QUANTUM ALGORITHM FOR THE DISCRETE LOGARITHM PROBLEM FOR MATRICES OVER FINITE GROUP RINGS

A. D. MYASNIKOV AND A. USHAKOV

Abstract. We propose a polynomial time quantum algorithm for solving the discrete logarithm problem in matrices over finite group rings. The hardness of this problem was recently employed in the design of a key-exchange protocol proposed by D. Kahrobaei, C. Koupparis, and V. Shpilrain [4]. Our result implies that the Kahrobaei et al. protocol does not belong to the realm of post-quantum cryptography.
Keywords and phrases: Group-based cryptography, semidirect product, matrix monoids, group-rings, Diffie-Hellman, key-exchange, discrete logarithm problem, quantum algorithms, post-quantum cryptography.
AMS Classification: 94A60, 68Q12, 81P68, 68W30.

1. Introduction

The discrete logarithm problem (DLP) in a finite cyclic group G is an algorithmic question to find for any given pair of elements $g, h \in G$ a number $n \in \mathbb{N}$ satisfying $g^n = h$. This problem is extremely important due to its relation to cryptography. One of the most prominent and long withstanding protocols, the Diffie-Hellman key-exchange protocol, is based on the assumption that DLP is hard in certain groups. The Diffie-Hellman protocol proposed in [1] was the first practical solution to the key distribution problem, allowing two parties (Alice and Bob), never having met in advance or shared keying material, to establish a shared secret by exchanging messages over an open channel ([9]). Its basic version works as follows:

Algorithm 1. Diffie-Hellman key-agreement.

One-time setup: Choose an appropriate prime p and a generator g of $\mathbb{F}_p^*$ with $2 \leq g \leq p-2$.

1: Alice chooses a random secret a with $1 \leq a \leq p-2$ and sends $g^a \mod p$ to Bob.
2: Bob chooses a random secret b with $1 \leq b \leq p-2$ and sends $g^b \mod p$ to Alice.
3: Alice receives g^b and computes the shared key as $K = (g^b)^a \mod p$.
4: Bob receives g^a and computes the shared key as $K = (g^a)^b \mod p$.

Date: October 9, 2012.
The work of the second author was partially supported by NSF grant DMS-0914773.

To break this scheme a passive eavesdropper must solve the Diffie-Hellman problem or, more generally, the discrete logarithm problem (DLP) in $\mathbb{F}_p$. After 30 years of extensive research DLP still looks hard for a conventional computer. Nevertheless, it can be efficiently solved using a quantum computer. Shor in [18] showed that DLP can be solved by a quantum algorithm in polynomial time in any finite field $\mathbb{F}_{p^s}$ (where p is prime and $s \in \mathbb{N}$). Currently quantum computers are weak, but a full scale quantum computer (if ever built) will defeat all DLP-based and factorization-based schemes. This is a powerful motivator for the design and construction of quantum computers and for the study of new quantum computer algorithms. It also facilitates research on new cryptosystems that are secure against quantum computers, collectively called post-quantum cryptography. Currently post-quantum cryptography is mostly focused on four different approaches:

- Lattice-based cryptography such as NTRU ([3]) and GGH ([2]).
- Multivariate cryptography such as *unbalanced oil and vinegar* ([5]).
- Hash-based signatures such as Lamport signatures ([6]) and Merkle ([10]) signature scheme.
- Code-based cryptography that relies on error-correcting codes, such as McEliece encryption ([7]) and Niederreiter signatures ([13]).

For a recent survey of quantum-resistant public-key schemes see [16]. There are also attempts to employ the ideas from combinatorial group theory in the design of cryptographic primitives secure in a post-quantum world ([11, 12]). In particular, there are ideas of how to generalize the original Diffie-Hellman protocol using different group-oriented constructions. For instance, Odoni, Varadharajan, and Sanders in [14] suggested to use exponentiation in a group of non-singular matrices over a finite field $\mathrm{GL}_n(\mathbb{F}_{p^s})$. That proposal was cryptanalyzed by Meneses and Wu in [8] who showed that there exists a probabilistic polynomial time reduction of DLP in $\mathrm{GL}_n(\mathbb{F}_{p^s})$ to DLP in some small extension field of $\mathbb{F}_{p^s}$, proving that the proposal brings nothing new to the field.

More recently, D. Kahrobaei, C. Koupparis, and V. Shpilrain in [4] considered yet another variation of the Diffie-Hellman key-exchange protocol which uses the ring of 3×3 matrices over a group-ring $\mathbb{F}_7[S_5]$. The authors claim that the new scheme can withstand quantum algorithm attacks and provide some supporting arguments. In this paper we disprove that claim. In more detail, we prove that the ring $M_3(\mathbb{F}_7[S_5])$ can be embedded into a ring $M_{360}(\mathbb{F}_7)$ (see below for precise definitions) and generalize the Meneses-Wu reduction to the case of a singular base matrix. This efficiently reduces DLP in $M_3(\mathbb{F}_7[S_5])$ to DLP in some small extension field of $\mathbb{F}_{p^s}$ which is finally solved by Shor's quantum algorithm. This proves the following results:

Theorem 1. *Let G be a finite group and p a prime number. The discrete logarithm problem in the ring $M_n(\mathbb{F}_{p^s}[G])$ can be solved by a probabilistic quantum algorithm in (expected) polynomial time in $n, \log_2(p), s, |G|$.* □

Corollary 2. *Let G be a finite group and p a prime number. The discrete logarithm problem in the group-ring $\mathbb{F}_{p^s}[G]$ can be solved by a probabilistic quantum algorithm in (expected) polynomial time in $\log_2(p), s, |G|$.* □

In Section 2 we give the definition of a group ring and describe the Kahrobaei et al. protocol. In Section 3 we recall the Meneses-Wu reduction and extend it to singular matrices. In Section 4 we describe the embedding construction and briefly discuss the results of experiments.

2. Group rings and Kahrobaei et al. protocol

Let $G = \{g_1, \ldots, g_k\}$ be a finite group of order k and R is a commutative ring. The *group-ring* $R[G]$ is the set of formal linear combinations of g_i's:

$$\sum_{i=1}^{k} a_i g_i, \qquad a_i \in R$$

equipped with addition and multiplication defined as follows:

$$\left(\sum_{i=1}^{k} a_i g_i\right) + \left(\sum_{i=1}^{k} b_i g_i\right) = \sum_{i=1}^{k} (a_i + b_i) g_i$$

and

$$\left(\sum_{i=1}^{k} a_i g_i\right) \cdot \left(\sum_{i=1}^{k} b_i g_i\right) = \sum_{i=1}^{k} \left(\sum_{g_j g_k = g_i} (a_j b_k)\right) g_i.$$

It is easy to see that multiplication is not commutative unless the group G is commutative. For more on group-rings see [15]. By S_n we denote the group of permutations on n elements. We denote by $\mathrm{GL}_m(\mathbb{F}_p[S_n])$ the group of invertible $m \times m$ matrices over the ring $\mathbb{F}_p[S_n]$ and by $M_m(\mathbb{F}_p[S_n])$ the ring of all $m \times m$ matrices over the ring $\mathbb{F}_p[S_n]$.

The protocol proposed by Kahrobaei et al. [4] works exactly the same way as the original Diffie-Hellman. We describe it here just to fix the notation and parameter values:

Algorithm 2. Kahrobaei-Koupparis-Shpilrain key-agreement.

One-time setup: Choose a matrix $M \in M_3(\mathbb{F}_7[S_5])$.

1: Alice chooses a random secret a and sends M^a to Bob.
2: Bob chooses a random secret b and sends $M^b \mod p$ to Alice.
3: Alice receives M^b and computes the shared key as $K = (M^b)^a$.
4: Bob receives M^a and computes the shared key as $K = (M^a)^b$.

---

3. Menezes-Wu reduction and singular matrices

The original reduction is described for invertible matrices only. To design an algorithm for matrices over group rings we need a more general technique which works with singular matrices as well. We start out with the description of the original reduction following by the modifications which extend the reduction to arbitrary matrices.

Let $A \in GL(n, q)$ (where $q = p^s$ and p is prime) and $B = A^k$. Our goal is to find a number $l \in \mathbb{N}$ satisfying $B = A^l$. Below we sketch the Menezes-Wu algorithm which uses Shor's quantum algorithm for factoring integers [18].

(1) Using Hessenberg algorithm compute the characteristic polynomial $p_a(x)$ for A and using Ben-Or's algorithm express it as a product:
$$p_a(x) = f_1^{e_1}(x) \dots f_s^{e_s}(x),$$
where f_i's are distinct and irreducible.

(2) Some sufficiently large extension E of $\mathbb{F}_q$ contains the eigenvalues $\lambda_1, \dots, \lambda_s$ for A. Unfortunately, E can be very large. To avoid this problem consider the following extensions separately:
$$\mathbb{F}_q(\lambda_i) \simeq \mathbb{F}_q[x]/\langle f_{\lambda_i}(x)\rangle,$$
where f_{λ_i} is the irreducible polynomial for λ_i, and describe the structure of the Jordan form for A. This can be done regardless of M being invertible or not.

(3) By [8, Theorem 2] the order of A in G can be found as:
$$\mathrm{ord}(A) = \mathrm{lcm}(\mathrm{ord}(\lambda_1), \dots, \mathrm{ord}(\lambda_s)) \cdot p\{t\}$$
where $\mathrm{ord}(\lambda_i)$ is the order of λ_i in $\mathbb{F}_q(\lambda_i)$, t is the size of the largest Jordan block and $p\{t\}$ is the least power of p greater than or equal to t. The number l is uniquely determined modulo $\mathrm{ord}(A)$.

(4) Using quantum computer we can efficiently find prime power factorization for the numbers $|(\mathbb{F}_q[x]/\langle f_{\lambda_i}(x)\rangle)^*| = q^{\deg(f_{\lambda_i})} - 1$. Given the factorization of $q^{\deg(f_{\lambda_i})} - 1$ it is straightforward to compute $\mathrm{ord}(\lambda_i)$.

(5) For every eigenvalue λ_i of A find (conjugating by an appropriate matrix) the corresponding eigenvalue λ_i^l of B. Using quantum computer solve the DLP in $\mathbb{F}_q(\lambda_i)$ which gives a number l_i satisfying $\lambda_i^{l_i} = \lambda_i^l$ in $\mathbb{F}_q(\lambda_i)$. This gives a relation
$$l_i \equiv l \mod \mathrm{ord}(\lambda_i).$$

(6) Compute $l \mod p\{t\}$ as described in [8].

(7) Finally, compute $l \mod \mathrm{ord}(A)$ using the generalized Chinese remainder theorem.

For a detailed description of the algorithm we refer the reader to the original paper by Menezes and Wu.

Now, if A is a singular matrix, then some eigenvalues λ_i are trivial and the Jordan form of A is a direct sum $N \oplus Z$ of a non-singular block N and

a singular block Z. Recall that a matrix A is called *nilpotent* if $A^n = 0$ for some $n \in \mathbb{N}$. The least positive n satisfying $A^n = 0$ is called the *degree* of nilpotency. It is easy to see that a singular Jordan $d \times d$-block is nilpotent of degree d. Hence, the singular block Z is nilpotent of degree r, where r is the size of a largest singular Jordan block in Z. Therefore, for some invertible matrix S we have:

$$\begin{aligned} A^r &= S^{-1}(N \oplus Z)^r S \\ &= S^{-1}(N^r \oplus 0)S \\ &= S^{-1}(N^{r+ord(N)} \oplus 0)S \\ &= A^{r+\mathrm{ord}(N)}. \end{aligned}$$

Furthermore, r and $\mathrm{ord}(N)$ are the least positive numbers satisfying the equality above. The number $\mathrm{ord}(N)$ can be computed as in Menezes-Wu and the number r can be computed by observing the structure of the Jordan form.

Next, to solve an instance (A, B) of DLP in $M_n(\mathbb{F}_q)$ we do the following:

- Describe the Jordan normal form for A and B. Let N_A and N_B be the non-singular blocks of A and B respectively.
- Applying Menezes-Wu and Shor algorithms, solve the DLP for the instance (N_A, N_B) and obtain the number l' satisfying:
$$N_B = N_A^{l'} \text{ and } l' \leq \mathrm{ord}(N_A).$$
- Take into account the singular block in the Jordan's matrix for A. One number l from the set
$$\{l' + c \cdot \mathrm{ord}(N_A) \mid c \in \mathbb{N} \cup \{0\},\ l' + c \cdot \mathrm{ord}(N_A) \leq r + \mathrm{ord}(N_A)\}.$$
satisfies $B = A^l$. The set contains up to r numbers and, hence, we can enumerate it and find the required number.

This gives a quantum algorithm for singular matrices.

4. The embedding

In this section we describe the reduction of the discrete logarithm problem in $M_n(\mathbb{F}_{p^s}[G])$ to the discrete logarithm problem in some extension of $\mathbb{F}_{p^s}$. In a more general setting, fix a finite group $G = \{g_1, \ldots, g_k\}$ and a commutative ring R. Let $a, b \in R[G]$ and $c = a \cdot b$ where

$$a = \sum_{g \in G} a_g \cdot g,\ b = \sum_{g \in G} b_g \cdot g, \quad \text{and} \quad c = \sum_{g \in G} c_g \cdot g,$$

for some $a_g, b_g \in R$. For $a \in R[G]$ define a matrix $M_a \in M_k(R)$ and a vector $\overline{v}_a \in R^k$ as follows:

$$M_a = \begin{pmatrix} a_{g_1 g_1^{-1}} & \ldots & a_{g_1 g_k^{-1}} \\ \ldots & & \\ a_{g_k g_1^{-1}} & \ldots & a_{g_k g_k^{-1}} \end{pmatrix} \text{ and } \overline{v}_a = \begin{pmatrix} a_{g_1} \\ \ldots \\ a_{g_k} \end{pmatrix}.$$

It is easy to see that:

$$M_a \cdot \overline{v}_b = \overline{v}_c. \tag{1}$$

Therefore, the right multiplication in $R[G]$ is a linear transformation of R^k and can be naturally interpreted in $M_k(R)$.

Proposition 3. *For any $a, b \in R[G]$ we have $M_{a\cdot b} = M_a \cdot M_b$. Furthermore, the map $a \mapsto M_a$ is a ring monomorphism.*

Proof. Pick arbitrary $a, b \in R[G]$. Obviously, $M_{a+b} = M_a + M_b$. To prove that $M_{a\cdot b} = M_a \cdot M_b$ consider arbitrary $1 \leq i, j \leq n$. The (i, j)'s entry in the matrix $M_{a\cdot b}$ is:

$$(ab)_{g_i g_j^{-1}} = \sum_{gh = g_i g_j} a_g b_h,$$

which is the same as the (i, j)'s entry in the matrix $M_a \cdot M_b$:

$$\sum_{m=1}^{k} a_{g_i g_m^{-1}} a_{g_m g_j^{-1}}.$$

Therefore, $M_{a\cdot b} = M_a \cdot M_b$ and the map $a \mapsto M_a$ is a ring homomorphism. Finally, we note that we can easily reconstruct a from M_a. Thus, the map $a \mapsto M_a$ is a monomorphism. □

Next, any matrix $A = (a_{ij}) \in M_n(R[G])$ defines a linear transformation of $(R[G])^n$ in the usual way:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & & \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ \dots \\ b_n \end{pmatrix} = \begin{pmatrix} \sum a_{1i} b_i \\ \dots \\ \sum a_{ni} b_i \end{pmatrix}.$$

For $A = (a_{ij}) \in M_n(R[G])$ define a block matrix A^* and for a vector column $\overline{b} = (b_1, \dots, b_n) \in (R[G])^n$ a joint vector $b^* \in R^{kn}$:

$$A^* = \begin{pmatrix} M_{a_{11}} & \dots & M_{a_{1n}} \\ \dots & & \\ M_{a_{n1}} & \dots & M_{a_{nn}} \end{pmatrix} \text{ and } b^* = \begin{pmatrix} \overline{v}_{b_1} \\ \dots \\ \overline{v}_{b_n} \end{pmatrix}.$$

Let $\overline{c} = A \cdot \overline{b}$. Then it is straightforward to check that:

$$c^* = A^* \cdot b^*. \tag{2}$$

Proposition 4. *Let G be a finite group of order k and R a commutative ring. Then the map $\varphi : M_n(R[G]) \to M_{nk}(R)$ given by $A \mapsto A^*$ is a ring monomorphism.*

Proof. Pick arbitrary $A, B \in M_n(R[G])$. Obviously, $(A + B)^* = A^* + B^*$. It follows from Proposition 3 that:

$$A^* \cdot B^* = (AB)^*$$

and, hence, φ is a homomorphism. The map φ is obviously injective because given A^* one can easily reconstruct the original matrix A. □

Now let $R = \mathbb{F}_{p^s}$. By Proposition 4, we can reduce the discrete logarithm problem in $M_n(\mathbb{F}_{p^s}[G])$ to DLP in $M_{nk}(\mathbb{F}_{p^s})$ which further can be reduced to DLP in some extension of $\mathbb{F}_{p^s}$ using the Menezes-Wu algorithm. The latter can be solved by Shor's algorithm. This proves Theorem 1.

Finally observe that DLP in the ring $M_3(\mathbb{F}_7[S_5])$ used by Kahrobaei et al. is a particular case of the problem described above and, therefore, can be solved efficiently on a quantum computer using the described reduction.

Out of curiosity we implemented the embedding and obtained the following statistics: 30% of randomly uniformly generated matrices $M \in M_3(\mathbb{F}_7[S_5])$ have $M^* \in \mathrm{GL}_{360}(\mathbb{F}_7)$. This means that 30% of instances of DLP $M_3(\mathbb{F}_7[S_5])$ reduce to elements of $\mathrm{GL}_{360}(\mathbb{F}_7)$ and the original Meneses-Wu reduction works for them. Other 70% of the instances require generalized technique described in the end of Section 3.

5. Conclusion

We presented a probabilistic polynomial-time quantum algorithm for solving the discrete logarithm problem in the ring $M_n(\mathbb{F}_{p^s}[G])$ for any fixed finite group G. As a consequence we showed that the protocol proposed by Kahrobaei et al. is vulnerable to quantum algorithm attacks and does not belong to the realm of post-quantum cryptography. It is not clear how to improve the protocol to resist this type of attacks.

Adding conjugation (as in [17]) helps, because on step (5) one can not immediately find the eigenvalue λ_i^l of B corresponding to the eigenvalue λ_i of A. But that does not look like a serious improvement since conjugation preserves the Jordan blocks and to break the new scheme it will just require to find the associated blocks in A and in B. Furthermore, our method reduces the Diffie-Hellman problem with conjugation in $M_3(\mathbb{F}_7[S_5])$ to the same problem in $M_{360}(\mathbb{F}_7)$, which means that the system with conjugations over $\mathbb{F}_7[S_5]$ does not bring much new to the field either.

Another idea that comes to mind is taking a large group G. Unfortunately, this will make exponentiation in $M_n(\mathbb{F}_{p^s}[G])$ computationally infeasible because of the growth of the size of elements representing large powers in $\mathbb{F}_{p^s}[G]$.

References

[1] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE T. Inform. Theory*, IT-22:644–654, 1976.

[2] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In *Advances in Cryptology – CRYPTO 1997*, volume 1294 of *Lecture Notes Comp. Sc.*, pages 112–131, London, UK, 1997. Springer-Verlag.

[3] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. Silverman, and W. Whyte. Ntruencrypt and ntrusign: efficient public key algorithms for a post-quantum world. In *PQCrypto 2006: International Workshop on Post-Quantum Cryptography*, PQCrypto 2006, pages 141–158, 2006.

[4] D. Kahrobaei, C. Koupparis, and V. Shpilrain. Public key exchange using matrices over group rings. preprint. Available at `http://www.sci.ccny.cuny.edu/~shpil/Sn_groupring.pdf`.
[5] A. Kipnis, J. Patarin, and L. Goubin. Unbalanced oil and vinegar signature schemes. In *Proceedings of the 17th international conference on Theory and application of cryptographic techniques*, EUROCRYPT'99, pages 206–222, Berlin, Heidelberg, 1999. Springer-Verlag.
[6] L. Lamport. Constructing digital signatures from a one-way function. technical report SRI-CSL-98, SRI International Computer Science Laboratory, Oct. 1979.
[7] R. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. DSN Progress Report 42-44, 1978.
[8] A. Menezes and Y. Wu. The discrete logarithm problem in $GL_n(F_q)$. *Ars Combinatorica*, 47:23–32, 1997.
[9] A. J. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
[10] R. Merkle. A certified digital signature. In *Proceedings on Advances in cryptology*, CRYPTO '89, pages 218–238. Springer-Verlag, 1989.
[11] A. G. Miasnikov, V. Shpilrain, and A. Ushakov. *Group-based Cryptography*. Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser Basel, 2008.
[12] A. G. Miasnikov, V. Shpilrain, and A. Ushakov. *Non-Commutative Cryptography and Complexity of Group-Theoretic Problems*. Mathematical Surveys and Monographs. AMS, 2011.
[13] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problemy Upravlenija i Teorii Informacii*, 15:159–166, 1986.
[14] R. Odoni, V. Varadharajan, and R. Sanders. Public key distribution in matrix rings. *Electronic Lett.*, 20:386–387, 1984.
[15] D. Passman. *The Algebraic Structure of Group Rings*. Dover Publications, 2011.
[16] R. Perlner and A. Cooper. Quantum resistant public key cryptography: a survey. In *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, volume 2904 of *IDtrust '09*, pages 85–93, New York, NY, USA, 2009. ACM.
[17] L. Sakalauskas, P. Tvarijonas, and A. Raulynaitis. Key agreement protocol (kap) using conjugacy and discrete logarithm problems in group representation level. *Informatica*, 18:115–124, 2007.
[18] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

Department of Mathematics, Stevens Institute of Technology, Hoboken, NJ, USA

E-mail address: `amyasnik,aushakov@stevens.edu`