IET Information Security

Research Article

IET Journals
The Institution of Engineering and Technology

Non-quantum cryptanalysis of the noisy version of Aaronson–Christiano's quantum money scheme

ISSN 1751-8709
Received on 1st August 2017
Revised 14th June 2018
Accepted on 2nd November 2018
E-First on 1st March 2019
doi: 10.1049/iet-ifs.2018.5307
www.ietdl.org

Marta Conde Pena[1], Raul Durán Díaz[2], Jean-Charles Faugère[3,4,5], Luis Hernández Encinas[1] ✉, Ludovic Perret[3,4,5]

[1]*Instituto de Tecnologías Físicas y de la Información (ITEFI), Consejo Superior de Investigaciones Científicas (CSIC), C/ Serrano 144, 28006-Madrid, Spain*
[2]*Universidad de Alcalá, 28871-Alcalá de Henares, Spain*
[3]*Sorbonne Universités, UPMC Univ Paris 06, POLSYS, UMR 7606, LIP6, F-75005, Paris, France*
[4]*INRIA, Paris-Rocquencourt Center, POLSYS Project, 4, place Jussieu, LIP6, F-75252, Paris Cedex 05, France*
[5]*CNRS, UMR 7606, LIP6, F-75005, Paris, France*
✉ *E-mail: luis@iec.csic.es*

Abstract: At STOC 2012, Aaronson and Christiano proposed a noisy and a noiseless version of the first public-key quantum money scheme endowed with a security proof. This paper addresses the so-called *noisy hidden subspaces problem*, on which the noisy version of their scheme is based. The first contribution of this work is a non-quantum cryptanalysis of the above-mentioned noisy quantum money scheme extended to prime fields $\mathbb{F}$, with $|\mathbb{F}| \neq 2$, that runs in randomised polynomial time. This finding is supported with experimental results showing that, in practice, the algorithm presented is efficient and succeeds with overwhelming probability. The second contribution is a non-quantum randomised polynomial-time cryptanalysis of the noisy quantum money scheme over $\mathbb{F}_2$ succeeding with a certain probability for values of the noise lying within a certain range. This result disproves a conjecture made by Aaronson and Christiano about the non-existence of an algorithm that solves the noisy hidden subspaces problem over $\mathbb{F}_2$ and succeeds with such probability.

1 Introduction

The impossibility of creating cash that is theoretically impossible to forge seems to be an inherent limitation of money constructed under the laws of classical physics.

However, around 1980 Wiesner proposed to construct money taking advantage of the laws of quantum mechanics instead: the no-cloning theorem states that it is impossible to create identical copies of an unknown quantum state, so Wiesner thought of adding to the banknotes a certain number of photons polarised in secret directions only known by the bank [1]. As a consequence of the no-cloning theorem, the probability of a successful forgery decreases exponentially with the number of photons.

The idea of Wiesner brought hope to the possibility of *unforgeable* money, but it also presented several drawbacks, some of which have been corrected over time (e.g. the need for a huge database with information about the circulating banknotes in [2] or the fact that money can only be verified by the bank that issued it in [3, 4]). Nevertheless, most efforts in the field of quantum money today are put into a more ambitious aim: constructing quantum money that can be verified by anyone (note that this was not the approach of [3, 4]). This kind of quantum money is called public-key quantum money.

In a public-key quantum money scheme, anyone (and not only the issuing bank) endowed with the appropriate quantum device can verify whether a banknote is genuine. Aaronson gave in [5] the first formal treatment of public-key quantum money and he states that a public-key quantum money scheme must rely on a computational hardness assumption rather than on the uncloneability of quantum states alone. Some work has been done in the construction of public quantum money schemes so far: the first public-key quantum money scheme was proposed by Aaronson [5], and it was based on random stabiliser states (a certain type of quantum states), but it was broken in [6]. Depending on the parameters of the scheme, the break was achieved either using the verification circuit description to recover the secret information, or by generating states that were different from an intended money state but still passed the verification procedure with high probability. Later Farhi *et al.* [7] proposed a scheme based on knot theory, which has been followed up by the work of [8]. However, all these schemes present a common issue: they lack formal security proofs. Aaronson and Christiano are the first ones to propose a public-key quantum money scheme [9] and achieve a security proof assuming the hardness of a certain computational problem. This scheme of Aaronson and Christiano is the focus of this paper.

A high-level description of the base problem on which Aaronson and Christiano construct their scheme is as follows. Denoting by $\mathbb{F}$, a finite field of prime order and setting $\boldsymbol{x} = (x_1, \ldots, x_n)$, given a pair of m-tuples of polynomials $(\boldsymbol{p}, \boldsymbol{q}) = ((p_1, \ldots, p_m), (q_1, \ldots, q_m)) \in \mathbb{F}[\boldsymbol{x}]^m \times \mathbb{F}[\boldsymbol{x}]^m$, where the polynomial components of $\boldsymbol{p}$ vanish on an unknown subspace $A \subset \mathbb{F}^n$ and the polynomial components of $\boldsymbol{q}$ vanish on its orthogonal, $A^\perp$, all the components being of the same degree, d, the problem is to recover A (or $A^\perp$, indistinctly). They also propose a modification of the former problem by adding some noise to further disguise the subspaces. This new problem is the same as the previous one except that now some polynomials in $\mathbb{F}[\boldsymbol{x}]$ vanishing on subspaces other than A and $A^\perp$ are added as noise. These two problems, which the authors refer to as the *hidden subspaces problem* and the *noisy hidden subspaces problem,* respectively, are at the core of the noise-free and the noisy version of Aaronson–Christiano's scheme.

The hidden subspaces problem is similar to other problems used as a basis for multivariate cryptography, so it is reasonable to assume that it might be hard. However, provided that the choice of parameters is as specified by Aaronson and Christiano in [9], it is shown in [10] that the hidden subspaces problem is solved in polynomial time over $\mathbb{F}$ when its order is a large prime and in heuristic polynomial time over $\mathbb{F}_2$. The results of [10] heuristically break Aaronson–Christiano's scheme in its noise-free version and

invalidate the possibility of an extension of the noise-free version of the scheme to $\mathbb{F}$ for large prime orders of the base field $\mathbb{F}$, which was an open question. The noisy version of the scheme is not considered in [10], but it has recently been tackled in [11] (and reported on in [12]), where a break of the noisy scheme is achieved via a quantum reduction from the problem of breaking the noisy scheme to the problem of breaking the noiseless scheme, which was already solved in [10]. At this point, the authors want to stress out that, to the best of our knowledge, here, the authors are the first ones to reach significant results regarding the cryptanalysis of the noisy version of Aaronson–Christiano's scheme from a non-quantum perspective.

Contributions and outline. Here, the authors build upon the work of [10], now focusing on the noisy version of the scheme. As an extension of the results of [9, 10], the authors first show that there exists a randomised polynomial-time attack for the noisy version of Aaronson–Christiano's scheme extended to a field $\mathbb{F}$, with $|\mathbb{F}| > d$, where d is the degree of the instance $(\boldsymbol{p}, \boldsymbol{q})$ considered. This means that, analogously to what happens with the noise-free version, the noisy version of the scheme extended to a prime field of size different from 2 is not secure. The authors then support our theoretical findings by reporting experimental results which show that the attack is efficient and succeed with overwhelming probability in practice. Finally, the authors present an attack for the noisy version of Aaronson–Christiano's scheme over $\mathbb{F}$, with $|\mathbb{F}| = 2$, which happens to disprove a conjecture of Aaronson–Christiano in [9, Conjecture 32] – stating that no polynomial-time algorithm recovers A with a probability of success $\Omega(2^{-n/2})$, where n is the number of variables of the instance – for values of the noise within a certain range. The authors want to remark that our algorithms are the first non-quantum ones that achieve a break of the noisy scheme of Aaronson and Christiano.

The authors dedicate Section 2 to define the hidden subspaces problem and its noisy counterpart and the authors include preliminary results of [9, 10] that will be used or referred to. In Section 3, the authors develop our first main result: in Section 3.1, they present our cryptanalysis of the noisy hidden subspaces problem over $\mathbb{F}$ when $|\mathbb{F}| > d$ and in Section 3.2, they report experimental results that show the efficiency of the attack in practice. In Section 4, the authors describe our non-quantum polynomial-time cryptanalysis of the noisy hidden subspaces problem over $\mathbb{F}$, with $|\mathbb{F}| = 2$. In Section 5, the authors finish with the conclusions.

2 Preliminaries

The authors dedicate this section to fix some notation and to define precisely both the hidden subspaces problem over $\mathbb{F}$ (the $\mathrm{HSP}_{|\mathbb{F}|}$ for short) and the noisy hidden subspaces problem over $\mathbb{F}$ (the $\mathrm{NHSP}_{|\mathbb{F}|}$ for short), where $\mathbb{F}$ is a finite field of prime order. The authors also state some facts from [9, 10] that will be assumed or referred to in the rest of the paper.

Throughout this paper, $\mathbb{F}$ always denotes a finite field of prime order. The authors write $\boldsymbol{x} = (x_1, \ldots, x_n)$ and so they denote by $\mathbb{F}[\boldsymbol{x}]$ the polynomial ring in n variables over $\mathbb{F}$. The authors set $\gamma_{|\mathbb{F}|}(n)$ to be the probability that a $n \times n$ matrix over $\mathbb{F}$ is invertible. Finally, n always denotes an even integer and $(\boldsymbol{p}, \boldsymbol{q}) = ((p_1, \ldots, p_m), (q_1, \ldots, q_m)) \in \mathbb{F}[\boldsymbol{x}]^m \times \mathbb{F}[\boldsymbol{x}]^m$.

The authors start by defining the hidden subspaces problem:

Hidden Subspaces Problem ($\mathrm{HSP}_{|\mathbb{F}|}$)

Input: $p_1, \ldots, p_m, q_1, \ldots, q_m \in \mathbb{F}[\boldsymbol{x}]$ of degree $d \geq 3$, with $n \leq m \leq 2n$.

Find: a subspace $A \subset \mathbb{F}^n$ of dimension $n/2$ such that

$$p_i(A) = 0 \text{ and } q_i(A^{\perp}) = 0, \quad \forall i \in \{1, \ldots, m\},$$

where $A^{\perp}$ denotes the orthogonal complement of A with respect to the usual scalar product in $\mathbb{F}^n$.

The way the input polynomials for $\mathrm{HSP}_{|\mathbb{F}|}$ are chosen is specified by Aaronson and Christiano in [9]: once the degree d is fixed, each $p_i \in \mathbb{F}[\boldsymbol{x}]$ is chosen uniformly at random among the polynomials of degree d that vanish on A, and analogously each $q_i \in \mathbb{F}[\boldsymbol{x}]$ is chosen uniformly at random among the degree-d polynomials that vanish on $A^{\perp}$ (Lemma 28). From now on and unless otherwise said, a degree-d instance $(\boldsymbol{p}, \boldsymbol{q})$ of $\mathrm{HSP}_{|\mathbb{F}|}$ refers to one generated under these conditions.

Now the authors move on to define the noisy version of the hidden subspaces problem:

The Noisy Hidden Subspaces Problem (The $\mathrm{NHSP}_{|\mathbb{F}|}$)

Input: polynomials $p_1, \ldots, p_m, q_1, \ldots, q_m \in \mathbb{F}[\boldsymbol{x}]$ of degree $d \geq 3$, $m = \lceil \beta n \rceil$, where $\beta \geq 3/(1-2\varepsilon)^2$ and $0 < \varepsilon < 1/2$.

Find: a subspace $A \subset \mathbb{F}^n$ of dimension $n/2$ such that

$$p_i(A) = 0, \quad \forall i \in I_{\boldsymbol{p}} \text{ and } q_j(A^{\perp}) = 0, \quad \forall j \in I_{\boldsymbol{q}},$$

for some $I_{\boldsymbol{p}}, I_{\boldsymbol{q}} \subset \{1, \ldots, m\}$ with $\#I_{\boldsymbol{p}} = \#I_{\boldsymbol{q}} = \lceil (1-\varepsilon)m \rceil$, where $A^{\perp}$ denotes the orthogonal complement of A with respect to the standard scalar product in $\mathbb{F}^n$. In what follows, the authors say that a polynomial $p_i \in \boldsymbol{p}$ (resp. $q_i \in \boldsymbol{q}$) is non-noisy if $i \in I_{\boldsymbol{p}}$ (resp. $i \in I_{\boldsymbol{q}}$), and the authors say that it is noisy otherwise.

The way the input polynomials for the $\mathrm{NHSP}_{|\mathbb{F}|}$ are chosen is also given in [9]. For the non-noisy polynomials, the criterion is the same as for $\mathrm{HSP}_{|\mathbb{F}|}$, this is, if $i \in I_{\boldsymbol{p}}$, then p_i is chosen uniformly at random among the polynomials of degree d vanishing on A (analogously, if $i \in I_{\boldsymbol{q}}$, then q_i is chosen uniformly at random among the polynomials of degree d vanishing on $A^{\perp}$). The way to generate the noisy polynomials is as follows: if $i \notin I_{\boldsymbol{p}}$, then p_i is chosen uniformly at random among the polynomials of degree d that vanish on a random $n/2$-dimensional $A_i^{\boldsymbol{p}} \subset \mathbb{F}^n$. Analogously, if $i \notin I_{\boldsymbol{q}}$, then q_i is chosen uniformly at random among the polynomials that vanish on a random $n/2$-dimensional subspace $A_i^{\boldsymbol{q}} \subset \mathbb{F}^n$. Note that in the $\mathrm{NHSP}_{|\mathbb{F}|}$, there is no orthogonality relation between $A_i^{\boldsymbol{p}}$ and $A_i^{\boldsymbol{q}}$ and that $A_i^{\boldsymbol{p}}$ (respectively $A_i^{\boldsymbol{q}}$) is in principle different for each $i \in \{1, \ldots, m\} \backslash I_{\boldsymbol{p}}$ (respectively for each $i \in \{1, \ldots, m\} \backslash I_{\boldsymbol{q}}$). Unless it is otherwise stated, from now on a degree-d instance $(\boldsymbol{p}, \boldsymbol{q}) \in \mathbb{F}[\boldsymbol{x}]^m \times \mathbb{F}[\boldsymbol{x}]^m$ of the $\mathrm{NHSP}_{|\mathbb{F}|}$ is one satisfying these conditions.

Furthermore, to avoid overcomplicated notation later on, given an instance $(\boldsymbol{p}, \boldsymbol{q})$ of the $\mathrm{NHSP}_{|\mathbb{F}|}$, the authors define the weight of a vector $v \in \mathbb{F}^n$ with respect to $\boldsymbol{p}$, denoted by $w_{|\mathbb{F}|}^{\boldsymbol{p}}(v)$, as the cardinal of the set

$$W_v^{\boldsymbol{p}} = \{p_i : p_i(v) \neq 0\},$$

that is, $w_{|\mathbb{F}|}^{\boldsymbol{p}}(v) = \left|W_v^{\boldsymbol{p}}\right|$. The authors also define the set $Z_{|\mathbb{F}|}^{\boldsymbol{p}} \subset \mathbb{F}^n$ as

$$Z_{|\mathbb{F}|}^{\boldsymbol{p}} = \{v \in \mathbb{F}^n : w_{|\mathbb{F}|}^{\boldsymbol{p}}(v) < (|\mathbb{F}| - 1)\varepsilon\beta n\}.$$

Both of these definitions can be written analogously with respect to $\boldsymbol{q}$.

The authors finish this section recalling three results: the first one is a result from [9] that will be needed in section 3, the second one is the main theorem from [10] about the cryptanalysis of the HSP_2 and the third one states a conjecture made in [9] claiming that no polynomial-time algorithm could recover A with success probability $\Omega(2^{-n/2})$.

Lemma 1: ([9], Lemma 30): Let $(\boldsymbol{p}, \boldsymbol{q})$ be an instance of the NHSP_2. Then, $A \subseteq Z_2^{\boldsymbol{p}}$ and $\Pr[A = Z_2^{\boldsymbol{p}}] = 1 - 2^{-\Omega(n)}$, where $\Pr[\cdot]$ denotes the probability of an event and Ω refers to the standard big Ω asymptotic notation ([9], Lemma 30).

This result allows to test whether or not a given element in $\mathbb{F}^n$ belongs to A. Note too that Lemma 1 can be extended to a field $\mathbb{F}$ with $|\mathbb{F}| \neq 2$.

Theorem 1: (Theorem 4): There is a (heuristic) randomised polynomial-time algorithm solving HSP_2 with a complexity of

$$\mathcal{O}\left(n^{2\omega(d+1)}\right),$$

where $2 \leq \omega \leq 3$ is the linear algebra constant, and with success probability $\gamma_2(n/2)$, where $\gamma_2(k)$ denotes the probability that a random $k \times k$ matrix with entries in $\mathbb{F}_2$ is invertible ([10], Theorem 4).

Conjecture 1: ([9], Conjecture 32): Set $\varepsilon < 1/2$ and $\beta = 3/(1-2\varepsilon)^2$ and let $(\boldsymbol{p}, \boldsymbol{q}) \in \mathbb{F}_2[\boldsymbol{x}]^m \times \mathbb{F}_2[\boldsymbol{x}]^m$ be a degree d instance of the NHSP_2. Under these conditions, there is no polynomial-time quantum algorithm that can solve the NHSP_2 with success probability $\Omega(2^{-n/2})$ ([9], Conjecture 32).

3 $\mathrm{NHSP}_{|\mathbb{F}|}$ for $|\mathbb{F}| > d$

This section is dedicated to describe our first main contribution. In Section 3.1, the authors present our randomised polynomial-time cryptanalysis of the $\mathrm{NHSP}_{|\mathbb{F}|}$, with $|\mathbb{F}| > d$. In Section 3.2, the authors report experimental results showing that this algorithm is very efficient in practice and that its probability of success is overwhelming.

3.1 Cryptanalysis of the $\mathrm{NHSP}_{|\mathbb{F}|}$ for $|\mathbb{F}| > d$

The cryptanalysis of the $\mathrm{NHSP}_{|\mathbb{F}|}$ with the constraint $|\mathbb{F}| > d$ turns out to be an extension of the attack for degree- 1 instances of the NHSP_2 mentioned by Aaronson and Christiano in [9]. This extension is possible due to a key observation which authors state in Lemma 3. The attack mentioned in [9] for linear instances of the NHSP_2 is as follows:

Lemma 2: If $(\boldsymbol{p}, \boldsymbol{q}) \in \mathbb{F}_2[\boldsymbol{x}]^m \times \mathbb{F}_2[\boldsymbol{x}]^m$ is a degree 1 instance of the NHSP_2, there exists an attack that recovers A in randomised polynomial time ([9], Claim 35).

The attack makes use of the fact that if $(\boldsymbol{p}, \boldsymbol{q}) \in \mathbb{F}_2[\boldsymbol{x}]^m \times \mathbb{F}_2[\boldsymbol{x}]^m$ is a degree 1 instance of the NHSP_2, then it occurs that

$$q_i \text{ vanishes on } A^{\perp} \Leftrightarrow q_i(\boldsymbol{x}) = \lambda_i^{\boldsymbol{q}} \boldsymbol{x} \text{ for some } \lambda_i^{\boldsymbol{q}} \in A\,. \tag{1}$$

The analogous property holds for the components of $\boldsymbol{p}$, but for simplicity of exposition the authors assume that it is the characterisation (1) that the authors use. This property implies the existence of as many $\lambda_i^{\boldsymbol{q}} \in A$ as non-noisy polynomials vanishing on $A^{\perp}$ there exist, that is, $\lceil (1-\varepsilon)m \rceil$.

Since deciding if a given element of $\mathbb{F}_2^n$ belongs to A can be done efficiently by applying Lemma 1, the authors can recover $\mathcal{O}(\lceil (1-\varepsilon)m \rceil)$ elements of A. Now the authors can extract $n/2$ linearly independent elements from the $\mathcal{O}(\lceil (1-\varepsilon)m \rceil)$ recovered elements with a probability at least equal to the probability that a certain $\lceil (1-\varepsilon)m \rceil \times n/2$ has rank $n/2$, which according to the formula of Theorem 1.1 in [13], is

$$\frac{\gamma_2(\lceil (1-\varepsilon)m \rceil)}{\gamma_2(\lceil (1-\varepsilon)m \rceil - n/2)} = \prod_{i=\lceil (1-\varepsilon)m \rceil - n/2 + 1}^{\lceil (1-\varepsilon)m \rceil} \left(1 - \frac{1}{|\mathbb{F}|^i}\right).$$

The attack of Lemma 2 is formulated for $\mathbb{F}_2$, but it is clear that it can also be applied when the size of the field is different from two. In fact, the attack of Lemma 2 serves as a basis for the cryptanalysis of degree d instances of the $\mathrm{NHSP}_{|\mathbb{F}|}$ when $|\mathbb{F}| > d$ due to the following key observation (a similar idea was already used in [14]):

Lemma 3: For $|\mathbb{F}| > d$, any degree d instance $(\boldsymbol{p}, \boldsymbol{q}) \in \mathbb{F}[\boldsymbol{x}]^m \times \mathbb{F}[\boldsymbol{x}]^m$ of the $\mathrm{NHSP}_{|\mathbb{F}|}$ can be reduced to a degree 1 instance of the $\mathrm{NHSP}_{|\mathbb{F}|}$.

Input: polynomials $p_1, \ldots, p_m, q_1, \ldots, q_m \in \mathbb{F}[\mathbf{x}]$ of degree $d \geq 3$, $m = \lceil \beta n \rceil$, with $\beta \geq 3/(1-2\varepsilon)^2$, $0 < \varepsilon < 1/2$.
$E_A \leftarrow \emptyset$
for j=1 to m **do**
  $\omega \leftarrow w_{|\mathbb{F}|}^{\mathbf{p}}\left(\lambda_j^{\mathbf{q}}\right)$
  if $m - \omega \geq \lceil (1-\varepsilon) \rceil m$ **then**
    $E_A \leftarrow E_A \cup \{\lambda_j^{\mathbf{q}}\}$
  end if
end for
if $\dim(\mathrm{span}(E_A)) = n/2$ **then**
  $A \leftarrow \mathrm{span}(E_A)$.
  Return A.
else
  print "The algorithm fails"
end if

Fig. 1 *Algorithm to solve the* $\mathrm{NHSP}_{|\mathbb{F}|}$

Proof: Let $(\boldsymbol{p}, \boldsymbol{q}) \in \mathbb{F}[\boldsymbol{x}]^m \times \mathbb{F}[\boldsymbol{x}]^m$ be a degree d instance of the $\mathrm{NHSP}_{|\mathbb{F}|}$ and recall that A is a solution of that instance of the $\mathrm{NHSP}_{|\mathbb{F}|}$ if $p_i(A) = 0$ and $q_j(A^{\perp}) = 0$ for all $i \in I_{\boldsymbol{p}}, j \in I_{\boldsymbol{q}}$. Note now that any element of the subspace $A \subset \mathbb{F}^n$ can be written as $\boldsymbol{y}A$, where $\boldsymbol{y} = (y_1, \ldots, y_{n/2}) \in \mathbb{F}^{n/2}$ is a vector of formal variables and A is, abusing notation, a basis matrix of the subspace A.

Since for $i \in I_{\boldsymbol{p}}$, every polynomial p_i vanishes on $\boldsymbol{y}A$ and keeping in mind that $|\mathbb{F}| > d$, it must occur that all the coefficients of $p_i(\boldsymbol{y}A)$ are zero. In particular, it occurs that $p_i^{(1)}(\boldsymbol{y}A) = 0$ for all $i \in I_{\boldsymbol{p}}$.

An analogous argument can be used to infer that $q_i^{(1)}\left(\boldsymbol{y}A^{\perp}\right) = 0$ for all $i \in I_{\boldsymbol{q}}$, and so the authors can state that if A is a solution of the degree d instance $(\boldsymbol{p}, \boldsymbol{q})$ of the $\mathrm{NHSP}_{|\mathbb{F}|}$, then A is also a solution of the degree 1 instance $\left(\boldsymbol{p}^1, \boldsymbol{q}^1\right)$ of the $\mathrm{NHSP}_{|\mathbb{F}|}$. This way the authors conclude that the degree d instance $(\boldsymbol{p}, \boldsymbol{q}) \in \mathbb{F}[\boldsymbol{x}]^m \times \mathbb{F}[\boldsymbol{x}]^m$ of the $\mathrm{NHSP}_{|\mathbb{F}|}$ can be reduced to the degree 1 instance $\left(\boldsymbol{p}^{(1)}, \boldsymbol{q}^{(1)}\right)$ of the $\mathrm{NHSP}_{|\mathbb{F}|}$.

Furthermore, it is worth noting that the algorithm of the HSP_2 in [10] ensures that, whenever it succeeds, the solution of an instance of the HSP_2 has an unique solution. This implies that the solution of the degree 1 instance $\left(\boldsymbol{p}^{(1)}, \boldsymbol{q}^{(1)}\right)$ is necessarily A. □

The use of Lemmas 2 and 3 together allows us to obtain a cryptanalysis for degree d instances of the $\mathrm{NHSP}_{|\mathbb{F}|}$ when $|\mathbb{F}| > d$:

Theorem 2: There is a randomised polynomial-time algorithm that solves the $\mathrm{NHSP}_{|\mathbb{F}|}$ when $|\mathbb{F}| > d$ with complexity $\mathcal{O}(m^3(\log|\mathbb{F}|)^2)$ and probability of success at least

$$\frac{\gamma_{|\mathbb{F}|}(\lceil (1-\varepsilon)m \rceil)}{\gamma_{|\mathbb{F}|}(\lceil (1-\varepsilon)m \rceil - n/2)} \cdot \sum_{i=\lceil (1-\varepsilon)m \rceil}^{m} \binom{m}{i} \left(1 - \frac{1}{q^n}\right)^i \left(\frac{1}{q^n}\right)^{m-i}.$$

Proof: Let $(\boldsymbol{p}, \boldsymbol{q}) \in \mathbb{F}[\boldsymbol{x}]^m \times \mathbb{F}[\boldsymbol{x}]^m$ be a degree d instance of the $\mathrm{NHSP}_{|\mathbb{F}|}$ with $|\mathbb{F}| > d$. Denoting the linear parts of the components of $\boldsymbol{p}$ and $\boldsymbol{q}$ by

$$p_i^{(1)}(\boldsymbol{x}) = \lambda_i^{\boldsymbol{p}} \boldsymbol{x}, \quad q_i^{(1)}(\boldsymbol{x}) = \lambda_i^{\boldsymbol{q}} \boldsymbol{x}, \quad \forall i \in \{1, \ldots, m\},$$

where $\lambda_i^{\boldsymbol{p}}, \lambda_i^{\boldsymbol{q}} \in \mathbb{F}^n$, the algorithm showed in Fig. 1 solves the $\mathrm{NHSP}_{|\mathbb{F}|}$ as an application of both Lemmas 2 and 3.

The algorithm above succeeds if among the $\lceil (1-\varepsilon)m \rceil$ elements from E_A there are $n/2$ linearly independent ones, that is, if the corresponding $\lceil (1-\varepsilon)m \rceil \times n$ matrix has rank $n/2$. The probability that a $\lceil (1-\varepsilon)m \rceil \times n$ matrix has rank $n/2$ is greater than the probability that a certain $\lceil (1-\varepsilon)m \rceil \times n/2$ submatrix has rank $n/2$, which equals

Table 1 Performance of the cryptanalysis (Theorem 2) of the $\mathrm{NHSP}_{|\mathbb{F}|}$

Parameters	$d = 3, \varepsilon = 0.25, m = \lceil \beta n \rceil$							
field	$\lvert\mathbb{F}\rvert = 5$				$\lvert\mathbb{F}\rvert = 2^{16}+1$			
n	10	12	14	20	10	12	14	20
time (in sec.)	0.25	0.6	1.59	13.13	0.43	1.03	3.09	20.14

Table 2 Performance of the cryptanalysis (Theorem 2) of the $\mathrm{NHSP}_{|\mathbb{F}|}$

Parameters	$d = 4, \varepsilon = 0.25, m = \lceil \beta n \rceil$					
field	$\lvert\mathbb{F}\rvert = 5$			$\lvert\mathbb{F}\rvert = 2^{16}+1$		
n	10	12	14	10	12	14
time (in sec.)	1.28	4.41	11.32	2.54	7.85	17.96

$$\frac{\gamma_{|\mathbb{F}|}(\lceil (1-\varepsilon)m \rceil)}{\gamma_{|\mathbb{F}|}(\lceil (1-\varepsilon)m \rceil - n/2)},$$

following the formula in Theorem 1.1 of [13], which makes sense because the elements $\lambda_j^{\boldsymbol{q}}$ are random (recall that q_i is randomly selected).

However, the algorithm above works only for degree-d instances $(\boldsymbol{p}, \boldsymbol{q})$ of the $\mathrm{NHSP}_{|\mathbb{F}|}$ such that there are at least $\lceil (1-\varepsilon)m \rceil$ components of $\boldsymbol{q}$ with linear terms (so Lemma 2 can be applied). It can be easily seen that the probability of this event (which can be computed using the binomial distribution) equals:

$$\sum_{i=\lceil (1-\varepsilon)m \rceil}^{m} \binom{m}{i} \left(1-\frac{1}{q^n}\right)^i \left(\frac{1}{q^n}\right)^{m-i}.$$

Therefore, the overall success probability of the algorithm is

$$\frac{\gamma_{|\mathbb{F}|}(\lceil (1-\varepsilon)m \rceil)}{\gamma_{|\mathbb{F}|}(\lceil (1-\varepsilon)m \rceil - n/2)} \cdot \sum_{i=\lceil (1-\varepsilon)m \rceil}^{m} \binom{m}{i} \left(1-\frac{1}{|\mathbb{F}|^n}\right)^i \left(\frac{1}{|\mathbb{F}|^n}\right)^{m-i}.$$

Regarding the complexity, the computational cost of the loop that obtains ω is $\mathcal{O}(m^2 n(\log|\mathbb{F}|)^2)$. Computing a row echelon form to find $n/2$ linearly independent elements costs $\mathcal{O}(\lceil (1-\varepsilon)m \rceil^3)$, so the total complexity is the sum of both, which is $\mathcal{O}(m^3(\log|\mathbb{F}|)^2)$ as expected. □

This result means that there is a randomised polynomial-time algorithm solving the $\mathrm{NHSP}_{|\mathbb{F}|}$ when $|\mathbb{F}| > d$, with the choice of parameters given in [9]. However, it is worth mentioning that our attack could be avoided if a set of parameters other than the one proposed by the authors of [9] is used (e.g. considering homogeneous instances).

3.2 Experimental results

Here, the authors present experimental results (see Tables 1 and 2) to complete the theoretical result of our randomised polynomial-time algorithm of Theorem 2. The experiments show that the cryptanalysis of the noisy version of Aaronson–Christiano's scheme extended to a field $\mathbb{F}$ (with $|\mathbb{F}| > d$) is not only very efficient in practice but also succeeds with overwhelming probability.

All experiments were run on a 2.93 GHz Intel PC with 128 Gb of RAM with the Magma software [15] (V2.19-1). The Magma source code is available upon request.

Regarding the speed, we can see that the cryptanalysis is very fast and that an increase in the size of the field does not entail a significant decrease of the speed.

Regarding the probability of success, the first factor in the probability of success given in Theorem 2 with parameters $n = 10$, $d = 3$, and $\varepsilon = 0.25$ is

$$\frac{\gamma_{|\mathbb{F}|}(\lceil (1-0.25)120 \rceil)}{\gamma_{|\mathbb{F}|}(\lceil (1-0.25)120 \rceil - 5)} \simeq 0.9^{(58}\cdots 9303,$$

whereas the second factor amounts to

$$\sum_{i=90}^{1} 20\binom{120}{i}\left(1-\frac{1}{5^n}\right)^i\left(\frac{1}{5^n}\right)^{m-i} \simeq 0.9^{(895}\cdots 9897.$$

The probability of success – which is the probability of both factors – for those parameters is already overwhelming. Furthermore, both factors of the probability in Theorem 2 increase with n and $|\mathbb{F}|$, and so asymptotically speaking the situation only improves.

4 NHSP_2

Here, the authors show that there exists a randomised polynomial-time algorithm solving the NHSP_2 with success probability $\Omega(2^{-n/2})$ provided that the proportion of noise lies within a certain range. This demonstrates that Conjecture 1, precisely claiming the contrary, is false. Even more, the conjecture states that no such quantum algorithm exists and our algorithm solving the NHSP_2 is purely classical.

The algorithm that breaks Conjecture 1 combines both an exhaustive search and the algorithm solving HSP_2 from [10]. Given a degree-d instance of the NHSP_2 $(\boldsymbol{p}, \boldsymbol{q}) = ((p_1, \ldots, p_m), (q_1, \ldots, q_m)) \in \mathbb{F}_2[\boldsymbol{x}]^m \times \mathbb{F}_2[\boldsymbol{x}]^m$, where $\boldsymbol{x} = (x_1, \ldots, x_n)$, the intuitive idea of the algorithm is choosing n polynomials at random from $\boldsymbol{p}$ and hoping that they happen to be non-noisy. If they are, the algorithm for the HSP_2 of Theorem 1 can be applied (at this point we want to stress out that the heuristic randomised polynomial-time algorithm solving a degree-d instance $(\boldsymbol{p}, \boldsymbol{q}) \in \mathbb{F}_2[\boldsymbol{x}] \times \mathbb{F}_2[\boldsymbol{x}]$ of HSP_2 presented in [10] also works if $\boldsymbol{q}$ is not known). If the randomised algorithm for HSP_2 succeeds, the output is a solution for the NHSP_2, and if the algorithm for the HSP_2 fails, the authors repeat the process.

The following result approximates the probability that n polynomials chosen at random from $\boldsymbol{p}$ are non-noisy.

Lemma 4: Given a degree-d instance $(\boldsymbol{p}, \boldsymbol{q}) \in \mathbb{F}_2[\boldsymbol{x}]^m \times \mathbb{F}_2[\boldsymbol{x}]^m$ of the NHSP_2, the probability of choosing n polynomials from $\boldsymbol{p}$ (analogously from $\boldsymbol{q}$) that are non-noisy is given by the quotient

$$\frac{\binom{\lceil (1-\varepsilon)\beta n \rceil}{n}}{\binom{\lceil \beta n \rceil}{n}}.$$

The asymptotic expression of the above probability, which the authors denote by $P_n^{\varepsilon,\beta}$, is as follows:

$$P_n^{\varepsilon,\beta} = \left[\left(\frac{\beta-1}{\beta}\right)^{\beta-1} \cdot \left(1+\frac{1}{(\varepsilon-1)\beta}\right)^{(\varepsilon-1)\beta} \cdot \left(1-\varepsilon-\frac{1}{\beta}\right)\right]^n.$$

Proof: We rely on the following asymptotic approximation of a binomial coefficient,

$$\log_2\binom{b}{a} \simeq bH_2\left(\frac{a}{b}\right), \quad a,b \in \mathbb{N},$$

which derives from Stirling's approximation

$$\log n! \simeq n\log,$$

where

$$H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$$

is the binary entropy. By means of these approximations, we get the expression above. □

As the algorithm solving HSP_2 is randomised, we also need to take into consideration its probability of success to determine the probability of success of the algorithm. The following result sums it up.

Theorem 3: Given a degree-d instance $(\boldsymbol{p},\boldsymbol{q}) \in \mathbb{F}_2[\boldsymbol{x}]^m \times \mathbb{F}_2[\boldsymbol{x}]^m$ of the NHSP_2, the algorithm runs in polynomial time and succeeds with probability

$$\gamma_2(n/2) \cdot P_n^{\varepsilon,\beta}.$$

Proof: Choosing n random polynomials from $\boldsymbol{p}$ takes $\mathcal{O}(n)$ time, and so the running time of the algorithm is $\mathcal{O}(n)$ times the running time of the algorithm for HSP_2, which was polynomial (Theorem 1). Concerning the probability, on the one hand, the probability that the n randomly chosen polynomials are non-noisy is $P_n^{\varepsilon,\beta}$, and on the other hand, the algorithm for HSP_2 works with probability $\gamma_2(n/2)$. □

Finally, the authors prove that if the proportion of noise lies within a certain range, the algorithm succeeds with probability $\Omega(2^{-n/2})$.

Theorem 4: Let $\beta = 3/(1-2\varepsilon)^2$. Given a degree-$d$ instance $(\boldsymbol{p},\boldsymbol{q}) \in \mathbb{F}_2[\boldsymbol{x}]^m \times \mathbb{F}_2[\boldsymbol{x}]^m$ of the NHSP_2, the algorithm has an asymptotic probability of success

$$c_\varepsilon^{-n/2}, \quad \text{with } c_\varepsilon < 2,$$

for $\varepsilon \in (0, \varepsilon_\beta]$,

$$0.2836336067907370 < \varepsilon_\beta < 0.2836336067907371.$$

Proof: Once a proportion of noise ε is fixed, the expression $P_n^{\varepsilon,\beta}$ depends solely on n. Since the success probability of the algorithm is $\gamma_2(n/2) \cdot P_n^{\varepsilon,\beta}$ and considering that $\lim_{n\to\infty} \gamma_2(n/2) \simeq 0.288788$, the success probability of the algorithm is $\Omega(2^{-n/2})$ if and only if $P_n^{\varepsilon,\beta}$ is $\Omega(2^{-n/2})$, namely, if $P_n^{\varepsilon,\beta} > 2^{-n/2}$. Solving numerically the latter inequality, the authors obtain that this happens whenever $0 \le \varepsilon \le \varepsilon_\beta$, with $0.2836336067907370 < \varepsilon_\beta < 0.2836336067907371$.□

Remark 1: The success probability $\Omega(2^{-n/2})$ of our algorithm can be made any higher (e.g. $\Omega(2^{-n/3})$) at the expense of suitably reducing the width of the interval $(0, \varepsilon_\beta]$ within which such success probability is reached.

Remark 2: It is also easy to check that increasing (but fixed) values of β give increasing values of the ε_β boundary; this fact justifies the choice of β in the statement of Theorem 4.

In particular, this theorem implies that, for $\varepsilon \in (0, \varepsilon_\beta]$, there is a non-quantum polynomial-time algorithm for the NHSP_2 with a success probability that is, at least, $\Omega(2^{-n/2})$, thus contradicting the conjecture of Aaronson–Christiano on the noisy version of their scheme.

5 Conclusions

This work is concerned with the cryptanalysis of the noisy version of Aaronson–Christiano's public-key quantum money scheme from a non-quantum point of view. Our first contribution is an algorithm solving the $\mathrm{NHSP}_{|\mathbb{F}|}$ with the constraint $|\mathbb{F}| > d$, where d is the degree of the instance of the problem. Our second contribution is an algorithm solving the NHSP_2 that disproves the conjecture of Aaronson–Christiano for certain values of the noise.

Along the present paper, the authors have presented a non-quantum algorithm that solves the $\mathrm{NHSP}_{|\mathbb{F}|}$ in randomised polynomial-time when $|\mathbb{F}| > d$, thus achieving a total break of the noisy version of Aaronson–Christiano's scheme extended to fields under this requirement. They have also carried out several experiments (summarised in Tables 1 and 2), which clearly show that this algorithm is very efficient in practice and succeeds with overwhelming probability.

Finally, the authors have presented a non-quantum randomised polynomial-time algorithm that solves the NHSP_2 with probability $\Omega(2^{-n/2})$ for noise values within the interval $(0, \varepsilon_\beta]$ where

$$0.2836336067907370 < \varepsilon_\beta < 0.2836336067907371$$

in the worst-case scenario $\beta = 3/(1-2\varepsilon)^2$ and ε_β increases with an increase of β. This way the authors disprove a conjecture that Aaronson and Christiano made for the noisy version of their quantum money scheme [9, Conjecture 32].

To the best of our knowledge, this is the first work that focuses on Aaronson–Christiano's noisy scheme from a purely classical (as opposed to quantum) perspective and achieves significant results regarding its cryptanalysis.

6 Acknowledgment

This work has been partially supported by Ministerio de Economía, Industria y Competitividad (MINECO), Agencia Estatal de Investigación (AEI), and Fondo Europeo de Desarrollo Regional (FEDER, UE) under project COPCIS, reference TIN2017-84844-C2-1-R, and by Comunidad de Madrid (Spain) under project reference S2013/ICE-3095-CIBERDINE-CM, also co-funded by European Union FEDER funds.

7 References

[1] Wiesner, S.: 'Conjugate coding', *ACM SIGACT News*, 1983, **15**, (1), pp. 78–88

[2] Bennett, C.H., Brassard, G., Breidbard, S., *et al.*: 'Quantum cryptography, or unforgeable subway tokens'. Advances in Cryptology (CRYPTO 1982), 1982, pp. 267–275

[3] Gavinsky, D.: 'Quantum money with classical verification'. IEEE 27th Annual IEEE Conf. on Computational Complexity (CCC), 2012, pp. 42–52, Also published in arXiv:1109.0372v2

[4] Mosca, M., Stebila, D.: 'Quantum coins', *Error-Correcting Codes, Finite Geometry and Cryptography*, 2010, **523**, pp. 3–47

[5] Aaronson, S.: 'Quantum copy-protection and quantum money'. IEEE 24th Annual IEEE Conf. on Computational Complexity (CCC), 2009, pp. 229–242

[6] Lutomirski, A., Aaronson, S., Farhi, E., *et al.*: 'Breaking and making quantum money: toward a new quantum cryptography protocol'. Innovations in Computer Science (ICS), 2010, pp. 20–31

[7] Farhi, E., Gosset, D., Hassidim, A., *et al.*: 'Quantum money from knots'. Innovations in Theoretical Computer Science (ITCS), 2012, pp. 276–289

[8] Lutomirski, A.: 'Component mixers and a hardness result for counterfeiting quantum money', arXiv: 1107.0321, 2011

[9] Aaronson, S., Christiano, P.: 'Quantum money from hidden subspaces'. 44th Symp. on Theory of Computing Conf. (STOC), 2012, pp. 41–60

[10] Conde Pena, M., Faugère, J.-C., Perret, L.: 'Algebraic cryptanalysis of a quantum money scheme: the noise-free case'. 18th IACR Int. Conf. on Practice and Theory in Public-Key Cryptography (PKC), 2015, pp. 194–213

[11] Aaronson, S.: 'Public-key quantum money'. Lecture notes for the 28th McGill Invitational Workshop on Computational Complexity, 2016, pp. 81–88, Also published in arXiv:1607.05256

[12] Ben-David, S., Sattath, O.: 'Quantum tokens for digital signatures', IACR Cryptology ePrint Archive, 2017. Available at http://eprint.iacr.org/2017/094

[13] Brent, R.P., McKay, B.D.: 'Determinants and rank of random matrices over $\mathbb{Z}_m$', *Discrete Math.*., 1987, **66**, pp. 35–50

[14] Faugère, J.C., Perret, L.: 'Polynomial equivalence problems: algorithmic and theoretical aspects'. Advances in Cryptology (EUROCRYPT 2006), 2006, pp. 30–47

[15] Bosma, W., Cannon, J.J., Playoust, C.: 'The magma algebra system I: the user language', *J. Symb. Comput.*, 1997, **24**, (3–4), pp. 235–265