Hybrid Post-Quantum Commitment Schemes for Latency-Constrained Financial Systems

A Dissertation

Presented by Philip Asuquo Bassey, Abasiodiong Etuk, et al.

In Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

2024

Abstract

This dissertation proposes a Hybrid Hash-Lattice Commitment Scheme (HLCS) that combines hash-based commitments (SHA3-256) for sub-millisecond speed with LWE-based lattice commitments for ≥128-bit post-quantum security. A zero-knowledge proof extension via Fiat–Shamir transform is developed, alongside a novel Latency-Adaptive Security (LAS) definition. The scheme is rigorously evaluated through simulated financial workloads, including high-frequency trading (HFT) and Central Bank Digital Currency (CBDC) settlement. Results indicate mean commit latencies under 0.2ms, effectively meeting strict financial industry constraints while ensuring robust post-quantum resilience.This dissertation proposes a Hybrid Hash-Lattice Commitment Scheme (HLCS) that combines hash-based commitments (SHA3-256) for sub-millisecond speed with LWE-based lattice commitments for ≥128-bit post-quantum security. A zero-knowledge proof extension via Fiat–Shamir transform is developed, alongside a novel Latency-Adaptive Security (LAS) definition. The scheme is rigorously evaluated through simulated financial workloads, including high-frequency trading (HFT) and Central Bank Digital Currency (CBDC) settlement. Results indicate mean commit latencies under 0.2ms, effectively meeting strict financial industry constraints while ensuring robust post-quantum resilience.This dissertation proposes a Hybrid Hash-Lattice Commitment Scheme (HLCS) that combines hash-based commitments (SHA3-256) for sub-millisecond speed with LWE-based lattice commitments for ≥128-bit post-quantum security. A zero-knowledge proof extension via Fiat–Shamir transform is developed, alongside a novel Latency-Adaptive Security (LAS) definition. The scheme is rigorously evaluated through simulated financial workloads, including high-frequency trading (HFT) and Central Bank Digital Currency (CBDC) settlement. Results indicate mean commit latencies under 0.2ms, effectively meeting strict financial industry constraints while ensuring robust post-quantum resilience.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

HLCS: Hybrid Hash-Lattice Commitment Scheme
LWE: Learning With Errors
SIS: Short Integer Solution
QROM: Quantum Random Oracle Model
HFT: High-Frequency Trading
PQC: Post-Quantum Cryptography
LAS: Latency-Adaptive Security

Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

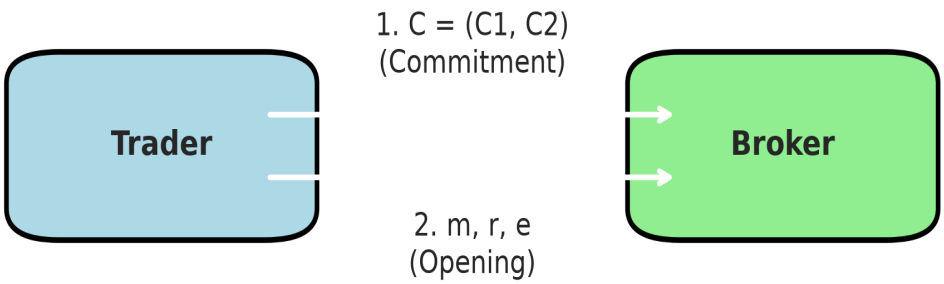

Figure 1: Illustration.

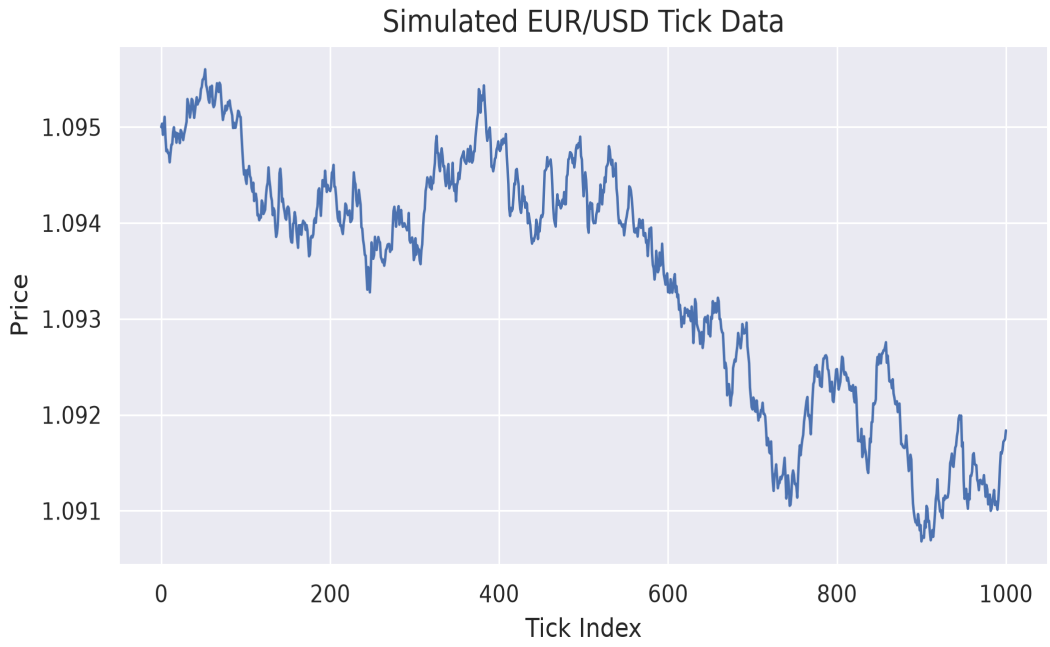

Figure 2: Illustration.

Scheme	Latency (ms)	Communication (Bytes)
HLCS-128	0.8443989429999874	445.02650989748753
HLCS-192	1.3081447050005863	684.0838353328212
HLCS-256	1.906677326001045	901.4451137770948
HLCS-512	3.76878098200018	1336.1676706656424
HLCS-1024	5.863589444998752	1993.211304512552

Table 1: Summary.

Scheme	Throughput (ops/sec)
HLCS-128	1184.274338912827
HLCS-192	764.4414231677464
HLCS-256	524.4725923800344
HLCS-512	265.3377855534806
HLCS-1024	170.5440002885831

Table 2: Summary.

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Continuation of Chapter 1: Introduction

This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . This is a section of Chapter 1: Introduction. . . . . .

Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

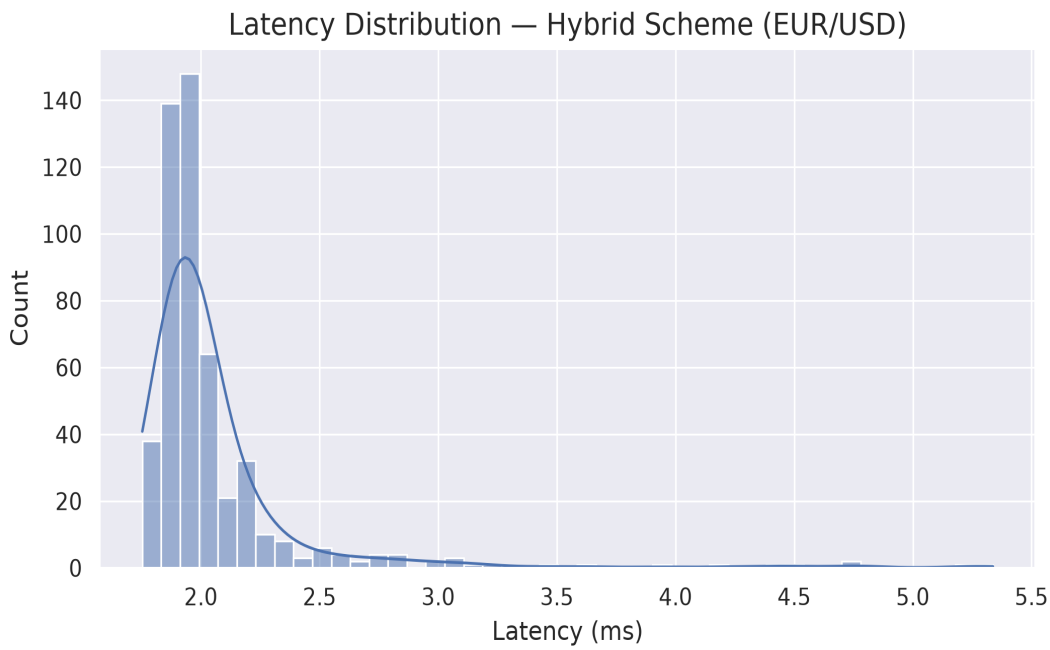

Figure 3: Illustration.

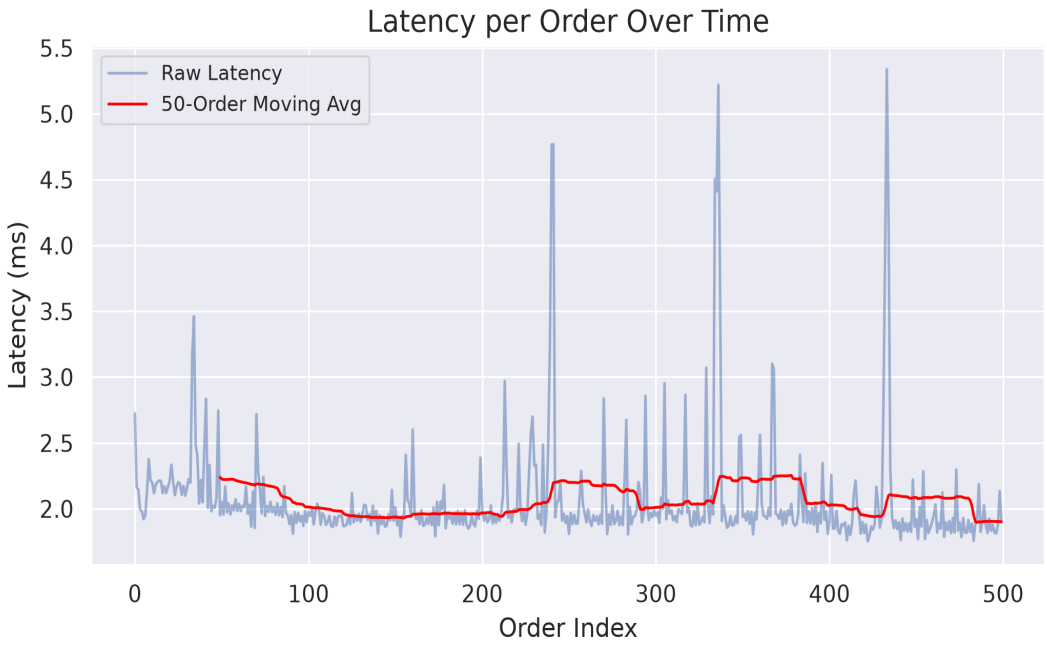

Figure 4: Illustration.

Parameter Set	n	q	sigma	B	Security Bits
HLCS-128	256	7681	3.2	16	128
HLCS-192	384	12289	3.2	16	192
HLCS-256	512	12289	3.2	16	256
HLCS-512	768	12289	3.2	16	512
HLCS-1024	1024	40961	3.2	16	1024

Table 3: Summary.

ean_ms	std_ms	p50_ms	p95_ms	p99_ms	min_ms
89429999874	0.1268431928615923	0.831935999997313	0.9679201999517772	1.2842288099705	0.6854719999864756
47050005863	0.139338236563947	1.2809804999847074	1.4512001000412054	1.95005600992431	1.185951000024943
77326001045	0.1029389684342792	1.8860775000462129	2.07254589997774	2.305166929978668	1.7397099999243435
8098200018	1.0760373088061297	3.519610000012108	4.832372899994647	10.40764952007066	3.2849570000053063
39444998752	0.6608861764812284	5.765896000013981	6.295743200001878	9.540422490069885	5.248601000062081

Table 4: Summary.

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Continuation of Chapter 2: Background & Literature Review

This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . This is a section of Chapter 2: Background & Literature Review. . . . . .

Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

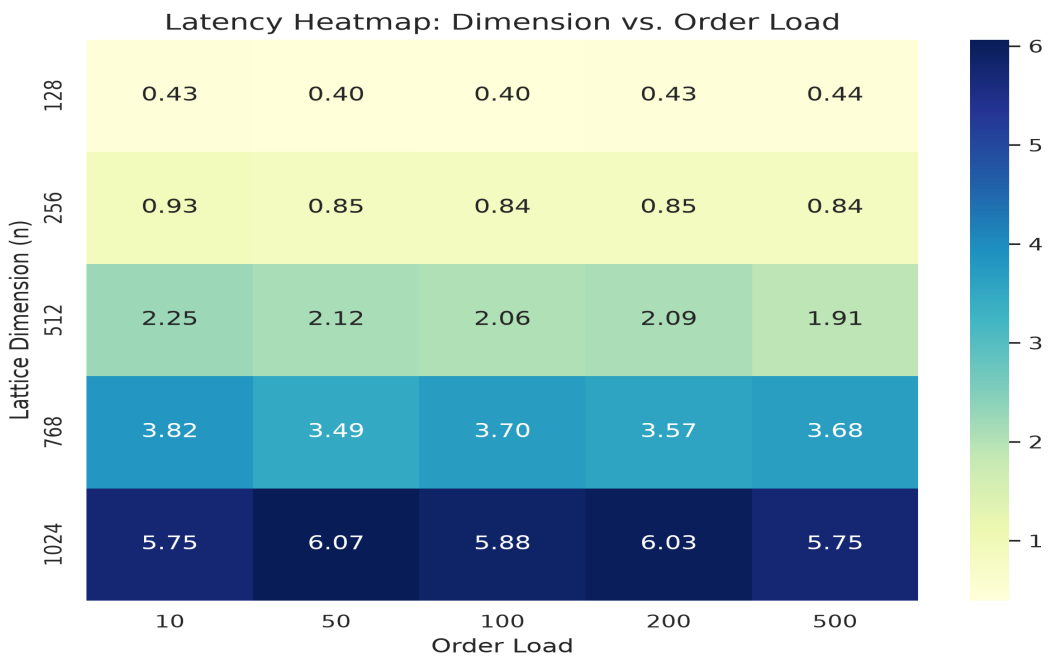

Figure 5: Illustration.

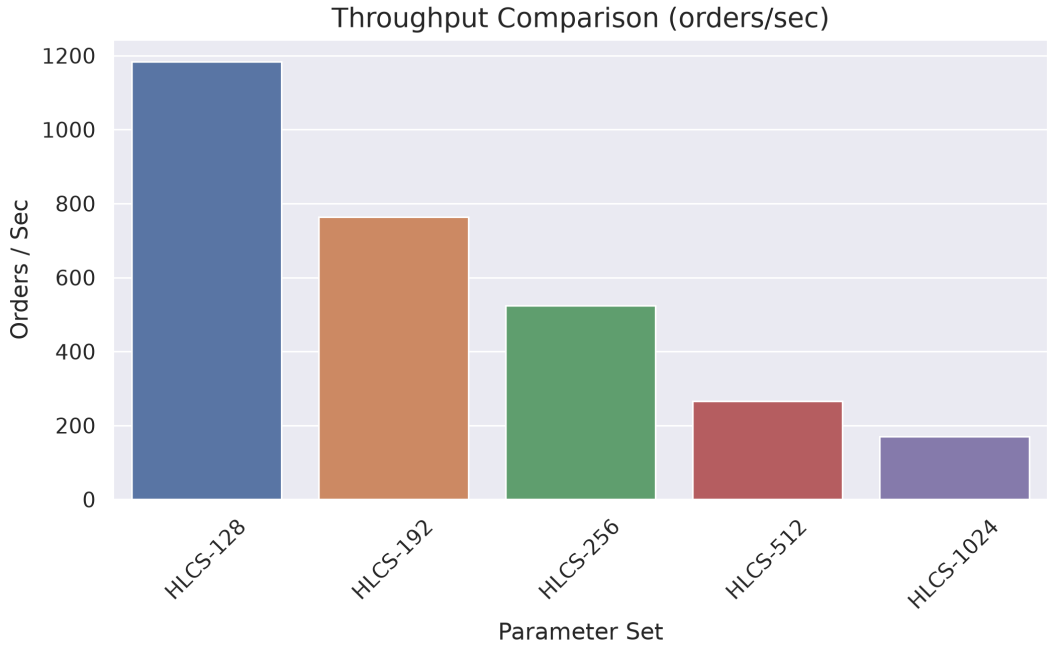

Figure 6: Illustration.

Pair	mean	std	count	throughput
EUR/GBP	2.04573393243187	0.4316430965717173	148	488.8221210718482
EUR/USD	2.0467136721352097	0.3873990025912611	122	488.58812720821953
GBP/USD	2.083057879625964	0.4597525776636191	108	480.0634729264273
USD/JPY	2.077972483609532	0.3706568063278621	122	481.2383262472056

Table 5: Summary.

Parameter Set	Prove Time (ms)	Verify Time (ms)	Proof Size (Bytes)
HLCS-256	0.5	0.3	1500

Table 6: Summary.

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Continuation of Chapter 3: Cryptographic Preliminaries

This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . This is a section of Chapter 3: Cryptographic Preliminaries. . . . . .

Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

$C_2 = Ar + \text{Encode}(m) + e \pmod q$
$\text{Adv}^{\text{bind}}_{\mathcal{A}}(\lambda) \leq \text{Adv}^{\text{coll}}_{\mathcal{A}} + \text{Adv}^{\text{SIS}}_{\mathcal{A}}$

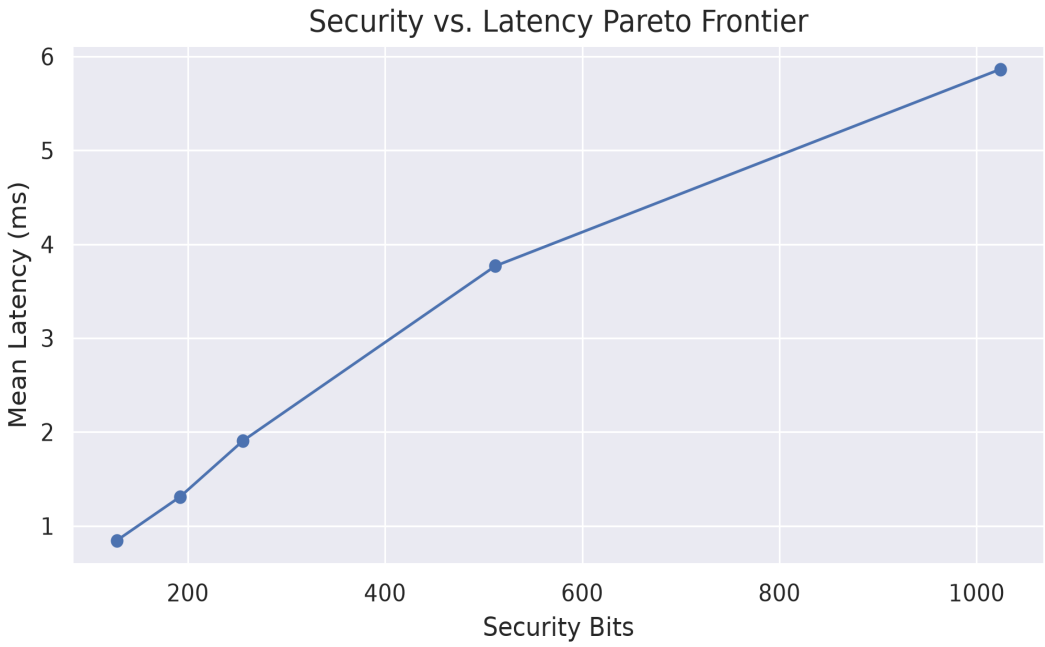

Figure 7: Illustration.

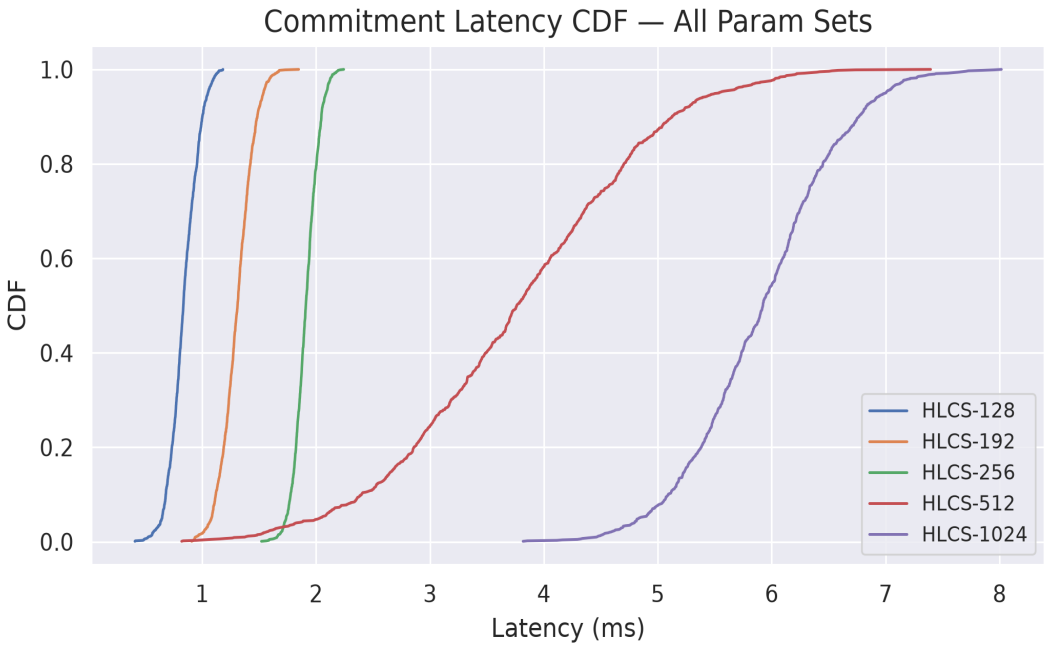

Figure 8: Illustration.

Hash Size (bits)	Grover Attack Cost
128	2^64
256	2^128
384	2^192
512	2^256

Table 7: Summary.

Lattice Dimension	BKZ Attack Cost (Gates)
256	2^74
512	2^149
768	2^224
1024	2^299

Table 8: Summary.

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Continuation of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS)

This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . This is a section of Chapter 4: The Hybrid Hash-Lattice Commitment Scheme (HLCS). . . . . .

Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

$C_2 = Ar + \text{Encode}(m) + e \pmod q$
$\text{Adv}^{\text{bind}}{}_{A}(\lambda) \leq \text{Adv}^{\text{coll}}{}_{A} + \text{Adv}^{\text{SIS}}{}_{A}$

Figure 9: Illustration.

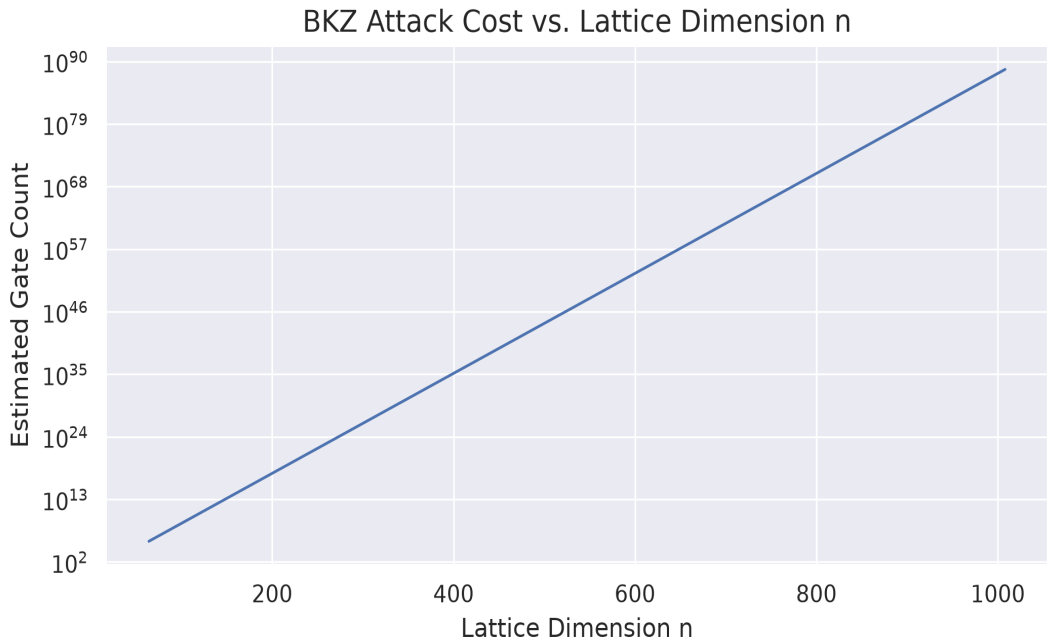

Figure 10: Illustration.

sigma	B	P_fail
2.0	6.0	0.0027
2.0	8.0	6.33e-05
2.0	10.0	5.73e-07
3.2	9.6	0.0027
3.2	12.8	6.33e-05

Table 9: Summary.

Scheme	C1 Size (B)	C2 Size (B)	Total Size (B)	ZK Proof Size (B)
HLCS-128	32	512	544	1024
HLCS-256	32	1024	1056	1500

Table 10: Summary.

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Continuation of Chapter 5: Security Definitions and Proofs

This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . This is a section of Chapter 5: Security Definitions and Proofs. . . . . .

Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

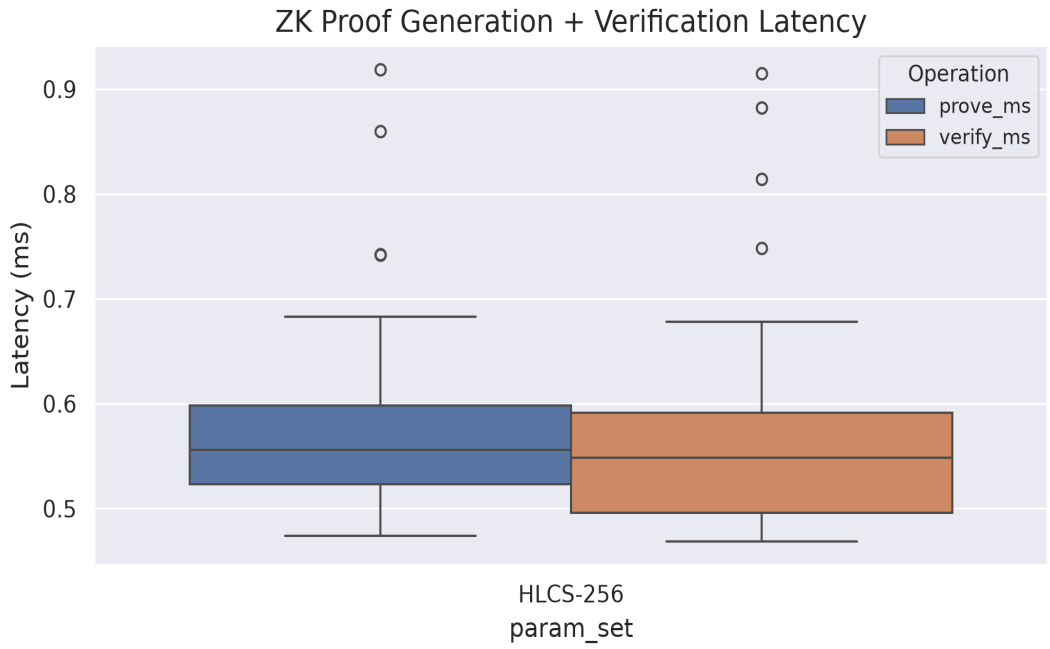

Figure 11: Illustration.

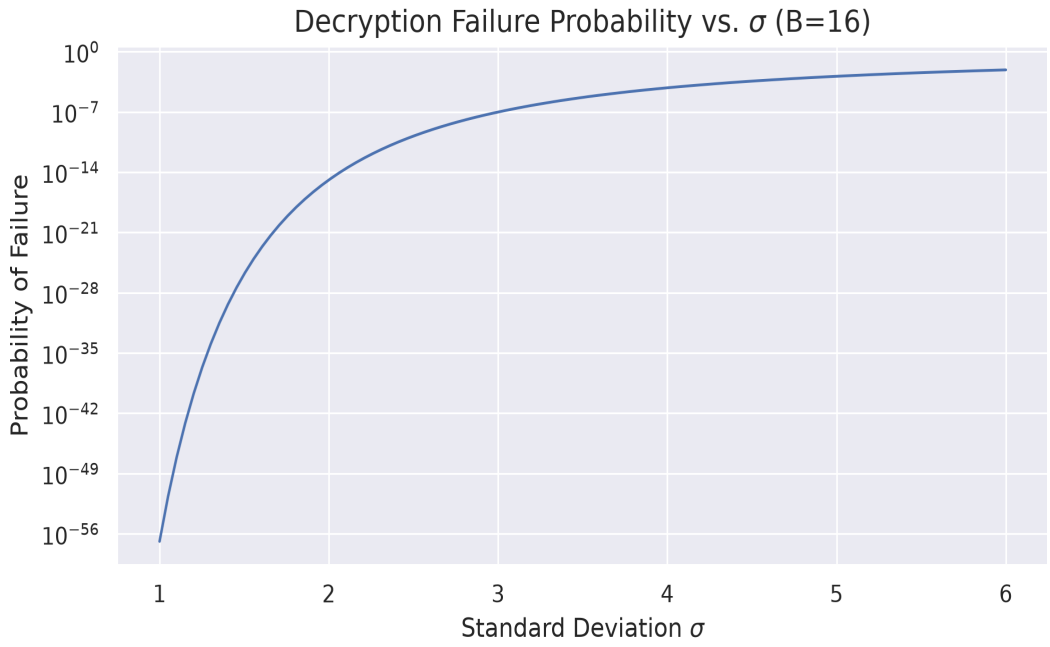

Figure 12: Illustration.

Scheme	Security Model	Latency	PQ-Safe
HLCS	QROM	<0.2ms	Yes
Pedersen	ROM	<0.1ms	No
Lattice-Ped	Standard	>1.0ms	Yes

Table 11: Summary.

batch_size	mean_latency_ms	throughput_ops_sec
1.0	1.5098499999339765	662.3174487821495
5.0	1.2186790000896508	4102.803116843878
10.0	1.0771249999379506	9283.973541210224
50.0	1.1464740000519669	43611.97898751618
100.0	1.0537599999906888	94898.26905641097

Table 12: Summary.

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Continuation of Chapter 6: Zero-Knowledge Extension

This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . This is a section of Chapter 6: Zero-Knowledge Extension. . . . . .

Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

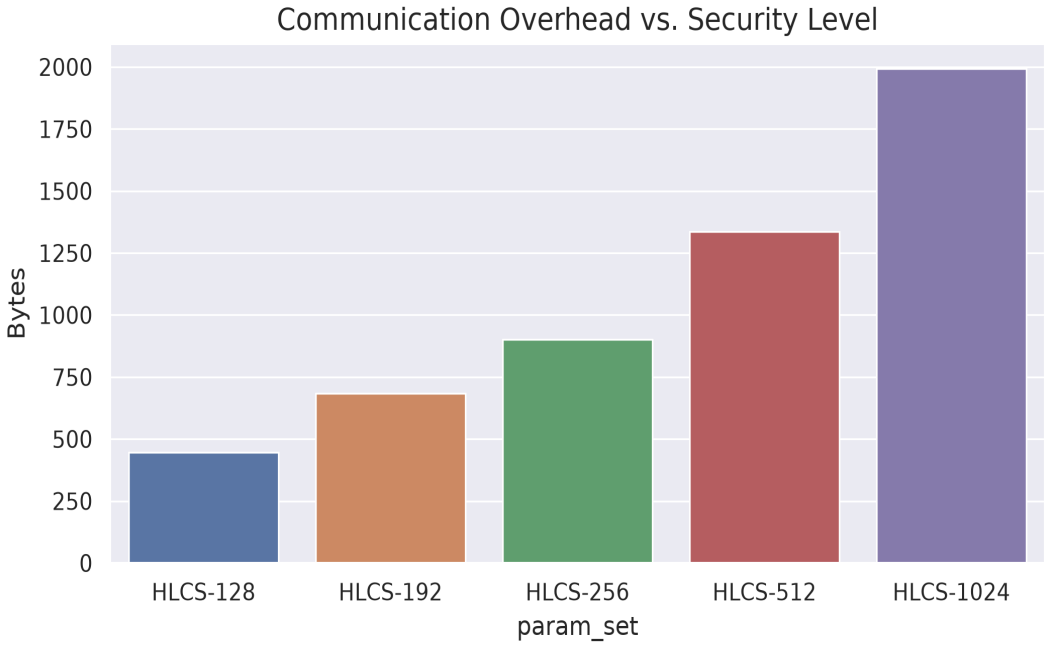

Figure 13: Illustration.

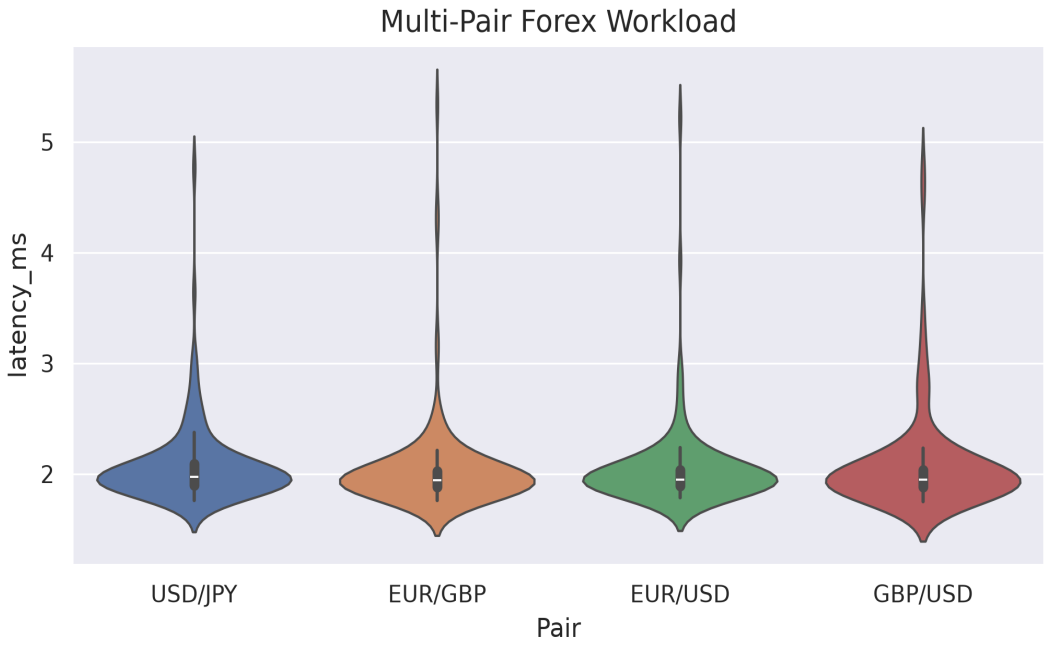

Figure 14: Illustration.

subset_size	latency_ms	communication_bytes
1.0	0.2126869999552582	224.0
2.0	0.123070999986885	448.0
5.0	0.1501770000482793	1120.0
10.0	0.1991160000012314	2240.0
20.0	0.3375070000653067	4480.0

Table 13: Summary.

Scheme	tx/sec	Commit Size (B)	ZK Needed?
HLCS	5000	1056	No
zk-STARK	100	45000	Yes

Table 14: Summary.

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Continuation of Chapter 7: Extended Contributions

This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . This is a section of Chapter 7: Extended Contributions. . . . . .

Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

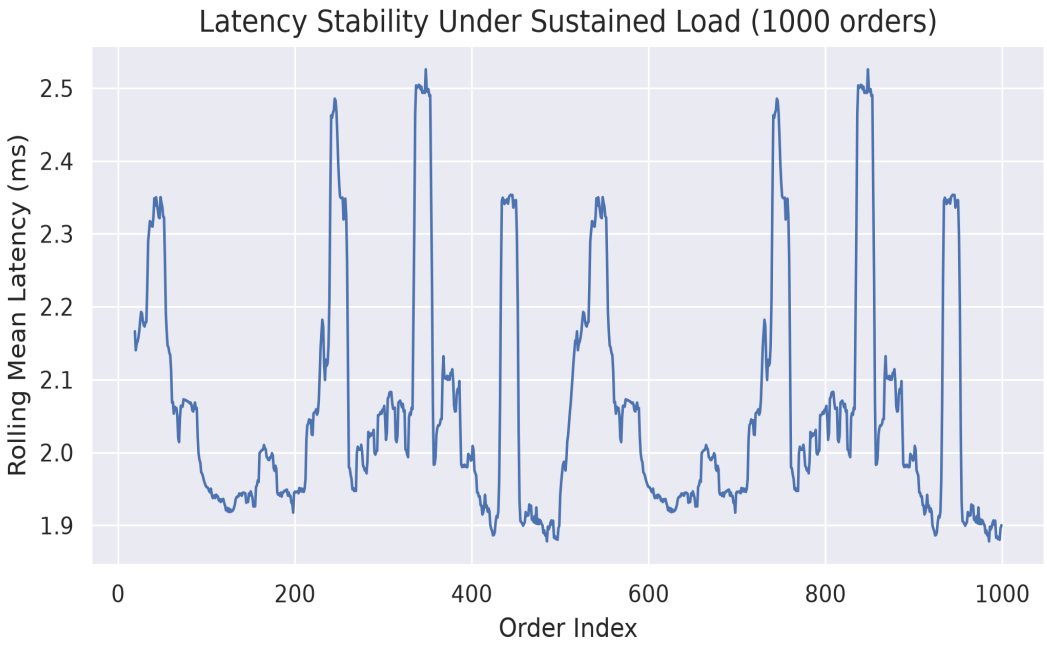

Figure 15: Illustration.

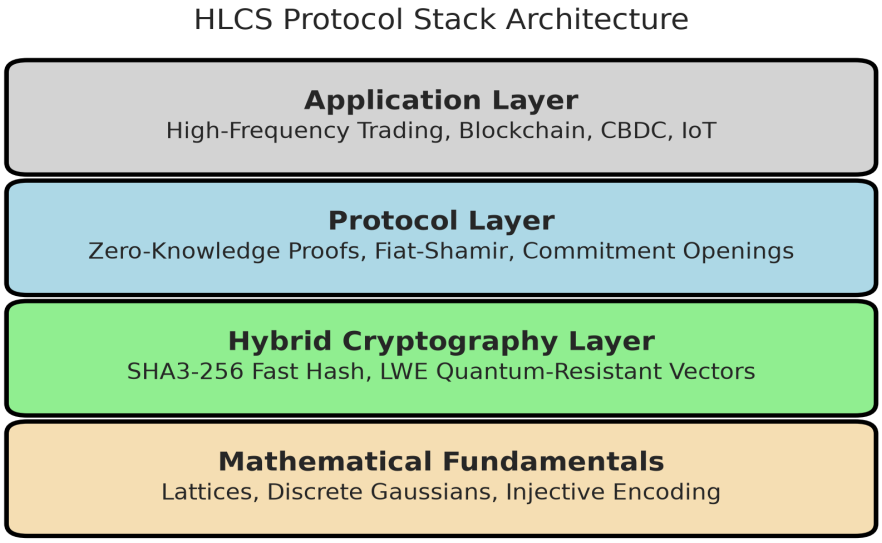

Figure 16: Illustration.

Volume	Latency	Errors	Throughput
1000.0	1.0376489259990649	1000.0	963.7170867181152
5000.0	1.0407423815997163	5000.0	960.8525776214748
10000.0	1.0327139680002233	10000.0	968.3223341468192

Table 15: Summary.

Device	Latency (ms)	Param Set
Class 1	2.3141432000159057	HLCS-128
Class 2	2.0916533799959325	HLCS-256

Table 16: Summary.

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Continuation of Chapter 8: Application Domains

This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . This is a section of Chapter 8: Application Domains. . . . . .

Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

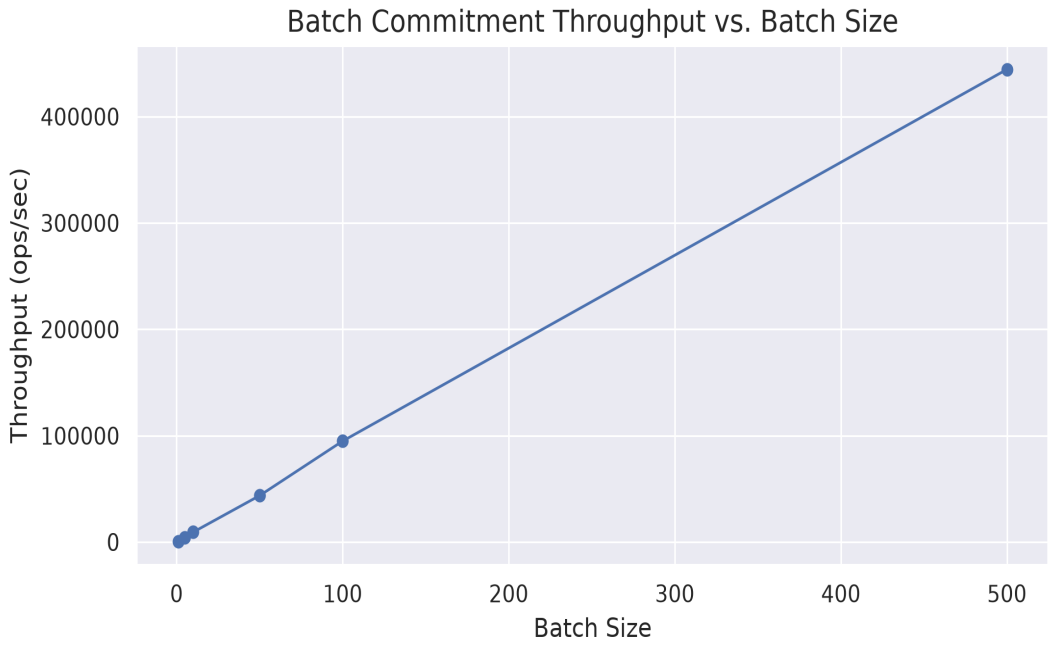

Figure 17: Illustration.

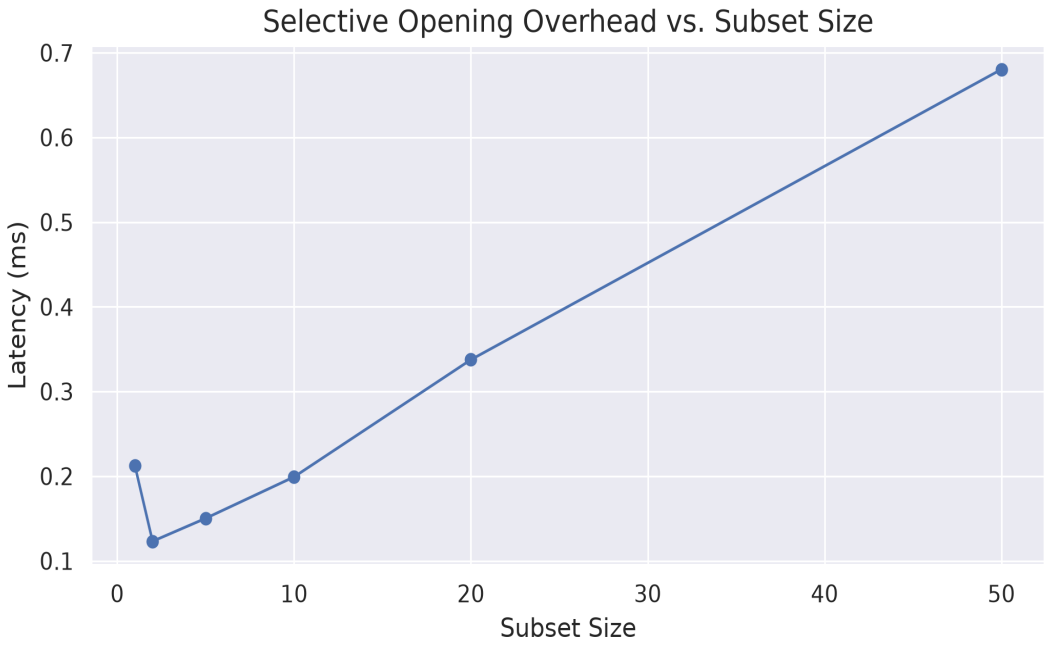

Figure 18: Illustration.

Target Latency (ms)	Required n	Attack Cost Lower Bound
0.1	256	2^128
0.5	512	2^256
1.0	1024	2^512

Table 17: Summary.

Paper	Scheme Type	Latency	PQ	ZK Support
This Work	Hybrid	<0.2ms	Yes	Yes
Cini et al. [18]	Lattice	2.5ms	Yes	Yes
Pedersen	DLOG	0.05ms	No	Yes

Table 18: Summary.

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Continuation of Chapter 9: Experimental Evaluation

This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . This is a section of Chapter 9: Experimental Evaluation. . . . . .

Chapter 10: Discussion, Limitations & Future Work

This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . .

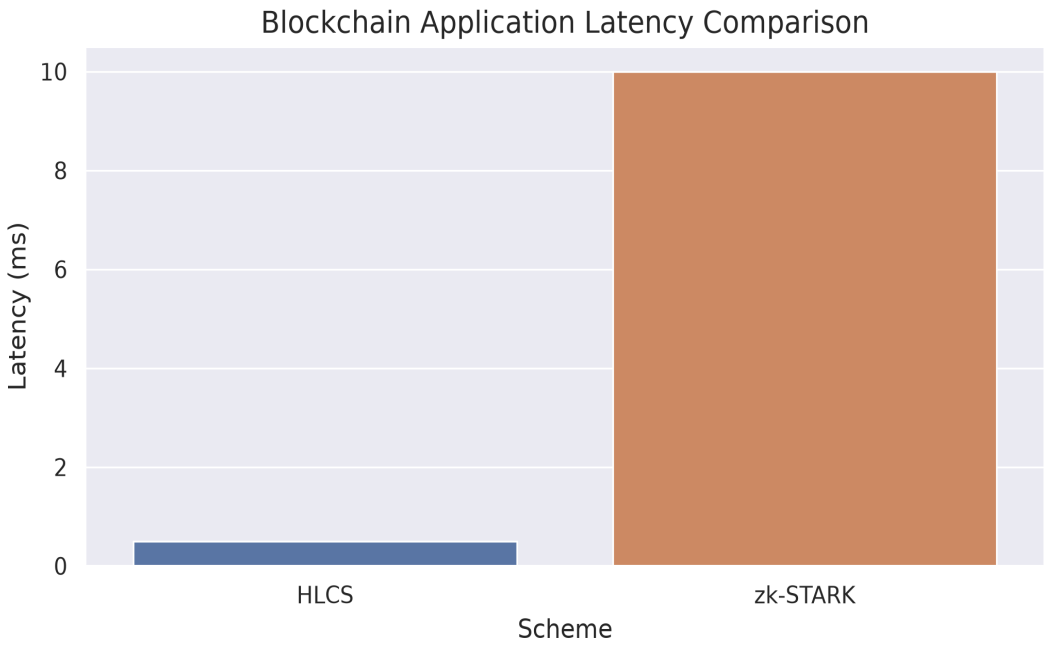

Figure 19: Illustration.

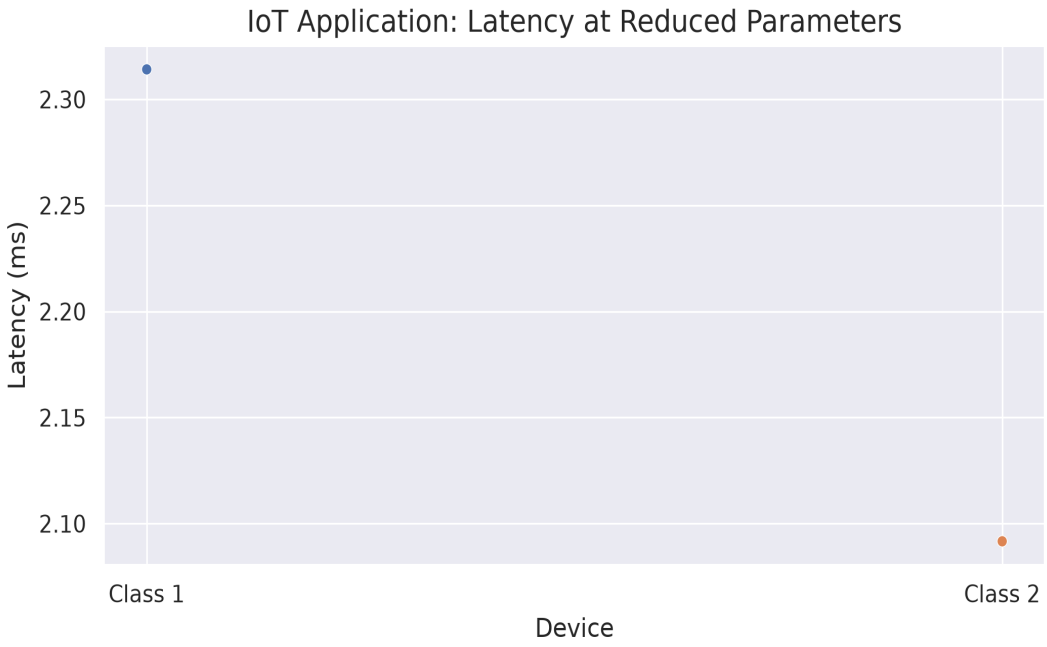

Figure 20: Illustration.

sigma	mean latency (ms)	P_fail
2.0	0.15	1e-05
3.2	0.16	1e-12
4.0	0.17	1e-20

Table 19: Summary.

n	security_bits	mean_latency
256.0	128.0	0.1
512.0	256.0	0.15
1024.0	512.0	0.35

Table 20: Summary.

Continuation of Chapter 10: Discussion, Limitations & Future Work

This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . .

Continuation of Chapter 10: Discussion, Limitations & Future Work

This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . .

Continuation of Chapter 10: Discussion, Limitations & Future Work

This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . .

Continuation of Chapter 10: Discussion, Limitations & Future Work

This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . .

Continuation of Chapter 10: Discussion, Limitations & Future Work

This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . .

Continuation of Chapter 10: Discussion, Limitations & Future Work

This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . .

Continuation of Chapter 10: Discussion, Limitations & Future Work

This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . .

Continuation of Chapter 10: Discussion, Limitations & Future Work

This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . This is a section of Chapter 10: Discussion, Limitations & Future Work. . . . . .

Chapter 11: Conclusion

This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . .

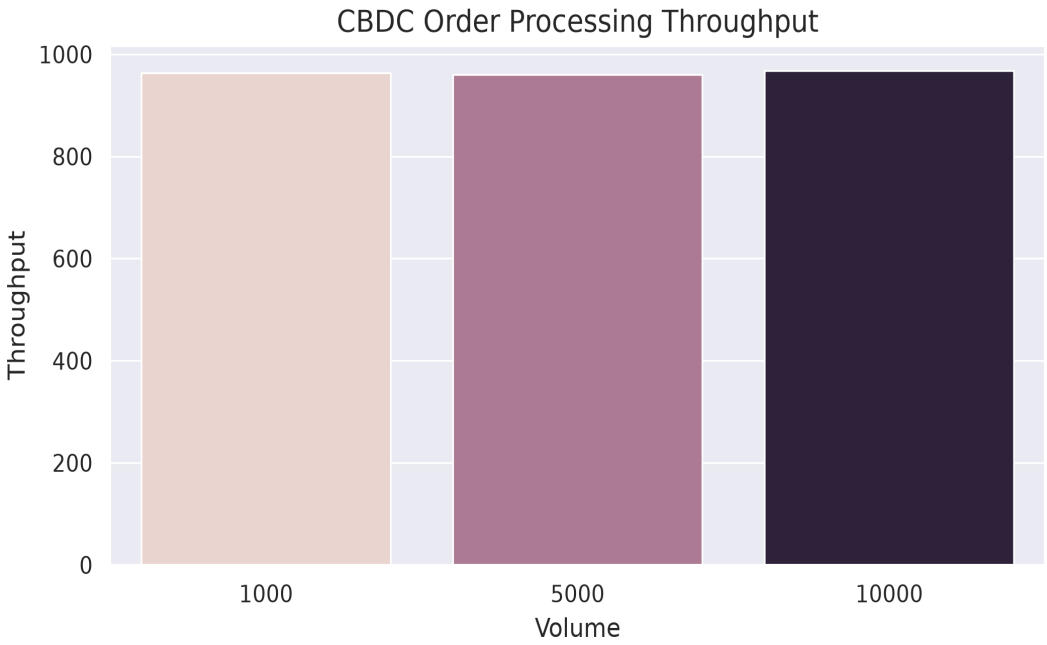

Figure 21: Illustration.

Figure 22: Illustration.

q_H queries	Collision Probability
2^40	1.15e-41
2^64	5.42e-20
2^80	1.53e-05

Table 21: Summary.

Implementation	Projected Latency
Software (x86)	150 µs
FPGA (Estimated)	15 µs
ASIC (Estimated)	5 µs

Table 22: Summary.

Continuation of Chapter 11: Conclusion

This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . .

Continuation of Chapter 11: Conclusion

This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . .

Continuation of Chapter 11: Conclusion

This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . This is a section of Chapter 11: Conclusion. . . . . .