Cryptographic Corollaries of the Classification of Finite Simple Groups

Analysis of a candidate problem in post-quantum cryptography

Christopher Battarbee[1], **Giacomo Borin**[2], Ryann Cartor, Nadia Heninger, David Jao, Delaram Kahrobaei, Laura Maddison, Edoardo Persichetti, Angela Robinson, Daniel Smith-Tone, Rainer Steinwandt.

Presented at the NIST Crypto Reading Club on 2024-07-10

[1]Sorbonne University, [2]IBM Research Zurich & University of Zurich

Outline

Introduction to SDLP

Motivation

PQC Candidates	Classical Crypto
Lattices	Cyclic groups
Linear codes	Residue groups
Isogenies	
Multivariate	

Can we study cryptography in more complicated group structures?

Definitions

Semidirect Product

Let G be a finite group and $Aut(G)$ its group of automorphisms. We define $G \rtimes Aut(G)$ to be the group of pairs in $G \times Aut(G)$ equipped with the following multiplication:

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

Notice

$$\begin{tikzcd} G \arrow[rr, leftrightarrow] \arrow[d, dashed] & & Aut(G) \\ G & & \end{tikzcd}$$

$$\begin{aligned} (g, \phi)^2 &= (g\phi(g), \phi^2) \\ (g, \phi)^3 &= (g, \phi)(g\phi(g), \phi^2) \\ &= (g\phi(g)\phi^2(g), \phi^3) \\ (g, \phi)^4 &= (g, \phi)(g\phi(g)\phi^2(g), \phi^3) \\ &= (g\phi(g)\phi^2(g)\phi^3(g), \phi^4) \end{aligned}$$

Definitions

Semidirect Exponentiation

Fix $(g, \phi) \in G \rtimes Aut(G)$. Define $s_{g,\phi} : \mathbb{Z} \to G$ to be the group element such that

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

We have seen that

$$s_{g,\phi}(x) = g\phi(g)...\phi^{x-1}(g)$$

SDLP

Fix $G \rtimes Aut(G)$ and a pair (g, ϕ). Suppose we are given $s_{g,\phi}(x)$ for some $x \in \mathbb{Z}$. The **S**emidirect **D**iscrete **L**ogarithm **P**roblem is to recover x.

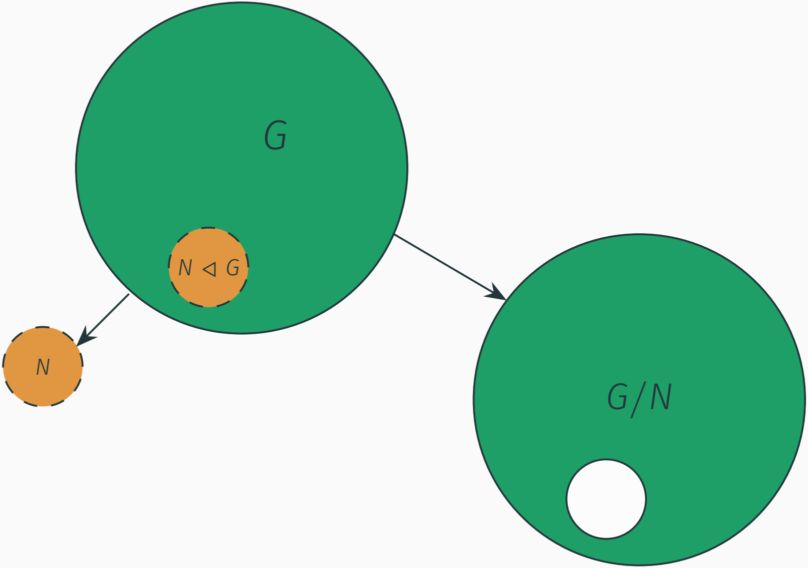
Background

- Various works addressing SDPKE, an analogue of DHKE based on SDLP*
- Work linking SDLP to group actions and signatures in a potentially desirable fashion†
- Recent fast algorithms for SDLP in certain classes of group‡

*Habeeb et al. 2013.
†B. et al. 2023.
‡Mendelsohn et al. 2023; Imran and Ivanyos 2024.

Reduction to Simple Groups

Intuition



The Decomposition Tool

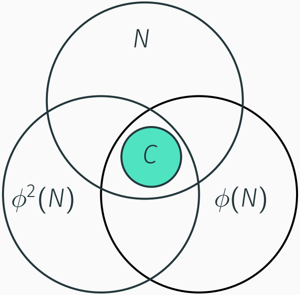
Imran and Ivanyos 2024, Theorem 3

Consider SDLP with respect to a pair $(g, \phi) \in G \rtimes Aut(G)$. Given a ϕ-invariant normal subgroup N of G, it suffices to solve an instance of SDLP in G/N and an instance of SDLP in N.

Given an oracle that solves SDLP in a simple group we are done if

- We can compute ϕ-invariant normal subgroups
- The recursion implied by the decomposition tool terminates in SDLP in simple groups

Computing the Invariant Subgroup



- We may assume there is a characteristic subgroup; and we know how to obtain a maximal normal subgroup (Ivanyos et al. 2001, Theorem 4)
- Imran and Ivanyos 2024 show that the intersection

$$N \cap \phi(N) \cap \ldots \cap \phi^i(N) \cap \ldots$$

  stabilises with a ϕ-invariant subgroup; not the trivial group if N contains a characteristic subgroup C
- We show that if such C exists, *every* maximal normal subgroup contains a characteristic subgroup!

Recursion to Simple Groups

Correspondence theorem: the subgroups of G/N are of the form N'/N where $N \subset N' \leq G$; and $(G/N)/(N'/N) \cong G/N'$

$$\begin{tikzcd}
 & & & G \arrow[dll] \arrow[drr] & & & \\
 & N \arrow[dl] \arrow[dr] & & & & G/N \arrow[dl] \arrow[dr] & \\
N_0 & & N/N_0 & & N_1/N & & G/N_1
\end{tikzcd}$$

Recursion to Simple Groups

Correspondence theorem: the subgroups of G/N are of the form N'/N where $N \subset N' \triangleleft G$; and $(G/N)/(N'/N) \cong G/N'$

$$\begin{tikzcd}
 & & G \arrow[dl] \arrow[dr] & \\
 & N \arrow[dl] \arrow[dr] & & G/N \\
N_0 & & N/N_0 \arrow[dl] \arrow[dr] & \\
 & N_{00} & & N_0/N_{00}
\end{tikzcd}$$

Simple Groups Analysis

Simple Groups

Theorem (Classification of Finite Simple Groups)

Every finite simple group is isomorphic to a member of one of four infinite classes:

1. the **cyclic groups** of prime order,
2. the **alternating groups** of degree at least 5,
3. the **classical groups** of Lie type,
4. the **exceptional groups** of Lie type

or one of 26 groups called the **sporadic groups**.

Corollary

The Semidirect Discrete Logarithm Problem (SDLP) in any finite group is **not a secure assumption** for quantum resistant primitives.

Let G be a cyclic group of prime order, then for any $g \in G$ and $\phi \in \mathsf{Aut}(G)$ we have $\phi(g) = g^a$ for some $a \in \mathbb{N}$, so:

$$s_{g,\phi(x)} = g\phi(g)\cdots\phi^x(g) = g \cdot g^a \cdots g^{a^x} = g^{\sum_{i=0}^{x} a^i} \ .$$

With a Quantum Computer we can recover $\sum_{i=0}^{x} a^i$ and solve the SDLP with basic algebra tricks.

Simple Groups

Theorem (Classification of Finite Simple Groups)

Every finite simple group is isomorphic to a member of one of four infinite classes:

1. ~~the **cyclic groups** of prime order~~,
2. the **alternating groups** of degree at least 5,
3. the **classical groups** of Lie type,
4. the **exceptional groups** of Lie type

or one of 26 groups called the **sporadic groups**.

Reduction to Inner Automorphisms

Memo: $\mathsf{Inn}(G) := \{G \ni g \mapsto sgs^{-1} \in G \mid s \in G\}$ is a normal subgroup of $\mathsf{Aut}(G)$.

Theorem (Kohl 2003)

If G is a non-abelian finite simple group, then for all $\phi \in \mathsf{Aut}(G)$ there exists an integer $x \leq \log_2 |G|$ such that $\phi^x \in \mathsf{Inn}(G)$.

Memo: by Imran and Ivanyos 2024, we can solve SDLP(G, ϕ) by solving most y instances of SDLP(G, ϕ^y).

Consequence

We can limit ourselves to solve SDLP for inner authormorphism, i.e. conjugations.

Linear Groups Analysis

SDLP on Matrix Groups (Imran and Ivanyos 2024)

Consider $G \leq \mathrm{GL}_n(\mathbb{F})$ and $\phi \in \mathsf{Inn}(G)$ such that $\phi(\mathsf{G}) = \mathsf{SGS}^{-1}$, then:

$$s_{\mathsf{G},\phi}(x) = \mathsf{G} \cdot \mathsf{SGS}^{-1} \cdot \mathsf{S}^2\mathsf{GS}^{-2} \cdots \mathsf{S}^{x-1}\mathsf{GS}^{-x+1} \cdot \mathsf{S}^x\mathsf{GS}^{-x} =$$
$$= \mathsf{GS} \cdot \mathsf{GS} \cdot \mathsf{GS} \cdots \mathsf{SG} \cdot \mathsf{S}^{-x} = (\mathsf{GS})^x \cdot \mathsf{G} \cdot \mathsf{S}^{-x}$$

So if we vectorize the matrices we get:

$$\begin{aligned}
\mathrm{vec}(s_{\mathsf{G},\phi}(x)) &= \mathrm{vec}\left((\mathsf{GS})^x \cdot \mathsf{G} \cdot \mathsf{S}^{-x}\right) \\
&= \mathrm{vec}\left((\mathsf{GS}) \cdot (\mathsf{GS})^{x-1} \cdot \mathsf{G} \cdot \mathsf{S}^{-(x-1)} \cdot \mathsf{S}^{-1}\right) \\
&= \mathrm{vec}\left((\mathsf{GS}) \cdot s_{\mathsf{G},\phi}(x-1) \cdot \mathsf{S}^{-1}\right) \\
&= \left[(\mathsf{GS}) \otimes \mathsf{S}^{-1}\right] \mathrm{vec}(s_{\mathsf{G},\phi}(x-1)) \\
&\text{...repeating the argument } x-1 \text{ more times...} \\
&= \left[(\mathsf{GS}) \otimes \mathsf{S}^{-1}\right]^x \mathrm{vec}(\mathsf{G})
\end{aligned}$$

Matrix Power Problem

By the provious discussion SDLP reduces to:

Matrix Power Problem

Given vectors $\mathbf{a}, \mathbf{b} \in V$ and a matrix $\mathbf{T} \in \mathrm{GL}(V)$ find $x \in \mathbb{N}$ such that:

$$\mathbf{b} = \mathbf{T}^{x} \cdot \mathbf{a} \ .$$

Nice Fact: Thanks to Imran and Ivanyos 2024, Kannan and Lipton 1986 the problem can be reduced to a discrete logarithm over $\mathrm{GL}(W)$ for W subspace of V.

Nice Fact: We can repeat the same arguments for projective linear groups $G \leq \mathbb{P}\mathrm{GL}$.

Linear Representations for Simple Groups

A *linear representation* (see Serre 1977) of a group G on a finite-dimensional vector space V is a non trivial group homomorphism

$$\psi : G \to \mathrm{GL}(V).$$

We also consider *projective* linear representations, i.e., injective homomorphisms $G \to \mathbb{P}\mathrm{GL}(V)$

Remark

For our case the codomain G is a simple group $\implies$
the kernel $\ker(\psi)$ is trivial $\implies$
ψ is injective, i.e. the representation is always faithful.

Combination of the Frameworks

If we have an efficiently computable linear representation $\psi : G \to \mathrm{GL}(V)$ we move the problem to matrix groups (where we can solve it in Quantum Polynomial Time):

$$\begin{tikzcd} G \arrow[r, "\psi"] \arrow[d, "\rho_{g,\phi}"'] & \mathrm{GL}_n(\mathbb{F}) \arrow[r, "\mathrm{vec}"] & \mathbb{F}^{n^2} \arrow[d, "\psi(gs) \otimes \psi(s)^{-1}"] \\ G \arrow[r, "\psi"'] & \mathrm{GL}_n(\mathbb{F}) \arrow[r, "\mathrm{vec}"'] & \mathbb{F}^{n^2} \end{tikzcd}$$

Where $\phi(g) = sgs^{-1}$ and $\rho_{g,\phi}(h) = g\phi(h)$

Simple Groups

Theorem (Classification of Finite Simple Groups)

Every finite simple group is isomorphic to a member of one of four infinite classes:

1. ~~the **cyclic groups** of prime order~~,
2. the **alternating groups** of degree at least 5, <- Linear
3. the **classical groups** of Lie type, <- Linear
4. the **exceptional groups** of Lie type <- Linear

or one of 26 groups called the **sporadic groups**.

Like for DLOG with division over $\mathbb{Z}/p\mathbb{Z}$, this do not directly implies that SDLP is broken.

Constructive Recognition Problem

Since Lie groups and alternating groups are defined as (projective) linear groups the SDLP reduces to the following:

Constructive Recognition Problem, Babai and Beals 1999

Given a simple black-box group G, the problem require to find a computationally efficient isomorphism between G and an explicitly defined simple group.

Black-Box Groups

A **black-box group** $G \subset \{0,1\}^n$ is a group endowed with an oracle that performs the group operations, multiplication and inversion, and can check for the identity.

Simple Groups

Theorem (Classification of Finite Simple Groups)

Every finite simple group is isomorphic to a member of one of four infinite classes:

1. ~~the **cyclic groups** of prime order~~,
2. ~~the **alternating groups** of degree at least 5~~, <- Jambor et al. 2013
3. the **classical groups** of Lie type,
4. the **exceptional groups** of Lie type

or one of 26 groups called the **sporadic groups**.

Simple Groups

Theorem (Classification of Finite Simple Groups)

Every finite simple group is isomorphic to a member of one of four infinite classes:

1. ~~the **cyclic groups** of prime order~~,
2. ~~the **alternating groups** of degree at least 5~~,
3. ~~the **classical groups** of Lie type~~, <- Dietrich et al. 2015, but we need to:
   - ~~use *number theory oracles*~~ <- Shor 1994
   - ~~solve recognition problem from $\mathbb{P}\mathrm{SL}(2, q)$~~
     3.1 solved on quotient of matrix groups Babai et al. 2009
     3.2 solved for any BBG, up to DLOG in Borovik and Yalçınkaya 2020
4. the **exceptional groups** of Lie type

or one of 26 groups called the **sporadic groups**.

Simple Groups

Theorem (Classification of Finite Simple Groups)

Every finite simple group is isomorphic to a member of one of four infinite classes:

1. ~~the **cyclic groups** of prime order~~,
2. ~~the **alternating groups** of degree at least 5~~,
3. ~~the **classical groups** of Lie type,~~
4. the **exceptional groups** of Lie type

$$\xcancel{G_2(q)}, q \geqslant 3; \xcancel{F_4(q)}; \xcancel{E_6(q)}; \xcancel{{}^2E_6(q)}; {}^3D_4(q)^*; \xcancel{E_7(q)}; \xcancel{E_8(q)}$$

$$\xcancel{{}^2B_2\left(2^{2n+1}\right)}, n \geqslant 1; \xcancel{{}^2G_2\left(3^{2n+1}\right)}, n \geqslant 1; {}^2F_4\left(2^{2n+1}\right), n \geqslant 1$$

In Kantor and Magaard 2013 and 2015 reduce the problem to $\mathbb{P}\mathrm{SL}(2, q)$, using *number theory oracles*.

or one of 26 groups called the **sporadic groups** and ${}^2F_4(2)'$.

*solved if q is odd

Simple Groups

Theorem (Classification of Finite Simple Groups)

Every finite simple group is isomorphic to a member of one of four infinite classes:

1. ~~the **cyclic groups** of prime order,~~
2. ~~the **alternating groups** of degree at least 5,~~
3. ~~the **classical groups** of Lie type,~~
4. ~~the **exceptional groups** of Lie type~~*

or one of 26 groups called the **sporadic groups** and ${}^2F_4(2)'$.

Sporadic Groups

There are 26 finite simple groups that are not part of the infinite families discussed earlier, plus the Tits Group ${}^2F_4(2)'$, The largest of the 26 *sporadic* groups is the Fischer-Griess monster group $\mathbb{M}$ of cardinality:

$$808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000$$

$$\approx 2^{179.07}$$

With the exception of six *pariahs*, all sporadic groups are part of the *happy family*, i. e., they are subquotients of $\mathbb{M}$. Additionally, the Tits group ${}^2F_4(2)'$ can be considered as part of this family since it is a maximal subgroup of the Fischer Group Fi_{22}.

1. Baby-Step Giant-Step algorithm can be adapted to SDLP, cutting the bit security of $\mathbb{M}$ to 89.6;
2. Actually if G is a sporadic group clearly we can restrict without loss of generality to

$$x \leq \max_{g \in G}(\mathrm{ord}(g)) \cdot \max_{\phi \in \mathrm{Aut}(G)}(\mathrm{ord}(\phi)) =: b(G) \; ;$$

3. For $\mathbb{M}$ we have $b(G) = 119^2 \approx 2^{14}$;
4. For G in the happy family $b(G) \leq 2 \cdot 119^2 \approx 2^{15}$;
5. For G one of the six pariahs $b(G) = 67^2 \approx 2^{13}$;

Simple Groups

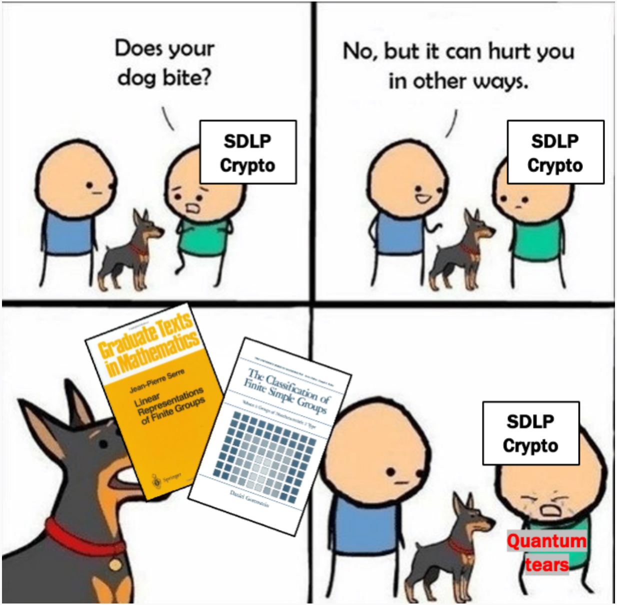
Theorem (Classification of Finite Simple Groups)

Every finite simple group is isomorphic to a member of one of four infinite classes:

1. ~~the **cyclic groups** of prime order~~,
2. ~~the **alternating groups** of degree at least 5~~,
3. ~~the **classical groups** of Lie type,~~
4. ~~the **exceptional groups** of Lie type~~*

or one of ~~26 groups called the **sporadic groups**~~ and $\cancel{{}^2F_4(2)'}$.

Meme


Does your dog bite?
SDLP Crypto
No, but it can hurt you in other ways.
SDLP Crypto
Graduate Texts in Mathematics
Jean-Pierre Serre
Linear Representations of Finite Groups
The Classification of Finite Simple Groups
SDLP Crypto
Quantum tears

Questions?

Thank you for your attention!

`eprint.iacr.org/2024/905`

References

B., Christopher et al. (2023). ***SPDH-Sign: towards Efficient, Post-quantum Group-based Signatures.*** Cryptology ePrint Archive, Paper 2023/595. `https://eprint.iacr.org/2023/595`. URL: `https://eprint.iacr.org/2023/595`.

Babai, László and Robert Beals (1999). **"A polynomial-time theory of black box groups I".** In: *London Mathematical Society Lecture Note Series*, pp. 30–64.

Babai, László et al. (2009). **"Polynomial-time theory of matrix groups".** In: *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*. STOC '09. Bethesda, MD, USA: Association for Computing Machinery, pp. 55–64.

- Borovik, Alexandre and Şükrü Yalçınkaya (2020). ***Natural representations of black box groups encrypting $SL_2(\mathbb{F}_q)$.*** arXiv: `2001.10292 [math.GR]`.
- Dietrich, Heiko et al. (2015). **"Effective black-box constructive recognition of classical groups".** In: *Journal of Algebra* 421, pp. 460–492.
- Habeeb, Maggie et al. (2013). **"Public key exchange using semidirect product of (semi)groups".** In: *International Conference on Applied Cryptography and Network Security*. Springer, pp. 475–486.
- Imran, Muhammad and Gábor Ivanyos (May 2024). **"Efficient quantum algorithms for some instances of the semidirect discrete logarithm problem".** In: *Designs, Codes and Cryptography*.
- Ivanyos, Gábor et al. (2001). **"Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem".** In: *Proceedings of the 13th Annual ACM Symposium on Parallel Algorithms and Architectures*, pp. 263–270.

Jambor, Sebastian et al. (2013). **“Fast recognition of alternating groups of unknown degree”.** In: *Journal of Algebra* 392, pp. 315–335.

Kannan, Ravindran and Richard J. Lipton (1986). **“Polynomial-time algorithm for the orbit problem”.** In: *Journal of the ACM (JACM)* 33.4, pp. 808–821.

Kantor, W.M̃. and K. Magaard (2013). **“Black box exceptional groups of Lie type”.** In: *Trans. Amer. Math. Soc.* 365.9, pp. 4895–4931.

Kohl, Stefan (2003). ***A bound on the order of the outer automorphism group of a finite simple group of given order.*** Available at https://stefan-kohl.github.io/preprints/outbound.pdf.

Mendelsohn, Andrew et al. (2023). ***A Small Serving of Mash: (Quantum) Algorithms for SPDH-Sign with Small Parameters.*** Cryptology ePrint Archive, Paper 2023/1963. URL: https://eprint.iacr.org/2023/1963.

Serre, Jean-Pierre (1977). *Linear Representations of Finite Groups.* Vol. 42. Graduate Texts in Mathematics. Springer.

Shor, Peter W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134.