Chapter 4 – Show the Total, Hide Each Gift

"Treasurer checks sums without seeing amounts."

ndhy

July 2, 2025

Prove sums, reveal nothing else.

Outline

1. Motivation: the privacy gap when values stay in plaintext
2. Pedersen commitments — binding and hiding
3. Commitments as Merkle leaves, root already signed
4. Capstone: study roadmap and next projects

Plain Values Leak Too Much

- Chapter 3 delivered integrity but not confidentiality.
- An auditor who downloads every leaf can read each gift amount.
- Goal: hide individual gifts while still proving the total budget equals the announced number.

Key idea: replace each cleartext leaf with a commitment— a sealed box carrying a unique serial number.

Definition

Let $G = \langle g \rangle$ be a cyclic group of prime order q and let h be an independent generator. For a value $m \in \mathbb{Z}_q$ and random blinding $r \in \mathbb{Z}_q$,

$$C(m, r) = g^m \, h^r.$$

- **Hiding** (perfect): C reveals no information about m.
- **Binding** (computational): producing two openings for the same C breaks discrete log.
- *Additive homomorphism*: $C(m_1, r_1)\, C(m_2, r_2) = C(m_1 + m_2,\ r_1 + r_2)$.

From Equation to Intuition

$$\overbrace{g^m}^{\text{serial number}} \cdot \overbrace{h^r}^{\text{opaque paint}} = C$$

- Anyone can recognise the same box by its serial number, yet the content remains hidden by the paint.
- Opening requires the pair (m, r); verification simply checks $g^m h^r = C$.

Security Sketch

- **Perfect hiding**: for any m_0, m_1 there exist r_0, r_1 such that $C(m_0, r_0) = C(m_1, r_1)$.
- **Binding**: two openings give $g^{m-m'} = h^{r'-r} \Rightarrow$ discrete-log of h in base g.

Private Ledger Pipeline

1. Commit each gift: $L_i = C(m_i, r_i)$.
2. Hash leaves with Poseidon $\rightarrow$ Merkle root (Chapter 4).
3. Santa signs the root with Ed25519 (Chapter 3).
4. To prove the total, reveal openings (m_i, r_i) for a subset S where $\sum_{i \in S} m_i$ equals the claimed amount, plus Merkle proofs of each L_i.
5. Verifier checks openings, paths, and the signed root; unseen gifts remain private.

Next Steps

- **Proofs, Arguments, and Zero-Knowledge** (Justin Thaler) — free online text.
- **Circom with Poseidon** — practical path to zk-SNARK circuits.
- Assignment: prepare a two-page brief on assumptions, common pitfalls, and open questions.

Cheat-Sheet

- Pedersen commitments provide perfect hiding and binding under discrete-log.
- Homomorphism enables sum proofs without revealing parts.
- Commitment $\rightarrow$ Merkle root $\rightarrow$ signature creates a compact, private, tamper-proof ledger.

Questions?