CONJURA · OPEN PROBLEM

Average-Case Hardness of Planted k-Orthogonal Vectors

A planting that preserves every marginal below k, proposed as a basis for fine-grained cryptography

Status. Statement: AI-written from David Kühnemann, Adam Polak and Alon Rosen, *The Planted Orthogonal Vectors Problem*, IACR ePrint 2025/780. Not yet checked by a human. This is their Conjecture 10, and it is a *newly proposed* average-case assumption rather than a question the literature already asked — see Remark 1. Its worst-case counterpart, that k-OV requires $n^{k-o(1)}$ time, is a central conjecture of fine-grained complexity. The structural evidence the source supplies is that the planting preserves all marginals below k, and that search reduces to decision.

Category. *Fine-Grained Cryptography.*

Conjecture (informal). *Fine-grained complexity has a small stock of worst-case conjectures that most of its lower bounds rest on, and k-Orthogonal Vectors is one of them: given k sets of n binary vectors, pick one from each so that at every coordinate some vector is zero, and this is believed to need essentially n^k time. Cryptography needs average-case hardness, not worst-case, and it needs planted instances with a unique known solution. The source supplies a planting with an unusual property: look at fewer than k of the vectors and you cannot tell a planted instance from a purely random one, because the marginals agree exactly. The conjecture is that the planted instances are as hard as the worst case.*

1 The setting

In the k-Orthogonal Vectors problem one is given k sets, each containing n binary vectors of dimension $d = n^{o(1)}$, and must pick one vector from each set so that at each coordinate at least one of the chosen vectors has a zero. It is a central problem in fine-grained complexity, conjectured to require $n^{k-o(1)}$ time in the worst case, and a large body of conditional lower bounds rests on that

conjecture.

The source's motivation is stated plainly: "The security of cryptographic systems crucially relies on heuristic assumptions about average-case hardness of certain computational problems." The specific target is fine-grained asymmetric cryptography — "[a] key goal of fine-grained cryptography is to devise an advanced asymmetric cryptography scheme – such as public key encryption – whose security is based on hardness of a well understood problem from fine-grained complexity" — where the source records that the closest existing work is the key exchange protocol of LaVigne, Lincoln and Vassilevska Williams.

The contribution is a way to plant a solution among vectors with i.i.d. p-biased entries, for an appropriately chosen p, so that the planted solution is the unique one. What makes the planting worth studying is a structural property, stated in the source's abstract: "Our planted distribution has the property that any subset of strictly less than k vectors has the same marginal distribution as in the model distribution, consisting of i.i.d. p-biased random vectors."

2 Notation and parameters

- k is the number of sets; n the number of vectors in each; $d = n^{o(1)}$ the dimension.
- p is the bias: entries are i.i.d. p-biased, with p chosen so the planted solution is unique.
- $k\text{-OV}_0^\alpha(n)$ is the model distribution and $k\text{-OV}_1^\alpha(n)$ the planted one; $\alpha(n)$ parameterizes the family, and the conjecture is stated for $\alpha(n) = \omega(1)$.
- An algorithm *solves the decision* $k\text{-OV}^\alpha$ *problem with success probability* $\delta(n)$ if for both $b \in \{0,1\}$ and large enough n, $\Pr_{U \sim k\text{-OV}_b^\alpha(n)}[A(U) = b] \geq \delta(n)$.

3 The conjecture

Conjecture 1 ([KPR25, Conjecture 10]). *For any $\alpha(n) = \omega(1)$ and $\varepsilon > 0$, there exists no algorithm A that solves the planted decision k-OV problem with any constant success probability $\delta > \frac{1}{2}$ in time $O(n^{k-\varepsilon})$.*

Remark 1 (What kind of statement this is). It is an average-case hardness assumption the source is proposing, not a question the literature had already posed, and it is recorded here on that footing. Two features distinguish it from a security claim about a particular construction, which is why it is published rather than declined. First, the underlying object is canonical: k-OV is one of the handful of problems fine-grained complexity is organized around, and the worst-case conjecture it mirrors is widely studied. Second, the planting is principled rather than ad hoc, and the source proves things about it (Remarks 2 and 3) rather than only conjecturing. A reader should nonetheless treat it as an assumption awaiting cryptanalysis, and the absence of an attack after one paper is weak evidence.

Remark 2 (The marginal property, and what it does and does not give). Any subset of strictly fewer than k vectors has the same marginal distribution under the planted and model distributions. So no algorithm that inspects fewer than k vectors at a time can distinguish them at all — the planting is invisible below its own arity. That rules out a natural family of attacks outright, which is more than most freshly proposed assumptions come with. It does not rule out algorithms that look at k or more vectors, which is where any real attack would live, and it says nothing about the $n^{k-\varepsilon}$ running-time threshold.

Remark 3 (Search reduces to decision). The source's Theorem 12: for any $\alpha(n) = \mathrm{polylog}(n)$, if there is an algorithm solving the planted decision k-OV problem with success probability at least $1 - \delta(n)$ in time $T(n)$, then there is one solving the planted *search* problem with success probability at least $1 - (13k \cdot \delta(n) - n^{-k})$ in expected time $O(T(n) + n\,\mathrm{polylog}(n)\log(1/\delta(n)))$. The reduction is a binary search: split a set in two, resample one half, and use $(k-1)$-wise independence to argue the resampled instance follows the model distribution.

Note the parameter mismatch. The reduction is stated for $\alpha(n) = \mathrm{polylog}(n)$; Conjecture 1 is stated for $\alpha(n) = \omega(1)$, which is a weaker constraint. A resolution should say which regime of α it addresses.

Remark 4 (Where a refutation would live). In an algorithm exploiting the planting at arity exactly k. By Remark 2 nothing below that can help, so an attack must use the joint structure of k-

tuples — which is also what the honest solver does. The interesting question for a cryptanalyst is whether the uniqueness of the planted solution, which is what makes the problem useful, is itself a handle: unique-solution promises have historically made problems easier rather than harder.

Remark 5 (The worst-case conjecture is not this one). That k-OV requires $n^{k-o(1)}$ time in the worst case is a separate, older and much better studied conjecture, and it is not what Conjecture 1 asserts. Neither implies the other in any way the source claims: worst-case hardness does not give average-case hardness for this planting, and a refutation of Conjecture 1 would not touch the worst-case conjecture unless the algorithm happened to work on arbitrary instances.

4 Bibliography

[KPR25] David Kühnemann, Adam Polak and Alon Rosen. *The planted orthogonal vectors problem.* IACR ePrint 2025/780. The source. Definition 8 and the search formulation are on pages 10–11, Conjecture 10 on page 11, and the search-to-decision reduction (Theorem 12) on page 12.

[Wil05] Ryan Williams. *A new algorithm for optimal 2-constraint satisfaction and its implications.* Theoretical Computer Science, 2005. The origin of the Orthogonal Vectors conjecture in fine-grained complexity. [UNVERIFIED] — not cited under this name in the source's reference list as read during this harvest; the attribution here is inferred from the standard literature.

[LLW19] Rio LaVigne, Andrea Lincoln and Virginia Vassilevska Williams. *Public-key cryptography in the fine-grained setting.* CRYPTO 2019. The key exchange protocol the source names as the closest existing work toward fine-grained asymmetric cryptography. [UNVERIFIED] — cited in the source by number as [23]; the bibliographic detail here is inferred.