Public Parameters as a First-Class Cost: A Three-Dimensional View of Updatable Vector Commitments, and a Group/Lattice Separation

Kefan Liu

Nanyang Technological University, Singapore

Abstract. Updatable vector commitments are judged by how a k-position update affects the broadcast update information S and the per-proof update time T; Tas and Boneh (AFT 2023) tightly characterize this (S, T) plane. We argue that a third quantity—the size $P = |\mathsf{pp}|$ of the public parameters—has been treated as free, yet it is exactly where group-based schemes pay for fast updates. We promote P to a first-class metric, place the standard dynamic VCs in the resulting three-dimensional (S, T, P) landscape, and prove a separation in the generic group model: every *linear* group-model VC with position-binding requires $P \geq N$, whereas the lattice homomorphic Merkle tree is simultaneously sublinear-update and pp-succinct. The separation rests on two simple lemmas—a reachable-set bound on what a proof-update can output, and an injectivity argument showing the per-update effect is k-dimensional—and explains, as a theorem, why the sublinear pairing construction is forced into gigabyte-scale parameters while its lattice sibling is not. Finally we show the P-axis is orthogonal, in both scope and realizable values, to the known lower bounds of Christ–Bonneau, Bonneau et al., and Camacho–Hevia.

Keywords: vector commitments · updatable commitments · public parameters · generic group model · lower bounds

1 Introduction

A vector commitment (VC) commits to a vector and later opens individual positions with short proofs. Where the vector is long-lived and frequently edited—stateless blockchains, verifiable databases—the *dynamic* costs dominate: after k positions change, how many bits of update information $S = |U|$ must be broadcast, and how long is each holder's proof-update T? Tas and Boneh [1] settled the (S, T) plane, with a tunable family achieving $S = \tilde{O}(k^{\nu})$, $T = \tilde{O}(k^{1-\nu})$ and a matching lower bound.

This two-dimensional accounting silently fixes a third axis: the public-parameter size $P = |\mathsf{pp}|$. The Tas–Boneh sublinear *pairing* construction buys its (S, T) profile with gigabyte-scale pp; their *lattice* construction keeps pp small but pays a 110 MB constant in S. P is never optimized or bounded. We ask: **what is the public-parameter cost of fast updates, and is the group-vs-lattice split fundamental?** We answer that in the generic group model it is: fast updates and succinct pp are incompatible for linear group commitments, and the lattice scheme escapes only by abandoning that structure.

Contributions.

E-mail: KEFAN001@e.ntu.edu.sg (Kefan Liu)

- *(Framework, Section 3)* We promote P to a first-class metric and place every standard dynamic VC—Merkle, Verkle, KZG, RSA/bilinear accumulators, both Tas–Boneh trees—in the 3D (S, T, P) landscape. A dichotomy is immediate: every group-based sublinear scheme is pp-large; the only pp-succinct sublinear scheme is lattice-based.
- *(Lemmas, Section 4)* In a generic-group model we prove (i) a *reachable-set* lemma: a T-step proof-update outputs only group elements spanned by the old proof, the broadcast U, and pp; and (ii) an *effect-dimension* lemma: as the update varies, the corrected proof's effect spans a k-dimensional space, via a clean injectivity argument.
- *(Separation, Section 4)* Any group-model *linear* VC with position-binding has $P_g \geq N$; the lattice homomorphic Merkle tree escapes precisely because its binding is not generator-independence. This turns the empirical group/lattice gap into a theorem.
- *(Orthogonality, Section 5)* Our axis (one-time setup size) is independent of the known dynamic-VC lower bounds of Christ–Bonneau [3] and Bonneau et al. [4, 5], which bound per-update broadcast or digest-vs-update-frequency, not setup size.

2 Model

Dynamic VC syntax. $(\mathsf{KeyGen}, \mathsf{Commit}, \mathsf{Open}, \mathsf{Verify}, \mathsf{Update}, \mathsf{ProofUpdate})$; $\mathsf{KeyGen}(1^\lambda, N) \to \mathsf{pp}$; Update for a k-position change outputs $(C', U, data')$; $\mathsf{ProofUpdate}$ refreshes one proof from U and the diffs. U excludes the public positions and diffs.

Security. Position-binding (standard; GGM form in Section 4.2). Hiding is scoped out (generically addable).

Three cost metrics. $P = |\mathsf{pp}|$ (one-time), $S = |U|$ (per k-update, excluding diffs), T (operations to refresh one proof).

Definitions. Succinct in x means $\mathrm{polylog}(x)$. A scheme has *sublinear update* if $S = o(k) \cdot \mathrm{poly}(\lambda)$ and $T = o(k)$. It is *pp-succinct* if $P = \mathrm{polylog}(N) \cdot \mathrm{poly}(\lambda)$, else *pp-large*.

3 The three-dimensional landscape

Table 1 places the standard schemes in (S, T, P). Asymptotics are in N and k; λ suppressed. "sublinear?" means both S, T are $o(k)$; "pp?" means succinct/large in N.

Table 1: The (S, T, P) landscape. Among sublinear rows, "pp?" splits along "assumption": pairing ⇒ large, SIS ⇒ succinct.

Scheme	S	T	P	sublinear? / pp?	setup	assumption
Merkle	$\tilde{\Theta}(k)$	$\tilde{O}(1)$	$\mathrm{polylog}(N)$	No / succ.	transparent	CRHF
Verkle	$\tilde{\Theta}(k)$	$\tilde{O}(1)$	$O(c)$	No / succ.	trusted	KZG
flat KZG (+table)	$\tilde{O}(1)$	$\tilde{\Theta}(k)$	$\Theta(N)$–$\Theta(N^2)$	No / large	trusted	pairing
RSA accumulator	$\tilde{O}(1)$	$\tilde{\Theta}(k)$	$\mathrm{poly}(\lambda)$	No / succ.	trusted	unknown-order
Bilinear accum.	$\tilde{O}(1)$	$\tilde{\Theta}(k)$	$\Theta(N)$	No / large	trusted	pairing
TB homom. tree	$\tilde{\Theta}(k^\nu)$	$\tilde{\Theta}(k^{1-\nu})$	$\Omega(N)$, GB	**Yes** / large	trusted	pairing
TB homom. Merkle	$\tilde{\Theta}(k^\nu)$	$\tilde{\Theta}(k^{1-\nu})$	$\mathrm{poly}(\lambda)\,\mathrm{polylog}(N)$	**Yes** / succ.	transparent	SIS

Among sublinear-update rows, "pp?" splits exactly along "assumption": pairing implies large, SIS implies succinct. Section 4 shows this is forced, not incidental: the linear-group structure the pairing scheme uses is exactly what makes its pp large, and the lattice scheme avoids it by not being a linear-group commitment.

4 Group model, lemmas, and the separation

4.1 The generic group model and formal-dlog framework

Fix a cyclic group $G = \langle g \rangle$ of prime order p (with a pairing where a scheme needs one). We use the generic group model in its standard formal-indeterminate form.

Setup randomness as indeterminates. KeyGen's secret randomness is a tuple of formal indeterminates $X = (X_1, \ldots, X_t)$ over $\mathbb{Z}_p$ (KZG: $t = 1$, $X = \tau$). Every group element e has $\delta(e) := \mathrm{dlog}_g(e) \in \mathbb{Z}_p(X)$; for the schemes we treat, $\delta(e) \in \mathbb{Z}_p[X]$.

Group-model VC. $\mathsf{pp}_{\mathrm{grp}} = (P_1, \ldots, P_{P_g}) \in G^{P_g}$, the commitment, all proofs, and all U_{grp} are group elements, and Commit/Open/Update/ProofUpdate touch group elements only via the group oracle (add, subtract, scalar-multiply by a known scalar, equality test).

No fresh encodings. These algorithms never introduce a group element whose $\delta(\cdot)$ involves a new indeterminate; equivalently every output group element has $\delta(\cdot) \in \mathrm{span}_{\mathbb{Z}_p}\{\delta(\text{inputs})\}$. (For VCs, proof maintenance is homomorphic recombination of existing material, never sampling of independent group elements.)

Dimension. For a finite set E of group elements, $\dim(E) := \dim_{\mathbb{Z}_p} \mathrm{span}_{\mathbb{Z}_p}\{\delta(e) : e \in E\} \subseteq \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p[X]$ is infinite-dimensional, N elements can be independent here even though their dlogs at a *fixed* instantiation $x \in \mathbb{Z}_p^t$ are scalars in $\mathbb{Z}_p$ (necessarily dependent for $N > 1$). All independence/dimension claims below are over $\mathbb{Z}_p[X]$. This is the point that makes "$P_g \geq N$" meaningful rather than vacuous.

Schwartz–Zippel bridge. For nonzero $f \in \mathbb{Z}_p[X]$ of total degree d and uniform $x \in \mathbb{Z}_p^t$, $\Pr[f(x) = 0] \leq d/p$. Used to pass between formal identities and identities at the sampled pp.

The model captures Verkle, KZG, bilinear/RSA accumulators, the Tas–Boneh pairing tree; it excludes the lattice homomorphic Merkle tree (binding from SIS, not the group oracle)—the intended boundary (Section 4.3).

4.2 Main separation theorem

A group-model VC is *linear* if $\mathsf{Commit}(m) = \sum_{l \in [N]} m_l \cdot G_l$ for fixed G_l. By no-fresh-encoding (take $m = e_l$), $G_l \in \mathrm{span}(\mathsf{pp}_{\mathrm{grp}})$, so $\gamma_l := \delta(G_l) \in \mathrm{span}_{\mathbb{Z}_p}\{\delta(P_1), \ldots, \delta(P_{P_g})\}$.

Position-binding (GGM form). For uniform secret x, no PPT adversary outputs $(i, \bar{m} \neq \bar{m}', \pi, \pi')$ with $\mathsf{Verify}(C, \bar{m}, i, \pi) = \mathsf{Verify}(C, \bar{m}', i, \pi') = 1$ for a common C, except with negligible probability.

Theorem 1. *A position-binding linear group-model VC has $\gamma_1, \ldots, \gamma_N$ linearly independent over $\mathbb{Z}_p$ in $\mathbb{Z}_p[X]$; hence $P_g \geq N$, and the scheme is pp-large.*

Proof. Suppose not: a nonzero $c \in \mathbb{Z}_p^N$ has $\sum_l c_l \gamma_l \equiv 0$ in $\mathbb{Z}_p[X]$. Then at *every* instantiation x, $\sum_l c_l G_l = 0_G$. Pick i with $c_i \neq 0$; for any m set $m' := m + c$, so $m_i \neq m'_i$ yet $\mathsf{Commit}(m) = \mathsf{Commit}(m') + \sum_l c_l G_l = \mathsf{Commit}(m')$ at every x. Honest openings give π, π' verifying m_i, m'_i at i against the *same* C—a position-binding collision succeeding with probability 1, contradicting binding. So $\{\gamma_l\}$ are formally independent; they span an N-dimensional subspace of $\mathbb{Z}_p[X]$ contained in $\mathrm{span}\{\delta(P_1), \ldots, \delta(P_{P_g})\}$ (dimension $\leq P_g$). Hence $P_g \geq N$. □

Consistency (converse direction). If $\{\gamma_l\}$ are formally independent, then for any fixed nonzero c, $\sum_l c_l\gamma_l$ is a nonzero polynomial, so $\sum_l c_l G_l = 0$ at the sampled pp only with probability $\leq \deg/p = \mathrm{negl}$; Commit is injective with high probability and binding is not generically broken. Thus binding $\iff$ formal independence of $\{\gamma_l\}$, pinning the bound exactly.

Remark 1. Theorem 1 is short—morally "a binding linear group commitment needs N independent generators, and generators live in pp." Its value is (i) being the group half of the separation (Section 4.3) and (ii) being invisible until pp is a first-class metric (Section 3). The finer technical content is Section 4.4.

4.3 The boundary: why the lattice witness escapes

The lattice homomorphic Merkle tree is not a linear group commitment in the sense of Section 4.2: its commitment is a tree of SIS-hash evaluations, not a fixed linear form $\sum m_l G_l$; its binding follows from SIS hardness, not generator-independence; its pp is a fixed SIS matrix pair reused across the tree ($\mathrm{poly}(\lambda)\cdot\mathrm{polylog}(N)$, transparent). Theorem 1 does not apply, consistent with the scheme being sublinear-update and pp-succinct.

Corollary 1. *Every pp-succinct sublinear-update VC lies outside the linear group model: it cannot be a position-binding linear group commitment. Escaping the $\Omega(N)$ public-parameter cost requires non-group (e.g. SIS/lattice) structure.*

This is the theorem-level explanation of the dichotomy in Section 3, and of why the Tas–Boneh pairing scheme is forced into $\Omega(N)$ (GB) parameters while its lattice sibling is not.

4.4 Reachable-set and effect-dimension lemmas

These refine "pp is large" into "exactly what a fast proof-update can produce," and are the tools for going beyond the linear class (Section 6).

Lemma 1 (reachable set)**.** *Consider one* $\mathsf{ProofUpdate}$ *making $\leq T$ group-oracle calls, with input group elements from the old proof π (q elements), U_{grp} (U_g), and $\mathsf{pp}_{\mathrm{grp}}$ (P_g); let B be this input set, $d = q + U_g + P_g$. Then every group element held—in particular every element of the output π'—has $\delta(\cdot) \in \mathrm{span}_{\mathbb{Z}_p}\{\delta(b) : b \in B\}$, and π' has $\leq q + T$ group elements.*

Proof. Maintain for each held element e a vector $r(e) \in \mathbb{Z}_p^d$ with $\delta(e) = \sum_{b\in B} r(e)_b \cdot \delta(b)$. Each input b starts with $r(b) = \chi_b$ (unit vector), valid by definition of B. A group-oracle call forms e from held e_1, e_2 and a known scalar s as $e_1 \pm e_2$ or $s \cdot e_1$; then $\delta(e)$ is the matching $\mathbb{Z}_p$-combination of $\delta(e_1), \delta(e_2)$, so set $r(e) := r(e_1) \pm r(e_2)$ or $s \cdot r(e_1) \in \mathbb{Z}_p^d$, preserving the invariant. Equality tests and bookkeeping (indices, diffs) create no group element and only steer control flow or choose scalars. By induction over the $\leq T$ calls every held group element, hence all of π', satisfies the invariant. Each call appends ≤ 1 new group element and π' may copy input proof elements, so $|\pi'| \leq q + T$. □

Definition 1 (C-binding verification)**.** A group-model linear VC has *C-binding verification* if its verification relation, as an equation in the commitment C with (m, i, π) fixed, has at most one solution C.

(KZG: $e(C \cdot g^{-m}, g) = e(\pi, g^{\tau - i})$ determines $e(C, g)$, hence C, as $e(\cdot, g)$ is injective; Verkle and the homomorphic tree hold level-by-level. We adopt it as a structural assumption, verified per scheme in Appendix A.)

Lemma 2. *Under C-binding verification, if one group element π verifies value m at position i against both C and $\tilde{C}$, then $C = \tilde{C}$.*

Proof. Both solve the same one-unknown verification equation, which has a unique solution. □

Lemma 3 (effect dimension)**.** *Let the VC be linear with C-binding verification. Fix i and $S \subseteq [N] \setminus \{i\}$, $|S| = k$. For $\delta \in \mathbb{Z}_p^S$ applied on S, write $C'(\delta) = C + \sum_{j\in S} \delta_j G_j$. Then: (a) the correct updated proof at i is $\pi_i'(\delta) = \pi_i + E(\delta)$ with $E(\delta) = \sum_{j\in S} \delta_j H_{i,j}$ linear in δ, $H_{i,j}$ depending only on i, j; (b) $\delta \mapsto E(\delta)$ is injective; (c) $\{\delta(E(\delta)) : \delta \in \mathbb{Z}_p^S\}$ spans a k-dimensional subspace of $\mathbb{Z}_p[X]$.*

Proof. (a) Since $i \notin S$, position i's value is unchanged, so $\pi_i'(\delta)$ verifies the same m_i at i against $C'(\delta)$. By C-binding verification the correct proof is a well-defined function of the commitment, and (verification being linear in (C, π) for a linear VC) an affine function of it; so π_i' is affine in $C'(\delta)$. As $C'(\delta) = C + \sum_j \delta_j G_j$ is affine in δ with $\pi_i'(0) = \pi_i$, we get $\pi_i'(\delta) = \pi_i + \sum_{j\in S} \delta_j H_{i,j}$, with $H_{i,j}$ the image of G_j under the linear proof map (independent of δ).

(b) If $E(\delta) = E(\delta')$ then $\pi_i'(\delta) = \pi_i'(\delta')$: one element verifies m_i at i against both $C'(\delta), C'(\delta')$. By Lemma 2, $C'(\delta) = C'(\delta')$, i.e. $\sum_{j\in S}(\delta_j - \delta_j')G_j = 0$ at the sampled pp. Theorem 1 restricted to S gives $\{\gamma_j\}_{j\in S}$ formally independent, so $\sum_{j\in S}(\delta_j - \delta_j')\gamma_j \equiv 0$ forces $\delta = \delta'$.

(c) A linear injection from $\mathbb{Z}_p^S$ (dimension k) has k-dimensional image, spanned by $\{\delta(H_{i,j})\}_{j\in S}$. □

These localize the cost of any fast update to Lemma 1's three pools and certify the per-update effect is genuinely k-dimensional—the backbone for the (S, T, P) trade-off (Section 6) and for non-linear schemes, where Theorem 1 fails but Lemmas 1–3 still constrain updates.

5 Orthogonality to known lower bounds

Our quantity is the one-time setup size $P = |\mathsf{pp}|$. The established lower bounds for dynamic/updatable VCs and accumulators each constrain a *different* resource. We make the independence precise in two senses—scope (Section 5.1) and realizable values (Section 5.2)—and conclude that P is a genuinely new axis.

5.1 Scope of each bound

Table 2: Each prior bound lives on the $\{S, T, D, F\}$ axes—per-update or per-commitment quantities. P is the only quantity fixed once, at KeyGen.

Lower bound	Resource constrained	In our axes	Bounds P?
Tas–Boneh [1]	update-info vs proof-update time	S vs T	No
Christ–Bonneau [3]	global state vs proof-update rate	state vs freq. F	No
Bonneau et al. [4, 5]	digest size vs proofs invalidated	D vs F	No
Camacho–Hevia [6]	bits to delete k elements ($\geq \Omega(k)$)	S (broadcast)	No
This work (Thm 1)	**setup parameter size**	P **($\geq N$)**	**Yes**

5.2 P moves independently of the bounded axes

Independence is witnessed by existing schemes sitting in opposite cells (Table 3).

- *Known bounds do not imply a P-bound.* Merkle and the RSA accumulator are pp-succinct dynamic VCs nonetheless subject to the per-update bounds above; hence

Table 3: Real schemes occupy opposite cells, so P and the bounded axes move independently.

Scheme	P	S	T	what it witnesses
Merkle	succinct	$\Theta(k)$	$\tilde{O}(1)$	large S bites, yet P succinct
KZG (+table)	$\Theta(N)$	$\tilde{O}(1)$	$\tilde{\Theta}(k)$	P large, yet S minimal
RSA accumulator	succinct	$\tilde{O}(1)$	$\tilde{\Theta}(k)$	small P and small S together
TB pairing tree	$\Omega(N)$	$\tilde{O}(k^{\nu})$	$\tilde{O}(k^{1-\nu})$	P large with sublinear S, T

those bounds are consistent with P succinct and cannot force P large. (Both are non-linear-group, so Theorem 1 does not apply—consistent.)

- *Theorem 1 is not implied by the known bounds.* KZG has $P = \Theta(N)$ while $S = \tilde{O}(1)$ is nowhere near any S-lower-bound regime, so large P is not a consequence of the $S/T/D/F$ bounds. Conversely Theorem 1 says nothing about S, T, D, F: KZG (P large, S tiny) and Merkle (P small, S large) lie on opposite diagonals.

5.3 Conclusion

P is orthogonal to prior bounds both in scope and in realizable values. Theorem 1 is the first lower bound on this axis for the linear group class, and Corollary 1 the first separation it exposes. In particular, the result is not a corollary of Christ–Bonneau, Bonneau et al., or Camacho–Hevia.

6 Discussion and open problems

Beyond linear commitments. Theorem 1 covers linear group commitments $C = \sum m_l G_l$, which is where every fast group-based scheme in Section 3 lives; but a non-linear group commitment could in principle evade the generator-counting argument. The natural route is a cross-user charge: fix a single-position update and count the dimension spanned by $\{H_{i,j}\}_i$, its effect on all other proofs. This dimension is $\Omega(N)$ for KZG (the rational functions $L_j(\tau)/(\tau - i)$ have distinct poles, hence are independent), yielding a $P_g + U_g + \Pi = \Omega(N)$ joint bound there; a model-level proof for all group commitments would push Theorem 1 past linearity. We leave it open.

The (T, P) trade-off. Large pp lowers not S but T: a precomputed dictionary of effect elements $\{H_{i,j}\}$—concretely KZG's $\Theta(N^2)$ table of Lagrange openings—lets a holder assemble $E_i(\delta)$ in few group operations, whereas succinct pp forces recomputation and hence larger T. Lemma 1 and Lemma 3 are exactly the tools to convert this into a quantitative (T, P) lower bound. Formalizing it is the most promising next step.

Closing the lattice gap. The lattice witness is pp-succinct and sublinear, but pays a large constant in S (110 MB). Whether this is necessary—whether a pp-succinct sublinear VC must pay in S regardless of assumption—would be a model-independent (S, P) statement complementing both our group-only result and the per-update (S, T) bound of Tas–Boneh. A positive answer would complete the three-dimensional picture; a pp-succinct sublinear scheme with small S would itself be a striking construction.

A C-binding verification, per scheme

Lemmas 2 and 3 assume C-binding verification (Definition 1): with (m, i, π) fixed, the verification relation has at most one solution C. We check it for the linear group schemes

of Section 3.

KZG. Verification is $e(C \cdot g^{-m}, g_2) = e(\pi, g_2^{\tau - i})$. The right side is fixed by (π, i); the left equals $e(C, g_2) \cdot e(g, g_2)^{-m}$. With m fixed this determines $e(C, g_2)$, and $e(\cdot, g_2) : G_1 \to G_T$ is injective (non-degenerate pairing, g_2 a generator), so C is unique.

Verkle. A Verkle commitment is a depth-d tree whose every node is a KZG commitment to its children. Verifying position i checks one KZG opening per level along the root-to-leaf path. By the KZG case each level's check pins that level's node value given the level below; inducting from the leaf up the path pins the root commitment C.

Homomorphic (AMT/Hyperproofs-style) tree. Verification is a pairing equation linear in C, of the form $e(C, A_i) \cdot e(\pi, B_i) = t_i$ with verification key $A_i \neq 1$. Fixing (m, i, π) fixes $e(\pi, B_i)$ and t_i, hence $e(C, A_i)$; non-degeneracy in the first argument (with $A_i \neq 1$) makes $C \mapsto e(C, A_i)$ injective, so C is unique.

In each case Open is deterministic and the correct proof is a linear function of C, so the affine dependence used in Lemma 3(a) holds.

References

[1] E. N. Tas and D. Boneh. Vector commitments with efficient updates. In *Advances in Financial Technologies (AFT)*, 2023. Cryptology ePrint Archive, Report 2023/1830.

[2] C. Papamanthou, E. Shi, R. Tamassia, and K. Yi. Streaming authenticated data structures. In *EUROCRYPT*, LNCS 7881, pages 353–370. Springer, 2013.

[3] M. Christ and J. Bonneau. Limits on revocable proof systems, with applications to stateless blockchains. In *Financial Cryptography (FC)*, 2023. Cryptology ePrint Archive, Report 2022/1478.

[4] J. Bonneau et al. Lower bounds on the update frequency of short accumulators and vector commitments. In *CRYPTO*, 2025.

[5] E. Giunta et al. Lower bounding the update frequency of short accumulators and vector commitments. Cryptology ePrint Archive, 2025.

[6] P. Camacho and A. Hevia. On the impossibility of batch update for cryptographic accumulators. In *LATINCRYPT*, LNCS 6212, pages 178–188. Springer, 2010.

[7] D. Catalano and D. Fiore. Vector commitments and their applications. In *Public-Key Cryptography (PKC)*, LNCS 7778, pages 55–72. Springer, 2013.

[8] A. Nitulescu. SoK: Vector commitments. Manuscript, Protocol Labs.

[9] A. Kate, G. M. Zaverucha, and I. Goldberg. Constant-size commitments to polynomials and their applications. In *ASIACRYPT*, LNCS 6477, pages 177–194. Springer, 2010.

[10] S. Srinivasan, A. Chepurnoy, C. Papamanthou, A. Tomescu, and Y. Zhang. Hyperproofs: Aggregating and maintaining proofs in vector commitments. In *USENIX Security*, 2022. Cryptology ePrint Archive, Report 2021/599.

[11] U. Maurer. Abstract models of computation in cryptography. In *Cryptography and Coding*, LNCS 3796, pages 1–12. Springer, 2005.

[12] G. Fuchsbauer, E. Kiltz, and J. Loss. The algebraic group model and its applications. In *CRYPTO*, LNCS 10992, pages 33–62. Springer, 2018.