A Note on the Permutated Puzzles Toy Conjecture

Keller Blackwell∗ and Mary Wootters†

September 17, 2021

Abstract

In this note, we show that a “Toy Conjecture” made by (Boyle, Ishai, Pass, Wootters, 2017) is false, and propose a new one. Our attack does not falsify the full (“non-toy”) conjecture in that work, and it is our hope that this note will help further the analysis of that conjecture. Independently, (Boyle, Holmgren, Ma, Weiss, 2021) have obtained similar results.

1 Introduction

Recently, two independent works [BIPW17, CHR17] proposed a notion called oblivious locally decodable codes, (OLDCs), motivated by applications in private information retrieval (PIR). These works gave candidate constructions of OLDCs based on a new conjecture regarding the hardness of distinguishing a uniformly random set of points from a permutation of local-decoding queries in a Reed-Muller code. In order to encourage study of this conjecture, [BIPW17] proposed a simplified “Toy Conjecture,” which we reproduce below as Conjecture 1. In this note, we show that this Toy Conjecture is false, and propose a new one that is resistant to our attack. We note that this does not refute the full conjecture of [BIPW17, CHR17].

Independently of this note, Boyle, Holmgren, Ma and Weiss have also established that the Toy Conjecture is false [BHMW21], and have proposed a new Toy Conjecture.

2 The Toy Conjecture and an Attack

The Toy Conjecture of [BIPW17] is the following.

Conjecture 1 (Toy Conjecture 4.6 in [BIPW17]). Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = q \approx \lambda^2$. Let $p_1, \ldots, p_m$ be uniformly random polynomials of degree at most $\lambda$ in $\mathbb{F}[X]$, for $m = \lambda^{100}$. Let $q_1, \ldots, q_m$ be uniformly random functions from $\mathbb{F}$ to $\mathbb{F}$. Let $\pi \in S_{\mathbb{F} \times \mathbb{F}}$ be a uniformly random permutation. Then the following two distributions are computationally indistinguishable:

1. $(S_1, \ldots, S_m)$, where $S_i = \{ \pi(x, p_i(x)) : x \in \mathbb{F} \}$.
2. $(T_1, \ldots, T_m)$, where $T_i = \{ \pi(x, q_i(x)) : x \in \mathbb{F} \}$.

To show that this conjecture is false, we give below an efficient algorithm to distinguish the two distributions.

• Input: $(U_1, \ldots, U_m)$, where $U_i \subset \mathbb{F} \times \mathbb{F}$
• Construct that matrix $M \in \mathbb{F}^{m \times (\mathbb{F} \times \mathbb{F})}$ that is given by

$$M_{i, (\alpha, \beta)} = 1[(\alpha, \beta) \in U_i].$$

∗Stanford University. kellerb@stanford.edu
†Stanford University. marykw@stanford.edu
1The OLDC terminology is from [BIPW17]; in [CHR17], the corresponding notion is designated-client doubly-efficient PIR.
On the other hand, suppose that

First, observe that

Proof. To prove that this algorithm is correct, we will show that under distribution (2), the matrix $M$ has rank exactly $q^2 - q + 1$ with high probability; while under distribution (1), the matrix has rank strictly less than that.

Suppose that $f_1, \ldots, f_m$ are the functions that drawn (either $f_i = p_i$ in case (1), or $f_i = q_i$ in case (2)). Let $A \in \mathbb{F}^{m \times (F \times F)}$ be the matrix that is given by

$$A_{i,(\alpha,\beta)} = 1[f_i(\alpha) = \beta].$$

Notice that $M$ is a column permutation of $A$, so $\text{rank}(A) = \text{rank}(M)$. Thus, to show that the algorithm above is correct, it suffices to study the random of $A$ in cases (1) and (2). In the following, we let $A_i$ denote the $i$’th row of $A$.

Let

$$K = \left\{ v \in \mathbb{F}^{\mathbb{F} \times F} : v(\alpha,\beta) = w_\alpha \text{ for some } w_\alpha \in \mathbb{F} \text{ so that } \sum_{\alpha \in \mathbb{F}} w_\alpha = 0 \right\}.$$ 

Notice that $K$ is a subspace of $\mathbb{F}^{\mathbb{F} \times F}$ and that $\dim(K) = q - 1$.

Claim 1. Suppose that case (2) holds, so $f_i = q_i$ is a uniformly random function. Then $\text{Ker}(A) = K$ with probability at least $1 - \lambda^{-97}$ over the choice of the functions $f_i$.

Proof. First, observe that $K \subseteq \text{Ker}(A)$, since for any $i \in [m],$

$$\sum_{\alpha,\beta \in \mathbb{F}} A_{i,(\alpha,\beta)} v(\alpha,\beta) = \sum_{\alpha,\beta \in \mathbb{F}} 1[f_i(\alpha) = \beta] w_\alpha = \sum_{\alpha \in \mathbb{F}} w_\alpha = 0.$$

On the other hand, suppose that $v \notin K$. If $v(\alpha,\beta) = w_\alpha$ for some $w \in \mathbb{F}$ so that $\sum_{\alpha \in \mathbb{F}} w_\alpha \neq 0$, then clearly $v \notin \text{Ker}(A)$. So suppose that $v_{(a, b)} \neq v_{(a, b')}$ for some $a, b, b' \in \mathbb{F}$. Then let

$$X_i = \sum_{\alpha \neq a} \sum_{\beta \in \mathbb{F}} A_{i,(\alpha,\beta)} v(\alpha,\beta).$$

This is a random variable over the choice of $f_i$. Now, for any $i$, and for any $x \in \mathbb{F},$

$$\Pr\left[ A_i^T v = 0 \mid X_i = x \right] = \Pr\left[ \sum_{\beta \in \mathbb{F}} A_{i,(\alpha,\beta)} v(\alpha,\beta) = -x \right] = \Pr\left[ v_{(a, f_i(a))} = -x \right],$$

where again the probability is over the choice of $f_i$. Since $v_{(a, b)} \neq v_{(a, b')}$, there is at least a $1 - 1/q$ chance that $v_{a, f_i(a)} \neq -x$, if $f_i = q_i$ is a uniformly random function. Thus, for all $i \in [m]$ and for all $x \in \mathbb{F}_q,$

$$\Pr\left[ v_{(a, f_i(a))} \neq -x \right] \leq 1 - 1/q.$$ 

This implies that for all $i \in [m],$

$$\Pr\left[ A_i^T v = 0 \right] = \sum_{x \in \mathbb{F}} \Pr[X_i = x] \Pr[A_i^T v = 0 \mid X_i = x] \leq 1 - 1/q.$$
By the independence of the \( f_i \),
\[
\Pr[A_i^T v = 0 \forall i \in [m]] \leq (1 - 1/q)^m \leq e^{-m/q}.
\]
By the union bound over all \( v \) of this form,
\[
\Pr[\exists v \notin K, A_i^T v = 0 \forall i \in [m]] \leq q^m e^{-m/q} \leq q^m e^{-m/k} = e^{-λ97},
\]
using the choice of \( q \approx λ^2 \) and \( m = λ^{100} \).

This establishes that, in case (2), with probability at least \( e^{-λ97} \), \( A \) has rank
\[
\text{rank}(K) = q^2 - \dim(K) = q^2 - q + 1.
\]

On the other hand, in case (1), \( A \) has kernel vectors that are not in \( K \). One example is the vector \( v \in \mathbb{F}_2 \) given by \( v(α,β) = β \). To see that \( v \in \text{Ker}(A) \), when \( f_i = p_i \) is a polynomial of degree \( λ \leq q - 1 \), observe that
\[
A_i^T v = \sum_{α,β ∈ \mathbb{F}} 1[p_i(α) = β] · β = \sum_{α ∈ \mathbb{F}} p_i(α) = 0,
\]
where in the final equality we have used the fact that \( \sum_{α ∈ \mathbb{F}} α^c = 0 \) for any \( 0 ≤ c < q - 1 \).

This establishes that, in case (1), \( \text{Ker}(A) ⊊ K \), which implies that \( A \) has rank
\[
\text{rank}(K) = q^2 - \dim(K) < q^2 - q + 1.
\]

This shows that the algorithm above correctly distinguishes between cases (1) and (2), with probability at least \( 1 - e^{-λ97} \). \qed

### 3 A New Toy Conjecture

We note that the attack above does not work if the evaluation points for the \( f_i \) are a random subset resampled each time (which is indeed the case for the more general permuted puzzles conjecture of [BIPW17]). Thus, we propose the following replacement toy conjecture:

**Conjecture 2** (New Toy Conjecture). Let \( \mathbb{F} \) be a finite field with \( |\mathbb{F}| = q \approx λ^2 \). Let \( p_1, \ldots, p_m \) be uniformly random polynomials of degree at most \( λ \) in \( \mathbb{F}[X] \), for \( m = λ^{100} \). Let \( q_1, \ldots, q_m \) be uniformly random functions from \( \mathbb{F} \) to \( \mathbb{F} \). Let \( π ∈ S_{\mathbb{F}×\mathbb{F}} \) be a uniformly random permutation. Let \( Ω^{(1)}, \ldots, Ω^{(m)} \subset \mathbb{F} \) be independent uniformly random sets of size \( 100 · λ \). Then the following two distributions are computationally indistinguishable:

1. \((S_1, \ldots, S_m)\), where \( S_i = \{π(x, p_i(x)) : x ∈ Ω^{(i)}\} \).
2. \((T_1, \ldots, T_m)\), where \( T_i = \{π(x, q_i(x)) : x ∈ Ω^{(i)}\} \).

### Acknowledgements

We thank Elette Boyle, Justin Holmgren, Fermi Ma and Mor Weiss for helpful conversations and for pointing out typos in an earlier version of this note.
References

[BHMW21] Elette Boyle, Justin Holmgren, Fermi Ma, and Mor Weiss. On the security of doubly-efficient PIR, 2021.

[BIPW17] Elette Boyle, Yuval Ishai, Rafael Pass, and Mary Wootters. Can we access a database both locally and privately? In *Theory of Cryptography Conference*, pages 662–693. Springer, 2017.

[CHR17] Ran Canetti, Justin Holmgren, and Silas Richelson. Towards doubly efficient private information retrieval. In *Theory of Cryptography Conference*, pages 694–726. Springer, 2017.