Reaction Attacks on Public Key Cryptosystems Based on the Word Problem

María Isabel González Vasco[†1]   Rainer Steinwandt[‡]

[†]Departamento de Matemáticas, Universidad de Oviedo,
c/Calvo Sotelo, s/n, 33007 Oviedo, Spain
mvasco@orion.ciencias.uniovi.es

[‡]Institut für Algorithmen und Kognitive Systeme,
Arbeitsgruppe Systemsicherheit, Prof. Dr. Th. Beth,
Universität Karlsruhe, 76128 Karlsruhe, Germany
steinwan@ira.uka.de

Abstract

Wagner and Magyarik outlined a general construction for public key cryptosystems based on the hardness of the word problem for finitely presented groups. At the same time, they gave a specific example of such a system. We prove that their approach is vulnerable to so-called reaction attacks, namely, it is possible to retrieve the private key just by watching the performance of a legitimate recipient.

1 Introduction

Since the dawning of public key cryptography there have been several attempts to use combinatorial group theory for constructing cryptographic tools. In particular, the evidenced hardness of the classical problems for finitely presented groups (the word problem and the conjugacy problem) has inspired many cryptographic constructions.

Recently, there have been several suggestions for deriving cryptographic primitives from the hardness of the conjugacy problem in braid groups [1, 2, 3, 5, 10]. The cryptanalytic results in [7, 9, 11] demonstrate that these schemes still need further exploration before they can represent a realistic potential alternative to the 'classical' number theoretical cryptosystems. Nevertheless,

[1]Work partially supported by the projects BFM2001-3239-C03-01, GE-EXP01-08

the cryptographic results obtained so far are indeed rather interesting and certainly deserve a closer exploration.

Unfortunately, most of the proposals based on the word problem in finitely presented groups are merely theoretical ([6, 13, 14]), though some have drawn a lot of attention from the cryptographic community (see, for instance, the public key schemes proposed by Yamamura [15, 16] and broken in [4, 12]).

In a seminal work [14] Wagner and Magyarik outlined a construction for a cryptosystem based on the word problem, and illustrated their proposal with a concrete suggestion for the choice of the system parameters.

In this contribution we present an attack on Wagner and Magyarik's scheme which doesn't transgress the hardness of the underlying word problem. The attack is in the spirit of [8] and shows that for any choice of the finitely presented group it is possible to recover the private key by observing the reaction of some legitimate recipient. This observation is modelled by means of an oracle $\mathcal{O}$ which recognizes 'properly ciphered' texts without giving further information about the corresponding plaintext. This setting is far less restrictive than that of a chosen ciphertext attack, in which the adversary selects the ciphertext and is then given the corresponding plaintext. In our model, the adversary chooses a certain bitstring and is only able to verify whether it actually is a valid ciphertext.

2 Wagner and Magyarik's cryptosystem

Let us recall some basic notions on finitely presented groups which will be necessary in the sequel. A group G is called *finitely presented* if it can be specified by means of finite sets of generators and relators, that is, if it has a finite presentation. Recall that a pair of sets (X, R), where R is a set of finite words in $X \cup X^{-1}$, is a *presentation* of a group G if G is a quotient of the free group on X by its normal subgroup generated by the set R. Note that the set of relators R defines an equivalence relation $(\sim)$ in the set $\{X \cup X^{-1}\}^*$, whose classes correspond with the group elements. The group law can be seen as juxtaposition of words.

Given a finitely presented group G, the *word problem* for G is the decision problem of determining whether a given word w is equivalent to the empty word (usually denoted by e), which represents the identity of the group. The fact that for several types of groups this problem is undecidable, gives us an idea of the incredibly complex objects finitely presented groups are. In this setting, Wagner and Magyarik introduce their general construction.

2.1 The general scheme

Let G be a group defined by the finite presentation (X, R), for which the word problem is hard to solve. Moreover, suppose S is a set of words in $\{X \cup X^{-1}\}^*$ such that for the quotient group $\widetilde{G}$, specified by the presentation $(X, R \cup S)$, there exists a polynomial time algorithm $\mathcal{A}$ for solving the word problem.

Let Σ be a finite alphabet and $W(\Sigma) = \{ w_\sigma \mid \sigma \in \Sigma \}$ a subset of $\{X \cup X^{-1}\}^*$ such that if $\sigma \neq \tau$, then w_σ and w_τ are neither equivalent over G nor over $\widetilde{G}$. For decrypting ciphertexts one should be able to decide whether a given word is equivalent in $\widetilde{G}$ to a certain $w_\sigma \in W(\Sigma)$. Thus, for most quotient groups of G with easy word problem all the words in $W(\Sigma)$ should be equivalent to the empty word.

While the presentation (X, R) and the set $W(\Sigma)$ are made public, the set S is kept secret. To encrypt an element $\sigma \in \Sigma$ we proceed as follows:

1. Set $w := w_\sigma$.

2. Rewrite w using the public relations specified by R.

3. The word w obtained from this rewriting process is the ciphertext.

To decrypt, a recipient runs the algorithm $\mathcal{A}$ with inputs $w{w_\sigma}^{-1}$ $(\sigma \in \Sigma)$.

2.2 A concrete proposal

In [14], the authors also propose a concrete method of constructing schemes based on the aforementioned idea. They suggest the choice of a group G given by a finite set of generators $X = \{x_1, \ldots, x_n\}$ subject to relations of three types:

(R1) $x_i x_j x_k x_l = x_l x_j x_k x_i \quad (x_i, x_j, x_k, x_l \in X \cup X^{-1})$

(R2) $x_i x_j x_k = x_k x_j x_i \quad (x_i, x_j, x_k \in X \cup X^{-1})$

(R3) $x_i x_j x_k = x_j x_k x_i \quad (x_i, x_j, x_k \in X \cup X^{-1})$

These relations can all be made trivial imposing a set of relations S of the types:

(S1) $x = e \quad (x \in X)$

(S2) $x_i = x_j \quad (x_i, x_j \in X \cup X^{-1})$

(S3) $x_i x_j = x_j x_i \quad (x_i, x_j \in X)$

Namely, by adding that set of relations S, we build a quotient group $\widetilde{G}$ which has a presentation formed by a subset of X and a set of commutativity relations. There is a polynomial time algorithm for solving the word problem for such a group, and thus for decrypting.

Now, the set of public words $W(\Sigma)$ is constructed in such a way that most sets of relations of the mentioned types which make the public relations trivial, also force that all words in $W(\Sigma)$ become equivalent to the empty word. The authors of [14] suggest that for that purpose, the designer of the cryptosystem may select a (small) set $\mathcal{P}$ of non-commuting pairs, such that in each quotient of G for which any pair in $\mathcal{P}$ commutes the words in $W(\Sigma)$ vanish to e, while if any other pair of generators commutes those words remain inequivalent.

3 The attack

For the sake of simplicity, let us suppose the alphabet Σ is binary and the public set $W(\Sigma)$ consists of two words, w_i , $i = 1, 0$ representing the corresponding bits. As an extra rather irrelevant assumption, we assume that not only the words w_0 and w_1 are inequivalent in G and $\widetilde{G}$, but also the strings $w_0 w_1$ and $w_1 w_0$ (e. g., this assumption is superfluous if the attacker is allowed to learn for valid chosen ciphertexts whether they decrypt to w_0 or w_1). As explained in the introduction, we also suppose having access to an oracle $\mathcal{O}$ such that given a word $w \in \{X \cup X^{-1}\}^*$, $\mathcal{O}(w) = 1$ if w corresponds to a correct ciphertext, (i. e., if $w \sim w_i$ for some $i \in \{0, 1\},$) and $\mathcal{O}(w) = 0$ otherwise.

Another assumption we make (which in particular is met by the concrete proposal of Wagner and Magyarik) is that we have at hand a set of words $A \in \{X \cup X^{-1}\}^*$ such that an exhaustive search over A is feasible. Moreover, from its subset

$$\bar{S} = \{a \in A \mid a \sim e \text{ in } \widetilde{G}\}$$

one can derive a set $\bar{\mathcal{S}}$ so that $(X, \bar{\mathcal{S}})$ is a presentation of $\widetilde{G}$ (or either of another quotient of G that also provides a valid private key—see [14, Section 4.2, Attack (b)]).

Our goal is to find $\bar{S}$ by making use of the oracle $\mathcal{O}$. This can be done by exhaustive search through A; namely, for each $a \in A$ we send ≤ 2 queries to the oracle $\mathcal{O}$ (resp. a legitimate recipient) to decide whether $a \in \bar{S}$:

i. aw_0:

- If $\mathcal{O}(aw_0) = 0$, then obviously $a \notin \bar{S}$.
- If $\mathcal{O}(aw_0) = 1$, then $a \in \bar{S}$ or in $\widetilde{G}$ we have $aw_0 \sim w_1$ (and hence $a \notin \bar{S}$). To distinguish these cases, a second query can be used:

ii. w_0a:

- If $\mathcal{O}(w_0a) = 0$, then obviously $a \notin \bar{S}$.
- If $\mathcal{O}(w_0a) = 1$, then $a \in \bar{S}$ or in $\widetilde{G}$ we have $w_0a \sim w_1$ (and hence $a \notin \bar{S}$). In the latter case ($a \notin \bar{S}$) we conclude that $w_0aw_0 \sim w_1w_0$. But from the previous query we know that the situation $a \notin \bar{S}$ occurs only if $aw_0 \sim w_1$, i. e., $w_0aw_0 \sim w_0w_1$—in contradiction to $w_0w_1 \not\sim w_1w_0$. In summary, the situation $\mathcal{O}(w_0a) = 1$ and $a \notin \bar{S}$ is impossible, and $\mathcal{O}(w_0a) = 1$ implies $a \in \bar{S}$.

Note that for concrete instances of the general Wagner and Magyarik scheme, there might be much more information at hand which can be used in order to improve the above explained attack. Let us illustrate how things could be done for the example described in Section 2.2:

In correspondence with the three types of relations (S1), (S2), and (S3) we apply the above procedure three times. First we look for relations of type (S1) by searching through the set

$$A_1 = X$$

(of size n). This yields a subset $\bar{S}_1$ of A_1 with words (actually generators) that vanish in $\widetilde{G}$, and we denote by $X_2 = X \setminus \bar{S}_1$ the set of remaining 'non-vanishing' generators. Next, we search through the set

$$A_2 = \{x_i x_j^{-1} \mid x_i \neq x_j \text{ and } x_i, x_j \in X_2 \cup X_2^{-1}\}$$

(of size $\mathrm{O}(n^2)$) to identify relations of type (S2). This yields another set $\bar{S}_2$ of words vanishing in $\widetilde{G}$, and when looking for relations of type (S3) we can restrict our attention to words in those generators which have not been identified as superfluous so far; we denote this subset of X_2 by X_3. Then the final exhaustive search covers the set

$$A_3 = \{x_i x_j x_i^{-1} x_j^{-1} \mid x_i \neq x_j \text{ and } x_i, x_j \in X_3\}$$

(of size $\mathrm{O}(n^2)$) and yields a set $\bar{S}_3$ of words vanishing in $\widetilde{G}$. Now the desired set $\bar{S}$ is given as $\bar{S} = \bar{S}_1 \cup \bar{S}_2 \cup \bar{S}_3$. Namely, $(X, R \cup \bar{S})$ is a presentation of the secret quotient $\widetilde{G}$ (where $G = (X, R)$).

4 Conclusion

We have given evidence of the effectiveness of reaction attacks against the general Wagner and Magyarik public key scheme, and thus against any of its particular instances. Although the underlying mathematical problem may be intractable, the above discussion shows that in the current state this design cannot be considered as a safe theoretical basis for deriving practical cryptosystems.

Reaction attacks were first presented by Hall, Goldberg, and Schneier [8], who succeeded in respectively decrypting ciphertexts and recovering the private key of the McEliece and Ajtai-Dwork cryptosystems. Our attack on Wagner and Magyarik's scheme is in a sense more powerful, as we access fewer information about the legitimate recipient's actions, i. e., we know nothing about the plaintext corresponding to correct ciphertexts. Nevertheless, the word problem in finitely presented groups remains an interesting candidate for deriving one way functions.

Acknowledgement. The authors are indebted to Consuelo Martínez for several helpful comments and discussions.

References

[1] Iris Anshel, Michael Anshel, Benji Fisher, and Dorian Goldfeld. New Key Agreement Protocols in Braid Group Cryptography. In David Naccache, editor, *"Topics in Cryptology — CT-RSA 2001"*, volume 2020 of *Lecture Notes in Computer Science*, pages 13–27. Springer, 2001.

[2] Iris Anshel, Michael Anshel, and Dorian Goldfeld. An Algebraic Method for Public-Key Cryptography. *Mathematical Research Letters*, 6:287–291, 1999.

[3] Iris Anshel, Michael M. Anshel, and Dorian Goldfeld. A Method and Apparatus for Cryptographically Secure Algebraic Key Establishment Protocols. International Application Published Under the Patent Cooperation Treaty (PCT). International Publication Number WO 99/44324, September 1999.

[4] Simon R. Blackburn and Steven Galbraith. Cryptanalysis of two cryptosystems based on group actions. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, *Advances in Cryptology — ASIACRYPT '99*, volume 1716 of *Lecture Notes in Computer Science*, pages 52–61. Springer, 1999.

[5] Eonkyung Lee and Sang Jin Lee and Sang Geun Hahn. Pseudorandomness from Braid Groups. In Joe Kilian, editor, *Advances in Cryptology — CRYPTO 2001*, volume 2139, pages 486–502. Springer, 2001.

[6] Max Garzon and Yechezkel Zalcstein. The Complexity of Grigorchuk groups with application to cryptography. *Theoretical Computer Science*, 88:83–98, 1991.

[7] Rosario Gennaro and Daniele Micciancio. Cryptanalysis of a Pseudorandom Generator Based on Braid Groups. In Lars Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 1–13. Springer, 2002.

[8] Chris Hall, Ian Goldberg, and Bruce Schneider. Reaction Attacks Against Several Public-Key Cryptosystems. In Vijay Varadharajan and Yi Mu, editors, *Information and Communication Security, Second International Conference, ICICS'99*, volume 1726 of *Lecture Notes in Computer Science*, pages 2–12. Springer, 1999.

[9] Jim Hughes. A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem. In Lynn Batten and Jennifer Seberry, editors, *Information Security and Privacy. 7th Australasian Conference, ACISP 2002*, volume 2384 of *Lecture Notes in Computer Science*, pages 176–189. Springer, 2002.

[10] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju sung Kang, and Choonsik Park. New Public-Key Cryptosystem Using Braid Groups. In Mihir Bellare, editor, *Advances in Cryptology — CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 166–183. Springer, 2000.

[11] Sang Jin Lee and Eonkyung Lee. Potential Weaknesses of the Commutator Key Agreement Protocol Based On Braid Groups. In Lars Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 14–28. Springer, 2002.

[12] Rainer Steinwandt. Loopholes in Two Public Key Cryptosystems Using the Modular Group. In Kwangjo Kim, editor, *Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001*, volume 1992 of *Lecture Notes in Computer Science*, pages 180–189. Springer, 2001.

[13] Neal R. Wagner. Searching for Public-Key Cryptosystems. In *Proceedings of the 1984 Symposium on Security and Privacy (SSP '84)*, pages 91–98, Los Angeles, Ca., USA, 1990. IEEE Computer Society Press.

[14] Neal R. Wagner and Marianne R. Magyarik. A Public Key Cryptosystem Based on the Word Problem. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology: Proceedings of CRYPTO 84*, volume 196 of *Lecture Notes in Computer Science*, pages 19–36. Springer, 1985.

[15] Akihiro Yamamura. Public-Key Cryptosystems Using the Modular Group. In Hideki Imai and Yuliang Zheng, editors, *Public Key Cryptography. First International Workshop on Practice and Theory in Public Key Cryptography, PKC'98*, volume 1431 of *Lecture Notes in Computer Science*, pages 203–216. Springer, 1998.

[16] Akihiro Yamamura. A Functional Cryptosystem Using a Group Action. In Josef Pieprzyk, Rei Savafi-Naini, and Jennifer Seberry, editors, *Information Security and Privacy. 4th Australasian Conference, ACISP'99*, volume 1587 of *Lecture Notes in Computer Science*, pages 314–325. Springer, 1999.