E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 18-11-2025
Accepted: 23-12-2025
Published: 21-01-2026

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 4; Issue 1; 2026; Page No. 22-26

To The Study of Platforms for the Semidirect Product Key Exchange

[1]Deepak Kumar Gupta, [2]Pratima Ojha and [3]Ajay Kumar Singh

[1-3]Department of Mathematics, Madhyanchal Professional University, Bhopal, Madhya, Pradesh, India

DOI: https://doi.org/10.5281/zenodo.18336833

Corresponding Author: Deepak Kumar Gupta

Abstract

It starts with the Semidirect Product Key Exchange (SDPKE), which is an extension of the Diffie-Hellman Key Exchange, and uses the difficulty of the Semidirect Computational Diffie-Hellman Problem to analyze various cryptosystems. We also think of the semidirect discrete logarithm problem as a cryptographic group action and classify its quantum complexity as a result. This problem has been overlooked despite its relevance. In particular, our protocol may be based on any non-commutative group. There are some superficial parallels between our method and the standard Diffie-Hellman protocol, but we believe our technique is preferable due to many important changes.

Keywords: Semidirect, Exchange, Diffie-Hellman, Computational and Protocol

Introduction

When p is prime and g is primitive mod p, the original and simplest way to implement the protocol is to utilize the multiplicative group of integers modulo p. A protocol description that is more generic makes use of any finite cyclic group. An ongoing effort is being made to identify alternative platforms that might provide a more efficient Diffie-Hellman or comparable key exchange, especially with smaller public/private keys. Several promising new avenues have emerged as a result of this investigation; one of them is elliptic curve cryptography. We also direct the reader to for an overview of suggested non-abelian (= non-commutative) group based cryptographic primitives. Our aim in this study is to propose a novel key exchange protocol that relies on the extension of a (semi)group via automorphisms, not to conduct a review of these previous attempts.

Any group, and especially any non-commutative group, may serve as the basis for our protocol. Although it has certain outward similarities with the conventional Diffie-Hellman protocol, our approach has a number of key differences that we think make it superior. Specifically, unlike the standard Diffie-Hellman protocol, the parties here only broadcast a portion of the result when computing the big power of a public element. A more complicated suggestion for a key agreement based on the semidirect product of two monoids and an alternative, rather different, cryptosystem based on the semidirect product of two groups are also mentioned. We strongly disagree with both of these suggestions. Lastly, it is worth mentioning that other algebraic systems, such as associative rings or Lie rings, may easily adopt the fundamental architecture (semidirect product) used in this study with minor adjustments. From there, key exchange protocols comparable to ours can be constructed.

A group is defined by the following four axioms: closure, associativity, identity, and inverse. Any two items in a closed group may be binary-operated upon to produce another element of the same type. Any three variables a, b, and c may be multiplied by any other to get a * (b * c), since the order of operations is unimportant in associativity groups. The unique element in the group, frequently symbolized by the letter e, is verified by the fact that for any element an in the group, the equation e * a = a * e = a hold. You can't have an element an in a group without also having an element a^-1, such that the product of a and a^-1 is equal to e. The inverse property describes this. A few examples of groups are the additive group of integers (represented by (Z, +)), the multiplicative group of non-zero rational numbers (Q*, ×), and the group of symmetries of a regular polygon (which includes all the polygon's rotations and reflections with composition as the binary operation).

Among the many significant concepts in group theory are subgroups, homomorphisms, isomorphisms, and costs. Any set of elements that, when combined using the same binary

operation, also constitute a group is called a subgroup. To be considered a homomorphism, a function must preserve the binary operation between the two groups, meaning that for every element a and element b in the group, f(a * b) = f(a) * f(b). Bijective homomorphisms include isomorphisms, which are one-to-one and onto. Transforming a subgroup by one of the members of the group forms a coset, which is a subset of the group. An important result in group theory, Lagrange's theorem states that the order of a subgroup divides the order of the group. The order of a group is proportional to the number of its members, whereas the order of an element is the smallest positive integer n that makes a^n = e, with the identity element of the group being e.

Literature Review

Deepa Jaiswal (2024) [1] The use of group theory offers a solid basis for the development of cryptographic systems that are both effective and secure. Its use encompasses a variety of public-key cryptography methods, such as the widely employed RSA and ECC algorithms, in addition to the more recent developments in post-quantum cryptography. A group is a reasonably common algebraic object, and the majority of cryptographic algorithms make use of groups in some form or another. Finite cyclic groups are used in particular for the purpose of the Diffie–Hellman key exchange. Therefore, the term "group-based encryption" is most often used to refer to cryptographic techniques that make use of infinite non-abelian groups.

Alex Musa and Udoka Otobong G (2024) [2]. In this research, a resilient digital signature technique that is based on lattices and makes use of matrix groups to improve post-quantum security is presented. Our system is able to show both theoretical and practical security since it is constructed on the difficulty of lattice problems such as the Shortest Vector Problem (SVP) and Learning with Errors (LWE), in addition to the complexity of the Matrix Group Conjugacy Problem. In order to comprehensively assess performance, we meticulously develop the mathematical underpinnings of the (MGCP), conduct an analysis of the computational complexity, and give numerical simulations. The use of this method brings about a novel combination of lattice and matrix group theory, which enables the development of post-quantum cryptography with fresh perspectives and opportunities.

Emerencia, C. (2024) [3]. The fact that there is no known classical efficient method that can convert huge numbers into primes ensures that modern cryptosystems that are used on a daily basis, such as RSA, continue to be secure. However, the security of current cryptosystems is placed in jeopardy by the imminent arrival of quantum computers, which are predicted to become available shortly. To provide a more tangible example, Shor's quantum method, for instance, is capable of solving the integer factorization problem in very short polynomial time. I explored the group-theoretical generalization of integer factorization, which is known as the Hidden Subgroup issue, as part of my PhD thesis. I also studied the state-of-the-art of the many approaches and algorithms that have been discovered to address this issue in a variety of situations. For instance, this issue has previously been addressed in an effective manner for the scenario in which the associated group G is abelian, also known as Hamiltonian.

Vasco, María et al. (2024) [4]. A (relatively) uncharted territory in the theory of finite simple groups might provide intriguing computing challenges and modelling tools applicable to cryptography. We give the necessary definitions to make the material comprehensible for both group theorists and cryptographers, with the aim of encouraging additional communication between these two (non-disjoint) groups, and we examine various scenarios where finite non-abelian simple groups are obviously fundamental in cryptography. Specifically, we examine constructs that stem from different group-theoretic factorization issues, describe completely homomorphic encryption using simple groups, and survey group theoretical hash functions. Also, in this context, the Hidden Subgroup Problem is briefly examined.

Dr. Gyanvendra, Pratap et al. (2024) [5]. To better understand the border between a home system and one that does not, we provide an analysis of several mathematical ideas in this study. The mysterious algebra of organic device biology and group cognition are both uncovered by our work. In this paper, we argue that, in terms of ordering, it is often feasible to use the perturbation principle to force a fast examination of the changes in the near 64-time area of the genome.

Research Methodology

The numerous cases of the so-called Semidirect Product Key Exchange, also known as SDPKE, are discussed in this aforementioned section. To be more specific, we conduct an analysis of the difficulty of the underlying security problem for a wide range of different mathematical objects, providing a comprehensive survey of the current state of the art.

First, for obvious reasons, it is crucial to build a landscape of post-quantum methods based on a wide range of computational issues for security concerns. For example, solving one class of computational problems shouldn't mean that all postquantum cryptography is broken.

Second, noninteractive key exchanges, which provide the following general benefit, are not a part of the NIST standardization process.

Data Analysis

This section addresses the several occurrences of the Semidirect Product Key Exchange, or SDPKE. We specifically examine the complexity of the foundational security issue across various mathematical constructs, providing an extensive review of the current advancements; we also critique existing literature in this domain and address certain technical deficiencies that have been implicitly overlooked by these contributions.

The Semidirect Product

Definition 1: Consider the endomorphism semigroup of a finite semigroup G, denoted as *End (G). G ⋋ End(G)*, which is the semidirect product of G by End(G), is composed of the ordered pairings *G x End (G)* that are multiplication-equipped, identified by

$$(g, \phi)(h, \psi) = (\psi(g)h, \psi\phi)$$

where $\psi\phi$ refers to the function that is obtained by applying ϕ first, and then ψ after that.
If G is in fact a semigroup, which means that at least one of its elements does not have an inverse, then the structure that is produced by G ⋉ End(G) could be considered a semigroup in and of itself. On the other hand, if we take into account the possibility of invertibility, we do in fact obtain a group. The following is a typical model that has been slightly modified to accommodate our particular notation.

Theorem 1: Consider G as a semigroup that is finite. $H = G \ltimes End(G)$ has the property of being a semigroup, and if G is a complete group, then $G \ltimes Aut(G)$ is also a full group.
Proof. (1, id.) This is the identity. To demonstrate associativity, let $(p,\phi),(q,\psi),(r,\omega)$ be components of H, therefore after performing the computations, one has

$$((p,\phi)(q,\psi))(r,\omega) = (\psi(p)q,\psi\phi)(r,\omega)$$

$$= (\omega\psi(p)\omega(q)r,\omega\psi\phi)$$

$$= (p,\phi)(\omega(q)r,\omega\psi)$$

$$= (p,\phi)((q,\psi)(r,\omega))$$

In conclusion, if G is a complete group, for any $(g,\phi) \in G \ltimes Aut(G)$ There is a

$$(g,\phi)(\phi^{-1}(g^{-1}),\phi^{-1}) = (\phi^{-1}(g^{-1}),\phi^{-1})(g,\phi) = (1,\text{id.}),$$

And with that, we come to an end.
In the general situation, the setup of a finite group and its automorphism group, as well as the setup of a finite semigroup and its endomorphism semigroup, are used more or less interchangeably in the exposition for this chapter. As we progress through this discussion, we will examine certain instances of groups and semigroups in which invertibility is either expressly required or ignored; nonetheless, these instances ought to be obvious from the context. In point of fact, we favor the definitions that are expressed in terms of a finite semigroup and the endomorphism semigroup of that semigroup in the general situation.

SDPKE
We will examine the impact of allowing for invertibility in greater detail in the following section, which comes after this one. For the time being, we are not especially interested with the semidirect product itself; rather, we are more concerned with the quantity that it gives rise to, which is as follows:

Definition 2: Let G be a finite semigroup, and let End(G) be the semigroup that represents its endomorphism. Every pair of $(g,\phi) \in G \ltimes End(G)$ causes the function to occur $s_{g,\phi}: \mathbb{N} \to G,$ in which for each $x \in \mathbb{N}, s_{g,\phi}(x)$ as the component of G that is specified in such a way that

$$(g,\phi)^x = (s_{g,\phi}(x),\phi^x)$$

Checking that is not a tough task at all that $s_{g,\phi}(x) = \phi^{x-1}(g) \ldots \phi(g)g.$ Nevertheless, the following is the most important understanding that contributes to the substantial amount of interest in cryptography:

$$\begin{aligned}(s_{g,\phi}(x+y),\phi^{x+y}) &= (g,\phi)^{x+y}\\ &= (g,\phi)^x(g,\phi)^y\\ &= (s_{g,\phi}(x),\phi^x)(s_{g,\phi}(y),\phi^y)\\ &= (\phi^y(s_{g,\phi}(x))\, s_{g,\phi}(y),\phi^{x+y})\end{aligned}$$

It is consequent that $s_{g,\phi}(x+y) = \phi^y\left(s_{g,\phi}(x)\right)s_{g,\phi}(y).$ An argument that is completely symmetrical demonstrates that $s_{g,\phi}(x+y) = \phi^x\left(s_{g,\phi}(y)\right)s_{g,\phi}(x);$ To put it another way, allow $s_{g,\phi}(x),$ We are able to compute $s_{g,\phi}(x+y)$ to the extent that one is exclusively aware of y, and vice versa. The significance of this realization is so great that we have decided to encapsulate it in a theorem.

Theorem 2: Let G represent a semigroup, and let End (G) be its endomorphism semigroup. For every $(g,\phi) \in G \ltimes End(G)\ and\ x,y \in \mathbb{N},$ There is a
$\phi^x(s_{g,\phi}(y))s_{g,\phi}(x) = s_{g,\phi}(x+y) = \phi^y(s_{g,\phi}(x))s_{g,\phi}(y)$
Indeed, it is specifically these equalities that make it possible to define SDPK.

Definition 3: (Semidirect Product Key Exchange). Let's say two parties Alice and Bob concur on a finite semigroup G, End(G), which is its endomorphism, and a set $(g,\phi) \in G \ltimes End(G).$ Let
$N = |\{s_{g,\phi}(i)\}: i \in \mathbb{N}|$ $\mathbb{N}$ is finite, as we know from each value of $s_{g,\phi}(i)$ exists within G, which is a finite entity in and of itself. In the following manner, the two parties are able to arrive at a shared group element:

- In order to calculate $A = s_{g,\phi}(x)$, Alice selects an integer x at random from the set of numbers $\{1,\ldots,N\}$. This is the value that she sends to Bob.
- In order to calculate $B = s_{g,\phi}(y)$, Bob selects an integer y at random from the set of numbers $\{1,\ldots,N\}$. This is the value that she sends to Alice.
- As soon as Alice is in possession of Bob's value B, she employs her own integer x to compute the equation $K_A := \phi^x(B)s_{g,\phi}(x)$.
- In the same manner, Bob utilizes his integer y to compute the equation $K_B := \phi^y(A)s_{g,\phi}(y)$.

Remark. Our presentation of SDPKE makes use of a notation that is not conventional, and beyond a doubt, none of the provided examples of the scheme make use of this

notation. The notation used in the cryptanalytic work is its closest relative. In this notation, ai is defined as our $s_{g,\phi}(i)$.. Despite the fact that this work does not explore the finite quantity N that denotes the size of this set, the similarity is possibly one of the few works in the literature that takes into consideration the set of all possible exchange values.

Semidirect Product Key Exchange Key Recovery

We are going to look at some of the techniques that were described above in order to solve SCDH in a variety of different groups throughout the rest of this chapter. Our objective is to standardize the many different methods, as was said in the introduction; however, before we proceed with this, let us have a look at the list of platforms that are currently being suggested.

SDPKE Platforms

Following that, we will list the platforms that have been suggested in chronological order. Furthermore, given that a new suggestion of platform is directly a reaction to some cryptanalytic notion on a prior platform, this will also serve as the incentive for picking semigroups that seem to be fairly random as a platform according to the literature.

The first semigroup that was suggested for use with SDPKE was included in the first proposal for the key exchange. Semigroup platform created by the authors $M_3(\mathbb{Z}_7|A_5|)$ matrix multiplication, and a base pair automorphism is described as conjugation by a semigroup matrix that can be turned upside down. This, $\mathbb{Z}_7|A_5|$ represents the group ring that is made out by formal sums that make up the kind

$$\sum_{g\in A_5} a_g.g \quad a_g \in \mathbb{Z}_7.$$

A concept of addition and multiplication may be defined on this ring; when we are endowed with these operations, we have a ring that is simultaneously an $|A_5|$ dimensions over $\mathbb{Z}_7$.

On Finite Group Representation Theory

The examination of maps $\rho : G \to GL(V)$ The theory of representations for groups is defined for each given group G and vector space V. A pair (ρ, V) is referred to be a representation over $\mathbb{F}$ if the vector space is over a field F. After establishing a foundation, it is always possible to see GL(V) as a matrix group for finite-dimensional vector spaces V, as every finite group allows a finite-dimensional description (as shown by Theorem 4.12). $GL(k,\mathbb{F})$, where k is the size of V and F is the field underneath it. r = ρ is a map that meets the conditions of Theorem 4.11 when ρ is injective. This kind of depiction is called accurate: $GL(k,\mathbb{F})$ Components may be conceptualized as k^2-dimensional vectors endowed with the conventional framework of matrix multiplication. In summary, any faithful, finite-dimensional representation (ρ, V) of a group G entails that ρ is an injective homomorphism from G into a m^2-dimensional algebra, where m represents the dimension of V over a field $\mathbb{F}$.

The examination of the effectiveness of the dimension assault concerning a platform G is precisely the analysis of the dimension of accurate representations of G. Let us summarize the preceding debate by documenting the below outcome.

MAKE

The Dimension Attack

The natural occurring group as the additive group of an algebra is the subject of debate. As we observed, the dimension assault strategy would have a hard time adapting to such a platform. Keeping this in mind, the 'MAKE' SDPKE method is proposed for a certain prime p and the platform group $M_3(\mathbb{Z}_p)$ is added. The failure of the dimension attack has been shown; now let us see a successful implementation of the telescoping assault.

Telescoping Attack

Keep in mind that the writers propose the base pair (M, ϕ), where M might be any $M_3(\mathbb{Z}_p)$ matrix, and $\phi(g) = \phi_{H_1,H_2} = H_1MH_2$ relies on selecting appropriate auxiliary matrices $H_1,H_2 \in M_3(\mathbb{Z}_p)$ Due to this, we're experiencing

$$s_{M,\phi}(x) = \sum_{i=0}^{x-1} H_1^i M H_2^i$$

Accordingly, a base pair is the pertinent data for a SCDH instance with regard to this platform option. (M,ϕ_{H_1,H_2}) and two $M_3(\mathbb{Z}_p)$ elements $A := \sum_{i=0}^{x-1}(H_1^iMH_2^i)$ and $B := \sum_{i=0}^{y-1}(H_1^iMH_2^i)$.. Recovering the value is the job that we have. $\sum_{i=0}^{x+y-1}(H_1^iMH_2^i)$ Recall the fact that we are able to compute employing this publicly available data.

$$M + \phi_{H_1,H_2}(A) - A = \phi^x_{H_1,H_2}(M)$$

There is still the need of describing a technique of calculation $\sum_{i=0}^{x+y-1}(H_1^iMH_2^i)$with access to $\phi^X_{H_1,H_2}$. We provide a proof of this issue that uses this consequence of the Cayley-Hamilton theorem:

Conclusion

A novel key exchange mechanism based on automorphism extension of a (semi)group has been introduced and many concrete examples of this concept have been detailed. Any group, and especially any noncommutative group, may serve as the basis for our protocol. An extension of the Diffie-Hellman Key Exchange, the Semidirect Product Key Exchange (SDPKE) analyses the difficulty of the Semidirect Computational Diffie-Hellman Problem to test various cryptosystems. The first key exchange proposal included the

first semigroup that was proposed for use with SDPKE. To be more precise, we explore the state of the art in a thorough manner and analyze the severity of the underlying security challenge for various mathematical objects.

References

1. Jaiswal D. Group theory and cryptography. Journal of Emerging Technologies and Innovative Research. 2024 Jul;11(7). ISSN: 2349-5162.
2. Musa A, Otobong GU. Enhanced security in post-quantum cryptography: a comprehensive lattice-based signature scheme using matrix groups. Asian Journal of Mathematics and Computer Research. 2024;31(4):33–39. doi:10.56557/ajomcor/2024/v31i48966.
3. Emerencia C. A mathematical approach to post-quantum cryptography [PhD thesis]. Brussels: Vrije Universiteit Brussel; 2024.
4. Vasco M, Kahrobaei D, McKemmie E. Applications of finite non-abelian simple groups to cryptography in the quantum era. La Matematica. 2024;3:Article 96. doi:10.1007/s44007-024-00096-z.
5. Pratap G, Prajapati S. Review of group theory and its application. International Journal of Science and Research Archive. 2024;12(1):706–712. doi:10.30574/ijsra.2024.12.1.0841.
6. El Assad S, Lozi R, Puech W. Special issue on cryptography and its applications in information security. Applied Sciences. 2022;12(5):2588. doi:10.3390/app12052588.
7. Fine B, Kreuzer M, Rosenberger G. Further potential applications of group theory in information security. International Journal of Computer Mathematics: Computer Systems Theory. 2021;6(4):375–380. doi:10.1080/23799927.2021.1931455.
8. Finston D, Morandi P. Groups and cryptography. In: Groups St Andrews 2013. Cham: Springer; c2014. doi:10.1007/978-3-319-04498-9_8.
9. Lanel GHJ, et al. A survey of public-key cryptography over non-abelian groups. International Journal of Computer Science and Network Security. 2021;21(4):289–300.
10. Lanel GHJ, et al. Cryptographic protocols using semidirect products of finite groups. International Journal of Computer Science and Network Security. 2021 Aug;21(8).
11. D'Alconzo G, di Scala AJ. Representations of group actions and their applications in cryptography. Finite Fields and Their Applications. 2024;99:102476. doi:10.1016/j.ffa.2024.102476.
12. Guo X, He Z. The applications of group theory. Advanced Materials Research. 2012;430–432:1265–1268. doi:10.4028/www.scientific.net/AMR.430-432.1265.