Theoretical and Applied Informatics
Vol. 28 (2016), no. 3, pp. 8–16
DOI: 10.20904/283008

Cryptography with right-angled Artin groups

Ramón Flores[1*] Delaram Kahrobaei[2,3†]

[1]Department of Geometry and Topology, University of Seville, Spain

[2]CUNY Graduate Center, PhD program in computer science, City University of New York

[3]Tandon School of Engineering, Computer Science Department, New York University

Abstract In this paper we propose right-angled Artin groups as a platform for secret sharing schemes based on the efficiency (linear time) of the word problem. Inspired by previous work of Grigoriev-Shpilrain in the context of graphs, we define two new problems: Subgroup Isomorphism Problem and Group Homomorphism Problem. Based on them, we also propose two new authentication schemes. For right-angled Artin groups, the Group Homomorphism and Graph Homomorphism problems are equivalent, and the later is known to be NP-complete. In the case of the Subgroup Isomorphism problem, we bring some results due to Bridson who shows there are right-angled Artin groups in which this problem is unsolvable.

Keywords authentication schemes; group homomorphism; graph homomorphism

Received 24 NOV 2016 **Revised** 14 FEB 2017 **Accepted** 05 APR 2017

1 Introduction

Using algorithmic group theoretic problems in cryptography has been an active area of research since 1999 (see [1] for a thorough account). The complexity of different algorithmic problems (Conjugacy Problems, Membership Problems, etc.) have made available a lot of families of groups as platform groups for cryptographic protocols, as for example:

- braid groups, using the Conjugacy Search Problem [2],
- polycyclic groups, using the Conjugacy Search Problem [3, 4],
- Thompson groups, based on the Decomposition Search Problem [5],

*E-mail: cluje28@gmail.com
†E-mail: DKahrobaei@gc.cuny.edu

- hyperbolic groups, using properties of subgroup distortion and the Geodesic Length Problem [6],
- free metabelian groups, based on the Subgroup Membership Search Problem [7], and in the Endomorphism Search Problem [8],
- free nilpotent p-groups, for a semidirect product public key [9],
- linear groups [10],
- Grigorchuk groups, for cryptographic protocols [11],
- groups of matrices, for a Homomorphic Encryption scheme [12].

Note that some are infinite and some are finite, but they are all non-commutative.

As mentioned above, we propose here right-angled Artin groups for two secret sharing schemes, as well as two authentication schemes. For the first, we follow the approach of Habeeb-Kahrobaei-Shpilrain [8] and Shamir [13], while the second is a modification of two protocols developed by Grigoriev-Shpilrain [14] in the context of graphs, that we adapt to the language of right-angled Artin groups by using the graph which is always associated to these groups. Then, we take advantage of the fact that many graph-theoretic problems that are proved to be NP-complete can be translated to a group-theoretic setting in the right-angled Artin groups, and also of some unsolvability results which are proper from this context. Besides that it is always of interest to introduce new applications of Group Theory in cryptography, we also note that working with group presentation is easier and sometimes more practical than working with graphs. We note that Shpilrain-Zapata have proposed a key exchange based on Artin groups but this class is much bigger than right-angled Artin groups [7].

This article is structured as follows. In Sec. 2 we review the main features of right-angled Artin groups that will be useful for our purposes. Sec. 3 is devoted to the description of the sharing schemes, while the authentication schemes are treated in Sec. 4. Finally, in Sec. 5 we deal with study of the security of the proposed protocols.

2 Right Angled Artin Groups

First we will introduce the main facts concerning right-angled Artin groups, a class probably introduced first in [15] by Hauschild and Rautenberg (which called them *semifree* groups) in the seventies. Good surveys about the topic can be found in [16] and [17], while a good general introduction for the theory presentations of groups is [18].

Definition 1 (Right-angled Artin groups)**.** Let Γ denote a finite simplicial graph. We will write $V = V(\Gamma)$ for the finite set of vertices and $E(\Gamma) \subset V \times V$ for the set of edges, viewed as unordered pairs of vertices. The requirement that Γ be simplicial simply means that the diagonal of $V \times V$ is excluded from the set of edges. The right-angled Artin group on Γ is the group

$$A(\Gamma) = \langle V | [v_i, v_j] = 1 \text{ whenever } (v_i, v_j) \in E \rangle. \tag{1}$$

In other words, $A(\Gamma)$ is generated by the vertices of Γ, and the only relations are given by commutation of adjacent vertices.

Observe that right-angled Artin groups, that are associated to a finite simplicial graph (the *Artin graph*), are always finitely presented. It is clear from the definition that there is a bijective correspondence between isomorphism types of right-angled Artin groups and isomorphism types of finite simplicial graphs, in the sense that two right-angled Artin groups $A(\Gamma)$ and $A(\Lambda)$ are isomorphic if and only if $\Gamma = \Lambda$. Moreover, a map $f : A_1 \to A_2$ of right-angled Artin groups is a homomorphism if and only if it induces a graph homomorphism between the corresponding graphs.

We will be specially interested in the subgroups generated by subsets of the set S of generators. If $T \subset S$ is such a subgroup of a right-angled Artin groups A, it is usually denoted by A_T and called a *special subgroup* of A. Note that every special subgroup of A gives rise to a subgraph of Γ_A, but the converse is not true. For example, if we consider the graph with vertices $\{v_0, v_1\}$ and edge $[v_0, v_1]$, which corresponds to the free abelian group in two generators, the 0-dimensional subgraph defined by the two vertices produces the free group in two generators, which is not a subgroup of $\mathbb{Z}^2$. It is easy to see that a subgraph Γ' of an Artin graph Γ defines a special subgroup of the corresponding right-angled Artin groups if and only if Γ' is a *full* subgraph of Γ.

Definition 2. A subgraph Γ' of a graph Γ is *full* if for every pair of vertices $\{v, w\}$ in Γ' such that $[v, w]$ is an edge in Γ, $[v, w]$ is an edge in Γ'.

The full subgraphs are also called spanning or induced. This condition is important in order to use these subgroups as a platform for authentication.

3 Secret sharing threshold schemes

Habeeb-Kahrobaei-Shpilrain have proposed a cryptosystem based on efficiency of the word problem [8], and we intend to use it with right-angled Artin groups. Let us describe the two schemes.

In the first protocol, which is an (n, n)-threshold scheme, the dealer distributes a k-column $C = [c_1, c_2, \ldots, c_k]^\top$ consisting of bits (0's and 1's), among n participants in such a way that the column can be reconstructed only when all participants combine their information. A set of generators $X = \{x_1, \ldots, x_m\}$ is public. Then:

1. The dealer uses a secure channel to assign to each participant P_j a set of commutators R_j of the generators in $X^{\pm}$. Recall that each right-angled Artin group $G_j = \langle x_1, \ldots, x_m | R_j \rangle$ has efficiently solvable word problem (see Sec. 5.1 below).

2. The secret bit column C is split by the dealer in a mod 2 sum $\sum_{j=1}^{n} C_j$ on n bit columns, which are the secret shares to be distributed to the n participants. The i-th entry of C_j will be denoted by c_{ij}.

3. Words $w_{1j}, \ldots, w_{kj}$ in the generators of X are openly distributed by the dealer to the participant P_j, for every $1 \leq j \leq n$. The words are selected in such a way that $w_{ij} \neq 1$ if $c_{ij} = 0$ and $w_{ij} = 1$ if $c_{ij} = 1$.

4. Each participant P_j check, for each i, if the word w_{ij} in the right-angled Artin group G_j is trivial or not. Then, each participant can make the column $C_j = [c_{1j}, c_{2j}, \ldots, c_{kj}]^\top$, whose entries are 0's and 1's.

5. The secret can be now reconstructed by forming the vector sum $\sum_{j=1}^{n} C_j$, again with the sum taken mod 2.

The second protocol is a (t, n)-threshold scheme, and a modification of the previous one that takes into account some ideas from [13], and allows a subset of size t of the total number of participants n to reconstruct all the information. Now the secret is an element $x \in \mathbb{Z}_p$, and the dealer chooses a polynomial f of degree $t-1$ such that $f(0) = x$. In addition the dealer determines integers $y_i = f(i) \mod p$ that are distributed to participants P_i, $1 \leq i \leq n$ (we assume that all integers x and y_i can be written as k-bit columns). A set of group generators $\{x_1, \ldots, x_m\}$ is public.

1. A set of commutators R_j of the generators in X is secretly distributed to the participants by the dealer. The group $G_j = \langle x_1, \ldots, x_m | R_j \rangle$ is a right-angled Artin group, and hence it has an efficiently solvable word problem.

2. Now k-columns $b_j = [b_{1j}, b_{2j}, \ldots, b_{kj}]^\top$, with $1 \leq j \leq n$, are openly distributed by the dealer to each participant, being their entries words in the generators. The words b_{ij} are chosen in such a way that, after replacing them by bits (the bit '1' if b_{ij} is trivial in the right-angled Artin group G_j and '0' otherwise), the resulting column represents the integer y_i.

3. Now for each word b_{ij}, the participant P_j checks if this word is trivial or not in the right-angled group G_j, and in this way he/she obtains a binary representation of y_j.

4. Finally, every participant has a point $y_i = f(i)$ of the original polynomial, and then every set of t participants is able now to obtain f by polynomial interpolation, and also the secret number $x = f(0)$.

Note that every subset of t participants can recover the secret x by constructing the polynomial f via interpolation, and this scheme can be arranged in such a way that participants do not have to reveal their individual shares y_i to each other if they do not want to. More details of these protocols can be found in [8].

4 Authentication Schemes Based on the Group Homomorphism and the Subgroup Isomorphism problems

Grigoriev and Shpilrain have proposed in [14] some authentication protocols using graph homomorphisms problem and subgraph isomorphism problem. In the sequel, we introduce two different protocols, which are based on the group homomorphism and the subgroup isomorphism problems, and that we introduce using right-angled Artin groups as a platform. They are inspired by the work of these authors in the sense that they are originally (but not necessarily) addressed to be used with group graphs as a platform. In this sense, and as we will see below, we would make profit of unsolvability results for groups and also for graphs. We remark that we have developed no analogy of the protocol based in the classical Graph Isomorphism problem, as it has recently been shown by Babai [19] that its complexity is quasi-polynomial.

4.1 An Authentication scheme using Group Homomorphism problem

Consider two finitely presented groups $G_1 = \langle S_1|R_1\rangle$ and $G_2 = \langle S_2|R_2\rangle$, being S_i generators and R_i relations, $i = 1, 2$. The Group Homomorphism problem asks if there is a homomorphism $G_1 \to G_2$ that takes generators in S_1 to generators in S_2.

The authentication protocol is the following:

1. Alice's public key consists of two finitely presented groups $G_1 = \langle S_1|R_1\rangle$ and $G_2 = \langle S_2|R_2\rangle$. Alice's long term private key is a homomorphism α sending generators in S_1 to generators in S_2.

2. Alice selects another finitely presented group $G = \langle S|R\rangle$, and a homomorphism $\beta : G \to G_1$ which sends generators in S to generators in S_1. Then she sends $G = \langle S|R\rangle$ to Bob, and keeps the homomorphism β to herself.

3. Bob chooses a random bit and sends c to Alice:

   - When $c = 0$, Alice sends the homomorphism β to Bob, and Bob should check if $\beta(G) = G_1$, and if β is a homomorphism that takes generators in S to generators in S_1.
   - When $c = 1$, Alice sends the composite $\alpha\beta$ to Bob, and Bob checks whether $\alpha\beta(G) = G_2$, and if the composite is a homomorphism that takes generators in S to generators in S_2.

4.2 An Authentication Scheme Based on the Subgroup Isomorphism problem

The authentication protocol we propose is as follows:

1. Alice's public key consists of two isomorphic subgroups of a group Γ, G_1 and G_2. Alice's long-term private key is an isomorphism $\alpha : G_1 \to G_2$.

2. To begin authentication, Alice selects a group G together with the isomorphism $\beta : G \to G_1$ and sends the group G (the commitment) to Bob, while keeping β to herself.

3. Bob chooses a random bit c and sends it to Alice.

- If $c = 0$, then Alice sends the isomorphism β to Bob, and Bob checks whether $\beta(G) = G_1$ and whether β is an isomorphism.

- If $c = 1$, then Alice sends the composition $\alpha\beta = \beta(\alpha)$ to Bob, and Bob checks whether $\alpha\beta(G) = G_2$ and whether $\alpha\beta$ is an isomorphism.

5 Complexity and security

In this section we state the complexity results that make right-angled Artin groups a good platform for the previous protocols.

5.1 Word problem

To introduce a family of groups as a platform for the secret sharing scheme described [8] it is necessary that its word problem can be solved efficiently. In the mentioned paper, for example, the authors apply their cryptosystem for small cancellation groups. In the case of right-angled Artin groups, the easiness of the word problem was first proved in a paper by Liu-Wrathall-Zeger [20] which in a more general framework of free partially commutative monoids, describes an algorithm which is effective in linear polynomial time. More recently, Crisp-Goddelle-Wiest [21] have extended this result (with different methods) to some families of subgroups of right-angled Artin groups, as for example braid groups.

5.2 Security assumption, complexity analysis and platform groups (right-angled Artin groups)

The security of our proposed authentication schemes relies, for the first scheme, on the difficulty of the Graph Homomorphism problem, and for the second, on some Bridson unsolvability results. Let us analyze in detail both situations.

5.2.1 Group Homomorphism Problem and proposed authentication scheme:

We observe that the problem is equivalent to the Graph Homomorphism problem for graphs, as there is a bijection between right-angled Artin groups and finite simplicial graphs (see Sec. 2), and recall that this problem has been shown to remain NP-complete even when the graph in the right is a triangle [22]. Hence, it would be enough here to select two right-angled Artin groups Γ_1 and Γ_2 such that Γ_2 contains a free abelian group in three generators.

5.2.2 Subgroup Isomorphism Problem and proposed authentication scheme:

Martin Bridson has proved [23] that there exist families of right-angled Artin groups for which this problem is unsolvable, even for finitely presented subgroups. Let us briefly recall the construction. He starts with a free group in a finite number of generators, and performs over it Rips construction [24] in the specific version of Haglund and Wise ([25], Sec. 10). In this way we obtain an explicit presentation of a hyperbolic group Γ that possess a finite index subgroup $\Gamma_0 < \Gamma$, which is the fundamental group of a special cube complex. This complex is subject to certain restrictions ([25], Theorem 1.1), that give rise to the existence of a local isometry with a standard cube complex, and in particular imply the existence of an embedding of Γ_0 in the fundamental group of the latter, which is a right-angled Artin group and we call A. The group Γ_0 also projects onto a non-abelian free group, and the kernel is infinite and finitely-generated. Then, by a previous result of Bridson-Miller [26], the subgroup Isomorphism problem is unsolvable for every product $\Gamma_0 \times \Gamma_0 \times F$, being F any non-abelian free group. As $\Gamma_0 < A$, the problem is also unsolvable for $A \times A \times F$, and this is a right-angled Artin group itself, as it is the product of right-angled Artin groups.

In general, to compare the Subgroup Isomorphism problem and the Subgraph Isomorphism problem we need that the generators and relators on the groups can be represented as a graph. But this is only a necessary condition. For example, in right-angled Artin groups there are plenty

of subgroups that cannot be represented by a subgraph of the Artin graph (for example, the cyclic group generated by the product of two generators). An authentication scheme based in this problem for right-angled Artin groups only should make use of the special subgroups, and should take into account the fact that not every subgraph of the Artin graph represents a special subgroup. This approach is closer to the problem of subgroup isomorphism for full subgraphs of a finite graph, usually called the *induced Subgraph Isomorphism problem*, which is known to be NP-complete in general (see [27] for a reference). For the classical Subgroup Isomorphism problem, it is more straightforward to appeal to Bridson unsolvability results described above.

Acknowledgemnts We thank the referees for their comments and suggestions, which have improved the quality and readiness of this paper.

Delaram Kahrobaei is partially supported by a PSC-CUNY grant from the CUNY Research Foundation, the City Tech Foundation, and ONR (Office of Naval Research) grant N00014-15-1-2164. Part of the work was done while visiting the UPV/EHU in Bilbao funded by the ERC grant PCG-336983, especially we thanks Montse Casals for the fruitful discussions. Delaram Kahrobaei has also partially supported by an NSF travel grant CCF-1564968 to IHP in Paris. Ramón Flores is partially supported by MEC grant MTM2010-20692.

References

[1] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Non-commutative cryptography and complexity of group-theoretic problems*. American Mathematical Society, 2011.

[2] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J.-s. Kang, and Ch. Park. *New Public-Key Cryptosystem Using Braid Groups*, pages 166–183. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000. 10.1007/3-540-44598-6_10.

[3] B. Eick and D. Kahrobaei. Polycyclic groups: a new platform for cryptography, preprint arxiv: math.gr/0411077. Technical report, 2004.

[4] J. Gryak and D. Kahrobaei. The status of the polycyclic group-based cryptography: A survey and open problems. *Groups Complexity Cryptology, De Gruyter*, 8(2):171–186, 2016. 10.1515/gcc-2016-0013.

[5] V. Shpilrain and A. Ushakov. *Thompson's Group and Public Key Cryptography*, volume 3531, pages 151–163. Springer Berlin Heidelberg, 2005. 10.1007/11496137_11.

[6] I. Chatterji, D. Kahrobaei, and N. Lu. Cryptosystems using subgroup distortion. *arXiv:1610.07515v1.*

[7] V. Shpilrain and G. Zapata. Combinatorial Group Theory and Public Key Cryptography. *Applicable Algebra in Engineering, Communication and Computing*, 17(3):291–302, 2006. 10.1007/s00200-006-0006-9.

[8] M. Habeeb, D. Kahrobaei, and V. Shpilrain. A secret sharing scheme based on group presentations and the word problem. *Contemp. Math., Amer. Math. Soc.*, 582:143–150, 2012. 10.1090/conm/582/11557.

[9] D. Kahrobaei and V. Shpilrain. *Using Semidirect Product of (Semi)groups in Public Key Cryptography*, volume 9709, pages 132–141. Springer International Publishing, 2016. 10.1007/978-3-319-40189-8_14.

[10] G. Baumslag, B. Fine, and X. Xu. Cryptosystems using linear groups. *Applicable Algebra in Engineering, Communication and Computing*, 17(3):205–217, 2006. 10.1007/s00200-006-0003-z.

[11] G. Petrides. *Cryptanalysis of the Public Key Cryptosystem Based on the Word Problem on the Grigorchuk Groups*, volume 2898, pages 234–244. Springer Berlin Heidelberg, 2003. 10.1007/978-3-540-40974-8_19.

[12] D. Grigoriev and I. Ponomarenko. Homomorphic public-key cryptosystems and encrypting boolean circuits. *Applicable Algebra in Engineering, Communication and Computing*, 17(3):239–255, 2006. 10.1007/s00200-006-0005-x.

[13] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979. 10.1145/359168.359176.

[14] Dima Grigoriev and Vladimir Shpilrain. Authentication schemes from actions on graphs, groups, or rings. *Annals of Pure and Applied Logic*, 162(3):194–200, 2010. 0.1016/j.apal.2010.09.004.

[15] K. Hauschild and W. Rautenberg. Interpretierbarkeit in der gruppentheorie. *Algebra Universalis*, 1:136–151, 1971.

[16] T. Korbeda. Right-angled Artin groups and their subgroups. *Lecture notes Yale University*, pages 1–50, 2013.

[17] Ruth Charney. An introduction to right-angled Artin groups. *Geometriae Dedicata*, 125(1):141–158, 2007. 10.1007/s10711-007-9148-6.

[18] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial group theory.* Dover Publications, New York, 1976.

[19] László Babai. Graph isomorphism in quasipolynomial time. In *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, STOC '16, pages 684–697. ACM, 2016. 10.1145/2897518.2897542.

[20] Hai-Ning Liu, C. Wrathall, and Kenneth Zeger. Efficient solution of some problems in free partially commutative monoids. *Information and Computation*, 89(2):180 – 198, 1990. 10.1016/0890-5401(90)90010-F.

[21] J. Crisp, E. Godelle, and B. Wiest. The conjugacy problem in right-angled Artin groups and their subgroups. *Journal of topology*, 2(3):442–460, 2009. 10.1112/jtopol/jtp018.

[22] M. Garey and J. Johnson. *Computers and Intractability, A Guide to NP-Completeness.* W. H. Freeman, 1979.

[23] M. Bridson. Cube complexes, subgroups of mapping class groups, and nilpotent genus. *Geometric group theory, IAS/Park City Math. Ser.*, 21(21), 2014.

[24] E. Rips. Subgroups of small cancellation groups. *Bulletin of the London Mathematical Society*, 14(1):45–47, 1982. 10.1112/blms/14.1.45.

[25] F. Haglund and D. T. Wise. Special cube complexes. *Geometric and Functional Analysis*, 17(5):1551–1620, 2008. 10.1007/s00039-007-0629-4.

[26] Martin R. Bridson and Charles F. Miller. Recognition of subgroups of direct products of hyperbolic groups. *Proceedings of the American Mathematical Society*, 132(1):59–65, 2004.

[27] Shuji Kijima, Yota Otachi, Toshiki Saitoh, and Takeaki Uno. Subgraph isomorphism in graph classes. *Discrete Mathematics*, 312(21):3164–3173, 2012. 10.1016/j.disc.2012.07.010.