APPLICATIONS OF FINITE NON-ABELIAN SIMPLE GROUPS TO CRYPTOGRAPHY IN THE QUANTUM ERA

MARÍA ISABEL GONZÁLEZ VASCO, DELARAM KAHROBAEI,
AND EILIDH MCKEMMIE

Abstract. The theory of finite simple groups is a (rather unexplored) area likely to provide interesting computational problems and modelling tools useful in a cryptographic context. In this note, we review some applications of finite non-abelian simple groups to cryptography and discuss different scenarios in which this theory is clearly central, providing the relevant definitions to make the material accessible to both cryptographers and group theorists, in the hope of stimulating further interaction between these two (non-disjoint) communities. In particular, we look at constructions based on various group-theoretic factorization problems, review group theoretical hash functions, and discuss fully homomorphic encryption using simple groups. The Hidden Subgroup Problem is also briefly discussed in this context.

1. Introduction

Cryptography is built upon the computational hardness of certain mathematical problems. One of the main tools within this area are *one-way* functions (informally, functions that can be efficiently evaluated while there are no efficient methods to compute preimages, possibly unless there is a secret key giving additional information). Computational tasks like factoring large integers or decoding with respect to random codes are flagship examples of mathematical problems naturally defining one-way functions. Of course, considering different computational models has a large impact in how such cryptographic-amenable problems can be selected; in particular, since the 1980s the appearance of quantum computing has necessitated the search for problems that will remain hard even if a quantum computer is available. The field of *post-quantum* cryptography revolves around cryptographic designs whose security relies on these kind of problems.

There have been many cryptographic proposals based on problems in group theory, see the recent book and survey by Kahrobaei et al [34, 35]. While it is not easy to classify problems as quantum resistant in a reasonable way, we do know of some problems that quantum computers can tackle with a significant advantage. The main menance is Shor's [70] quantum algorithm, which gives an exponential gain for solving problems that fit a certain "period-finding" description. Factoring large integers or solving discrete logarithms in finite cyclic groups fall into this category. Remarkably, it seems that the ideas behind Shor's algorithm can be extended to exploit normal subgroup structure in other groups. Simple groups are those with no non-trivial normal subgroups, so it is natural to ask whether finite simple groups may be harder than other groups for quantum computers to deal with. This leads us to suggest that the finite simple groups may be a good setting for post-quantum cryptographic schemes.

In the literature there are proposals using finite non-abelian simple groups for constructing many different tools: encryption and digital signature schemes, fully homomorphic encryption designs and hash functions. In this survey, we will take a closer look at the status of some proposed applications of the theory of finite simple groups to the design of hash functions, public-key encryption and fully homomorphic encryption. Our aim is not to be exhaustive but simply to give the reader a glimpse of the vast amount of unexplored avenues within this area, with a focus on some challenging group-theoretic and computational problems relevant to building sound cryptographic constructions.

Paper Roadmap. We start with a brief introduction to the finite simple groups and their classification in Section 2. In Section 3, we introduce Cayley hash functions and give an example cryptographic construction. We then discuss the difficulty of a certain factorization problem in groups that is linked to their security, and a related group theoretic conjecture. In Section 4, we define logarithmic signatures and another factorization problem in groups which has been used as justification for several public key cryptosystems. We give an example of a cryptographic construction and discuss a related group-theoretic conjecture. Section 5 discusses fully homomorphic encryption schemes and a method of building them from homomorphic encryption on groups, while in Section 6 we discuss the Hidden Subgroup Problem for cryptanalysis of proposed schemes using finite non-abelian simple groups against possible quantum attacks. Section 7 concludes the paper with a summary of the exciting open problems we discussed.

2. Preliminaries: Finite Simple Groups

A *simple group* is a non-trivial group whose only normal subgroups are itself and the trivial group. We are also interested in some *quasisimple* groups: G is quasisimple if it is perfect (i.e. equal to its own commutator subgroup $G = [G, G]$) and its group of inner automorphisms $\mathrm{Inn}(G)$ is simple. We focus here on finite groups since our cryptography applications require finite data structures.

There is a classification of all finite simple groups whose proof was completed in the 2000s after many years of work by a large number of mathematicians. For a brief historical overview, see [3]. The list of finite simple groups is as follows:

Theorem 1. *If G is a finite simple group then either G is abelian, in which case it is a cyclic group of prime order, or G is non-abelian, in which case one of the following holds:*

- *$G \cong A_n$ is an alternating group on $n \geq 5$ letters*
- *G is a group of Lie type*
- *G is one of 26 sporadic groups.*

The proof takes up many books, see for example the series [14]. For a more introductory textbook describing all the groups in detail, see [81].

The groups of Lie type are the classical groups and the exceptional groups over finite fields. We describe these groups briefly here, and refer the reader to a standard textbook by Carter [15] for more details. These groups are defined over finite fields. We use p to denote the characteristic of the field, which is a prime, and q to denote the order of the field, which is a power of p. Each finite group of Lie type has an underlying root system which determines an integer known as the *rank* of the group.

The classical groups are those which are natural matrix groups, and there are four types for every integer $n \geq 2$ and prime power q. For example, the projective special linear group of $n \times n$ matrices over a field of order q, denoted $PSL_n(q)$, has rank $n-1$ and is simple except when $n=2$ and $q = 2, 3$. The other classical groups are the groups of unitary, orthogonal and symplectic matrices over finite fields. We are also interested in finite quasisimple classical groups, for example the special linear group $SL_n(q)$. In characteristic 2 we have that $SL_n(2^k) = PSL_n(2^k)$ which is simple for $k > 1$.

The exceptional groups do not have such natural representations as groups of matrices, and all have rank at most 8. There are 10 infinite families indexed by prime powers q. One such family is the Suzuki groups which are defined over fields of order 2^{2n+1} which we denote by $Sz(2^{2n+1})$.

3. Factorization Problem and Cayley Hash Functions

A hash function is a function whose input is an arbitrarily large message and whose output is a fixed-length *hash*. Hash functions are a cryptographic primitive with a variety of cryptographic applications, each requiring different security properties (see any cryptography textbook, for example [39, Chapter 6]). Desirable properties of a hash function $h : M \to N$ include *preimage resistance* – given $n \in N$ it should be computationally infeasible to find $m \in M$ such that $h(m) = n$ – and *collision resistance* – it should be computationally infeasible to find $m \neq m' \in M$ such that $h(m) = h(m')$.

Zémor [83] defined group theoretic hash functions based on Cayley graphs of finitely-generated groups, following work of Bosset and Camion [13].

Definition 3.1. Let G be a finitely generated group with a generating set $S = \{g_1, ..., g_k\}$ which is closed under taking inverses.

- The Cayley graph $\Gamma(G, S)$ is a graph with vertex set G and an edge from g to h if and only if $g = g_i h$ for some i.
- The Cayley hash function $h_{G,S} : \{1, ..., k\}^* \to G$ is defined by $h_{G,S}(m_1, m_2, ..., m_r) = g_{m_1} g_{m_2} \cdots g_{m_r}$. We refer to $(m_1, m_2, ..., m_r) \in \{1, ..., k\}^*$ as a *word of length r*.

Note that evaluation of $h_{G,S}$ at $(m_1, m_2, ..., m_r)$ corresponds to traversing the path $(1, g_{m_1}, g_{m_1} g_{m_2}, \cdots, g_{m_1} g_{m_2} \cdots g_{m_r})$ in the Cayley graph $\Gamma(G, S)$.

Preimage resistance for Cayley hash functions is equivalent to the difficulty of writing a given element of G as a product of elements of S, or finding a path from 1 to the given element in the Cayley graph. This is called the Factorization Problem.

Factorization Problem. *Given $h \in G$ find a "short" word $(m_i)_i$ such that $\prod_i g_{m_i} = h$. Equivalently, given $h \in G$ find a "short" path from 1 to h in $\Gamma(G, S)$.*

It should be noted that finding minimal such words or paths is the NP-hard Minimum Generator Sequence Problem [22].

3.1. Cryptographic constructions.

There have been several choices of generating sets proposed for Cayley hash functions over $SL_2(q)$ [61, 62, 75, 83, 84], but there are known attacks in each case [27, 59, 60, 77]. Recently, Le Coz, Battarbee, Flores, Koberda and Kahrobaei [19] proposed a generating set for the quasisimple group $SL_n(p)$ for prime p. The Factorization Problem in this case can be reduced to solving a system of n^2 multivariate polynomial equations in $O(\log p)$ unknowns over $\mathbb{F}_p$ [19, Section 3.2] which is known to be NP-hard in the worst case.

As an example, we describe a particularly simple scheme proposed by Zémor [83].

Let p be a prime and associate to the bit 0 the matrix $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(p)$ and to the bit 1 the matrix $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in SL_2(p)$. Then the hash function $h_{SL_2(p),\{A,B\}}$ sends a binary number of arbitrary length to the appropriate product of As and Bs.

These parameters were chosen to allow efficient evaluation of the hash function, but the resulting hash function is not collision resistant: Tillich and Zémor [75, 76] show it is possible to find many factorizations of the group identity. Inserting any such factorization into any word gives a collision.

3.2. Progress towards solving the Factorization Problem.

Babai and Seress conjectured [5] that short paths exist in the Cayley graphs of finite simple groups:

Babai's conjecture. *There exists a constant $c > 0$ such that, for any h in a finite simple non-abelian group G, and any generating set S, there is a path from 1 to h in $\Gamma(G, S)$ of length at most $(\log |G|)^c$. That is, every* *element of G may be written as a word of length at most* $(\log |G|)^c$ *in the elements of S.*

For groups of Lie type of bounded rank, Babai's conjecture has been proved by Helfgott, Pyber, Szabo, Breuillard, Green and Tao [12, 30, 63]. The remaining cases are the alternating groups (for which Helfgott and Seress [31] have the best bound) and groups of Lie type of unbounded rank. In many cases there are partial results proving Babai's conjecture for certain generating sets. For example Babai and Hayes [7] prove Babai's conjecture for almost all generating sets of alternating groups, and Eberhard and Jezernik recently showed [21] that Babai's conjecture holds for large rank groups of Lie type for almost all large enough sets S. See [21, Section 1] for more details on the current status of Babai's conjecture.

Babai's conjecture would imply that for every $h \in G$ there is a path of length $(\log |G|)^{O(1)}$ from 1 to h in the Cayley graph, and the goal of cryptanalysts is to explicitly construct such short paths, while the goal of cryptographers is to find generating sets that make this as difficult as possible. There has been much activity in this area: Minkwitz [52] provided an optimization for the Schreier-Sims algorithm [42, 71] for solving the Factorization Problem in permutation groups. Babai and Hayes [7] (see also [6]) give a Las Vegas algorithm based on a random walk which is able to factorize elements of A_n for almost all generating sets, and Kalka, Teicher and Tsaban [36, Section 5] provide an algorithm which conjecturally and experimentally gives even shorter words. Babai, Kantor and Lubotzky [4] showed that every finite simple non-abelian group G has a set of generators S of size at most 7 for which there is an algorithm that finds words of length $O(\log |G|)$ in $O(\log |G|)$ time. Of the groups of Lie type, $PSL_n(q)$ and $SL_n(q)$ have been most closely studied and there are a handful of specially chosen generating sets for which there are efficient algorithms [38, 44, 59, 69]. Another approach of Kantor and Seress and Dietrich, Leedham-Green and O'Brien is to represent classical groups as so-called black-box groups and use a Las Vegas algorithm to attempt to construct standard generating sets in which to solve the Factorization Problem [20, 37]. For all generating sets of $SL_2(2^k)$ there is a subexponential-time algorithm giving subexponential-length words [58]. However, there is no efficient algorithm which works for all groups and generating sets.

4. Public Key Constructions from Logarithmic Signatures

Since the 1980s, there have been several attempts to exploit the computational properties of so-called factorization sequences of finite groups to derive one-way functions, including trapdoor functions – one-way functions for which it becomes easy to compute preimages given some extra information (see for instance [68]).

Definition 4.1. Let G be a finite group. We may identify G with a permutation group acting on n points where $n \leq |G|$. Call this n the *degree* of G.

Fix $s \in \mathbb{N}$ and for each $i = 1, ..., s$ let $\alpha_{ij} \in G$ and consider $\alpha = (\alpha_1, \ldots, \alpha_s)$ where $\alpha_i = (\alpha_{i1}, \ldots, \alpha_{in_i})$. We denote by $\ell(\alpha) = \sum_{i=1}^{s} n_i$ the *length* of α.

We say that $(i_1, \ldots, i_s) \in \mathbb{N}^s$ is a *factorization sequence for $g \in G$ w.r.t. α* if $g = \alpha_{1i_1} \cdots \alpha_{si_s}$. Denote by $n[\alpha, g]$ the number of different factorization sequences for g induced by α. We say that α is a

- *cover* if $n[\alpha, g] > 0$ for any $g \in G$.
- *logarithmic signature* if $n[\alpha, g] = 1$ for any $g \in G$. A logarithmic signature α is called *tame* if factorization sequences may be computed in polynomial time in the degree of G for every g w.r.t. α, and *wild* otherwise.

Note that by definition α is a logarithmic signature if and only if α is a cover and $\prod_{i=1}^{s} n_i = |G|$.

If the group law can be computed efficiently, it is "easy" to construct group elements by simply selecting one element from each α_i; the reverse process may, however, be rather involved computationally. The next section reviews several proposals exploiting this dichotomy to define useful one-way functions.

4.1. **Cryptographic Constructions.** The first private-key cryptographic construction using factorization sequences was PGM (Permutation Group Mappings) which was proposed by Magliveras [48] and uses logarithmic signatures for permutation groups to create one-way functions. Later, Magliveras et al. [50] proposed MST_1, a public-key cryptosystem built upon the same idea with an additional trapdoor for the one-way function of PGM. They also proposed a variant called MST_2 based on a special kind of cover called a *mesh*. Later, Lempken et al. [47] proposed MST_3 based on the difficulty of factoring group elements with respect to random covers for large subsets of finite non-abelian groups with large center.

We now give a description of MST_1, the simplest of these constructions. For a natural number m we denote by $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ the ring of integers modulo m. Fix a finite permutation group G and a tame logarithmic signature η for G, both publicly known. For any logarithmic signature $\alpha = (\alpha_1, \ldots, \alpha_s)$ we construct the mappings

$$\begin{array}{rccc} \lambda: & \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s} & \longrightarrow & \mathbb{Z}_{|G|} \\ & (r_1, \ldots, r_s) & \longmapsto & \sum_{i=1}^{s} \left(r_i \cdot \prod_{j=1}^{i-1} n_j \right) \end{array}$$

and

$$\begin{array}{rccc} \Theta_\alpha: & \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s} & \longrightarrow & G \\ & (r_1, \ldots, r_s) & \longmapsto & \alpha_{1r_1} \cdots \alpha_{sr_s} \end{array},$$

which one may check are bijective. Thus, the functional composition of Θ_α and λ^{-1} yields a bijection

$$\begin{array}{rccc} \breve{\alpha}: & \mathbb{Z}_{|G|} & \longrightarrow & G \\ & n & \longmapsto & (\Theta_\alpha \lambda^{-1})(n) = \Theta_\alpha \left(\lambda^{-1}(n) \right). \end{array}$$

We will use $\breve{\eta}^{-1}$ to identify G with $\mathbb{Z}_{|G|}$, allowing us to associate to each logarithmic signature α a permutation $\hat{\alpha} := \breve{\eta}^{-1}\breve{\alpha} \in S_{|G|}$.

For MST$_1$, the public key is a wild logarithmic signature $\alpha = (\alpha_1, \ldots, \alpha_s)$ and a tame logarithmic signature $\beta = (\beta_1, \ldots, \beta_s)$ for the same group G. The private key consists of a sequence $[\theta_1, \ldots, \theta_k]$ of tame logarithmic signatures such that $\hat{\beta}^{-1}\hat{\alpha} = \hat{\theta}_1 \cdots \hat{\theta}_k$, which opens the trapdoor to efficient computation of factorization sequences w.r.t. α. As discussed in [48], it is not known how to efficiently compute an appropriate sequence $[\theta_1, \ldots, \theta_k]$. The encryption scheme is depicted in Figure 1.

: **Public key:** Alice publishes a pair (α, β) of logarithmic signatures where α is wild and β is tame.

: **Secret key:** Alice knows a (short) sequence $[\theta_1, \ldots, \theta_k]$ of tame logarithmic signatures such that

$$\hat{\beta}^{-1}\hat{\alpha} = \hat{\theta}_1 \cdots \hat{\theta}_k.$$

: **Encryption:** to send the plaintext $m \in \mathbb{Z}_{|G|}$ to Alice, Bob transmits the ciphertext

$$c = \hat{\beta}^{-1}\hat{\alpha}(m) \in \mathbb{Z}_m.$$

: **Decryption:** Alice recovers (in polynomial time) the plaintext

$$m = \hat{\alpha}^{-1}\hat{\beta}(c) = \hat{\theta}_k^{-1} \cdots \hat{\theta}_1^{-1}(c).$$

FIGURE 1. MST_1 encryption scheme

4.2. **Producing hard factorizations.** All the above constructions base their security on the claimed hardness of computing factorizations of group elements with respect to some public cover. To support such a claim, the problem of factoring w.r.t a cover should be reduced as closely as possible to another computational problem that we can "safely" assume to be hard enough.

In the construction of MST$_1$, a critical point is the choice of the public wild logarithmic signature α along with a trapdoor (the factorization into the tame logarithmic signatures θ_i $(1 \leq i \leq k)$). Magliveras et al. [50] suggested picking α to be a *totally-non-transversal* logarithmic signature, meaning that none of the α_i is a coset of a non-trivial subgroup of G. This was later proven in [10] to be insufficient since for $n \geq 5$ there are tame totally-non-transversal logarithmic signatures for all alternating groups A_n and symmetric groups S_n.

Similarly, the security of MST_3 was questioned in [78] and further cryptanalyzed in [9], where it was proven that factoring with respect to the random covers used is not always a hard problem. While further schemes have been proposed in recent years (see, for instance, [18, 74]) at the writing of this survey, we are unfortunately not aware of a secure method for inducing hard group factorizations suited for cryptographic purposes.

4.3. **In search of Minimal Length Logarithmic Signatures.** Cryptographic applications motivate nice group-theoretic questions. For example, since the length of covers is a relevant parameter in real-life implementations, one may ask what the minimal length of a logarithmic signature can be, and try to construct logarithmic signatures of this length.

Let G be a finite group of order $|G| = \prod_{j=1}^{k} p_j^{a_j}$ with $p_1, \ldots, p_k$ distinct primes. González Vasco and Steinwandt [26] showed that for each logarithmic signature α for G we have

$$\ell(\alpha) \geq \sum_{j=1}^{k} a_j p_j, \tag{1}$$

and defined a *minimal length logarithmic signature* α to be a logarithmic signature for which equality in (1) holds. Then they constructed minimal length logarithmic sequences for symmetric and solvable groups. It is not yet known if minimal length logarithmic signatures exist for each finite group, although Magliveras [49] reduced the problem to simple groups, showing that a minimal counterexample of a group without a minimal length logarithmic signature must be simple. He also constructed minimal length logarithmic signatures for the alternating groups. The work in [26, 49] leads to the following conjecture for which a constructive proof is desired.

MLS Conjecture. *Every finite simple group has a minimal length logarithmic signature.*

This conjecture remains open in general, but has been proved in several cases. The constructive proofs for symmetric and alternating groups are in essence obtained by the same technique: given a permutation representation of a group G, identify a point P so that its stabilizer G_P can be factored through a minimal length logarithmic signature and such that there exists a complete set of representatives of G modulo G_P which moves P cyclically. The underlying idea is to factor the group into a 'product of disjoint pieces' for which a minimal length logarithmic signature exists. In the case that these 'disjoint pieces' are two subgroups, this is a rewriting of the group as a *knit (or Zappa-Szép) product* [51, 79].

Lempken and van Trung [46] use *double coset decomposition* to find minimal length logarithmic signatures for a number of special linear groups and projective special linear groups. Constructions of minimal length logarithmic sequences for all of the simple linear and symplectic groups, as well as some orthogonal groups, are found in [72, 73]. These papers consider the action of the group on the natural module, looking at point stabilizers and geometric objects called *spreads.* Furthemore, Holmes [32] produced minimal logarithmic signatures for the sporadic groups J_1, J_2, HS, McL, He and Co_3. Rahimipour, Ashrafi and Gholami [64–66] treat the cases of the sporadic groups J_3, Fi_{22}, Ru and Suz, as well as the Tits group ${}^2F_4(2)'$, the Ree groups ${}^2G_2(3^{2n+1})$, and some unitary and exceptional groups.

5. Fully Homomorphic Encryption Schemes

Broadly, homomorphic encryption enables computation over encrypted data. A *fully homomorphic encryption (FHE)* procedure is an encryption algorithm E taking as input an element from a ring $(R, +, \cdot)$ and producing an output in another ring $(S, +, \cdot)$ such that $E(r+s) = E(r) + E(s)$ and $E(r \cdot s) = E(r) \cdot E(s)$. Such an encryption mechanism allows a third party to do any computations involving $+$ and $\cdot$ without ever decrypting the data. For example, one can take the boolean circuit $(\{0,1\}, AND, XOR)$ as the ring, so that a fully homomorphic encryption function respects both AND and OR.

There are several known encryption schemes on rings $(\mathbb{Z}_n, +, \cdot)$ which allow homomorphic computation of only one of the two operations, for example textbook RSA, ElGamal and Goldwasser-Micali, but it appears far more difficult to construct a fully homomorphic scheme. For a detailed survey see [82].

The most widely known existing fully homomorphic encryption scheme appeared originally in the thesis of Craig Gentry [23]. The security of this solution relies on variants of the so called *bounded-distance decoding* problem. This problem enjoys a very relevant property for cryptographic purpose, namely, it is *random self reducible*, which basically means that it is about as hard on average as it is in the worst case. While this property allows for (practically meaningful) security proofs, it is unfortunaly the case that the resulting homomorphic encryption algorithm is too inefficient to be practical. Very informally, the reason is that, to provide semantic security, encryption has to be randomized, but on the other hand, a homomorphism should map zero to zero. To resolve this conflict, the ciphertext zero is "masked by noise". The problem now is that during any computation on encrypted data, this "noise" tends to accumulate and has to be occasionally reduced by re-encryption (also known as *bootstrapping*), a process that produces the equivalent ciphertext but with less noise. This is an expensive procedure, and its results in real-life computation being prohibitively slow.

The quest for more efficient techniques to overcome this issue has resulted in a number of rather efficient schemes. For instance, in [11, 24] a much slower growth of the noise during homomorphic computations was achieved, providing enough efficiency for practical applications. Later, in 2013, Gentry, Sahai and Waters [25] put forward the GSW scheme, a new method to derive more efficient FHE schemes. These techniques were further improved to develop efficient ring variants of the GSW scheme [17]. New efficient constructions are constantly being proposed (see [45]), and fully homomorphic encryption is indeed a reality in many practical applications.

5.1. **Simple groups and Fully Homomorphic Encryption.** The relevance of finite non-abelian simple groups to fully homomorphic encryption is that they open a door to designing new noise-free fully homomorphic encryption schemes, thus with the potential of being much more efficient than those needing some sort of bootstrapping.

This idea is quantified by the following theorem of Werner [80].

Theorem 2 ([56, 80])**.** *There is a fully homomorphic encryption scheme (over a non-zero ring) if and only if there is a finite non-abelian simple group over which there is a homomorphic encryption scheme.*

Ostrovsky and Skeith gave a constructive proof of this theorem [56, Corollary 4.26], see [41, Section 6] for more discussion. To construct a noise-free fully homomorphic encryption scheme from a group homomorphism $\phi : G \to H$, Ostrovsky and Skeith pick an element $g \in G$ of order 2 and identify the bit 0 with the identity of G, and the bit 1 with the element g. Since any binary function can be written as compositions of the $NAND$ function, it is enough to construct $NAND$ in the group. Ostrovsky and Skeith's proof gives a general formula, and they display an example for the group A_5. The details for A_n for $n \geq 6$ are especially short, so we describe them here.

Let $g = (1\,2)(3\,4)$ and e be the identity permutation. For $a, b \in \{e, g\}$. We will give a formula for $NAND(a, b)$. We follow Ostrovsky and Skeith's proof, noting that

$$g = [(1\,2)(5\,6), (1\,4)(2\,3)] = [g^{(3\,5)(4\,6)}, g^{(2\,4)(5\,6)}].$$

Therefore

$$\begin{aligned} NAND(a, b) &= g[a^{(3\,5)(4\,6)}, b^{(2\,4)(5\,6)}] \\ &= (1\,2)(3\,6\,4\,5)a(3\,6\,2\,4\,5)b(2\,6\,3\,5\,4)a(3\,6\,2\,4\,5)b(2\,4)(5\,6). \end{aligned}$$

Armknecht, Gagliardoni, Katzenbeisser and Peter [2] give an attack using quantum computers that undermines the security of any homomorphic encryption scheme whose plaintext and ciphertext spaces are abelian groups, thereby showing that it is impossible to have a quantum secure group homomorphic encryption scheme in this scenario. We are not aware of any literature proposing homomorphic encryption over non-abelian groups, but this is a research avenue worth exploring (see [55] for more discussion).

6. Hidden subgroup problem: post-quantum analysis

The search for quantum-resistant alternatives to today's common public-key constructions is extremely active. As we mentioned in the introduction, it is of paramount importance to identify and understand which mathematical problems are hard enough in a "post-quantum" sense. The *Hidden Subgroup Problem* (HSP) is a generic formulation englobing many such potentially hard problems. HSP can be seen as a way to understand the power of quantum algorithms and the limits of Shor's algorithm in group theoretical language.

Hidden Subgroup Problem (HSP). *Given a finitely generated group G, a finite set S and an efficiently computable function $f : G \to S$ such that f is constant and distinct on left cosets of a subgroup $H \leq G$ of finite index, find a generating set for H.*

Famously, Shor's [70] polynomial-time quantum algorithms for the Integer Factorization Problem and Discrete Logarithm Problem rely on a polynomial-time quantum algorithm for HSP in finite cyclic groups and groups of the form $\mathbb{Z}_p \times \mathbb{Z}_p$ for prime p. There are efficient quantum algorithms for HSP for all finite abelian groups and for a few classes of finite non-abelian groups. We describe some relevant cases here. See [33] for a full survey.

Hallgren, Russell and Ta-Shma [29, Theorem 2] gave a quantum algorithm for finding hidden normal subgroups. This result says nothing about finite simple groups since they have no non-trivial normal subgroups. Kuperberg in [43], and Regev in [67] give subexponential-time quantum algorithms for HSP in dihedral groups. Kuperberg's algorithm requires quantum space $2^{O(\log r)}$, while a generalized version of Regev's in [16, Theorem 5.2] is slower but less space-expensive. In [8], the authors extend these algorithms to construct a subexponential quantum algorithm for solving the Discrete Logarithm Problem in semi-direct products.

While we have efficient algorithms in some cases, providing solutions for HSP for all finite groups is considered one of the most important challenges in post-quantum cryptography. A solution to HSP in a finite group implies a solution in all subgroups. Since every finite group is a subgroup of a symmetric group, a solution to HSP for all finite groups is equivalent to a solution to HSP for symmetric groups. Note, however, that the representation of our group G as a subgroup of a symmetric group is relevant here, since if the dimension is large (for example if we consider the group G to be in $S_{|G|}$) we will see exponential blow-up in size and parameters.

Many of the techniques that have been successfully employed in the abovementioned cases have been shown to fail for symmetric groups [40, 43, 53, 54]. See [1, Section 3.2] for more discussion. Often the obstructions are large subgroups and high-dimensional irreducible representations. Therefore, many of the difficulties in the symmetric case also affect the classical group case [28, 54].

Understanding the complexity of HSP in finite non-abelian groups is a significant open question with strong connections to many well-known hard problems. This suggests study in this area could unearth one-way functions for the design of post-quantum cryptosystems.

7. The road ahead: some open problems

We have presented different problems related to non-abelian finite simple groups. We hope we have helped the reader in grasping their potential for cryptographic aplications. While it is hard to predict how the field will evolve, we can for sure identify a number of interesting problems on the frontier between cryptography and group theory:

– Babai's conjecture that short paths exist in Cayley graphs of finite simple groups is a widely-studied open problem in group theory. The Factorization Problem, equivalent to finding preimages for Cayley hash functions, requires *constructing* such short paths in Cayley graphs. For cryptographic applications it is desirable to either find a situation in which the Factorization Problem is computationally infeasible, or to show that it is always feasible, as discussed in Section 3.2. Progress in constructing short enough paths would imply progress on Babai's conjecture.

– Logarithmic signatures are a possible source of useful trapdoor functions for public-key cryptography, but there is more work to be done on understanding and constructing them. One direction, discussed in Section 4.2, is to find an algorithm that can produce wild logarithmic signatures, especially one which can also provide a rewriting in terms of tame ones. Another, discussed in Section 4.3, is to determine whether all finite groups have minimal length logarithmic signatures. This question has been reduced to simple groups, and the MLS Conjecture that minimal length logarithmic signatures exist for all simple groups remains open in some cases.

– Ostrovsky and Skeith [57] show how to convert a homomorphic encryption procedure on any finite simple group to a fully homomorphic encryption procedure on a ring by constructing $NAND$ in the finite simple groups. As discussed in Section 5.1, this opens up the question of finding secure homomorphic encryption on a finite simple group.

– The Hidden Subgroup Problem is central to post-quantum cryptography. As discussed in Section 6, understanding the hardness of HSP for symmetric groups could be useful in the analysis of post-quantum group-based cryptographic primitives.

Acknowledgement

We thank Greg Kuperberg for generously sharing his ideas on HSP on the non-abelian finite simple groups.

DK is grateful to MGV for the kind invitation to Madrid in February 2020 and great hospitality and generous support; when DK proposed the topic of this manuscript in that research trip.

References

[1] Gorjan Alagic and Alexander Russell, *Quantum-secure symmetric-key cryptography based on hidden shifts*, Advances in cryptology – eurocrypt 2017, 2017, pp. 65–93.

[2] Frederik Armknecht, Tommaso Gagliardoni, Stefan Katzenbeisser, and Andreas Peter, *General impossibility of group homomorphic encryption in the quantum world*, Public-key cryptography – PKC 2014, 2014, pp. 556–573.

[3] Michael Aschbacher, *The status of the classification of the finite simple groups*, Notices Amer. Math. Soc. **51** (2004), no. 7, 736–740. MR2072045

[4] L. Babai, W.M. Kantor, and A. Lubotsky, *Small-diameter Cayley graphs for finite simple groups*, European Journal of Combinatorics **10** (November 1989), no. 6, 507–522.

[5] László Babai and Ákos Seress, *On the diameter of permutation groups*, European Journal of Combinatorics **13** (1992), no. 4, 231–243.

[6] László Babai, Robert Beals, and Ákos Seress, *On the diameter of the symmetric group: Polynomial bounds*, Proceedings of the fifteenth annual acm-siam symposium on discrete algorithms, 2004, pp. 1108–1112.

[7] László Babai and Thomas P. Hayes, *Near-independence of permutations and an almost sure polynomial bound on the diameter of the symmetric group*, Proceedings of the sixteenth annual acm-siam symposium on discrete algorithms, 2005, pp. 1057–1066.

[8] C. Battarbee, D. Kahrobaei, L. Perret, and S. F. Shahandashti, *A subexponential quantum algorithm for the semidirect discrete logarithm problem*, 4th PQC NIST Conference 2022 (2022), 1–27.

[9] Simon R. Blackburn, Carlos Cid, and Ciaran Mullan, *Cryptanalysis of the* MST_3 *public key cryptosystem*, IACR Cryptol. ePrint Arch. (2009), 248.

[10] Jens-Matthias Bohli, Rainer Steinwandt, María Isabel González Vasco, and Consuelo Martínez, *Weak keys in* $\mathrm{MST}_{\mathit{1}}$, Des. Codes Cryptogr. **37** (2005), no. 3, 509–524.

[11] Zvika Brakerski and Vinod Vaikuntanathan, *Efficient fully homomorphic encryption from (standard)* LWE, SIAM J. Comput. **43** (2014), no. 2, 831–871.

[12] Emmanuel Breuillard, Ben Green, and Terence Tao, *Approximate subgroups of linear groups*, Geometric and Functional Analysis **21** (July 2011), no. 4, 774–819.

[13] Paul Camion, *Can a fast signature scheme without secret key be secure*, Applied algebra, algorithmics and error-correcting codes, 1986, pp. 215–241.

[14] Inna Capdeboscq, Daniel Gorenstein, Richard Lyons, and Ronald Solomon, *The classification of the finite simple groups*, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, Providence, RI, Unknown Month 1994. MR4244365

[15] Roger W Carter, *Simple groups of lie type*, Vol. 22, John Wiley & Sons, 1989.

[16] Andrew Childs, David Jao, and Vladimir Soukharev, *Constructing elliptic curve isogenies in quantum subexponential time*, Journal of Mathematical Cryptology **8** (2014), no. 1, 1–29.

[17] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène, *Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds*, Advances in cryptology - ASIACRYPT 2016 - 22nd international conference on the theory and application of cryptology and information security, hanoi, vietnam, december 4-8, 2016, proceedings, part I, 2016, pp. 3–33.

[18] Yue Cong, Haibo Hong, Jun Shao, Song Han, Jianhong Lin, and Shuai Zhao, *A new secure encryption scheme based on group factorization problem*, IEEE Access **7** (2019), 168728–168735.

[19] C. Le Coz, C. Battarbee, R. Flores, T. Koberda, and D. Kahrobaei, *Post-quantum hash functions using* $SL_n(\mathbb{F}_p)$, `arXiv:2207.03987` (2023), 1–20.

[20] Heiko Dietrich, C.R. Leedham-Green, and E.A. O'Brien, *Effective black-box constructive recognition of classical groups*, Journal of Algebra **421** (January 2015), 460–492.

[21] Sean Eberhard and Urban Jezernik, *Babai's conjecture for high-rank classical groups with random generators*, Inventiones mathematicae **227** (August 2021), no. 1, 149–210.

[22] S Even and O Goldreich, *The minimum-length generator sequence problem is NP-hard*, Journal of Algorithms **2** (1981), no. 3, 311–313.

[23] Craig Gentry, *Fully homomorphic encryption using ideal lattices*, Proceedings of the forty-first annual acm symposium on theory of computing, 2009, pp. 169–178.

[24] Craig Gentry, Shai Halevi, and Nigel P. Smart, *Fully homomorphic encryption with polylog overhead*, Advances in cryptology - EUROCRYPT 2012 - 31st annual international conference on the theory and applications of cryptographic techniques, cambridge, uk, april 15-19, 2012. proceedings, 2012, pp. 465–482.

[25] Craig Gentry, Amit Sahai, and Brent Waters, *Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based*, Advances in cryptology - CRYPTO 2013 - 33rd annual cryptology conference, santa barbara, ca, usa, august 18-22, 2013. proceedings, part I, 2013, pp. 75–92.

[26] M. I. González Vasco and R. Steinwandt, *Obstacles in Two Public Key Cryptosystems Based on Group Factorizations*, *Cryptology*, volume 25 of *Tatra Mountains Mathematical Publications* (2002), 23–37.

[27] Markus Grassl, Ivana Ilić, Spyros Magliveras, and Rainer Steinwandt, *Cryptanalysis of the Tillich–Zémor hash function*, Journal of Cryptology **24** (March 2010), no. 1, 148–156.

[28] Sean Hallgren, Cristopher Moore, Martin Rötteler, Alexander Russell, and Pranab Sen, *Limitations of quantum coset states for graph isomorphism*, J. ACM **57** (2010nov), no. 6.

[29] Sean Hallgren, Alexander Russell, and Amnon Ta-Shma, *Normal subgroup reconstruction and quantum computation using group representations*, Proceedings of the thirty-second annual ACM symposium on theory of computing, May 2000.

[30] H. A. Helfgott, *Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$*, Annals of Mathematics **167** (2008), no. 2, 601–623.

[31] Harald Helfgott and Ákos Seress, *On the diameter of permutation groups*, Annals of Mathematics **179** (March 2014), no. 2, 611–658.

[32] P. Holmes, *On minimal factorisations of sporadic groups*, Experimental Mathematics **13** (200401).

[33] K. Horan and D. Kahrobaei, *Hidden Subgroup Problem and Post-quantum Group-based Cryptography*, International congress on mathematical software – ICMS 2018, LNCS, 2018, pp. 218–226.

[34] D. Kahrobaei, R. Flores, and M. Noce, *Group-based cryptography in the quantum era*, Notices of the American Mathematical Society **70** (May 2023), no. 5, 752–763.

[35] D. Kahrobaei, R. Flores, M. Noce, M. Habeeb, and C. Battarbee, *Applications of group theory in cryptography*, The Mathematical Surveys and Monographs series of the American Mathematical Society, AMS, 1.

[36] Arkadius Kalka, Mina Teicher, and Boaz Tsaban, *Short expressions of permutations as products and cryptanalysis of the Algebraic Eraser*, Advances in Applied Mathematics **49** (July 2012), no. 1, 57–76.

[37] William M Kantor and Ákos Seress, *Black box classical groups*, Vol. 708, American Mathematical Soc., 2001.

[38] M. Kassabov and T.R. Riley, *Diameters of Cayley graphs of Chevalley groups*, European Journal of Combinatorics **28** (April 2007), no. 3, 791–800.

[39] Jonathan Katz and Yehuda Lindell, *Introduction to modern cryptography*, Chapman & Hall/CRC Cryptography and Network Security, CRC Press, Boca Raton, FL, 2021. Third edition [of 2371431]. MR4283554

[40] Julia Kempe and Aner Shalev, *The hidden subgroup problem and permutation group theory*, Proceedings of the sixteenth annual acm-siam symposium on discrete algorithms, 2005, pp. 1118–1125.

[41] Nirattaya Khamsemanan, Rafail Ostrovsky, and William E. Skeith, *On the black-box use of somewhat homomorphic encryption in noninteractive two-party protocols*, SIAM Journal on Discrete Mathematics **30** (2016), no. 1, 266–295, available at `https://doi.org/10.1137/110858835`.

[42] Donald E. Knuth, *Efficient representation of perm groups*, Combinatorica **11** (March 1991), no. 1, 33–43.

[43] Greg Kuperberg, *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem*, SIAM Journal on Computing **35** (2005), no. 1, 170–188.

[44] Michael Larsen, *Navigating the cayley graph of $SL_2((F)_p)$*, International Mathematics Research Notices **2003** (2003), no. 27, 1465.

[45] Yongwoo Lee, Daniele Micciancio, Andrey Kim, Rakyong Choi, Maxim Deryabin, Jieun Eom, and Donghoon Yoo, *Efficient FHEW bootstrapping with small evaluation keys, and applications to threshold homomorphic encryption*, Advances in cryptology - EUROCRYPT 2023 - 42nd annual international conference on the theory and applications of cryptographic techniques, lyon, france, april 23-27, 2023, proceedings, part III, 2023, pp. 227–256.

[46] Wolfgang Lempken and Tran van Trung, *On minimal logarithmic signatures of finite groups*, Exp. Math. **14** (2005), no. 3, 257–269.

[47] Wolfgang Lempken, Tran van Trung, Spyros S. Magliveras, and Wandi Wei, *A public key cryptosystem based on non-abelian finite groups*, J. Cryptology **22** (2009), no. 1, 62–74.

[48] Spyros S. Magliveras and Nasir D. Memon, *Algebraic properties of cryptosystem PGM*, J. Cryptol. **5** (1992), no. 3, 167–183.

[49] S.S. Magliveras, *Secret- and Public-key Cryptosystems from Group Factorizations*, Cryptology. Editors: K. Nemoga, O. Grošek, 2002, pp. 11–22. To appear.

[50] S.S. Magliveras, D.R. Stinson, and T. van Trung, *New Approaches to Designing Public Key Cryptosystems Using One-Way Functions and Trapdoors in Finite Groups*, Journal of Cryptology **15** (2002), no. 4, 285–297.

[51] P.W. Michor, *Knit Products of Graded Lie Algebras and Groups*, Proceedings of the winter school on Geometry and Physics, srni 1988, 1989, pp. 171–175.

[52] T. Minkwitz, *An algorithm for solving the factorization problem in permutation groups*, Journal of Symbolic Computation **26** (July 1998), no. 1, 89–95.

[53] Cristopher Moore, Alexander Russell, and Leonard J. Schulman, *The symmetric group defies strong fourier sampling*, SIAM Journal on Computing **37** (2008), no. 6, 1842–1864, available at `https://doi.org/10.1137/050644896`.

[54] Cristopher Moore, Alexander Russell, and Piotr Sniady, *On the impossibility of a quantum sieve algorithm for graph isomorphism*, Proceedings of the thirty-ninth annual acm symposium on theory of computing, 2007, pp. 536–545.

[55] Koji Nuida, *Towards constructing fully homomorphic encryption without ciphertext noise from group theory*, International symposium on mathematics, quantum theory, and cryptography, October 2020, pp. 57–78.

[56] Rafail Ostrovsky and William E. Skeith III, *Algebraic lower bounds for computing on encrypted data*, 2007. `https://eprint.iacr.org/2007/064`.

[57] Rafail Ostrovsky and William E. Skeith, *Communication complexity in algebraic two-party protocols*, Advances in cryptology – crypto 2008, 2008, pp. 379–396.

[58] Christophe Petit, *Towards factoring in $SL_2(\mathbb{F}_p)$*, Designs, Codes and Cryptography **71** (September 2012), no. 3, 409–431.

[59] Christophe Petit, Kristin Lauter, and Jean-Jacques Quisquater, *Full cryptanalysis of LPS and Morgenstern hash functions*, Lecture notes in computer science, 2008, pp. 263–277.

[60] Christophe Petit and Jean-Jacques Quisquater, *Preimages for the Tillich-Zémor hash function*, Selected areas in cryptography, 2011, pp. 282–301.

[61] ———, *Rubik's for cryptographers*, Notices of the American Mathematical Society **60** (January 2013), no. 06, 733.

[62] ———, *Cryptographic hash functions and expander graphs: The end of the story?*, The new codebreakers, 2016, pp. 304–311.

[63] László Pyber and Endre Szabó, *Growth in finite simple groups of lie type*, Journal of the American Mathematical Society **29** (October 2014), no. 1, 95–146.

[64] A. R. Rahimipour, A. R. Ashrafi, and A. Gholami, *The existence of minimal logarithmic signatures for the sporadic Suzuki and simple Suzuki groups*, Cryptography and Communications **7** (2015apr), no. 4, 535–542.

[65] ______, *The existence of minimal logarithmic signatures for some finite simple groups*, Experimental Mathematics **27** (2016oct), no. 2, 138–146.

[66] Ali Reza Rahimipour and Ali Reza Ashrafi, *The existence of minimal logarithmic signatures for some finite simple unitary groups*, Vietnam Journal of Mathematics **50** (2021apr), no. 1, 217–227.

[67] Oded Regev, *A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space*, arXiv preprint quant-ph (2004).

[68] Dominik Reichl, *Group factorizations and cryptology*, Ph.D. Thesis, 2015.

[69] T. Riley, *Navigating in the Cayley graphs of $SL_N(\mathbb{Z})$ and $SL_N(\mathbb{F}_p)$*, Geometriae Dedicata **113** (January 2005).

[70] P.W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings 35th annual symposium on foundations of computer science, 1994.

[71] Charles C. Sims, *Computational methods in the study of permutation groups*, Computational problems in abstract algebra, 1970, pp. 169–183.

[72] Nidhi Singhi, Nikhil Singhi, and Spyros S. Magliveras, *Minimal logarithmic signatures for finite groups of Lie type*, Des. Codes Cryptogr. **55** (2010), no. 2-3, 243–260.

[73] Nikhil Singhi and Nidhi Singhi, *Minimal logarithmic signatures for classical groups*, Des. Codes Cryptogr. **60** (2011), no. 2, 183–195.

[74] Pavol Svaba and Tran van Trung, *Public key cryptosystem MST3: cryptanalysis and realization*, J. Math. Cryptol. **4** (2010), no. 3, 271–315.

[75] Jean-Pierre Tillich and Gilles Zémor, *Hashing with SL_2*, Advances in cryptology — CRYPTO '94, pp. 40–49.

[76] Jean-Pierre Tillich and Gilles Zémor, *Group-theoretic hash functions*, Algebraic coding, 1994, pp. 90–110.

[77] Simran Tinani, *Methods for collisions in some algebraic hash functions*, 2023.

[78] Maria Isabel Gonzalez Vasco, Angel L. Pérez del Pozo, and Pedro Taborda Duarte, *A note on the security of* MST$_3$, Des. Codes Cryptogr. **55** (2010), no. 2-3, 189–200.

[79] María Isabel González Vasco, Martin Rötteler, and Rainer Steinwandt, *On minimal length factorizations of finite groups*, Exp. Math. **12** (2003), no. 1, 1–12.

[80] Heinrich Werner, *Finite simple nonabelian groups are functionally complete*, Notices of the american mathematical society, 1973, pp. A561–A561.

[81] Robert Wilson, *The finite simple groups*, Vol. 251, Springer Science & Business Media, 2009.

[82] A. Wood, K. Najarian, and D. Kahrobaei, *Homomorphic encryption for machine learning in medicine and bioinformatics*, ACM Comput. Surv. **53** (2020), no. 4, 1–35.

[83] G. Zémor, *Hash functions and graphs with large girths*, Advances in cryptology — EUROCRYPT '91, 1991, pp. 508–511.

[84] Gilles Zémor, *Hash functions and Cayley graphs*, Designs, Codes and Cryptography **4** (July 1994), no. 3, 381–394.

Catedratica de Universidad Departamento de Matematicas, Universidad Carlos III de Madrid Campus de Leganés, Madrid, Spain

Departments of Computer Science and Mathematics, Queens College, City University of New York, USA, Department of Computer Science, University of York, UK, Initiative for the Theoretical Sciences, Graduate Center, City University of New York, USA, Department of Computer Science and Engineering, Tandon School of Engineering, New York University, USA

Mathematics Department, Rutgers University, New Brunswick, New Jersey, USA