CONJURA · OPEN PROBLEM

A Four-Party NIKE with Quadratic Security in Maurer's Generic Group Model

Generic groups without labels, where discrete-log shortcuts are unavailable

Status. Statement: AI-written from Abtin Afshar, Geoffroy Couteau, Mohammad Mahmoody and Elahe Sadeghi, *Fine-Grained Non-Interactive Key-Exchange: Constructions and Lower Bounds*, IACR Cryptology ePrint Archive 2023, not yet checked by a human. The analogous statement in Shoup's generic group model, where group elements carry explicit labels, is settled by the paper itself (Construction 9 and Theorem 10), while the statement below — the same quadratic gap in Maurer's label-free model, where the paper's own attack shows that quadratic is the most that could be hoped for — is open.

Category. *Idealized Models & Non-Uniformity.*

Conjecture (informal). *Maurer's generic group model is the austere one: a group element is an entry in a private array, and a party can only ask the array to add two entries or to test whether a linear combination of entries is zero. It never sees a bit-string representation of a group element. The source paper builds a four-party non-interactive key exchange in the more permissive model, where elements do have explicit labels, with honest parties doing about n units of work and every eavesdropper doing less than n^2 work left with vanishing advantage. That construction leans on labels in an essential way: after two parties find a partial collision, one of them recovers a missing half-exponent by running a square-root-time generic discrete-logarithm algorithm on the labels, which is not something a party in the label-free model can do. The same paper also proves that in the label-free model no protocol among three or more parties can resist an eavesdropper making $O(n^2)$ queries, so a quadratic gap is the ceiling there. The conjecture is that the ceiling is reachable: a four-party protocol exists in the label-free model with honest parties making about n queries and every eavesdropper making fewer than n^2 queries left with vanishing advantage.*

1 The setting

Merkle's puzzles [Mer78] give a two-party fine-grained key exchange from an idealized hash function: honest parties do n work, an eavesdropper needs about n^2. The source paper asks how far algebraic structure pushes this for more parties, and gets a sharper answer in the permissive generic group model than in the austere one. Its four-party protocol lives in Shoup's model [Sho97], where group elements carry explicit labels, and achieves a quadratic gap. Its lower bound lives in Maurer's model [Mau05], where a group element is an array entry accessible only through addition and zero tests, and shows that no protocol among three or more parties there can survive an eavesdropper making $O(n^2)$ queries. So in Maurer's model quadratic is a ceiling, and whether the ceiling is reachable is what the paper leaves open.

There is a specific reason the paper's own construction does not transfer. It works over a group of size about n^4, so that honest parties cannot hope for a full collision among their n sampled elements — only a *prefix* collision, in which two exponents agree on their first half. A party that knows the whole exponent and a party that knows only its first half then reconcile by having the second run a generic discrete-logarithm algorithm — baby-step giant-step [Sha71] or Pollard's rho [Pol75] — over the remaining interval of size about n^2, which costs only $O(n)$ because generic discrete logarithm over an interval runs in the square root of the search space. That step operates on explicit labels. In Maurer's model there are no labels for a party to sort, hash, or feed to such an algorithm; the paper states plainly that its model is more limited for the honest parties as well as for the adversary. A construction meeting this conjecture therefore has to find a different way to let honest parties exploit algebraic structure using only additions and zero tests — or the conjecture is false, and its refutation would be a genuinely stronger impossibility for Maurer's model than the $O(n^2)$ attack the paper already proves. Note that Maurer's model is not vacuous for key exchange: as the paper observes, the Diffie–Hellman protocol [DH76] can be stated in it.

2 Notation and parameters

Throughout, λ is the security parameter, $p = p(\lambda)$ is a prime, $\mathbb{Z}_p$ is the additive group of integers modulo p, and $[k] = \{1, \ldots, k\}$. A function is negligible, written $\mathrm{negl}(\lambda)$, if it is $\lambda^{-\omega(1)}$; $\tilde{O}(\cdot)$ hides polylogarithmic factors. The quantity $n = n(\lambda)$ is the query budget of each honest party and q that of the eavesdropper; queries are the only cost measure, and all algorithms are otherwise computationally unbounded. The protocol parameters γ, α, β count, respectively, the group elements each party broadcasts, and the Add and Zero queries each party makes after receiving the messages. Party i's private randomness is r_i, its broadcast string is m_i, its broadcast group elements are $\overline{\mathsf{q}}_i = (\mathsf{q}_{i,1}, \ldots, \mathsf{q}_{i,\gamma})$, and its output key is $\mathsf{key}_i \in \mathbb{Z}_p$; $\mathsf{tran} = (\mathsf{m}_1, \ldots, \mathsf{m}_4)$. The eavesdropper is E, its advantage is ρ, and the protocol is Π.

The parameters of the statement are:

- λ, the security parameter.
- n, the query budget of each honest party; the fine-grained cost measure.
- p, the prime order of the generic group.
- γ, the number of group elements each party broadcasts (copies into the others' arrays).
- α, the number of Add queries each party makes after receiving the messages.
- β, the number of Zero (zero-test) queries each party makes after receiving the messages.
- q, the query budget of the eavesdropper.
- ρ, the eavesdropper's advantage, measured above the $1/p$ guessing probability.

3 The conjecture

Definition 1 (Maurer's generic group model). Let p be a prime. Each participant P holds a private array $\mathsf{Arr}_{\mathsf{P}}$ with entries in $\mathbb{Z}_p$, initialized so that $\mathsf{Arr}_{\mathsf{P}}[1] = 1$ and every other index is empty; let e denote the largest non-empty index (so $e = 1$ initially). The participant accesses group elements only through the following queries:

- $\mathsf{Add}(i_1, i_2, c_1, c_2)$, with $i_1, i_2 \in [e]$ and $c_1, c_2 \in \mathbb{Z}_p$: writes $c_1 \cdot \mathsf{Arr}_{\mathsf{P}}[i_1] + c_2 \cdot \mathsf{Arr}_{\mathsf{P}}[i_2]$ at index $e + 1$ and increments e. No value is returned.
- $\mathsf{Equal}(i_1, i_2)$, with $i_1, i_2 \in [e]$: returns 1 if $\mathsf{Arr}_{\mathsf{P}}[i_1] = \mathsf{Arr}_{\mathsf{P}}[i_2]$ and 0 otherwise.
- $\mathsf{Zero}(c_1, \ldots, c_e)$, with $c_i \in \mathbb{Z}_p$: returns 1 if $\sum_{i \in [e]} c_i \cdot \mathsf{Arr}_{\mathsf{P}}[i] = 0$ and 0 otherwise.
- $\mathsf{Write}(x)$, for $x \in \mathbb{Z}_p$: writes x at index $e+1$ and increments e.

A participant never receives a representation of a group element: the only information it learns from its array is the answers to its Equal and Zero queries. The cost of a participant is its number of queries; local computation is free.

Definition 2 (Four-party NIKE in Maurer's generic group model). Fix parameters α, β, γ, publicly known and fixed in advance. Four parties $\mathsf{P}_1, \ldots, \mathsf{P}_4$ each receive 1^λ and p, sample private randomness r_i, and each hold a private array as above, all over the same $\mathbb{Z}_p$. The protocol has two rounds.

1. Party P_i interacts with its array, then simultaneously (i) broadcasts a string m_i and (ii) issues $\mathsf{copy}(\gamma)$, which appends the last γ entries $\overline{\mathsf{q}}_i = (\mathsf{q}_{i,1}, \ldots, \mathsf{q}_{i,\gamma})$ of $\mathsf{Arr}_{\mathsf{P}_i}$ to the end of every other party's array, in a fixed canonical order. Set $\mathsf{tran} := (\mathsf{m}_1, \ldots, \mathsf{m}_4)$.
2. Each party then makes exactly α further Add queries and

β further Zero queries to its own array, and designates one entry of its array as its key $\mathsf{key}_i \in \mathbb{Z}_p$.

The protocol has *completeness error* δ if

$$\Pr[\mathsf{key}_1 = \mathsf{key}_2 = \mathsf{key}_3 = \mathsf{key}_4] \geq 1 - \delta$$

over the parties' randomness.
The eavesdropper E receives tran and holds its own array containing 1 followed by the 4γ broadcast elements $(\overline{\mathsf{q}}_1, \ldots, \overline{\mathsf{q}}_4)$ in the canonical order; it may make its own Add, Equal and Zero queries. E *wins* if it outputs an index j of its array with $\mathsf{Arr}_{\mathsf{E}}[j] = \mathsf{key}_1$, and it has *advantage* ρ if it wins with probability at least $1/p + \rho$.

Conjecture 1 (Quadratic security for four-party NIKE in Maurer's model). *There exist a prime family $p = p(\lambda)$, a function $n = n(\lambda)$ with $n(\lambda) \to \infty$, parameters $\alpha, \beta, \gamma \leq \tilde{O}(n)$, and a four-party NIKE protocol Π in Maurer's generic group model over $\mathbb{Z}_p$ (Definitions 1 and 2) such that:*

1. ***Efficiency.*** *Each party makes at most $\tilde{O}(n(\lambda))$ queries to its array, across both rounds.*
2. ***Correctness.*** *Π has completeness error $\mathrm{negl}(\lambda)$, i.e. $\Pr[\mathsf{key}_1 = \mathsf{key}_2 = \mathsf{key}_3 = \mathsf{key}_4] \geq 1 - \mathrm{negl}(\lambda)$.*
3. ***Quadratic security.*** *For every function q with $q(n) = o(n^2)$, every computationally unbounded eavesdropper E making at most $q(n(\lambda))$ queries has advantage $\rho(\lambda) = o(1)$ as $\lambda \to \infty$.*

Remark 1 (What is settled). Nothing towards the construction. The paper builds the analogous protocol in Shoup's model (Construction 9) and proves (Theorem 10) that a q-query generic adversary outputs the right key with probability

$$O\left(q^2/\lambda^4 + q/\lambda^2 + \mathrm{polylog}(\lambda)/\lambda\right),$$

with honest parties running in time about λ; this is where the $o(1)$ advantage benchmark in Conjecture 1 comes from. On the other side, the paper's Theorem 21 and its corollary show that

any protocol meeting this conjecture would be optimal in Maurer's model, since an $O(n^2)$-query eavesdropper always exists there. The paper also observes that the Shoup-model construction generalizes to a $2K$-NIKE with a quadratic gap in the generic $(K-1)$-linear group model, giving a 6-NIKE in the generic bilinear group model; that generalization also uses labels.

Remark 2 (Openness). The paper names the construction as one of the two routes to closing its own gap: "We view as an interesting question the goal of closing the gap between our positive and negative results, either by building a 4-NIKE protocol with quadratic security in Maurer's generic group model, or by extending our impossibility result to Shoup's generic group model" (p. 3). The gap itself is stated plainly: "In our third contribution, we prove our lower bound in Maurer's generic group model, whereas our positive result holds in Shoup's generic group model, which is more flexible: this leaves a gap between our positive and negative results" (p. 3). Conjecture 1 is the first of those two routes. What is proved is the Shoup-model form: "In particular, we show that there is a 4-party NIKE in Shoup's generic group model with a quadratic gap between the number of queries by the honest parties vs. that of the adversary" (p. 1).

Remark 3 (Why it would matter). It is the constructive half of the paper's own gap, and the answer is informative either way. A protocol would show that the label-free generic group model is as powerful as the labelled one for fine-grained multiparty key exchange, which would be surprising given that the only known route to the quadratic gap runs through a square-root-time discrete-logarithm computation on labels: "known generic discrete logarithm algorithms actually run in time square root of the search space when the exponent search space is an interval. Therefore, the party can recover x using, e.g., Pollard's rho algorithm in $O(n)$ time" (p. 5). A proof that no such protocol exists would be a strictly stronger impossibility result for Maurer's model than the paper's own, separating the two generic group models for a natural primitive rather than for a contrived one. The whole statement is a protocol plus two query counts, unconditional and information-theoretic. Maurer's model is small enough to write down completely — four query types on an array, and "there are no explicit labels for the

group elements" (p. 1) — and the target parameters are already fixed by the paper's matching attack, so a candidate protocol either meets the quadratic gap or does not, with nothing to negotiate.

Remark 4 (Caveats for a reviewer). Three things to check. First, resolution: this is a 2023 ePrint and the papers citing it have not been checked; a follow-up may have built the protocol or ruled it out. Second, the formalization of "quadratic security": it is read here as advantage $o(1)$ against every $o(n^2)$-query eavesdropper, because that is exactly what the paper's own Shoup-model theorem delivers (its bound is dominated by a $\mathrm{polylog}(\lambda)/\lambda$ term and is not negligible). A reviewer who reads "quadratic security" as negligible advantage would be asking for something stronger than the paper achieves anywhere except the random oracle model, so it is not stated that way here. Third, party count: the paper says four parties and Conjecture 1 says four parties, even though three is the more interesting case; the paper's construction is inherently even-party, since it pairs parties up.

4 Bibliography

[BGI08] E. Biham, Y. J. Goren, and Y. Ishai. *Basing weak public-key cryptography on strong one-way functions.* TCC 2008, LNCS 4948, pages 55–72, Springer, 2008.

[DH76] W. Diffie and M. E. Hellman. *New directions in cryptography.* IEEE Transactions on Information Theory, 22(6):644–654, 1976.

[Mau05] U. M. Maurer. *Abstract models of computation in cryptography (invited paper).* 10th IMA International Conference on Cryptography and Coding, LNCS 3796, pages 1–12, Springer, 2005.

[Mer78] R. C. Merkle. *Secure communications over insecure channels.* Communications of the ACM, 21(4):294–299, 1978.

[Pol75] J. M. Pollard. *A Monte Carlo method for factorization.* BIT, 15:331–334, 1975.

[Sha71] D. Shanks. *Class number, a theory of factorization, and genera.* Proc. of Symp. Math. Soc., 1971, pages 41–440, 1971.

[Sho97] V. Shoup. *Lower bounds for discrete logarithms and related problems.* EUROCRYPT'97, LNCS 1233, pages 256–266, Springer, 1997.

[Zha22] M. Zhandry. *To label, or not to label (in generic groups).* CRYPTO'22, 2022.