ *for some* $f \in \mathrm{E}(S)$;
(iv) $s = ts^{-1}s$;
(v) $s = ss^{-1}t$.

Proof. The equivalence is standard, but the main steps are included. If $s = te$ with $e^2 = e$, then

$$s^{-1}s = et^{-1}te$$

is idempotent and

$$ts^{-1}s = tet^{-1}te = te = s.$$

Thus (ii) implies (iv). From (iv), $s = (ts^{-1})s$ and ts^{-1} is compatible with the idempotent ss^{-1}; more directly,

$$s = ts^{-1}s = (ts^{-1}t)t^{-1}s,$$

and the standard inverse-semigroup identities yield the left-idempotent form $s = (ss^{-1})t$. The remaining implications follow by symmetry and by taking inverses. These identities show that the relation is reflexive, antisymmetric, and transitive. □

Under the representation by partial bijections, $s \leq t$ means exactly that s is a restriction of t.

2.2. Wagner–Preston representation

Let $\mathcal{I}(X)$ denote the symmetric inverse monoid of all partial bijections of a set X under composition.

Theorem 2.8 (Wagner–Preston)**.** *Every inverse semigroup is isomorphic to an inverse subsemigroup of a symmetric inverse monoid.*

Proof sketch. For $s \in S$, let

$$D_{s^{-1}s} = \{x \in S : xx^{-1} \leq s^{-1}s\}$$

and define $\rho_s : D_{s^{-1}s} \to D_{ss^{-1}}$ by $\rho_s(x) = sx$. One verifies that ρ_s is a bijection with inverse $\rho_{s^{-1}}$, and that $\rho_{st} = \rho_s \rho_t$ on the appropriate domain. The map $s \mapsto \rho_s$ is injective, yielding the required representation [10, 11, 3]. □

3. Free inverse semigroups and the universal property

Definition 3.1. Let X be a nonempty set. A pair (F, ι) is a *free inverse semigroup on* X if F is an inverse semigroup, $\iota : X \to F$ is a map whose image generates F as an inverse semigroup, and for every inverse semigroup S and every map $f : X \to S$, there exists a unique inverse-semigroup homomorphism $\widehat{f} : F \to S$ satisfying

$$\widehat{f} \circ \iota = f.$$

Denote $F = \mathrm{FIS}(X)$.

A homomorphism between inverse semigroups automatically preserves inversion.

Proposition 3.2. *If $\varphi : S \to T$ is a semigroup homomorphism between inverse semigroups, then*

$$\varphi(s^{-1}) = \varphi(s)^{-1}$$

for every $s \in S$.

Proof. Since $ss^{-1}s = s$ and $s^{-1}ss^{-1} = s^{-1}$,

$$\varphi(s)\varphi(s^{-1})\varphi(s) = \varphi(s),$$

$$\varphi(s^{-1})\varphi(s)\varphi(s^{-1}) = \varphi(s^{-1}).$$

Thus $\varphi(s^{-1})$ is an inverse of $\varphi(s)$. Uniqueness of inverses in T gives the result. □

Theorem 3.3 (Uniqueness of the free object)**.** *Any two free inverse semigroups on the same generating set X are uniquely isomorphic by an isomorphism that fixes X.*

Proof. Let (F, ι) and (G, κ) be free on X. By the universal property of F, there exists a unique homomorphism $\alpha : F \to G$ with $\alpha\iota = \kappa$. Similarly, there exists a unique $\beta : G \to F$ with $\beta\kappa = \iota$. Then $\beta\alpha : F \to F$ fixes $\iota(X)$. By uniqueness, $\beta\alpha = \mathrm{id}_F$. Likewise, $\alpha\beta = \mathrm{id}_G$. Hence α is the required isomorphism. □

4. Scheiblich's semilattice construction

The Scheiblich construction is most naturally described using the free group on X. Let $G = FG(X)$ be the free group generated by X, and let $\mathcal{P}_f(G)$ denote the finite subsets of G.

One standard realization of the free inverse monoid uses pairs (A, g) where A is a finite prefix-closed subset of the Cayley graph containing 1 and g. For the present paper, it is enough to use the following abstracted version of the construction.

Let $\mathcal{E}$ be a semilattice of finite connected subtrees of the Cayley graph of G containing the identity. Multiplication in $\mathcal{E}$ is union followed by connected closure, and the order is reverse inclusion or inclusion depending on convention. For $g \in G$, translation sends a subtree A to gA.

Define

$$\mathcal{S}(X) = \{(A, g) : A \in \mathcal{E},\ 1, g \in A\},$$

with multiplication

$$(A, g)(B, h) = \big(A \cup gB, gh\big) \tag{1}$$

and inversion

$$(A, g)^{-1} = \big(g^{-1}A, g^{-1}\big). \tag{2}$$

Proposition 4.1. *The structure $\mathcal{S}(X)$ is an inverse monoid with identity $(\{1\}, 1)$.*

Proof. Associativity follows from

$$\big(A \cup gB\big) \cup ghC = A \cup g(B \cup hC).$$

The identity is immediate. For $(A, g) \in \mathcal{S}(X)$, let $(A, g)^\dagger = (g^{-1}A, g^{-1})$. Then

$$(A, g)(A, g)^\dagger = (A, 1),$$

and

$$(A, g)^\dagger(A, g) = (g^{-1}A, 1).$$

Consequently,

$$(A, g)(A, g)^\dagger(A, g) = (A, g)$$

and similarly for $(A, g)^\dagger$. Idempotents have the form $(A, 1)$ and commute because their multiplication is induced by union. By Theorem 2.4, $\mathcal{S}(X)$ is inverse. □

The generator corresponding to $x \in X$ is

$$\eta(x) = \big(\{1, x\}, x\big).$$

The subsemigroup generated by $\eta(X)$ and their inverses is the free inverse monoid $\mathrm{FIM}(X)$; related classical refinements of free inverse-semigroup constructions are discussed by O'Carroll [15]; deleting the identity yields the free inverse semigroup, subject to the usual convention about whether the empty word is included.

Scheiblich's original description may also be formulated as a semigroup of isomorphisms between principal ideals of the idempotent semilattice. In that language, each element determines a partial symmetry of the semilattice, and multiplication is composition on the largest common domain. This makes the link with the Wagner–Preston theorem explicit [20, 18, 13].

5. Wagner's quotient construction from a free semigroup with involution

Let $X^{-1} = \{x^{-1} : x \in X\}$ be a disjoint copy of X, and put

$$Y = X \sqcup X^{-1}.$$

Let Y^+ be the free semigroup on Y. Define an involution on words by

$$(y_1 y_2 \cdots y_n)^* = y_n^* \cdots y_2^* y_1^*,$$

where $(x^{-1})^* = x$ and $x^* = x^{-1}$.

Proposition 5.1. *The semigroup Y^+ with $*$ is the free semigroup with involution on X.*

Proof. Let $(S, *)$ be any semigroup with involution and let $f : X \to S$. Extend f to Y by setting $f(x^{-1}) = f(x)^*$. Since Y^+ is a free semigroup, there is a unique homomorphism $\widehat{f} : Y^+ \to S$. For a word $w = y_1 \cdots y_n$,

$$\widehat{f}(w^*) = \widehat{f}(y_n^*) \cdots \widehat{f}(y_1^*) = \widehat{f}(y_n)^* \cdots \widehat{f}(y_1)^* = \widehat{f}(w)^*.$$

Thus $\widehat{f}$ preserves the involution, and uniqueness is inherited from the free-semigroup property. □

To obtain an inverse semigroup, impose the identities

$$ww^*w = w \tag{3}$$

and

$$ww^*vv^* = vv^*ww^* \tag{4}$$

for all words $w, v \in Y^+$. Let ρ be the least congruence on Y^+ containing all pairs determined by (3) and (4). Define

$$W(X) = Y^+/\rho.$$

Theorem 5.2. *The quotient $W(X)$ is a free inverse semigroup on X.*

Proof. Write $[w]$ for the ρ-class of w. By (3), $[w^*]$ is an inverse of $[w]$. By (4), all elements of the form $[w][w]^* = [ww^*]$ commute. Hence $W(X)$ is regular with commuting idempotents, and therefore inverse by Theorem 2.4.

Let S be an inverse semigroup and let $f : X \to S$. By Proposition 5.1, f extends uniquely to an involution-preserving homomorphism $\widetilde{f} : Y^+ \to S$. In every inverse semigroup,

$$\widetilde{f}(w)\widetilde{f}(w)^*\widetilde{f}(w) = \widetilde{f}(w),$$

and idempotents commute, so $\rho \subseteq \ker(\widetilde{f})$. Therefore $\widetilde{f}$ factors uniquely through a homomorphism

$$\widehat{f} : W(X) \to S.$$

This homomorphism extends f, and uniqueness follows because the classes of the generators generate $W(X)$. □

6. Equivalence of the Scheiblich and Wagner constructions

Theorem 6.1. *The inverse semigroups obtained from the Scheiblich and Wagner constructions are canonically isomorphic.*

Proof. By construction, both $\mathcal{S}(X)$ (or its generated free inverse subsemigroup) and $W(X)$ satisfy the universal property of a free inverse semigroup on X. Therefore, Theorem 3.3 gives a unique isomorphism

$$\Phi : W(X) \longrightarrow \mathcal{S}(X)$$

that sends the class of each generator x to the Scheiblich generator $(\{1, x\}, x)$. The inverse is the unique homomorphism induced in the opposite direction by the same generating map. □

The proof is short because the universal property contains all the needed rigidity. However, the two constructions emphasize different information:

7. A worked example on one generator

Let $X = \{a\}$. In the free group $FG(X) \cong \mathbb{Z}$, words reduce to integer powers a^n. In the free inverse monoid, however, the elements are not determined only by the group component a^n; they also retain domain information through an idempotent support.

For example, in the Scheiblich model, let

$$A = \{1, a, a^2\}, \qquad B = \{1, a^{-1}\}.$$

Table 1: Comparison of the two constructions.

Feature	Scheiblich/Munn-type model	Wagner quotient model
Basic objects	Finite subtrees or principal ideals in a semilattice	Words over generators and formal inverses
Multiplication	Translation and union/composition of partial maps	Concatenation modulo inverse identities
Inversion	Geometric reversal/translation	Formal word reversal with letter inversion
Idempotents	Semilattice elements such as $(A, 1)$	Classes $[ww^*]$
Main strength	Reveals geometry, order, and partial symmetries	Reveals universal algebra and presentations
Computational use	Munn trees and normal-form algorithms	Rewriting systems and congruence calculations

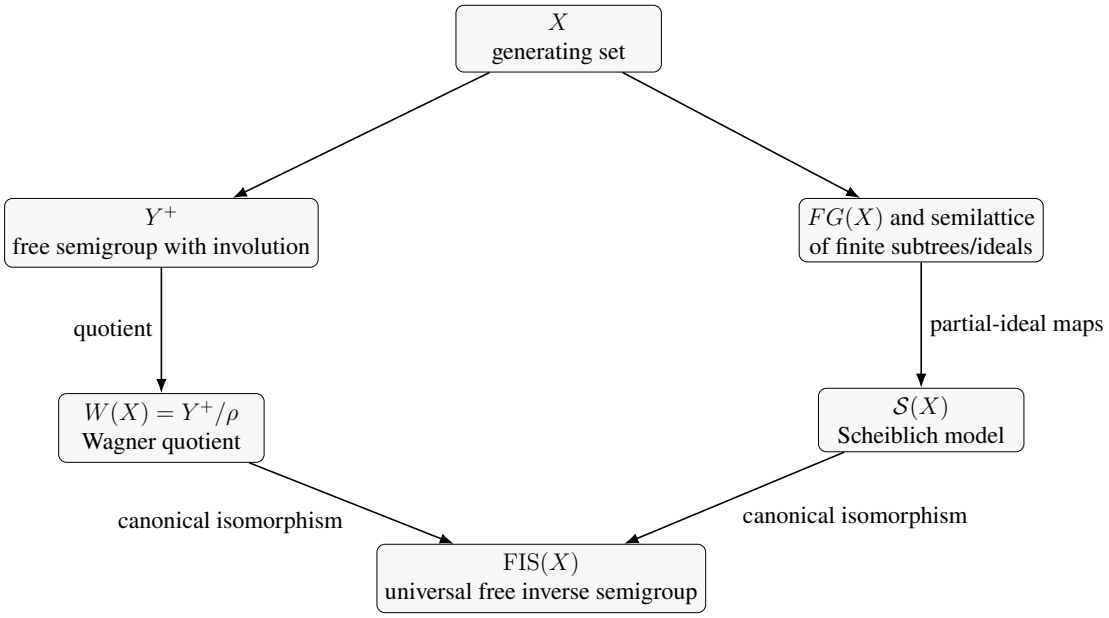

Figure 1: Two routes to the same free inverse semigroup.

Then

$$(A, a)(B, a^{-1}) = (A \cup aB, 1).$$

Since $aB = \{a, 1\}$,

$$(A, a)(B, a^{-1}) = (\{1, a, a^2\}, 1),$$

which is an idempotent. In contrast,

$$(B, a^{-1})(A, a) = (B \cup a^{-1}A, 1) = (\{1, a^{-1}, a\}, 1).$$

These are distinct idempotents, showing that the free inverse monoid on one generator is much richer than the infinite cyclic group.

In the Wagner model, the corresponding phenomenon appears through words such as

$$aa^{-1}, \qquad a^{-1}a,$$

which are idempotents but are not forced to be equal. They commute, but they encode different domains. This distinction is precisely what permits inverse semigroups to model partial rather than global symmetries.

8. Homomorphisms, subgroups, and transformation structure

The universal property makes homomorphisms out of $\mathrm{FIS}(X)$ particularly transparent: specifying the images of generators determines a unique homomorphism. This is analogous to free groups and free semigroups, but the target values automatically determine the images of formal inverses and idempotent supports.

Homomorphism-counting questions for finite groups, such as the quaternion group Q_8, illustrate how structural constraints affect the number of admissible maps [8]. In an inverse-semigroup setting, one must additionally preserve products and, automatically, inverses. When the target is a symmetric inverse monoid, a homomorphism selects compatible partial bijections, so domain idempotents play a central role.

Transformation semigroups provide another bridge. The rank and maximal subgroup structure of a full transformation semigroup reflects the interaction between noninvertible maps and local permutation groups [16]. Inverse subsemigroups isolate those transformations that are partially invertible, and the Wagner–Preston theorem shows that every inverse semigroup can be studied in this form.

9. Connections with algebraic cryptography

Noncommutative algebraic structures have repeatedly been proposed as platforms for cryptographic primitives. Conjugacy-search constructions use equations such as

$$y = g^{-1}xg,$$

where recovering g may be computationally difficult in a suitably chosen group. The key-agreement framework studied by John, Udoaka, and Musa uses conjugacy classes in finitely generated groups [6]. Free inverse semigroups provide a broader language in which transformations may be partially defined, making it possible to model protocols with state-dependent or domain-restricted operations.

Nilpotent and solvable groups are attractive because their subgroup structure and normal forms can be controlled while still supporting nontrivial computational problems. The studies on nilpotent-group key exchange and solvable groups with restricted character-theoretic properties

demonstrate this structural viewpoint [7, 9]. Although these papers work primarily in group theory, their methods motivate investigation of maximal subgroups and local groups inside inverse semigroups.

Elliptic-curve groups remain central to efficient public-key cryptography. The study of elliptic-curve groups in a quantum-era context emphasizes the continuing importance of algebraic structure and algorithmic representation [14]. An inverse-semigroup extension could encode partial scalar actions, restricted domains, or composable protocol states, but any cryptographic proposal would require a carefully stated hardness assumption and rigorous security analysis.

Topological variants show that freeness also interacts fruitfully with additional structure beyond the purely algebraic category [1]. These observations suggest three research directions:

(i) develop normal-form algorithms for finitely presented inverse semigroups that are suitable for implementation;
(ii) study hard search problems associated with partial conjugation, idempotent supports, and restricted-domain actions;
(iii) investigate whether inverse-semigroup actions can model access control, stateful protocols, or fault-tolerant transformations more naturally than groups alone.

10. Conclusion

This paper has developed a coherent account of free inverse semigroups from two classical viewpoints. The Scheiblich construction exhibits elements as geometric or semilattice-based partial symmetries, while the Wagner construction presents them as words with formal inverses modulo the identities of regularity and commuting idempotents. The universal property proves that the resulting inverse semigroups are canonically isomorphic.

Several structural features are essential. Idempotents form a commuting semilattice; the natural partial order records restriction; homomorphisms preserve inversion automatically; and the Wagner–Preston theorem embeds every inverse semigroup into partial bijections. Together, these facts explain why inverse semigroups are the correct algebraic setting for partial symmetry.

The connections with transformation semigroups, homomorphism theory, nilpotent and solvable groups, conjugacy-based key exchange, and elliptic-curve groups indicate a wider computational relevance. Future work should move beyond purely formal analogy by developing explicit algorithms, complexity estimates, and security definitions for inverse-semigroup-based constructions.

Funding

The author received no specific funding for this work.

Conflict of Interest

The author declares no conflict of interest.

Copyright and License

Copyright © 2026 The Author.

This article is published by *International Journal of Mathematics and Statistics (IJMS)* under Ktrend Journals and is distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

References

[1] T. Banakh, I. Guran, and O. Gutik, "Free topological inverse semigroups," *Topology and its Applications*, 2021.

[2] C. Carvalho, *Presentations of Semigroups and Inverse Semigroups*, University of St Andrews, 2003.

[3] K. Cheaney, *An Introduction to Inverse Semigroups and Their Connections to C^*-Algebras*, Carleton University, 2022.

[4] C. Hollings, "Three approaches to inverse semigroups," *European Journal of Pure and Applied Mathematics*, vol. 8, no. 3, pp. 294–323, 2015.

[5] J. M. Howie, *Fundamentals of Semigroup Theory*, Oxford University Press, Oxford, 1995.

[6] M. N. John and O. G. Udoaka, "Key agreement protocol using conjugacy classes of finitely generated group," *International Journal of Scientific Research in Science and Technology*, vol. 10, no. 6, pp. 52–56, 2023. doi: 10.32628/IJSRST2310645.

[7] M. N. John, O. G. Udoaka, and A. Musa, "Nilpotent groups in cryptographic key exchange protocol for $N \geq 1$," *Journal of Mathematical Problems, Equations and Statistics*, vol. 4, no. 2, pp. 32–34, 2023. doi: 10.22271/math.2023.v4.i2a.103.

[8] M. N. John, E. E. Bassey, O. G. Udoaka, J. T. Otobong, and O. U. Promise, "On finding the number of homomorphism from Q_8," *International Journal of Mathematics and Statistics Studies*, vol. 11, no. 4, pp. 20–26, 2023. doi: 10.37745/ijmss.13/vol11n42026.

[9] M. N. John, O. G. Udoaka, and A. Musa, "Solvable groups with monomial characters of prime power codegree and monolithic characters," *Bulletin of Mathematics and Statistics Research*, vol. 11, no. 7, pp. 98–102, 2023. doi: 10.33329/bomsr.11.4.98.

[10] M. V. Lawson, *Inverse Semigroups: The Theory of Partial Symmetries*, World Scientific, Singapore, 1998.

[11] M. V. Lawson, *Introduction to Inverse Semigroups*, Heriot-Watt University and Maxwell Institute for Mathematical Sciences, Edinburgh, 2023.

[12] J. Meakin, "Groups and semigroups: Connections and contrasts," Department of Mathematics, University of Nebraska-Lincoln, 2006.

[13] W. D. Munn, "Free inverse semigroups," *Proceedings of the London Mathematical Society*, 1974.

[14] B. O. Nwala, M. N. John, and O. G. Udoaka, "Elliptic-curve groups in quantum-era cryptography," *ISAR Journal of Science and Technology*, vol. 1, no. 1, pp. 21–24. doi: 10.5281/zenodo.10207536.

[15] L. O'Carroll, "A note on free inverse semigroups," Mathematical Institute, Edinburgh, 1973.

[16] O. G. Udoaka, "Rank of maximal subgroup of full transformation semigroup," *International Journal of Current Research*, 6(9), 8351–8354, 2014.

[17] F. Nwawuru and O. G. Udoaka, “Free Semigroup Presentations,” *International Journal of Applied Science and Mathematical Theory*, 4(3), 42–51, 2018.

[18] G. B. Preston, “Free inverse semigroups,” *Journal of the Australian Mathematical Society*, 1972.

[19] N. R. Reilly, “Free generators in free inverse semigroups,” *Bulletin of the Australian Mathematical Society*, vol. 7, pp. 407–424, 1972.

[20] H. E. Scheiblich, “Free inverse semigroups,” *Semigroup Forum*, vol. 4, pp. 351–359, 1972.