

Research Statement & Proposal (Informal)

Quan Shi
shiquan@std.uestc.edu.cn

September 2023

Obviously, as an undergraduate student, it is difficult to list a large amount of my publications in a specific field. However, I will try my best to focus on - ***Theory and Foundation of Cryptography***, to develop my Research Statement. Then, there is a detailed research proposal about ***Fine-Grained Cryptography against Bounded-Circuit-Depth*** and ***Cryptography from Time-Bounded Kolmogorov Complexity***. This document interprets my preliminary understanding and planning for the theory of cryptography.

Current Research Statement

1 Background

From 2020 to 2024, I am undergraduate student at the School of Information and Communication Engineering, UESTC, majoring in Electronic Information Engineering. Although the curriculum primarily focuses on electronic design and communication principles, I have developed a strong inclination towards mathematics modeling and privacy computing projects. Prior to June 2022, I dedicated a considerable amount of my after-school time to studying mathematics, ultimately achieving the title of Outstanding Winner (top 0.1%) in the Mathematical Contest In Modeling (MCM).

After stepping down from the competition team, my initial research interest gravitated towards Security in Machine Learning. For instance, I submitted a paper to TrustCom23, which incorporated computer vision with a series of secure multi-party computation (MPC) protocols, leveraging UAV edge computing. However, upon completion, I was filled with a sense of disappointment and shame as I realized that it did not meet the standards of rigorous security. Subsequently, I embarked on a journey to explore fundamental cryptography, uncovering an enduring passion for this field of study.

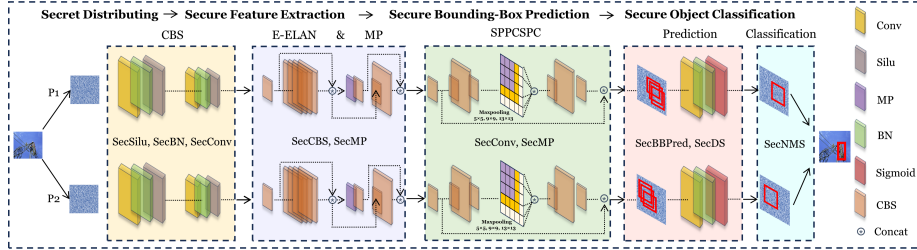
I started in reading exceptional papers from notable conferences in the field of cryptography, such as Crypto, EuroCrypt, and AsiaCrypt. The meticulous-

ness and rigour applied to proofs within these papers has left a profound impression on me. Through this process, I have further refined my interest in Provable Security, Computational Complexity, and Foundations of Cryptography. Presently, under the supervision of Prof. Yuyu Wang, I am engaged in research on Fine-Grained Cryptography and Non-Interactive Zero-Knowledge (NIZK) protocols.

2 Prior Research Overview

2.1 Secret Sharing

[SD23] We design a secure single-target detection model called SecYOLOv7 (SecureYOLOv7) which is proposed to safeguard the privacy of the object detection process in transmission line. Our approach is about **secure multi-party computation (MPC)**. Based on Shamir Secret Sharing and Gennaro’s Multiplication, a series of secure computing protocols are designed for the collaborative execution of the Secure Feature Contraction, Secure Bounding-Box Prediction, Secure Object Classification, and other computing modules by two non-edge servers. The security and privacy-preserving capabilities of SecYOLOv7 are theoretically analyzed and demonstrated. Practical performance evaluation shows that both the computational and communication costs, as well as the framework error, are considerably lower than those of to existing works.



I did almost all of this work, after which, I realized the weakness of applied cryptography, which in turn sparked my interest in foundations of cryptography.

2.2 Data Analysis

[SGSC23] This paper is mainly based on the customer information dataset of a foreign commercial bank in Kaggle, and we use *LightGBM algorithm* to build a classifier to classify customers, to help the bank judge the possibility of customer credit default. This paper mainly deals with characteristic engineering, such as missing value processing, coding, imbalanced samples, etc., which greatly improves the machine learning effect. The main innovation of this paper is to construct new feature attributes on the basis of the original dataset so that the accuracy of the classifier reaches 0.734, and the AUC reaches 0.772, which is

more than many classifiers based on the same dataset.

I am the third author, made major contribution to programming and modeling of Lightgbm algorithm.

2.3 Mathematical Modeling

Mathematical Contest in Modeling and Interdisciplinary Contest in Modeling (MCM/ICM) are annual international competitions that challenge undergraduate and graduate students to solve real-world problems using mathematical modeling and interdisciplinary approaches. The contests are organized by the Consortium for Mathematics and Its Applications (COMAP) and attract participants from universities and colleges worldwide. And our team's job is to develop a Power Planning Model for Cyclists in three days and complete a 25-page thesis.

We established a Rider Ability Evaluation Model based on 3P-CP, built an External Factor Analysis Model to identify the potential impact of external conditions. Finally, we extend the model to a Team Time-Trial Power Distribution Model, and obtain the extended multivariate nonlinear programming problem. This work won the 2022 **Outstanding Winner** ($< 0.1\%$).

As the Team Leader, my responsibilities include designing mathematical models, sharing my thoughts with team members, welcoming their input, and assigning specific tasks to team members. This competition has cultivated my ability to write English academic essays and cooperate with peers.

3 Current and Future Work

3.1 Fine-Grained Security

From 2023, I'm a research assistant supervised by Prof. Yuyu Wang, be responsible for collecting information and checking his papers. In this process, I have systematically learned about provable security and circuit complexity.

We mainly concentrate on non-interactive zero-knowledge proof systems in NC^1 and AC^0 -fine-grained setting. The technique is transforming a simple Σ -protocol into NIZK for linear languages, and constructing a OR-proof system for SAT.

3.2 Courses and Readings

During my free time, I have studied Jonathan Katz's course "CMSC 858K - Advanced Topics in Cryptography", attending Zhejiang University's "Crypto School", and Jin-Yi Cai's course "CS810: Introduction to Complexity Theory."

I have also read some classic textbooks, including "Computational Complexity - A Conceptual Perspective" by Oded Goldreich, "Computational Complexity - A Modern Approach" by Sanjeev Arora and Boaz Barak, "Kolmogorov Complexity and Algorithmic Randomness" by A. Shen, V.A. Uspensky and N. Vereshchagin.

3.3 Future Plan

I am interested in cryptography and its interplay with computational complexity. I plan to investigate the foundation in information security technology from a mathematical point of view. My research proposal is about fine-grained and Kolmogorov cryptography.

4 Research Principles

◇ **Collaboration & Communication.** Prior to winning the mathematical modeling award, I came across many different teammates, but I always ended up doing most of the work myself. Finding the optimal means of cooperation and coordination has remained a significant concern of mine. At times, fostering strong relationships with teammates and establishing mutual trust has proven to be more daunting than completing a research paper.

◇ **Rigour.** The field of application security, especially regarding AI, frequently emphasizes efficiency, with numerous articles merely providing a superficial level of "security" for AI. However, upon completing my paper [SD23], I realized my inclination towards rigour and subsequently decided to specialize in the area of Cryptography.

◇ **Philosophical thinking.** The capacity to extract philosophical insights from scientific theories is a valuable skill, particularly in fields that are replete with abstract symbols and mathematical equations. A prime example of this is the $P \neq NP$ hypothesis, which posits that not all problems that can be efficiently recognized can also be efficiently solved. This hypothesis transcends even Kant's and Wittgenstein's comprehension of the interplay between the tangible world and human cognition.

◇ **Sense of purpose.** During the course of scientific research, it becomes imperative to delve into uncharted territories that have not yet been thoroughly explored. Often, we find ourselves investing months of diligent effort only to realize that a particular idea is not feasible. These moments can feel akin to a compass malfunction, leaving us with no choice but to forge ahead in the direction we deem right, even in the face of adversity.

◇ **Adapt to being criticized.** Failures are an inevitable part of our journey through life. While accomplishing a project brings satisfaction, we must also acknowledge the challenges that lie ahead. Inevitably, we will encounter frequent criticism and skepticism from our colleagues.

5 Overview & Significance

We are interested in how to construct cryptography based on much mild assumptions or which form of security cryptography can be achieved if all classical assumptions do not hold. (Classical systems based on them would become insecure once quantum computers are developed.) For example, can we have a meaningful notion of cryptography even if we live in Pessiland or Heuristica? ¹

Generally, fine-grained cryptography is the study of cryptographic primitives that are:

- ◇ 1. Secure against adversaries with bounded resources;
- ◇ 2. Computable with fewer resources than these adversaries.

Fine-grained is not a strict concept, depending on the different assumptions and primitives. Based on established hardness conjectures about different problems, we hope to construct more primitives, such as average-case hard problems, one-way functions, NIZK, and public-key encryption.

A prevalent area is related to fine-grained cryptography – characterizing the existence of One-way function from the hardness of time-bounded Kolmogorov Complexity. What makes the string 10101010 less random than 57198325? The notion of Kolmogorov complexity measures the amount of “randomness”. We could provide a win-win paradigm, where either OWF exists, or we solve all NP problems in practice.

We believe these two tasks could be the way forward towards relations between worst-case & average-case complexities and OWF,PKE, eventually removing the computational assumptions necessary for doing cryptography.

6 Proposed Research

6.1 Aim #1: Fine-Grained Cryptography against Bounded Circuit Depth – Enrich & Recast

In this section, I’ll make conclusion and prospect about ACC^0 & AC^0 -fine-grained cryptography. My goal is **enriching its available tools, recasting normal cryptography** under such circuit restriction.

¹Impagliazzo defined five worlds, which capture the state of cryptography. The three worlds worst for cryptography are Algorithmica (NP in BPP), Heuristica (NP is not in BPP but NP problems are easy on average) and Pessiland (there are NP problems that are hard on average but solved hard instances are hard to sample, and OWFs do not exist).

6.1.1 Motivation

[DVV16] proposed fine-grained cryptographic primitives against adversaries captured by two (non-uniform) classes of adversaries, which are AC^0 and NC^1 (logarithmic-depth polynomial-sized) circuits consisting of AND, OR, and NOT gates of fan-in 2. They first constructed an unconditionally secure pseudorandom generator with arbitrary polynomial stretch, a weak pseudorandom function, and a secret-key encryption scheme, all of which are computable in AC^0 and secure against adversaries that are AC^0 circuits. Then, under the widely believed separation assumption $NC^1 \neq \oplus L/poly$, they constructed a OWF, a pseudorandom generator, a collision-resistant hash function, and a semantically secure PKE scheme that are computable in NC^1 and secure against NC^1 circuits. In the end, it left open problems:

Open Problem 1: *Unconditionally lower-bounds are known for slightly larger classes like $AC^0[p]$ when p is a prime power. Can we get cryptographic primitives from those lower-bounds?*

Open Problem 2: *Construct a public key encryption scheme secure against AC^0 .*

These questions are interesting. The concept of $AC^0[p]$ is also known as ACC^0 . Compared to AC^0 , it extends to a more general family of circuits, and the simplest extension is to allow other logic gates besides the \vee and \wedge gates, while still guaranteeing that the depth of the circuit is $O(1)$.

6.1.2 Introduction & Related Work

Fine-Grained Cryptography [DVV16] and [BRSV17] were the first to propose the notion of "*Fine-Grained Cryptography*". But similar motivations can be found in Merkle public-key exchange [Mer78].

Fine-grained cryptography [DVV16] designs cryptographic schemes in a setting where adversaries have only bounded resources and honest users have no more resources than adversaries, so that we may construct more efficient schemes and base their security on weaker, or extremely mild assumptions.

There is a scarcity of research accomplishments in the field of fine-grained cryptography, primarily focusing on primitives now. [DVV16] develops cryptographic protocols secure against adversaries that are at most as powerful as low circuit classes within P such as NC^1 — this is more fine-grained but does not address runtime. More recently, [BRSV17][BRSV18] provide several problems that are provably hard on average, under *SETH* or the $3 - SUM$ or *APSP* hypotheses. Then they use these problems to construct a Proof of Work scheme.

Circuit-Depth-Bounded Cryptography

In NC^1 -fine-grained,² as we do not know any lower bounds against NC^1 , we are forced to rely on an unproven assumption $NC^1 \neq \oplus L/poly$. Here $\oplus L/poly$ is the class of languages with polynomial-size branching programs, and all languages in NC^1 have polynomial-size branching programs of constant width [Bar86]. In AC^0 -fine-grained,³ circuit lower bounds could transform to meaningful cryptography, the first was one-way permutations against AC^0 adversaries.

Recast Normal Cryptography under circuit classes In the recent years, we are interested in which kind of cryptosystems can be constructed in this setting. We highlight the constructions of OWFs, symmetric-key and (leveled fully homomorphic) public-key encryption [CG18][DVV16], verifiable computation [CG18], hash proof systems (HPS) [EWT21], non-interactive zero-knowledge (NIZK) proof systems [WP22a][WP22b], attribute-based encryption and digital signature [WPC23]. However, due to the restriction on running resources, many important primitives remain unknown.

6.1.3 Proposed Plan

A. What hindrance is troubling us?

We have the following inclusions that are either proven strict (\subsetneq) or believed to be strict (\subseteq): $NC^0 \subsetneq AC^0 \subsetneq ACC^0[p] \subsetneq NC^1 \subseteq L \subseteq \oplus L$. We note that the inclusion $ACC^0[p] \subseteq NC^1$ is only known to be strict when p is prime.

Some NC^1 primitives can not be directly derived from existing ones by adopting previous generic conversions in the polynomial-time world since the resulting primitive may not be in NC^1 any more. For example, in standard settings the pseudorandom functions (PRF) are well known that can be constructed from OWF/OWPs. But in NC^1 , ones in NC^1 are neither implied by NC^1 -OWP nor the OWF. This necessities us to construct fine-grained primitives in *another way*.

Furthermore, all systems for unconditional AC^0 are harder to be constructed than $NC^1 \neq \oplus L/poly$. Many cryptographic primitives rely on the algebraic structures of pairing groups, which are not available in fine-grained settings. In NC^1 world, at least we could rely on [AIK06][IK00]. Now let's look at the case of AC^0 -cryptography (unconditionally secure). The AC^0 -fine-grained-system only involves simple operations in $GF(2)$.

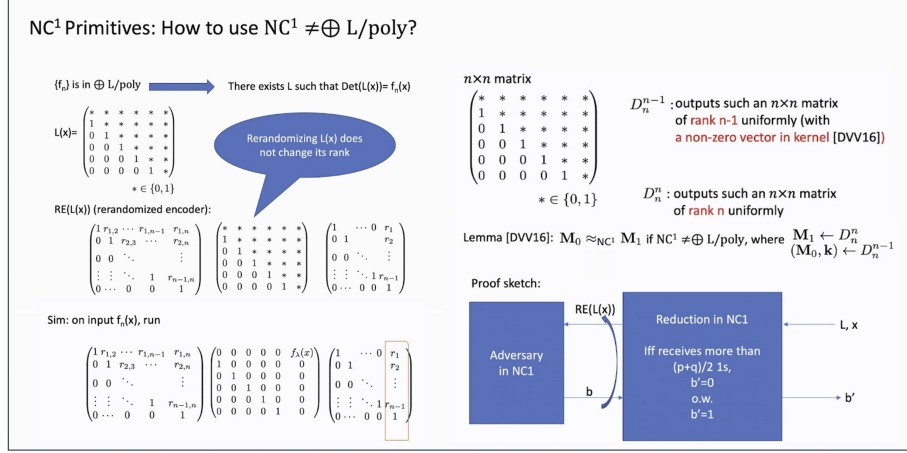
Fact 1 ([FSS81],[Ajt83]) $PARITY(\oplus) \notin AC^0$

² NC^i : \log^i -depth circuits with bounded fan-in AND/OR/NOT gates.

³ AC^i : \log^i -depth circuits with unbounded fan-in AND/OR/NOT gates.(become ACC if add MOD_p gates)

Setting	Paper	Assumption	Crypto Primitives	Honest	Adversary
Time-Bounded	[Mer78]	Random Oracles	Key Exchange	$O(N)$	$O(N^2)$
	[BGI08]	Exponentially-Strong OWFs	Key Exchange	$O(N)$	$O(N^2)$
	[BRSV18]	WC 3-Sum, OV, APSP, or SETH	Proof of Work	$O(N^2)$	/
	[LLVW19]	Zero-k-Clique or k-Sum	OWFs, Key Exchange, PKE	$O(N)$ $O(N)$	$O(N^{1+t})$ $O(N^{1.5-t})$
Storage-Bounded	[CM97]	/	Key Exchange	$O(S)$	$O(S^2)$
Circuit-Bounded (Parallel-time)	[DVV16]	$NC^1 \neq \oplus L / poly$	OWFs, PRGs, CRHFs, PKE	NC^1	NC^1
	[CG18]		SHE, VC		
	[EWT21]		OWP, HPS, CCA PKE, TDF		
	[BDSK20]		full domain TDF		
	[WPC23]		ABE, Quasi-Adaptive NIZK		
	[WP22a]		NIZK		
	[Has87]	/	OWP	AC^0	AC^0
	[DVV16]		weakPRGs, SKE, CRHFs		
	[WP22b]		NIZK		

Table 1: A table of previous works' result in this area. There have been several results characterizing different aspects of Fine-Grained Cryptography. The primitives and assumptions were previously studied in bounded amount of resources.



So a main technical hurdle is that in the AC^0 -fine-grained setting, many standard operations, such as computing the sum of a polynomial number of random elements and multiplication of two random matrices, are not allowed.

Fact 2 ([Raz87], [Smo87]) *For different primes p and q , the function MOD_p does not belong to $AC^0[q]$.*

This shows that ACC^0 is different from $AC^0_{CM}[2]$ in [CG18]. Although there are many works about $AC^0[2]$ -grained settings, it cannot transform to *Open Problem 1*.

B. Which techniques can potentially help us solve the problem?

♦ **NC¹-fine-grained** what can we get from the assumption? As shown in the figure, if assumption is $NC^1 \neq \oplus L/poly$, it uses randomized encodings of [IK00][AIK06] to construct the sampling distributions. By using LSamp, RSamp, it outputs ZeroSamp and OneSamp. These two matrices have ranks of $n-1$ and full, and exhibit indistinguishability in NC^1 . [DVV16] uses these techniques to construct OWF, PKE, PRG in NC^1

Based on the same assumption, [CG18] constructs Somewhat homomorphic encryption (SHE), however it can only compute $AC^0_Q[2]$ against adversaries in NC^1 .

♦ **AC⁰-fine-grained** In simple terms, we can look for primitives – are known to construct crypto-systems, which can also be constructed by techniques and primitives already available in AC^0 -Minicrypt world.(e.g.OWF, SKE, wPRG, OR-Proof)

For example, it seems that PKE were necessary for NIZK in the standard

model. (NIZK seemed to be in Cryptomania world) Even in the NC^1 -fine-grained setting, NIZK systems [WP22a] require the unproven assumption which also implies PKE schemes [DVV16]. [WP22b] found that OR-Proof techniques [GOS12][Raf15] can also construct a NIZK system for circuit SAT. They can transform NIZK for AC^0 -linear-language into OR-proof for the SAT of *1-out-of-2* statements, which could be extended to a fully-fledged one for *1-out-of-poly*. So the solution is to construct a AC^0 -linear-language NIZK.

C. Subsequent Work

♦ In NC^1 -fine-grained setting obtain a strong NC^1 -FHE scheme and FHE-based application

We notice that after [CG18] constructs the somewhat homomorphic encryption (SHE) in the NC^1 -fine-grained setting, there are no works which concentrate on the power of homomorphic computation and FHE-based applications. Recently, based on OR-Proof model [WP22a], we've already constructed a strong FHE in $AC^0[2]$ setting, which improves the previous SHE. Now I'm thinking about how to lower the public key size, and make such FHE a NC^1 scheme used XOR and AND gates.

♦ In AC^0 -fine-grained setting, obtain unconditionally secure Searchable Encryption, Proxy Re-Encryption (PRE) and Identity-Based Encryption (IBE).

We've already make breakthrough, jumping out of AC^0 -Minicrypt with the help of some newest techniques in computational complexity. OR-proof is a great mediation.

♦ Try to find fixed polylog-*wise* independent distribution that fools AC^0 circuits of arbitrary depth.

This is different from [Bra08] shows that any n^ϵ -*wise* independent distribution fools all AC^0 circuits. It may be the most difficult problem, which will imply PKE.

6.2 Aim #2: Cryptography against Bounded Running Time – Kolmogorov Complexity

6.2.1 Motivation

Recently, a series of elegant works by Liu and Pass [LP20] [LP21a] [LP21b] [LP] [LP23] show the connection between OWFs and Kolmogorov Complexity. We call it MK^tP -Cryptography. The reason I'm interested in this topic is that fine-grained Cryptography is related to MK^tP -Cryptography (program is taken to be a time-bounded Turing Machine). Fine-grained works have in common that if

we start off with a fine-grained lower bounds, the resulting cryptographic primitive (such as fine-grained OWFs⁴) we get will also only be secure against weak (a-priori bounded polynomial-time) attackers. MK^tP -Cryptography shows how to get different versions of OWFs parametrized by a threshold s . Sometimes, the gap between the time needed to evaluate and invert is super-polynomial (fine-grained cryptography needs fixed polynomial), from very weak fine-grained lower bounds.

We believe that more cryptographic primitives could be constructed based on techniques in MK^tP -Cryptography. As said in [LP23], an unpublished paper [BLMP23] demonstrates how to use Liu’s techniques (and in particular how restricting attention to an appropriate analog of computational depth) can be used to get a characterization of *key-exchange agreement* using the worst-case hardness of a Kolmogorov complexity-style problem. I can’t read it yet, anyway. But It encourages me to find the relationship between fine-grained world and Kolmogorov world, consider the similar equivalences hold in the fine-grained world, use the different versions of OWFs to construct other primitives.

6.2.2 Introduction & Related Work

Time-Bounded Fine-Grained Cryptography Fine-grained complexity is built upon “fine-grained” hypotheses on the (worst-case) hardness of a small number of key problems. Fine-grained uses fine-grained reductions between problems in a very tight way⁵, and obtains strong lower bounds for many problems. A few works developing cryptographic schemes assuming fine-grained hardness of some computational problems. (i.e. assuming hardness $n^{1+\alpha}$ – *time* attackers for some *fixed* constant $\alpha > 0$). [BRSV17][GR18][BABB21][DLW20] shows worst-case to average-case reductions for certain natural classes of problems in the fine-grained regimes. (OV, 3SUM, APSP). [BRSV18] shows the existence of “proof of work” assuming fine-grained worst-case hardness of these problems. [LLVW19][DLW20] constructs a fine-grained analog of OWF, assuming fine-grained average-case hardness of many languages.

Different Assumptions Some efficient cryptosystems like DSA, Diffie-Hellman have weaknesses – for instance, they are completely broken in a postquantum world as Shor’s algorithm breaks their assumptions in essentially quadratic time [Sho94]. Thus, it makes sense to look at the cryptosystems based on

⁴Fine-Grained One Way Function [BRSV17][LLVW19]: We say a function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is (t, ϵ) -one-way if it can be computed in $O(t(n)^{1-\delta})$ time for some $\delta > 0$, but for any $\delta' > 0$, any $O(t(n)^{1-\delta'})$ -time algorithm A , and all sufficiently large n ,

$$\Pr_{x \leftarrow \{0,1\}^n} [A(f(x)) \in f^{-1}(f(x))] \leq \epsilon(n, \delta')$$

⁵[VW15] Fine-grained reduction: if problem A has requires running time $a(n)^{1-o(1)}$, and one obtains an $(a(n), b(n))$ -fine-grained reduction from A to B, then problem B needs runtime $b(n)^{1-o(1)}$.

other assumptions. Some of the main hypotheses in fine-grained complexity (see [Wil15]) set K to be CNF-SAT (with $T(n) = 2^n$, where n is the number of variables), or the k -Sum problem (with $T(n) = n^{\lceil k/2 \rceil}$), or the All-Pairs Shortest Paths problem (with $T(n) = n^3$ where n is the number of vertices), or one of several versions of the k -Clique problem in weighted graphs. [BRSV17] used their fine-grained-complexity problems to build cryptographic primitives, but gave a barrier for their approach: extending their approach would falsify the NSETH, which encourages us to find different hardness assumption.

Win-win Paradigm and OWFs from Average-case Harness It is commonly known that if a problem is average-case hard and it is possible to efficiently sample an input from the hard distribution along with the corresponding solution, then this implies a one-way function⁶ (OWF). OWF is usually the simplest cryptographic primitives. Ideally, we would want an assumption that leads to a win-win scenario:

- ◇ If these problems are hard then we have secure OWFs (It can securely implement many other primitives in Minicrypt);
- ◇ If not, get some breakthroughs - such as we rule out “Pessiland”, get efficient algorithms for optimal file compression, inductive reasoning, optimal Machine Learning.

On OWFs and Kolmogorov Complexity The notion of Kolmogorov complexity (K-complexity), introduced by [Sol64][Kol65][Cha69], provides an elegant method for measuring the amount of “randomness” in individual strings⁷. The notion of $t(\cdot)$ -time-bounded Kolmogorov Complexity (K^t -complexity). [Kol65][Ko86][Sip83][Har83][All01][ABK⁺06] considers a time-bounded version of this problem (MKTP). Given a string x describing a truthtable, let $K^t(x)$ denote the t -bounded Kolmogorov complexity of x -that is, the length of the shortest string Π such that for every $i \in [n]$, $U(\Pi, i) = x_i$ within time $t(|\Pi|)$, where U is a fixed Universal Turing machine. Given a threshold, $s(\cdot)$, and a polynomial time-bound, $t(\cdot)$, let $\text{MK}^t\text{P}[s]$ denote the set of strings x such that $K^t(x) \leq s(|x|)$.

6.2.3 Proposed Plan

A. Which techniques can potentially help us solve the problem?

There are many ways to define time-bounded Kolmogorov complexity. We have introduced the “local compression” version in 6.2.2. All the versions are showed in the table.

⁶A one-way function (OWF) is a function f that can be efficiently computed in polynomial time, yet no probabilistic polynomial time (PPT) algorithm can invert f with inverse polynomial probability for infinitely many input lengths n .

⁷The K-complexity of a string is the length of the shortest program (to be run on some fixed universal Turing machine U) that outputs the string x

MKTP K-complexity	$K(x) = \min M \text{ s.t. } U(M) = x$
MKtP Kt-complexity	$K(x) = \min M \text{ s.t. } U(M) = x \text{ within time } t$
MK^tP Kt-complexity	$K(x) = \min M + \log t$ $\text{s.t. } U(M) = x \text{ within time } t$
MKTP KT-complexity	$K(x) = \min M + T$ $\text{s.t. } U(M) = x \text{ within time } t$
conditional	cK, McKP
Fixed threshld	MKtP $[n/2]$

[LP20] recently showed that when the threshold $s(\cdot)$ is "large", when $s(n) = n \log n$ for some constant c , then mild average-case hardness of this language w.r.t. the uniform distribution of instances, is equivalent to the existence of OWF. [LP21a] considered a notion of mild average-case hardness, and characterized quasi-polynomial or subexponential OWF. [LP23] considered the worst-case hardness of $MK^tP[s]$ and construct OWF-complete.

Existence of OWF	[LP20]	K^t w.r.t uniform distribution $MK^tP[n-O(\log n)]$ w.r.t uniform distribution
	[LP22]	cK^t w.r.t uniform distribution cK^t is NP-complete
	[LP21b],[RS21]	Kt w.r.t uniform distribution Kt is EXP-complete
	[IRS22],[LP]	MpKpolyP is (mildly) HOA w.r.t any distribution D MpKpolyP is (mildly) HOA w.r.t uniform distribution
	[LP23]	worst-case hardness w.r.t BPP
OWF in NC^0	[RS21]	MKTP w.r.t uniform
	[ACM ⁺]	McKTP w.r.t uniform McKTP is NP-complete
	[LP21b]	using space-bounded variant
SubExp OWF	[LP21a]	MK^tP polylogn w.r.t uniform Threshold s determines OWF hardness

B. Subsequent Work

◆ Can we get exponentially-hard OWFs from $MK^tP[s]$ problems?

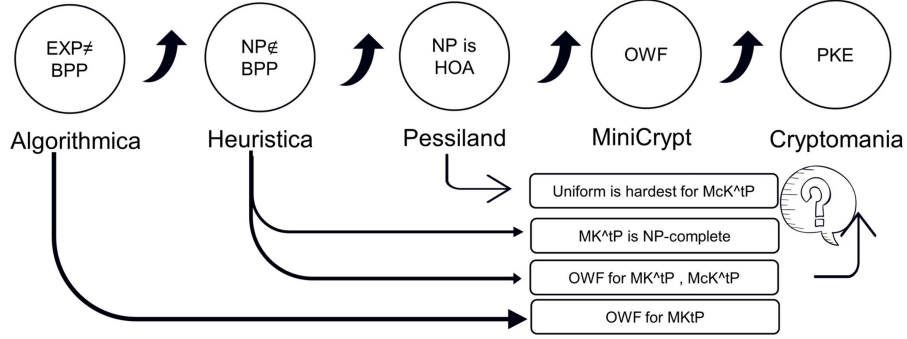
[LP21a] [LP23] all relies on a "nice" function classes, where the class of functions \mathcal{F} is said to be "nice" if: 1. for every function $T \in \mathcal{F}$, T is time-constructible and strictly increasing in the sense that there exists a constant $\nu > 0$ such that for all $n > 1$, $T(n+1) \geq T(n) + \nu$; 2. \mathcal{F} is closed under

(sublinear) polynomial compositions: for any $T \in \mathcal{F}$, for all $0 < \varepsilon_1, \varepsilon_2 < 1$, $(T(n^{\varepsilon_1}))^{\varepsilon_2} \in \mathcal{F}$.

$\mathcal{F}_{\text{subexp}} = \{2^{cn^\varepsilon}\}_{c>0, 0<\varepsilon<1}$ and $\mathcal{F}_{\text{poly}} = \{n^{c \log n}\}_{c>0}$ are considered as "nice" classes. They rely on this notion so as to capture classes of "polynomially-related" functions.⁸

However, characterizing the exponentially secure OWF is out of "nice" classes, and all theorems in their works would lose efficacy. We need to find another notion to show the relationship between $\text{MK}^t\text{P[s]}$.

♦ Can we construct PKE and NIZK from worst-case hardness of $\text{MK}^t\text{P[s]}$ problems?



We believe that there are various primitives in Cryptomania based on the hardness of Kolmogorov complexity problems. The key is to restrict attention to an appropriate analog of computational depth. Our goal is to find its application in Cryptomania, such as PKE and NIZK, which is similar to our discussion in fine-grained setting.

♦ Can we get a characterization w.r.t a single (non-meta) problem?

Briefly recall the high-level approach firstly used in [LP20]: An object called an entropy-preserving pseudorandom generator (EP-PRG) was introduced. Roughly speaking, an EP-PRG is a pseudorandom generator that expands n -bits to $n + O(\log n)$ bits, having the property that the output of the PRG is not only pseudorandom, but also preserves the entropy of the input (i.e., the seed): The Shannon-entropy of the output is $n - O(\log n)$. [LP20] [LP21a] constructed a relaxed form of an EP-PRG, called a conditionally secure entropy-preserving PRG (cond-EP PRG), and showed how such a cond EP-PRG can be constructed

⁸Almost all the reductions (considered in their works) are of form "if A is $T(n)$ -hard, B is $(T(n^{\Omega(1)})^{\Omega(1)} / n^{O(1)} - n^{O(1)})$ -hard".

from OWFs, and next showed that the existence of cond EP-PRGs implies that $\text{MK}^t\text{P}[n - O(\log n)]$ is mildly HoA.

The key obstacle is that their works relies on the security of a primitive *cond EP-PRF* for which it is hard to check if an attacker manages to break its security. [LP23] deals with this obstacle without non-uniform advice, but still relies on cond EP-PRF.(not only $\text{MK}^t\text{P}[s]$)

Meta-complexing problem means that we need a family of problems to characterize a primitive. Our goal is to get a characterization w.r.t a single (non-meta) problem, and design a totally different proof system.

7 Broader Impact

Crypto vs Complexity Achievements in cryptography theory often hinge upon captivating contributions in the realm of complexity, such as the ground-breaking work by the work [AIK06] that led to the development of circuit-bound-setting cryptography. Attaining success in this field requires a combination of luck and diligent effort. To further enhance my understanding, I aim to delve deeper into the vast array of works related to complexity theory (FOCS, STOC, SODA, CCC) as well as Cryptography (EuroCrypt, Crypto, AsiaCrypt).

Conjunction Use The fine-grained and Kolmogorov primitives can be used in conjunction with other primitives that are secure against many versions of adversaries under different assumptions; this would result in hybrids that are secure against polynomial-time adversaries under these stronger assumptions while also being secure against bounded adversaries under weaker assumptions. Our hope is that we can trade a small loss of efficiency for a big improvement in security.

Ephemeral security Primitives with limited security guarantees is best suited for applications that do not need additional security. One application scenario is cellular mobile communication, where the system is considered secure as long as an adversary cannot crack the encryption within a limited time and communication overhead. Another scenario is the stock market, where various pieces of information exist only for a few seconds. Any adversary who spends too much time disrupting these primitives will only obtain information that has already lost its value. In such situation, security is transient and only needs to be maintained for a short period of time.

Potential Risks

While Kolmogorov complexity and fine-grained complexity provide a method to measure the complexity of information, they are not complete. In future research, it is necessary to thoroughly evaluate their applicability and limitations. Currently, the primitives obtained in this field are highly secure but have complex constructions and low practicality. We need to further optimize

performance while ensuring security.

References

- [ABK⁺06] Eric Allender, Harry Buhrman, Michal Koucký, Dieter Van Melkebeek, and Detlef Ronneburger. Power from random strings. *SIAM Journal on Computing*, 35(6):1467–1493, 2006.
- [ACM⁺] Eric Allender, Mahdi Cheraghchi, Dimitrios Myrisiotis, Harsha Tirumala, and Ilya Volkovich. One-way functions and a conditional variant of mkt_p. In *41st IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2021)*.
- [AIK06] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in nc^0 . *SIAM Journal on Computing*, 36(4):845–888, 2006.
- [Ajt83] Miklós Ajtai. \sum_1^1 -formulae on finite structures. *Annals of pure and applied logic*, 24(1):1–48, 1983.
- [All01] Eric Allender. When worlds collide: Derandomization, lower bounds, and kolmogorov complexity. In *FST TCS 2001: Foundations of Software Technology and Theoretical Computer Science: 21st Conference Bangalore, India, December 13–15, 2001 Proceedings 21*, pages 1–15. Springer, 2001.
- [BABB21] Enric Boix-Adserà, Matthew Brennan, and Guy Bresler. The average-case complexity of counting cliques in erdos-rewy hypergraphs. *SIAM Journal on Computing*, (0):FOCS19–39, 2021.
- [Bar86] David A Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in nc . In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 1–5, 1986.
- [BDSK20] Marshall Ball, Dana Dachman-Soled, and Mukul Kulkarni. New techniques for zero-knowledge: leveraging inefficient provers to reduce assumptions, interaction, and trust. In *Annual International Cryptology Conference*, pages 674–703. Springer, 2020.
- [BGI08] Eli Biham, Yaron J Goren, and Yuval Ishai. Basing weak public-key cryptography on strong one-way functions. In *Theory of Cryptography: Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19–21, 2008. Proceedings 5*, pages 55–72. Springer, 2008.
- [Bra08] Mark Braverman. Polylogarithmic independence fools ac^0 circuits. *Journal of the ACM (JACM)*, 57(5):1–10, 2008.

- [BRSV17] Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. Average-case fine-grained hardness. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 483–496, 2017.
- [BRSV18] Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. Proofs of work from worst-case assumptions. In *Advances in Cryptology—CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I 38*, pages 789–819. Springer, 2018.
- [CG18] Matteo Campanelli and Rosario Gennaro. Fine-grained secure computation. In *Theory of Cryptography Conference*, pages 66–97. Springer, 2018.
- [Cha69] Gregory J Chaitin. On the simplicity and speed of programs for computing infinite sets of natural numbers. *Journal of the ACM (JACM)*, 16(3):407–422, 1969.
- [CM97] Christian Cachin and Ueli Maurer. Unconditional security against memory-bounded adversaries. In *Annual International Cryptology Conference*, pages 292–306. Springer, 1997.
- [DLW20] Mina Dalirrooyfard, Andrea Lincoln, and Virginia Vassilevska Williams. New techniques for proving fine-grained average-case hardness. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 774–785. IEEE, 2020.
- [DVV16] Akshay Degwekar, Vinod Vaikuntanathan, and Prashant Nalini Vasudevan. Fine-grained cryptography. In *Annual International Cryptology Conference*, pages 533–562. Springer, 2016.
- [EWT21] Shohei Egashira, Yuyu Wang, and Keisuke Tanaka. Fine-grained cryptography revisited. *Journal of Cryptology*, 34(3):23, 2021.
- [FSS81] Merrick Furst, James B Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. In *Proceedings of the 22nd Annual Symposium on Foundations of Computer Science*, pages 260–270, 1981.
- [GOS12] Jens Groth, Rafail Ostrovsky, and Amit Sahai. New techniques for noninteractive zero-knowledge. *Journal of the ACM (JACM)*, 59(3):1–35, 2012.
- [GR18] Oded Goldreich and Guy Rothblum. Counting t-cliques: Worst-case to average-case reductions and direct interactive proof systems. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 77–88. IEEE, 2018.

- [Har83] Juris Hartmanis. Generalized kolmogorov complexity and the structure of feasible computations. In *24th Annual Symposium on Foundations of Computer Science (sfcs 1983)*, pages 439–445. IEEE, 1983.
- [Has87] Johan Hastad. One-way permutations in nc^0 . *Information Processing Letters*, 26(3):153–155, 1987.
- [IK00] Yuval Ishai and Eyal Kushilevitz. Randomizing polynomials: A new representation with applications to round-efficient secure computation. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 294–304. IEEE, 2000.
- [IRS22] Rahul Ilango, Hanlin Ren, and Rahul Santhanam. Robustness of average-case meta-complexity via pseudorandomness. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1575–1583, 2022.
- [Ko86] Ker-I Ko. On the notion of infinite pseudorandom sequences. *Theoretical Computer Science*, 48:9–33, 1986.
- [Kol65] Andrei N Kolmogorov. Three approaches to the quantitative definition of information'. *Problems of information transmission*, 1(1):1–7, 1965.
- [LLVW19] Rio LaVigne, Andrea Lincoln, and Virginia Vassilevska Williams. Public-key cryptography in the fine-grained setting. In *Annual International Cryptology Conference*, pages 605–635. Springer, 2019.
- [LP] Yanyi Liu and Rafael Pass. One-way functions and the hardness of (probabilistic) time-bounded kolmogorov complexity w.r.t. samplable distributions. In *Advances in Cryptology – CRYPTO 2023*, pages 645–673.
- [LP20] Yanyi Liu and Rafael Pass. On one-way functions and kolmogorov complexity. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1243–1254. IEEE, 2020.
- [LP21a] Yanyi Liu and Rafael Pass. Cryptography from sublinear-time average-case hardness of time-bounded kolmogorov complexity. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 722–735, 2021.
- [LP21b] Yanyi Liu and Rafael Pass. On the possibility of basing cryptography on $\text{exp} \neq \text{bpp}$. In *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, Virtual Event, August 16–20, 2021, Proceedings, Part I 41*, pages 11–40. Springer, 2021.
- [LP22] Yanyi Liu and Rafael Pass. On one-way functions from np-complete problems. *Cryptology ePrint Archive*, 2022.

- [LP23] Yanyi Liu and Rafael Pass. On one-way functions and the worst-case hardness of time-bounded kolmogorov complexity. *Cryptology ePrint Archive*, 2023.
- [Mer78] Ralph C Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21(4):294–299, 1978.
- [Ràf15] Carla Ràfols. Stretching groth-sahai: Nizk proofs of partial satisfiability. In *Theory of Cryptography: 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part II 12*, pages 247–276. Springer, 2015.
- [Raz87] Alexander A Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987.
- [RS21] Hanlin Ren and Rahul Santhanam. Hardness of kt characterizes parallel cryptography. *Cryptology ePrint Archive*, 2021.
- [SD23] Quan Shi and Kaiyuan Deng. Privacy-preserving detection method for transmission line based on edge collaboration, 2023.
- [SGSC23] Y. Sun, Z. Gong, Quan Shi, and L. Chen. Efficient commercial bank customer credit risk assessment based on lightgbm and feature engineering, 2023.
- [Sho94] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.
- [Sip83] Michael Sipser. A complexity theoretic approach to randomness. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, pages 330–335, 1983.
- [Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 77–82, 1987.
- [Sol64] RJ Solmonoff. A formal theory of inductive inference. i. *II Information and Control*, 7:224–254, 1964.
- [VW15] Virginia Vassilevska Williams. Hardness of easy problems: Basing hardness on popular conjectures such as the strong exponential time hypothesis (invited talk). In *10th International Symposium on Parameterized and Exact Computation (IPEC 2015)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2015.
- [WP22a] Yuyu Wang and Jiaxin Pan. Non-interactive zero-knowledge proofs with fine-grained security. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 305–335. Springer, 2022.

- [WP22b] Yuyu Wang and Jiaxin Pan. Unconditionally secure nizk in the fine-grained setting. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 437–465. Springer, 2022.
- [WPC23] Yuyu Wang, Jiaxin Pan, and Yu Chen. Fine-grained secure attribute-based encryption. *Journal of Cryptology*, 36(4):33, 2023.