The Name of the Title Is Hope

tbd

ABSTRACT

tbd.

CCS CONCEPTS

• **Theory of computation → Cryptographic primitives**.

KEYWORDS

tbd

ACM Reference Format:
tbd. tbd. The Name of the Title Is Hope. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (Conference acronym 'XX)*. ACM, New York, NY, USA, 1 page. https://doi.org/tbd

1 INTRODUCTION

tbd

2 PRELIMINARY

2.1 Basic Notations

2.2 Distributed Point Function

Definition of distributed (multi-)point function, naive construction

2.3 Batch Codes

combinatorial/probabilistic batch codes, with cuckoo hashing a concrete instantiation

2.4 Oblivious Key-Value Stores

definition of OKVS, concrete instantiations(polynomial, sparse matrix). mention some connections to cuckoo hashing

3 NEW DMPF CONSTRUCTIONS

3.1 Big-State DMPF

display the big-state DMPF (plus distributed gen)

3.2 Batch-Code DMPF

display the batch-code DMPF

3.3 OKVS-based DMPF

display the OKVS-based DMPF (plus distributed gen)

3.4 Comparison

Comparison table dependent to PRG & F-MUL
analyze tradeoff
distributed gen advantage

4 APPLICATIONS

4.1 PCG for OLE from Ring-LPN

Characterize parameters
show nonregular optimization
plug in new DMPF and show overall optimization

4.2 PSI-WCA

plug in new DMPF and analyze advantage interval
plug in distributed gen

4.3 Heavy-hitters

private heavy-hitter
or parallel ORAM?

5 ACKNOWLEDGMENTS

tbd

REFERENCES

A BATCH-CODE DMPF SCHEME

B SECURITY PROOFS

Conference acronym 'XX, tbd, tbd

ACM ISBN tbd…$15.00
https://doi.org/tbd