CONJURA · OPEN PROBLEM

Distance from Lines Is Resilient to Reduction Modulo a Random Prime

A function far from every line stays far modulo a uniform κ-bit prime

Status. Statement: AI-written from Jack Doerner, Iftach Haitner, Yuval Ishai and Nikolaos Makriyannis, *From OT to OLE with Subquadratic Communication*, IACR ePrint 2025/1722. Not yet checked by a human. Numbered Conjecture 5.37 of the source, described there as "a natural but apparently new number-theoretic conjecture" whose study "may be of independent interest". Nothing is proved about it; the source notes a deterministic variant "might be easier to prove". The direction of the difference in the source's Definition 5.36 is corrected here — see Remark 1.

Category. *Information-Theoretic Cryptography.*

Conjecture (informal). *Take a randomized function f on a large integer domain, and ask how close it is, on a chosen set of points, to some line $x \mapsto ax + b$ — measured as the fraction of points where the two disagree. Now reduce everything modulo a uniformly random κ-bit prime p and ask the same question again: how close is $f \bmod p$ to a line mod p? Reduction can only help the adversary, since values that differ over the integers can collide mod p. The conjecture is that it barely helps: for domains as large as $2^{c\kappa}$, the expected gain in closeness is at most $2^{-c'\kappa}$, exponentially small in the prime's bit length, uniformly over the worst choice of f and of the evaluation set. The source needs exactly this to drop an expensive integer-commitment subprotocol from its OLE protocol.*

1 The setting

Oblivious linear evaluation (OLE) over $\mathbb{Z}_q$ lets a receiver holding x learn $ax + b$ for a sender's line, and nothing else. The source reduces OLE to oblivious transfer with subquadratic communication, by combining the Chinese remainder theorem with Gilboa's protocol [Gil99] and then protecting the CRT-based construction against a malicious sender. Its main protocol pays for that protection

with a commit-and-prove functionality whose implementation is, in the source's words, "rather costly or requires additional hardness assumptions".

Its Section 5.3.5 removes that functionality. The resulting protocol (its Protocol 5.38) is the same protocol with the integer-commitment steps deleted, and its Theorem 5.39 shows this variant UC-realizes OLE_q with statistical security $2^{-\kappa_s} + \delta_{2\kappa_s,n}$, where δ is the quantity below. So the whole security loss from dropping commit-and-prove is that quantity, and the source's summary of the situation is: "The security of this variant reduces to a natural but apparently new number-theoretic conjecture (see Conjecture 5.37) whose study may be of independent interest."

The quantity itself is elementary. A cheating sender's behaviour is modelled by a randomized function f; the proof knows that f is far, in expected relative Hamming distance over a chosen set S, from every line $ax + b$ with $a, b \in \mathbb{N}$. What it needs is that f stays far from every line *after* reduction modulo a random κ-bit prime, because the protocol reveals residues rather than integers. Reduction is exactly what could destroy the guarantee: a sender's answers can disagree with every line over $\mathbb{Z}$ while agreeing with one modulo many primes.

The source states no partial result. It observes only that the deterministic variant — where the worst case is taken over deterministic f alone — "might be easier to prove", and remains useful: its Remark 5.40 records that this variant yields a slightly less efficient protocol which still beats the commit-and-prove one for not too large q. It also notes, separately from the conjecture, that a better analysis of cheating calls to its Wmult subprotocol could improve the protocol "regardless of whether Conjecture 5.37 holds or not".

2 Notation and parameters

- For $n \in \mathbb{N}$, $(n) := \{0, \ldots, n\}$, following the source's notation section.
- $\mathcal{P}_\kappa$ is the set of all κ-bit primes; $p \leftarrow \mathcal{P}_\kappa$ is uniform on it.
- For equal-length vectors u, v of length t over a common alphabet, $\mathrm{Ham}(u, v) := |\{i \in [t] : u_i \neq v_i\}|/t$ is the relative Hamming distance. (The source defines Ham for $u, v \in \{0,1\}^t$ and applies it to vectors over (n); the formula is the same.)

- For a randomized function f, randomness r and a finite set $\mathcal{S}$, $f(\mathcal{S};r)$ is the vector $(f(x;r))_{x\in\mathcal{S}}$ under a fixed ordering of $\mathcal{S}$, and $f_p(x;r) := f(x;r) \bmod p$.
- For $a,b \in \mathbb{N}$, $g^{a,b}(x) := ax + b$, and $g^{a,b}_p(x) := g^{a,b}(x) \bmod p$.
- κ is the prime's bit length; n bounds the domain.

3 The conjecture

Definition 1 (Distance from linear functions, after [DHIM25, Definition 5.36]). Fix $\kappa, n \in \mathbb{N}$, a set $\mathcal{S} \subseteq (n)$ and a randomized function $f : (n) \mapsto (n)$. Put

$$\alpha := \min_{a,b\in\mathbb{N}} \mathbb{E}_r\big[\mathrm{Ham}(f(\mathcal{S};r),\, g^{a,b}(\mathcal{S}))\big], \qquad \widehat{\alpha}_\kappa := \mathbb{E}_{p\leftarrow\mathcal{P}_\kappa}\Big[\min_{a,b\in\mathbb{N}} \mathbb{E}_r\big[\mathrm{Ham}(f_p($$

and

$$\delta_{\kappa,n} := \max_{\mathcal{S}\subseteq(n),f} \big(\alpha - \widehat{\alpha}_\kappa\big).$$

So α measures how far f is, in expectation, from being linear over $\mathcal{S}$; $\widehat{\alpha}_\kappa$ how far it is from being linear modulo a uniform κ-bit prime; and $\delta_{\kappa,n}$ the worst-case gap between the two.

Conjecture 1 (Distance from lines is resilient to modulo, [DHIM25, Conjecture 5.37]). *There exist $c_\delta, c_n > 0$ such that $\delta_{\kappa,n} \le 2^{-c_\delta\cdot\kappa}$ for all $\kappa \in \mathbb{N}$ and all $n \le 2^{c_n\cdot\kappa}$.*

Remark 1 (The direction of the difference, corrected). The source's Definition 5.36 prints $\delta_{\kappa,\ell} := \max_{\mathcal{S},f}\{\widehat{\alpha}_\kappa - \alpha\}$ — the difference in the opposite order to Definition 1 above. As printed, the quantity is never positive, so the conjecture is vacuous: for any fixed p and any fixed a,b, agreement over $\mathbb{Z}$ implies agreement modulo p, hence $\mathrm{Ham}(f_p(\mathcal{S};r), g^{a,b}_p(\mathcal{S})) \le \mathrm{Ham}(f(\mathcal{S};r), g^{a,b}(\mathcal{S}))$ pointwise in r; taking expectations and minimising over a,b (with a,b chosen after p, which only helps) gives $\widehat{\alpha}_\kappa \le \alpha$ for every $\mathcal{S}$ and f, so $\max_{\mathcal{S},f}\{\widehat{\alpha}_\kappa - \alpha\} \le 0 \le 2^{-c_\delta\kappa}$ trivially.

Definition 1 therefore takes $\alpha - \widehat{\alpha}_\kappa$, which is the direction the rest of the source needs and asserts. The title of Conjecture 5.37 is that distance from lines is *resilient* to modulo, i.e. that the mod-p distance

does not fall far below the integer distance; the source's own gloss is that "$\delta_{\kappa,n}$ is the distance between the two"; and its Theorem 5.39 uses δ as an additive security loss, which is only meaningful if δ measures how much closer to a line the sender's answers can look after reduction. With the order as printed, Theorem 5.39 would carry no content. Nothing else about the statement is changed.

The source also writes the second subscript as ℓ in Definition 5.36 while using n in Conjecture 5.37 and Theorem 5.39; the index is the domain parameter, written n throughout here.

Remark 2 (What a proof has to beat). Two features make the statement more than a counting exercise. First, the minimising line may be chosen *after* the prime is drawn, so the adversary gets a fresh best line per prime. Second, n is allowed to be exponential in κ, so the domain can be far larger than the modulus and each residue class can contain many domain points. A bound that holds only for $n \le \mathrm{poly}(\kappa)$, or only when a single line must work for all primes at once, does not settle Conjecture 1.

Remark 3 (The deterministic variant). The source records that the variant of Conjecture 1 in which the maximum in Definition 1 ranges only over deterministic f "might be easier to prove" and is "also useful": by its Remark 5.40 that variant yields a protocol needing more small primes, still preferable to the commit-and-prove protocol for not too large q. Settling the deterministic variant is therefore a genuine partial result on this statement, and should be reported as such rather than as a resolution.

Remark 4 (The parameters the source's protocol needs). Conjecture 1 is stated with unspecified constants, as in the source. For the application, the source needs it at $c_\delta = 1/2$ and $c_n = \log n/\kappa_s \le 4\log q + 25\kappa_s$; at those settings its Protocol 5.38 is as secure as the commit-and-prove Protocol 5.14 up to $2^{-\kappa_s}$. A proof with worse constants would settle the conjecture but not automatically the application.

4 Bibliography

[DHIM25] Jack Doerner, Iftach Haitner, Yuval Ishai and Nikolaos Makriyannis. *From OT to OLE with subquadratic communication.* IACR ePrint 2025/1722. The source. Definition 5.36 and Conjecture 5.37 are

on page 39 (PDF page 42); Theorem 5.39 and Remark 5.40 on page 40; the summary quoted in Section 1 is on page 3 (PDF page 6). The notation $(n) = \{0, \ldots, n\}$ and $\mathcal{P}_\kappa$ are in Section 3.1, page 10.

[Gil99] Niv Gilboa. *Two party RSA key generation.* Annual International Cryptology Conference (CRYPTO), 1999, pages 116–129. The protocol whose communication the source reduces from $O(\ell^2)$ to $\widetilde{O}(\ell)$ using the Chinese remainder theorem, and whose malicious-sender security is what forces the machinery around Conjecture 1.