On the Semidirect Discrete Logarithm Problem in Finite Groups

Analysis of a candidate problem in post-quantum cryptography

Christopher Battarbee, **Giacomo Borin**, Julian Brough, Ryann Cartor, Tobias Hemmert, Nadia Heninger, David Jao, Delaram Kahrobaei, Laura Maddison, Edoardo Persichetti, Angela Robinson, Daniel Smith-Tone, Rainer Steinwandt.

Sorbonne University, IBM Research Zurich, University of Zurich

Outline

Introduction to SDLP

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:

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

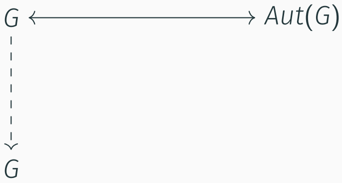
Definitions

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



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

Definitions

$\rho_{g,\phi}$

Fix $(g, \phi) \in G \rtimes Aut(G)$. Define $\rho_{g,\phi} : G \to G$ by

$$\rho_{g,\phi}(h) = g\phi(h)$$

We have seen that

$$\rho^{x}_{g,\phi}(1_G) = g\phi(g)...\phi^{x-1}(g)$$

Definitions

$\rho_{g,\phi}$

Fix $(g, \phi) \in G \rtimes Aut(G)$. Define $\rho_{g,\phi} : G \to G$ by

$$\rho_{g,\phi}(h) = g\phi(h)$$

We have seen that

$$\rho^{x}_{g,\phi}(1_G) = g\phi(g)...\phi^{x-1}(g)$$

SDLP

Fix $G \rtimes Aut(G)$ and a pair (g, ϕ). Suppose we are given $\rho^{x}_{g,\phi}(1_G)$ for some $x \in \mathbb{Z}$. The **S**emidirect **D**iscrete **L**ogarithm **P**roblem is to recover x.

Background

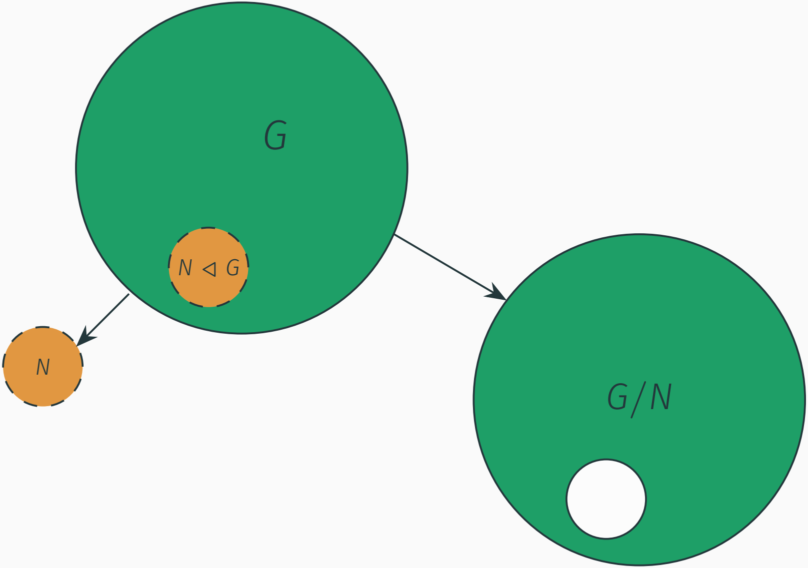
- Natural; outside the mainstream; feasibly post-quantum
- Turns out semidirect product cryptography can be described via commutative group actions*
- Commutative group actions give us Diffie-Hellman-style key exchanges (NIKEs)†, and digital signatures‡
- Recent fast algorithms for SDLP in certain classes of group§

---

*B. et al. 2023a.
†Habeeb et al. 2013.
‡B. et al. 2023b.
§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, the solutions of SDLP are a linear combination of solutions of an instance of SDLP in G/N and an instance of SDLP in N.

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, the solutions of SDLP are a linear combination of solutions of an instance of SDLP in G/N and an instance of SDLP in N.

Imran and Ivanyos 2024, Theorem 4

We can solve SDLP in solvable groups, and groups whose composition factors are small-dimensional matrix groups.

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, the solutions of SDLP are a linear combination of solutions of an instance of SDLP in G/N and an instance of SDLP in N.

Imran and Ivanyos 2024, Theorem 4

We can solve SDLP in solvable groups, and groups whose composition factors are small-dimensional matrix groups.

- Our contribution: reduce an arbitrary instance of SDLP in a finite group to instances of SDLP in simple groups, then solve those with the Classification. Requires a couple of (justified) computational group theory oracles.

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, the solutions of SDLP are a linear combination of solutions of an instance of SDLP in G/N and an instance of SDLP in N.

Imran and Ivanyos 2024, Theorem 4

We can solve SDLP in solvable groups, and groups whose composition factors are small-dimensional matrix groups.

- Our contribution: reduce an arbitrary instance of SDLP in a finite group to instances of SDLP in simple groups, then solve those with the Classification. Requires a couple of (justified) computational group theory oracles.
- To complete the reduction need to compute invariant subgroups and check the recursion terminates.

Computing the Invariant Subgroup

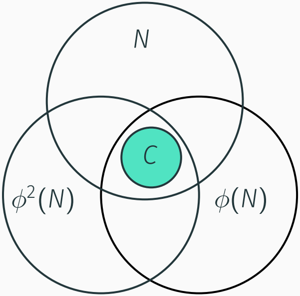


Figure 1: The ϕ-invariant subgroup cannot be smaller than the characteristic subgroup.

- Suppose we can compute a maximal normal subgroup of G, say N.
- 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[a]
- The algorithm doesn't terminate in the trivial subgroup if N contains a characteristic subgroup C (see left)
- We show there is a characteristic subgroup if and only if *every* maximal normal subgroup contains a characteristic subgroup.

[a] No proof that this is not the trivial subgroup.

Characteristically Simple Groups

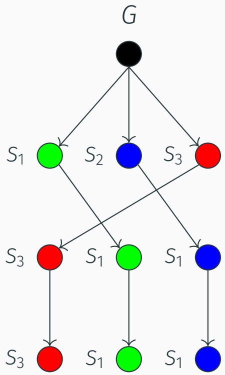


Figure 2: An automorphism of S^3.

- Well-known that groups with no characteristic subgroups (characteristically simple groups) are exactly of the form S^k for some simple group S.
- We show the algorithm for computing ϕ-invariant normal subgroups terminates in the identity exactly when $G = S^k$ and ϕ acts transitively on these components.
- In turn this gives us k^2 SDLP instances in S to solve.

Recursion to (Characteristically) Simple Groups

At each step of the recursion if the ϕ-invariant subgroup algorithm outputs trivial subgroup, call a simple/characteristically simple SDLP solver on that group.

Recursion to (Characteristically) Simple Groups

At each step of the recursion if the ϕ-invariant subgroup algorithm outputs trivial subgroup, call a simple/characteristically simple SDLP solver on that group.

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

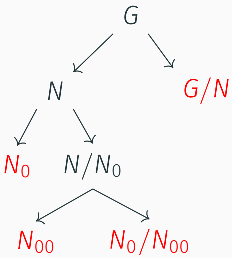


Figure 3: A recursion tree whose nodes are simple or characteristically simple.

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**.

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:

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

Cyclic Groups

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

$$\sum_{i=0}^{x} a^i = \frac{a^{x+1}-1}{a-1}$$

then use again it again to solve SDLP.

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**.

Linear Groups Analysis

Matrix Power Problem

Given $G \leq \mathrm{GL}_n(\mathbb{F})$

Matrix Power Problem

Given $G \leq \mathrm{GL}_n(\mathbb{F})$ and $\phi \in \mathrm{Inn}(G)$ (i.e. $\phi(\mathsf{G}) = \mathsf{SGS}^{-1}$)

Matrix Power Problem

Given $G \leq \mathrm{GL}_n(\mathbb{F})$ and $\phi \in \mathrm{Inn}(G)$ (i.e. $\phi(\mathsf{G}) = \mathsf{SGS}^{-1}$) , thanks to Imran and Ivanyos 2024, 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:

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

Matrix Power Problem

Given $G \leq \mathrm{GL}_n(\mathbb{F})$ and $\phi \in \mathrm{Inn}(G)$ (i.e. $\phi(\mathsf{G}) = \mathsf{SGS}^{-1}$) , thanks to Imran and Ivanyos 2024, 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 Kannan and Lipton 1986 the problem can be reduced to a discrete logarithm over $\mathrm{GL}(W)$ for W subspace of V.

Matrix Power Problem

Given $G \leq \mathrm{GL}_n(\mathbb{F})$ and $\phi \in \mathrm{Inn}(G)$ (i.e. $\phi(\mathbf{G}) = \mathbf{S}\mathbf{G}\mathbf{S}^{-1}$) , thanks to Imran and Ivanyos 2024, 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 Kannan and Lipton 1986 the problem can be reduced to a discrete logarithm over $\mathrm{GL}(W)$ for W subspace of V.

Result: We can do the same for projective linear groups $G \leq \mathbb{P}\mathrm{GL}$.

Reduction to Inner Automorphisms

Theorem (Kohl 2003)

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

Reduction to Inner Automorphisms

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.

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**.

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

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.

Constructive Recognition Problem

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.

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.

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*
    - solve recognition problem from $\mathbb{P}\mathrm{SL}(2, q)$
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 $\mathbb{P}\mathrm{SL}(2, q)$
4. the **exceptional groups** of Lie type

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

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

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

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

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

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

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

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

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

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:

Sporadic Groups

There are 26 finite simple groups:

1. 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

   $$\approx 2^{179.07}$$

There are 26 finite simple groups:

1. 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

   $$\approx 2^{179.07}$$

2. of the remaining 19 (+ 1) are part of the *happy family*, i. e., they are subquotients of $\mathbb{M}$,

There are 26 finite simple groups:

1. The largest of the 26 *sporadic* groups is the Fischer-Griess monster group $\mathbb{M}$ of cardinality:

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

   $$\approx 2^{179.07}$$

2. of the remaining 19 (+ 1) are part of the *happy family*, i. e., they are subquotients of $\mathbb{M}$,
3. the other are referred as the six *pariahs*, and have cardinality $\leq 2^{67}$

Breaking Sporadic Groups

1. **Result:** Baby-Step Giant-Step algorithm can be adapted to SDLP, cutting the bit security of $\mathbb{M}$ to 89.6;

1. **Result:** 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

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

1. Result: 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

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

3. For $\mathbb{M}$ we have $b(G) = 119^2 \approx 2^{14}$;

1. **Result:** 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 $b(G) \leq 2 \cdot 119^2 \approx 2^{15}$;

1. Result: 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

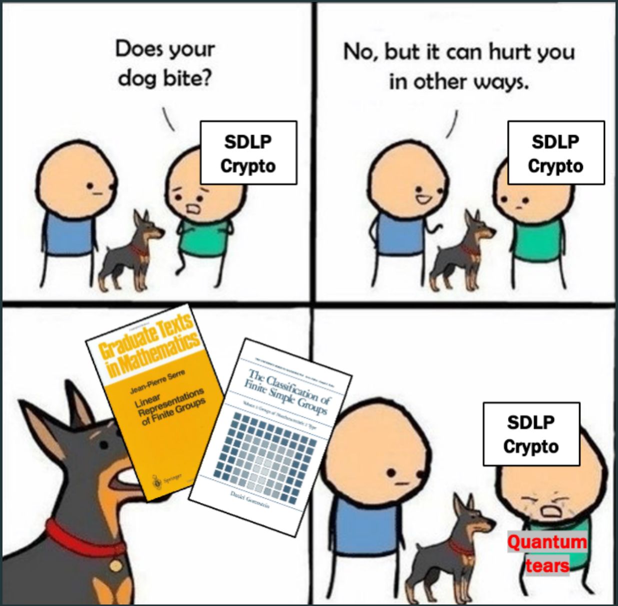
Theorem (Classification of Finite Simple Groups)

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 ~~$^2F_4(2)'$~~.

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

Thank you for your attention!

`eprint.iacr.org/2024/905`

References

B., Christopher et al. (2023a). *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.

B., Christopher et al. (2023b). "SPDH-Sign: towards Efficient, Post-quantum Group-based Signatures". In: *PQCrypto 2023-The 14th International Conference on Post-Quantum Cryptography*.

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. (1991). "Fast Monte Carlo algorithms for permutation groups". In: *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pp. 90–100.

- 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*.

- 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`.

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.

Additional Material

Finding Maximal Normal Subgroups

The task of finding a maximal normal subgroup is more subtle, since it depends on the particular implementation of the black-box group G.

Finding Maximal Normal Subgroups

The task of finding a maximal normal subgroup is more subtle, since it depends on the particular implementation of the black-box group G.

We can solve it via computing a composition series:

$$\{e\} = G_n \leq G_{n-1} \leq ... \leq G_1 \leq G \ ,$$

a well know problem in computational group theory

Finding Maximal Normal Subgroups

The task of finding a maximal normal subgroup is more subtle, since it depends on the particular implementation of the black-box group G.

We can solve it via computing a composition series:

$$\{e\} = G_n \leq G_{n-1} \leq ... \leq G_1 \leq G \ ,$$

a well know problem in computational group theory

However, this branch of literature typically wishes to achieve much stronger results and are thwarted by DLOG computation - we do not impose this limitation since we assume QCs.

Finding Maximal Normal Subgroups : Possible Solutions:

1. if we know the particular structure of the group G, we can use it to construct for any subgroup S the smallest normal subgroup containing $\langle S^G \rangle$ in linear time, as explained in Babai et al. 1991.

¶we need G/G_1 to have the unique encoding property

Finding Maximal Normal Subgroups : Possible Solutions:

1. if we know the particular structure of the group G, we can use it to construct for any subgroup S the smallest normal subgroup containing $\langle S^G \rangle$ in linear time, as explained in Babai et al. 1991.
2. Use Imran and Ivanyos 2024, but requires that every non-Abelian composition factor of G possesses a faithful small permutation representation;
3. Otherwise, with Babai and Beals 1999 and a QC we can find $G_1 \leq G$, with G/G_1:

¶we need G/G_1 to have the unique encoding property

Finding Maximal Normal Subgroups : Possible Solutions:

1. if we know the particular structure of the group G, we can use it to construct for any subgroup S the smallest normal subgroup containing $\langle S^G \rangle$ in linear time, as explained in Babai et al. 1991.
2. Use Imran and Ivanyos 2024, but requires that every non-Abelian composition factor of G possesses a faithful small permutation representation;
3. Otherwise, with Babai and Beals 1999 and a QC we can find $G_1 \leq G$, with G/G_1:
   3.1 simple and nonabelian, so G_1 is Maximal Normal Subgroup;

¶we need G/G_1 to have the unique encoding property

Finding Maximal Normal Subgroups : Possible Solutions:

1. if we know the particular structure of the group G, we can use it to construct for any subgroup S the smallest normal subgroup containing $\langle S^G \rangle$ in linear time, as explained in Babai et al. 1991.
2. Use Imran and Ivanyos 2024, but requires that every non-Abelian composition factor of G possesses a faithful small permutation representation;
3. Otherwise, with Babai and Beals 1999 and a QC we can find $G_1 \leq G$, with G/G_1:
   3.1 simple and nonabelian, so G_1 is Maximal Normal Subgroup;
   3.2 or abelian, so we can use point 1 to get the maximal normal subgroup $A_1 \lhd G/G_1$[¶] and A_1G_1 will be a maximal normal in G by the correspondence theorem.

¶we need G/G_1 to have the unique encoding property

SDLP on Matrix Groups (Imran and Ivanyos 2024)

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

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

SDLP on Matrix Groups (Imran and Ivanyos 2024)

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

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

SDLP on Matrix Groups (Imran and Ivanyos 2024)

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

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

$$= \mathsf{GS} \cdot \mathsf{GS} \cdot \mathsf{GS} \cdots \mathsf{SG} \cdot \mathsf{S}^{-x} = (\mathsf{GS})^{x} \cdot \mathsf{G} \cdot \mathsf{S}^{-x}$$

SDLP on Matrix Groups (Imran and Ivanyos 2024)

Consider $G \leq \mathrm{GL}_n(\mathbb{F})$ and $\phi \in \mathrm{Inn}(G)$ 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:

$$\mathrm{vec}(s_{\mathsf{G},\phi}(x)) = \mathrm{vec}\left((\mathsf{GS})^x \cdot \mathsf{G} \cdot \mathsf{S}^{-x}\right)$$

SDLP on Matrix Groups (Imran and Ivanyos 2024)

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

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

So if we vectorize the matrices we get:

$$
\begin{aligned}
\mathrm{vec}(s_{\mathsf{G},\phi}(x)) &= \mathrm{vec}\left((\mathsf{GS})^x \cdot \mathsf{G} \cdot \mathsf{S}^{-x}\right) \\
&= \mathrm{vec}\left((\mathsf{GS}) \cdot (\mathsf{GS})^{x-1} \cdot \mathsf{G} \cdot \mathsf{S}^{-(x-1)} \cdot \mathsf{S}^{-1}\right)
\end{aligned}
$$

SDLP on Matrix Groups (Imran and Ivanyos 2024)

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

$$
\begin{aligned}
s_{\mathsf{G},\phi}(x) &= \mathsf{G} \cdot \mathsf{SG}\cancelto{\mathsf{S}}{\mathsf{S}^{-1} \cdot \mathsf{S}^2}\mathsf{GS}^{-2} \cdots \mathsf{S}^{x-1}\mathsf{G}\cancelto{\mathsf{S}}{\mathsf{S}^{-x+1} \cdot \mathsf{S}^x}\mathsf{GS}^{-x} = \\
&= \mathsf{GS} \cdot \mathsf{GS} \cdot \mathsf{GS} \cdots \mathsf{SG} \cdot \mathsf{S}^{-x} = (\mathsf{GS})^x \cdot \mathsf{G} \cdot \mathsf{S}^{-x}
\end{aligned}
$$

So if we vectorize the matrices we get:

$$
\begin{aligned}
\mathrm{vec}(s_{\mathsf{G},\phi}(x)) &= \mathrm{vec}\left((\mathsf{GS})^x \cdot \mathsf{G} \cdot \mathsf{S}^{-x}\right) \\
&= \mathrm{vec}\left((\mathsf{GS}) \cdot (\mathsf{GS})^{x-1} \cdot \mathsf{G} \cdot \mathsf{S}^{-(x-1)} \cdot \mathsf{S}^{-1}\right) \\
&= \mathrm{vec}\left((\mathsf{GS}) \cdot s_{\mathsf{G},\phi}(x-1) \cdot \mathsf{S}^{-1}\right)
\end{aligned}
$$

SDLP on Matrix Groups (Imran and Ivanyos 2024)

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

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

$$= \mathsf{GS} \cdot \mathsf{GS} \cdot \mathsf{GS} \cdots \mathsf{SG} \cdot \mathsf{S}^{-x} = (\mathsf{GS})^{x} \cdot \mathsf{G} \cdot \mathsf{S}^{-x}$$

So if we vectorize the matrices we get:

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

SDLP on Matrix Groups (Imran and Ivanyos 2024)

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

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

$$= \mathsf{GS} \cdot \mathsf{GS} \cdot \mathsf{GS} \cdots \mathsf{SG} \cdot \mathsf{S}^{-x} = (\mathsf{GS})^x \cdot \mathsf{G} \cdot \mathsf{S}^{-x}$$

So if we vectorize the matrices we get:

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

...repeating the argument $x-1$ more times...

SDLP on Matrix Groups (Imran and Ivanyos 2024)

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

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

$$= \mathsf{GS} \cdot \mathsf{GS} \cdot \mathsf{GS} \cdots \mathsf{SG} \cdot \mathsf{S}^{-x} = (\mathsf{GS})^x \cdot \mathsf{G} \cdot \mathsf{S}^{-x}$$

So if we vectorize the matrices we get:

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