On the Legacy of Quantum Computation and Communication to Cryptography

X. Li, L. Leung, A. Kwan, X. Zhang, D. Kahanda, K. Tang, and M. Anshel

Department of Computer Science, Graduate Center of The City University of New York, 365 Fifth Avenue, New York, NY 10016, U.S.A

Abstract. We examine the legacy of quantum computation and communication to cryptography arising from a group-theoretic public-key establishment protocol, Anshel-Anshel-Goldfeld (AAG) protocol, which is of interest in connection to post-quantum cryptography. In the process we draw parallels with cryptography in the Age of the Enigma and contemporary quantum cryptographic research.

1 Introduction

Quantum computation and communication provide a growing legacy to the field of cryptography beginning with BB84 [1] and many algorithmic methods for objects appearing in the cryptographic domain. Study concerning asymmetric or public-key cryptosystems which can hope to withstand quantum cryptographic attacks is called post-quantum cryptography. Cryptographic systems which employ both public and private keys are called hybrid [2]. Those hybrid cryptographic systems which employ private keys created via quantum communication channels will be called quantum enabled. As an example one could use RSA together with a one-time pad created using BB84 to form a digital envelope for the plaintext message and transmit using that envelope via RSA. We are currently at work on such a quantum enabled hybrid system [3].
2 Quo Vadis Public-Key Cryptography

Two authorities [4] observe that it is a challenging task to develop public cryptosystems immune from quantum cryptographic attacks [5]. Thus far no one has found a quantum algorithm for the braid group cryptosystems based on the AAG protocol [6, 7], although there were many proposed conventional attacks [8] which concern the problem of random generation of secure keys.

3 AAG Key Establishment Protocol

A new direction in public-key cryptography has arisen from [6, 9] called braid-based cryptography in [8] and based on the theory of braids and braid groups [10]. In the Fall of 1999 following the publication of [6], an informal description of AAG protocol circulated on the Internet:

Two parties Alice and Bob publish, respectively words $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_m$ specifying group elements from a group $G = (S|D)$ with generating symbols $S$ and defining relations $D$. The common key $K$ is created by the following actions of Alice and Bob.

**Alice’s Actions:**

Alice transforms Bob’s public words in the following manner:

1. Alice selects a private word $X$ in the subgroup of $G$ generated by $a_1, a_2, \ldots, a_n$ and conjugates each $b_i$ by that $X$ producing $b_1^*, b_2^*, \ldots, b_m^*$

2. Alice selects a word $B_i$ in the generating symbols such that $B_i$ and $b_i^*$ define the same element of $G$ for $i = 1, \ldots, m$

3. Alice transmits to Bob $B_1, B_2, \ldots, B_m$

**Bob’s Actions:**

Bob transforms Alice’s public words in a similar manner:
1. Bob selects a private word \( Y \) in the subgroup of \( G \) generated by 
\[ b_1, b_2, \ldots, b_m \] and conjugates each \( a_i \) by that \( Y \) producing 
\[ a_1^*, a_2^*, \ldots, a_n^* \]

2. Bob selects a word \( A_i \) in the generating symbols such that \( A_i \) and \( a_i^* \) define the same element of \( G \) for \( i = 1, \ldots, n \)

3. Bob transmits to Alice \( A_1, A_2, \ldots, A_n \)

**Common Actions:**

4. Alice and Bob now compute, respectively \( V \) and \( W \) each of which specifies the commutator \( C = [X, Y] \) defined by the words \( X \) and \( Y \).

   Remark: This is accomplished by noting that since \( X \) and \( Y \) are words 
\[ X = x(a_1, \ldots, a_n) \] and \( Y = y(b_1, \ldots, b_m) \) then Alice computes 
a word \( V \) representing the commutator \( C = [X, Y] \) from 
\[ [X, Y] = X \ast (YXY^{-1})^{-1} = X \ast x(A_1, \ldots, A_n)^{-1} \] and Bob computes a word \( W \) representing the commutator \( C = [X, Y] \) from 
\[ [X, Y] = (XYX^{-1}) \ast Y^{-1} = y(B_1, \ldots, B_m) \ast Y^{-1}, \] where \( X^{-1} \) and \( Y^{-1} \) respectively denote 
the inverses of \( X \) and \( Y \).

5. Alice and Bob compute a common key \( K = F(V) = F(W) \) 
where \( F \) is a one-way hash function from the words in the generating 
symbols to words in the binary alphabet \( \{0, 1\} \) such that \( F(V) = F(W) \) 
whenever \( V \) and \( W \) define the same element of \( G \).

The AAG protocol above may be quantum enabled by using BB84 to create a one-time pad \( P \) for the key \( K \).

**The Braid Group Platform:**

By a *platform* for the protocol we mean a choice of group \( G \) to support 
both security and performance of a cryptographic system. One such 
group is the Artin Braid group \( B_n \) generated by \( \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \) and 
with two classes of defining relations:

\[ \sigma_i \sigma_j = \sigma_j \sigma_i, \quad |i - j| \geq 2 \quad \text{and} \quad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \quad 1 \leq i \leq n - 2 \] \( (1) \)
4 Beyond Braid-Based Cryptography

The platform most extensively explored in the literature employs the Artin Braid group $B_n$ on $n$ strands. Many researchers reject this platform believing that for fixed $n$ the subgroup-restricted conjugacy search problem is solvable in polynomial-time although computational evidence indicates that the degree of the polynomial bound grows with the number of strands $n$. We therefore propose to use the Dynnikov group as a platform, presented with the generators $a, b$ and three defining relations given by

$$[[a, b], a^2 ba^{-2}] = [[a, b], b^2 ab^{-2}] = [[a, b], [a^{-1}, b^{-1}]] = 1$$

(2)

where $[a, b] = aba^{-1}b^{-1}$, whose commutator subgroup is isomorphic to the braid group on infinitely many strands. Explicit information concerning this group may be found in [11].

*Can AAG running on the Dynnikov platform be secured against conventional and quantum cryptanalytic attacks by suitable choices of parameters and so satisfy the requirements of a post-quantum cryptographic protocol?*

A remarkable class of groups appears in [12] where the following theorem is proved: There exist finitely presented groups in which the conjugacy problem for elements is soluble, but the conjugacy problem for finite lists is not.

*Is there such a group as indicated in [12] suitable for use as a platform for AAG?*

5 Lessons from the Age of Enigma (1930-1950)

Recent work on group-theoretic equations underlying the Enigma highlight the issues faced by the Polish codebreakers [13]. The Polish story is told in part by two veterans of WWII [14].

The roots of the AAG protocol can be traced to the work of P. Hall (1933), E. Witt (1936) and E. Artin (1947) [15]. Both Hall and Witt were involved in cryptography during WWII. Interestingly the
lives of Hall and Witt were professionally connected with W. Magnus. Magnus later visited IBM shortly before the creation of the Data Encryption Standard (DES).

The uses of computation (digital and analogue) proved to be critical in breaking the Enigma and related ciphers of WWII allowing the Allied forces to prevail over the Axis forces. Finally we offer the reader the following challenge:

*Develop a quantum computational attack on the AAG protocol.*

References

[13] Lawrence J 2005 *Cryptologia* 29(3) 233-247