Bit Security of the CDH Problems over Finite Fields

Mingqiang Wang[1], Tao Zhan[1], and Haibin Zhang[2]

[1]School of Mathematics, Shandong University
wangmingqiang@sdu.edu.cn, zhantao@moe.edu.cn
[2]Department of Computer Science, University of North Carolina, Chapel Hill
haibin@cs.unc.edu

Abstract

It is a long-standing open problem to prove the existence of (deterministic) hard-core predicates for the Computational Diffie-Hellman (CDH) problem over finite fields, without resorting to the *generic* approaches for any one-way functions (*e.g.,* the Goldreich-Levin hard-core predicates). Fazio *et al.* (FGPS, Crypto '13) make important progress on this problem by defining a *weaker* Computational Diffie-Hellman problem over $\mathbb{F}_{p^2}$, *i.e.,* Partial-CDH problem, and proving, when allowing changing field representations, the unpredictability of every single bit of one of the coordinates of the secret Diffie-Hellman value. In this paper, we show that *all* the individual bits of the CDH problem over $\mathbb{F}_{p^2}$ and *almost all* the individual bits of the CDH problem over $\mathbb{F}_{p^t}$ for $t > 2$ are hard-core.

Key words: CDH, Diffie-Hellman problem, d-th CDH problem, finite fields, hard-core bits, list decoding, multiplication code, noisy oracle, Partial-CDH problem.

1 Introduction

Hard-core predicates [4, 13] are central to cryptography. Of particular interest is the hard-core predicate for the CDH problem, which is essential to establishing the security for Diffie-Hellman (DH) key exchange protocol [7] and ElGamal encryption scheme [9] without having to make a (potentially) much stronger DH assumption—the Decisional Diffie-Hellman (DDH) assumption.

However, despite the generic approaches for *randomized* predicates working for any computationally hard problems [12, 17], showing the existence of *deterministic* and *specific* hard-core predicates for the CDH problem over *finite fields* has proven elusive. This is in contrast to other conjectured hard problems such as discrete logs, RSA, and Rabin, whose deterministic hard-core predicates were discovered roughly three decades ago [2, 4]. Recently, Fazio, Gennaro, Perera, and Skeith III (FGPS) [10] made a significant breakthrough by introducing a relaxed variant of the CDH problem over finite fields $\mathbb{F}_{p^2}$, *i.e.,* the Partial-CDH problem and proving the unpredictability for a large class of predicates.

Partial-CDH problem. Given a prime p, there are many different fields $\mathbb{F}_{p^2}$ which are all isomorphic to each other. Let $h(x) = x^2 + h_1x + h_0$ be a monic irreducible polynomial of degree 2 in $\mathbb{F}_p$. We know that $\mathbb{F}_{p^2}$ is isomorphic to the field $\mathbb{F}_p[x]/(h)$, where $(h(x))$ is a principal ideal in the polynomial ring $\mathbb{F}_p[x]$ and elements of $\mathbb{F}_{p^2}$ can be written as linear polynomials. Namely, if $g \in \mathbb{F}_{p^2}$ then $g = g_1x + g_0$

and addition and multiplication are performed as polynomial operations modulo h. Given $g \in \mathbb{F}_{p^2}$ we denote by $[g]_i$ the coefficient of the degree-i term.

Let g denote a random generator of the multiplicative group of $\mathbb{F}_{p^2}$. FGPS defined the following Partial-CDH problem over $\mathbb{F}_{p^2}$ [10]: the Partial-CDH problem is hard over $\mathbb{F}_{p^2}$ if given random inputs $g, A = g^a, B = g^b \in \mathbb{F}_{p^2}$, it is computationally hard to output $K = [g^{ab}]_1 \in \mathbb{F}_p$ (*i.e.,* the coefficient of the degree 1 term of g^{ab}), for any representation of $\mathbb{F}_{p^2}$.

Assuming the hardness of the Partial-CDH problem, FGPS developed the idea of randomizing the problem representation originally suggested by Boneh and Shparlinski [5] and proved a large class of hard-core predicates over a *random representation* of the finite field $\mathbb{F}_{p^2}$. Namely, given an oracle that predicts any bit of $K = \left[g^{ab}\right]_1$ over a random representation of $\mathbb{F}_{p^2}$ with non-negligible advantage, one can recover K with non-negligible probability.

However, the Partial-CDH problem is clearly weaker than the regular CDH problem. Given a CDH oracle, one can easily solve the Partial-CDH problem. Note that the reason why we need hard-core predicates is exactly that we do not want to make stronger assumptions. Without characterizing the hardness of the Partial-CDH problem, the FGPS result can hardly be based on a firm foundation. Thus, studying the hardness of the Partial-CDH problem is left by FGPS as an important open problem [10, Section 6].

The d-th CDH problems. It is natural to generalize the Partial-CDH problem over $\mathbb{F}_{p^2}$ to define the d-th CDH problems over $\mathbb{F}_{p^t}$ for $t > 1$ (history and related work coming shortly). For a prime p and an integer $t > 1$, there are many different fields $\mathbb{F}_{p^t}$, but they are all isomorphic to each other. Let $h(x)$ be a monic irreducible polynomial of degree t in $\mathbb{F}_p$. It is well known that $\mathbb{F}_{p^t}$ is isomorphic to the field $\mathbb{F}_p[x]/(h)$, where $(h(x))$ is a principal ideal in the polynomial ring $\mathbb{F}_p[x]$ and elements of $\mathbb{F}_{p^t}$ can be written as polynomials of degree $t-1$. Namely, if $g \in \mathbb{F}_{p^t}$ then $g = g_{t-1}x^{t-1} + g_{t-2}x^{t-2} + \cdots + g_1 x + g_0$. Addition and multiplication of the elements in $\mathbb{F}_{p^t}$ are performed as polynomial operations modulo h. In the following, given $g \in \mathbb{F}_{p^t}$ we denote by $[g]_i$ the coefficient of the degree-i term, *i.e.,* $g_i = [g]_i$.

Let g be a random generator of the multiplicative group of $\mathbb{F}_{p^t}$ and d be an integer such that $0 \leq d \leq t-1$. Informally we say that the d-th CDH problem is hard in $\mathbb{F}_{p^t}$ if given $g, g^a, g^b \in \mathbb{F}_{p^t}$, it is computationally hard to compute $[g^{ab}]_d$, for any representations of $\mathbb{F}_{p^t}$.

Prior work on hardness of d-th CDH problems: Not yet perfect. FGPS and an earlier version of this paper did not realize (until very recently) that the hardness of d-th CDH problem has already been studied in [18, 20]. Verheul [20, Theorem 21] showed that given a *perfect* d-th CDH problem oracle (which always returns correct answers), one can solve the CDH problem over the same fields. Concretely, given a CDH instance $(g^x, g^y) \in (\mathbb{F}_{p^t})^2$, Verheul's algorithm needs to run the d-th CDH problem oracle on $(g^x, g^y \cdot g^r)$ for at least $poly(t)$ times, with the same g^x and g^y, yet uniformly chosen $r \xleftarrow{\$} \mathbb{Z}_{p^t-1}$. For some d, say, $d = \lceil t/2 \rceil$, Verheul's algorithm even has to run the d-th CDH oracle for at least 2^t times. Shparlinski [18] generalizes Verheul's result to handle the case of *noisy* oracles (which return correct answers with some probabilities). Shpalinski's reduction uses the same strategy to limit the behavior of the oracle. We note that a malicious d-th CDH problem oracle (adversary) may simply always return incorrect answers for any query of the form $(X, \cdot)$, if it has previously been given a query with the same X. Hence, Shparlinski's reduction is slightly problematic in the sense it failed to prove what's claimed.

1.1 Our Contributions

In this paper, we show that *all* the individual bits of the CDH problem over $\mathbb{F}_{p^2}$ and *almost all* the individual bits of the CDH problem over $\mathbb{F}_{p^t}$ for $t > 2$ are hard-core. Let's explain our main

contributions in a bit more detail.

THE HARDNESS OF d-TH CDH PROBLEM. In order to characterize the hardness of d-th CDH problem, we consider a case of noisy oracles which is more general than those of Verheul [20] and Shparlinski [18]. In our model, to compute the secret CDH value, we just require that the d-th CDH oracle return correct answers at some probability. Given a CDH instance $(g^x, g^y) \in (\mathbb{F}_{p^t})^2$, we need to run the d-th CDH oracle on inputs $(g^x \cdot g^r, g^y \cdot g^s)$ with uniformly chosen r and s. The analysis for general t turns out to take some work. With this model, we show that the 1-th CDH problem (i.e., the Partial-CDH problem) and 0-th CDH problem (which we call Dual-Partial-CDH problem) over finite fields $\mathbb{F}_{p^2}$ are strictly as hard as the regular CDH problem over the same fields. Regarding general extension fields, we are able to prove that all the d-th CDH problems over a random representation of finite fields $\mathbb{F}_{p^t}$ (with $t > 1$) are as hard as the regular CDH problem over the same fields; in particular, the 0-th CDH problem and $(t-1)$-th CDH problem given *any* field representation are as hard as the CDH problem. We comment that applying our approach to the case of perfect oracles, our reduction leads to no security loss, which is in contrast to Verheul's, where for many d's, the algorithm can easily have exponential running time in t.

THE CASE OF $\mathbb{F}_{p^2}$. At the heart of the FGPS result is the *list decoding* approach for hard-core predicates, which was developed by Akavia, Goldwasser and Safra [1], and extended by Morillo and Ràfols [16] and Duc and Jetchev [8]. Up to now, the list decoding approach has only been proven successful for multiplicative codes [1, 8, 16]. It is unclear if the approach can work more generally. In this paper, we will work *directly* on a non-multiplicative code. *Still* assuming the hardness of the Partial-CDH problem, we are able to prove the unpredictability of every single bit of the *other* coordinate (*i.e.,* the coefficient of the lower degree term) of the secret CDH value, by using a careful analysis of the Fourier coefficients of the function. To the best of our knowledge, this is the first positive result that list decoding approach can be applied to a non-multiplicative code, a result of independent interest.

Combining all the above-mentioned results, we are able to prove our main result for the regular CDH problem over $\mathbb{F}_{p^2}$: given an oracle $\mathcal{O}$ that predicts *any* bit of the CDH value over a random representation of the field $\mathbb{F}_{p^2}$ with non-negligible advantage, we can solve the *regular* CDH problem over $\mathbb{F}_{p^2}$ with non-negligible probability.

THE CASE OF $\mathbb{F}_{p^t}$. We go on to prove that assuming the hardness of the d-th CDH problem, every single bit of the d-th CDH coordinate for $d \neq 0$ is hard-to-compute. FGPS [10, Section 6] found that their technique was not powerful enough to solve the generalized problem. To overcome the difficulty, we identify a *general* yet *simplified* class of isomorphisms. The isomorphisms identified generalize that of finite field $\mathbb{F}_{p^2}$ in FGPS to the case of general finite fields $\mathbb{F}_{p^t}$ for any $t > 1$. More importantly, they simplify that of FGPS by adopting a more restrictive class of isomorphisms. We comment that it is the simplicity that is essential to overcoming the original technical difficulty and establishing the bit security for general finite fields. To achieve this result, we also use another idea of Boneh and Shparlinski [5] using d-th residues modulo p.

Together with the equivalence result between all the d-th CDH problems over $\mathbb{F}_{p^t}$ (with $t > 1$) and the regular CDH problem, we obtain another main result of the paper: all bits except the bits of the degree-0 term of the usual CDH problem over a random representation of the finite field $\mathbb{F}_{p^t}$ are hard-core.

2 Preliminaries

2.1 Notation

We use the standard symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ to denote the natural numbers, the integers, the real numbers and the complex numbers, respectively. Let $\mathbb{Z}_+$ and $\mathbb{R}_+$ stand for the positive integers and reals, respectively. A function $\nu(l)\colon \mathbb{N} \to \mathbb{R}$ is *negligible* if for every constant $c \in \mathbb{R}_+$ there exists $l_c \in \mathbb{N}$ such that $\nu(l) < l^{-c}$ for all $l > l_c$. A function $\rho(l)\colon \mathbb{N} \to \mathbb{R}$ is *non-negligible* if there exists a constant $c \in \mathbb{R}_+$ and $l_c \in \mathbb{N}$ such that $\rho(l) > l^{-c}$ for all $l > l_c$. For a Boolean function $f\colon \mathcal{D} \to \{\pm 1\}$ over an arbitrary domain $\mathcal{D}$, denote by $\mathsf{maj}_f = \mathsf{max}_{\{b=\pm 1\}} \Pr_{\alpha \in \mathcal{D}}[f(\alpha) = b]$ the *bias* of f toward its majority value.

2.2 Fourier Transform

Let $\mathbb{G}$ be a finite abelian group. For any two functions $f, g\colon \mathbb{G} \to \mathbb{C}$, their *inner product* is defined as $\langle f, g\rangle = 1/|\mathbb{G}| \sum_{x \in \mathbb{G}} \overline{f(x)} g(x)$. The l_2-norm of f on the vector space $\mathbb{C}(\mathbb{G})$ is defined as $\|f\|_2 = \sqrt{\langle f, f\rangle}$. A *character* of $\mathbb{G}$ is a homomorphism $\chi\colon \mathbb{G} \to \mathbb{C}^*$, *i.e.,* $\chi(x+y) = \chi(x)\chi(y)$ for all $x, y \in \mathbb{G}$. The set of all characters of $\mathbb{G}$ forms a *character group* $\widehat{\mathbb{G}}$, whose elements form an orthogonal basis (the *Fourier basis*) for the vector space $\mathbb{C}(\mathbb{G})$. One can then describe any function $f \in \mathbb{C}(\mathbb{G})$ via its *Fourier expansion* $\sum_{\chi \in \widehat{\mathbb{G}}} \widehat{f}(\chi)\chi$, where $\widehat{f}\colon \widehat{\mathbb{G}} \to \mathbb{C}$ is the *Fourier transform* of f and we have $\widehat{f}(\chi) = \langle f, \chi\rangle$. The coefficients $\widehat{f}(\chi)$ in the Fourier basis $\{\chi\}_{\chi \in \widehat{\mathbb{G}}}$ are the *Fourier coefficients* of f. The *weight* of a Fourier coefficient is denoted by $|\widehat{f}(\chi)|^2$. When $\mathbb{G} = \mathbb{Z}_n$ (*i.e.,* the additive group of integers modulo n) and $\widehat{\mathbb{G}} = \widehat{\mathbb{Z}}_n$, for each $\alpha \in \mathbb{Z}_n$, the α-character is defined as a function $\chi_\alpha\colon \mathbb{Z}_n \to \mathbb{C}$ such that $\chi_\alpha(x) = \omega_n^{\alpha x}$, where $\omega_n = e^{2\pi i/n}$. If Γ is a subset of $\mathbb{Z}_n$ then it is natural to consider the projection of f in set Γ, *i.e.,* $f_{|\Gamma} = \sum_{\alpha \in \Gamma} \widehat{f}(\alpha)\chi_\alpha$, where $\widehat{f}(\alpha) = \langle f, \chi_\alpha\rangle$. Since the characters are orthogonal, we have $\|f\|_2^2 = \sum_{\alpha \in \mathbb{Z}_n} |\widehat{f}(\alpha)|^2$ and $\|f_{|\Gamma}\|_2^2 = \sum_{\alpha \in \Gamma} |\widehat{f}(\alpha)|^2$.

Definition 1 (Fourier concentrated function [1]). *A function $f\colon \mathbb{Z}_n \to \mathbb{C}$ is Fourier ϵ-concentrated if there exists a set $\Gamma \subseteq \mathbb{Z}_n$ consisting of poly$(\log n, 1/\epsilon)$ characters, so that*

$$\|f - f_{|\Gamma}\|_2^2 = \sum_{\alpha \notin \Gamma} |\widehat{f}(\alpha)|^2 \leq \epsilon.$$

A function f is called Fourier concentrated if it is Fourier ϵ-concentrated for every $\epsilon > 0$.

Definition 2 (τ-heavy characters [1]). *Given a threshold $\tau > 0$ and an arbitrary function $f\colon \mathbb{Z}_n \to \mathbb{C}$, we say that a character $\chi_\alpha \in \mathsf{Heavy}_\tau(f)$ is τ-heavy if the weight of its corresponding Fourier coefficient is at least τ. The set of all heavy characters is denoted by*

$$\mathsf{Heavy}_\tau(f) = \{\chi_\alpha\colon |\widehat{f}(\alpha)|^2 \geq \tau\}.$$

2.3 Error Correcting Codes: Definitions and Properties

Error correcting codes can encode messages into codewords by adding redundant data such that it can be recovered even in the presence of noise. The code to be discussed here encodes each element $\alpha \in \mathbb{Z}_n$ into a codeword C_α of length n. Each codeword C_α can be represented by a function $C_\alpha\colon \mathbb{Z}_n \to \{\pm 1\}$. We now recall a number of definitions and lemmata [1, 8] about codes over $\mathbb{Z}_n$.

Definition 3 (Fourier concentrated code). *A code $\mathcal{C} = \{C_\alpha : \mathbb{Z}_n \to \{\pm 1\}\}$ is concentrated if each of its codewords C_α is Fourier concentrated.*

Definition 4 (Recoverable code). *A code $\mathcal{C} = \{C_\alpha : \mathbb{Z}_n \to \{\pm 1\}\}$ is recoverable, if there exists a recovery algorithm that, given a character $\chi \in \widehat{\mathbb{Z}}_n$ and a threshold τ, returns in time poly$(\log n, 1/\tau)$ a list of all elements α associated with codewords C_α for which χ is a τ-heavy coefficient (i.e., $\{\alpha \in \mathbb{Z}_n : \chi \in \mathsf{Heavy}_\tau(C_\alpha)\}$).*

Lemma 1 below shows that in a concentrated code $\mathcal{C}$, any corrupted ("noisy") version $\widetilde{C}_\alpha$ of codeword C_α share at least one heavy coefficient with C_α. Lemma 2 shows that when given query access to any function f one can efficiently learn all its heavy characters.

Lemma 1 ([1, Lemma 1]). *Let $f, g : \mathbb{Z}_n \to \{\pm 1\}$ such that f is concentrated and for some $\epsilon > 0$,*

$$\Pr_{\alpha \in \mathbb{Z}_n}[f(\alpha) = g(\alpha)] \geq \mathsf{maj}_f + \epsilon.$$

There exists a threshold τ such that $1/\tau \in poly(1/\epsilon, \log n)$, and there exists a non-trivial character $\chi \neq 0$ heavy for f and g: $\chi \in \mathsf{Heavy}_\tau(f) \cap \mathsf{Heavy}_\tau(g)$.

Lemma 2 ([1, Theorem 6]). *There is a probabilistic algorithm that, given query access to $w : \mathbb{Z}_n \to \{\pm 1\}$, $\tau > 0$ and $0 < \delta < 1$, outputs a list L of $O(1/\tau)$ characters containing $\mathsf{Heavy}_\tau(w)$ with probability at least $1 - \delta$, whose running time is $\widetilde{O}\left(\log(n) \cdot \ln^2 \frac{(1/\delta)}{\tau^{5.5}}\right)$.*

2.4 Review of List Decoding Approach for Hard-Core Predicates

Informally, a cryptographic one-way function $f : \mathcal{D} \to \mathcal{R}$ is a function which is easy to compute but hard to invert. Given a one-way function f and a predicate π, we say π is hard-core if there is an efficient probabilistic polynomial-time (PPT) algorithm that given $\alpha \in \mathcal{D}$ computes $\pi(\alpha)$, but there is no PPT algorithm $\mathcal{A}$ that given $f(\alpha) \in \mathcal{R}$ predicts $\pi(\alpha)$ with probability $\mathsf{maj}_\pi + \epsilon$ for a non-negligible ϵ.

Goldreich and Levin [12] showed hard-core predicates for general one-way functions by providing a general list decoding algorithm for Hadamard code. Akavia, Goldwasser, and Safra (AGS) [1] formalized the list decoding methodology and applied it to a broad family of conjectured one-way functions. In particular, they proved the unpredictability of *segment predicates* [1] for any one-way function f with the following *homomorphic* property: given $f(\alpha)$ and λ, one can efficiently compute $f(\lambda\alpha)$. This includes discrete logarithms in finite fields and elliptic curves, RSA, and Rabin. Morillo and Ràfols [16] extended the AGS result to prove the unpredictability of every individual bit for these functions. Duc and Jetchev [8] showed how to extend to elliptic curve-based one-way functions which do not necessarily enjoy the homomorphic property. Their result instead requires introducing a random description of the curve, an idea originally developed by Boneh and Shparlinski [5]. In their paper, Boneh and Shparlinski proved for the elliptic curve Diffie-Hellman problem that the least significant bit of each coordinate of the secret CDH value is hard-core over a random representation of the curve. Recently, FGPS extended the Boneh and Shparlinski idea to prove every individual bit (not merely the least significant bit) of the elliptic curve Diffie-Hellman problem is hard-core. By extending the same idea to the case of finite fields $\mathbb{F}_{p^2}$, FGPS also proved for a weak CDH problem (*i.e.* Partial-CDH problem) the unpredictability of every single bit of one of the coordinates of the secret CDH value.

LIST DECODING APPROACH OVERVIEW. Given a one-way function $f\colon \mathcal{D} \to \mathcal{R}$ and a predicate π, one would have to identify an error-correcting code $\mathcal{C}^\pi = \{C_\alpha\colon \mathcal{D} \to \{\pm 1\}\}_{\alpha\in\mathcal{D}}$ such that every input α of the one-way function is associated with a codeword C_α. The code needs to satisfy the following properties:

(1) *Accessibility.* One should be able to obtain a corrupted ("noisy") version $\widetilde{C}_\alpha$ of the original codeword C_α. Such a corrupted codeword must be close to the original codeword, *i.e.,* $\Pr_\lambda[C_\alpha(\lambda) = \widetilde{C}_\alpha(\lambda)] > \mathsf{maj}_\pi + \epsilon$ for a non-negligible ϵ.

(2) *Concentration.* Each codeword C_α should be a Fourier concentrated function, *i.e.,* each codeword can be approximated by a small number of heavy coefficients in the Fourier representation.

(3) *Recoverability.* There exists a $poly(\log n, \tau^{-1})$ algorithm that on input a Fourier character χ and a threshold τ outputs a short list L_χ which contains all the values $\alpha \in \mathcal{D}$ such that χ is τ-heavy for the codeword C_α.

We now show how to invert $y = f(\alpha)$ with the prediction oracle Ω. Querying Ω will allow one to have access to a corrupted codeword $\widetilde{C}_\alpha$ that is close to C_α. According to Lemma 1, we know that there should exist a threshold τ and at least one Fourier character that is τ-heavy for both $\widetilde{C}_\alpha$ and C_α. Applying the learning algorithm in Lemma 2, we can find the set of all τ-heavy characters for $\widetilde{C}_\alpha$. Due to the recovery property, we are able to produce for each heavy character a polynomial size list containing possible α. Note that one can identify the correct α since f is efficiently computable.

LIST DECODING VIA MULTIPLICATION CODE. The crux of list decoding approach is to identify the "right" code which is accessible, concentrated, and recoverable. To this end, AGS and subsequent work either define a multiplication code, or transform the original code to an equivalent multiplication code. (Such a multiplication code is of the form $C_\alpha(\lambda) = \pi(\lambda\alpha)$.) Indeed, as argued in [1, 8], this is at the basis of their proofs: multiplication codes can be proven to satisfy concentration and recoverability.

In Section 3, we will directly work on a code that is *not* multiplicative. Not surprisingly, this makes it hard to prove code concentration and recoverability. To our knowledge, we are the first to apply the list decoding approach to the case of a non-multiplicative code.

3 All Bits Security of the CDH Problems over $\mathbb{F}_{p^2}$

In this section, we show the following three results: (1) we show that over finite fields $\mathbb{F}_{p^2}$ the Partial-CDH problem [10] is as hard as the regular CDH problem. (2) assuming the hardness of the Partial-CDH problem over $\mathbb{F}_{p^2}$, we prove the unpredictability of every single bit of the *other* coordinate of the secret CDH value; (3) we go on to prove the unpredictability of *every* single bit of the secret CDH value for the regular CDH problem over $\mathbb{F}_{p^2}$.

THE PARTIAL-CDH ASSUMPTION IS EQUIVALENT TO THE CDH ASSUMPTION OVER $\mathbb{F}_{p^2}$. Throughout the paper we fix a security parameter l. We consider an instance generator $\mathcal{G}$ which takes as input 1^l and outputs an l-bit prime p. Let g be a random generator of the multiplicative group of $\mathbb{F}_{p^2}$. The Partial-CDH problem over $\mathbb{F}_{p^2}$ is a relaxed variant of the conventional CDH problem over $\mathbb{F}_{p^2}$, which we formally state as follows:

Assumption 1 (The CDH assumption over $\mathbb{F}_{p^2}$). *We say that the CDH problem is hard in $\mathbb{F}_{p^2}$ if for any PPT adversary $\mathcal{A}$, his CDH advantage*

$$\mathbf{Adv}^{\mathrm{cdh}}_{\mathcal{A},\mathbb{F}_{p^2}} \coloneqq \Pr\left[\mathcal{A}(p, g, g^a, g^b) = g^{ab} \middle| p \xleftarrow{\$} \mathcal{G}(1^l); a, b \xleftarrow{\$} \{1, \cdots, p^2 - 1\}\right]$$

is negligible in l.

Let $I_2(p)$ be the set of monic irreducible polynomials of degree 2 in $\mathbb{F}_p$. Informally we say that the *Partial-CDH* problem [10] is hard in $\mathbb{F}_{p^2}$ if for all $h \in I_2(p)$ no efficient algorithm given $g, A = g^a, B = g^b \in \mathbb{F}_{p^2}$ can output $\left[g^{ab}\right]_1 \in \mathbb{F}_p$. Formally we consider the following assumption:

Assumption 2 (The Partial-CDH assumption over $\mathbb{F}_{p^2}$ [10]). *We say that the Partial-CDH problem is hard in $\mathbb{F}_{p^2}$ if for any PPT adversary $\mathcal{A}$, his Partial-CDH advantage for all $h \in I_2(p)$*

$$\mathbf{Adv}^{\mathrm{pcdh}}_{\mathcal{A},h,\mathbb{F}_{p^2}} := \Pr\left[\mathcal{A}(p,h,g,g^a,g^b) = \left[g^{ab}\right]_1 \middle| p \xleftarrow{\$} \mathcal{G}(1^l); a,b \xleftarrow{\$} \left\{1,\cdots,p^2-1\right\}\right]$$

is negligible in l.

It is easy to see that the Partial-CDH problem is weaker than the regular CDH problem over $\mathbb{F}_{p^2}$. The following theorem shows in the case of noisy oracles, the regular CDH problem can be also reduced to the Partial-CDH problem in $\mathbb{F}_{p^2}$.

Theorem 1 *Suppose $\mathcal{A}$ is a Partial-CDH adversary that runs in time at most φ and achieves advantage $\mathbf{Adv}^{\mathrm{pcdh}}_{\mathcal{A},h,\mathbb{F}_{p^2}}$ for any $h \in I_2(p)$. Then there exists a CDH adversary $\mathcal{B}$, constructed from $\mathcal{A}$ in a blackbox manner, that runs in time at most 2φ plus the time to perform a small constant number of group operations and achieves advantage $\mathbf{Adv}^{\mathrm{cdh}}_{\mathcal{B},h,\mathbb{F}_{p^2}} \geq (1-\frac{1}{p}) \cdot (\mathbf{Adv}^{\mathrm{pcdh}}_{\mathcal{A},h,\mathbb{F}_{p^2}})^2$.*

We can define a *dual* variant of the Partial-CDH problem over $\mathbb{F}_{p^2}$: We say that the *Dual-Partial-CDH* problem is hard in $\mathbb{F}_{p^2}$ if for all $h \in I_2(p)$ no efficient algorithm given $g, A = g^a, B = g^b \in \mathbb{F}_{p^2}$ can output $\left[g^{ab}\right]_0 \in \mathbb{F}_p$. We can show that the Dual-Partial-CDH problem is also as hard as the conventional CDH problem. The formal definition and the proof can be found in Appendix B. Therefore, both the Partial-CDH and Dual-Partial CDH problems are as hard as the conventional CDH problem over $\mathbb{F}_{p^2}$.

Bit Security for the other coordinate. Let $B_k \colon \mathbb{F}_p \to \{\pm 1\}$ denote the k-th bit predicate (with a 0 bit being encoded as $+1$). Let β_k be the bias of B_k. For all $h, \widehat{h} \in I_2(p)$ there exists an easily computable isomorphism $\phi_{h,\widehat{h}} \colon \mathbb{F}_p[x]/(h) \to \mathbb{F}_p[x]/(\widehat{h})$. Informally we show that when given an oracle $\mathcal{O}$ that predicts the k-th bit of the degree 0 coefficient of the CDH value with non-negligible advantage, and the representation of the field, then we can break the Partial-CDH assumption with non-negligible advantage.

Theorem 2 *Under the Partial-CDH assumption over $\mathbb{F}_{p^2}$ (i.e., Assumption 2), for any PPT adversary $\mathcal{O}$, we have that for all $h \in I_2(p)$ the following quantity is negligible in l:*

$$\left|\Pr\left[\mathcal{O}(h,\widehat{h},g,g^a,g^b) = B_k\left(\left[\phi_{h,\widehat{h}}(g^{ab})\right]_0\right) \middle| \widehat{h} \xleftarrow{\$} I_2(p); a,b \xleftarrow{\$} \{1,\cdots,p^2-1\}\right] - \beta_k\right|.$$

We first give an informal intuition of the proof of the theorem. We aim at constructing a code similar to those of FGPS and Duc and Jetchev [8]. For an element $\alpha \in \mathbb{F}_{p^2}$ and a monic irreducible polynomial $h \in I_2(p)$, we would define the following codeword:

$$C_\alpha(\widehat{h}) = B_k([\phi_{h,\widehat{h}}(\alpha)]_0).$$

Similar to the code defined in FGPS, the above code is accessible using $\mathcal{O}$. However, the predicate B_k is evaluated on the *other* coordinate of $\phi_{h,\widehat{h}}(\alpha)$. In this case, it holds that $[\phi_{h,\widehat{h}}(\alpha)]_0 = \eta[\alpha]_1 + [\alpha]_0$ for some $\eta \in \mathbb{F}_p$ (and $\lambda \in \mathbb{F}_p^*$), according to FGPS [10, Lemma 5.3] (recalled in Lemma 3 below).

Lemma 3 ([10, Lemma 5.3]). *For any $h \in I_2(p)$, there exists a unique function $L_h \colon \mathbb{F}_p \times \mathbb{F}_p^* \to I_2(p)$ which takes a pair (η, λ) to the polynomial $\widehat{h} = L_h(\eta, \lambda)$ such that the matrix $\left(\begin{smallmatrix} 1 & \eta \\ 0 & \lambda \end{smallmatrix}\right)$ defines an isomorphism from $\mathbb{F}_p[x]/(h)$ to $\mathbb{F}_p[x]/(\widehat{h})$ that sends $[\alpha]_1 x + [\alpha]_0 \mapsto \lambda[\alpha]_1 x + \eta[\alpha]_1 + [\alpha]_0$.*

Intuitively, one would consider the following code: for $\alpha \in \mathbb{F}_{p^2}$ and for $\eta \in \mathbb{F}_p$ (and $\lambda \in \mathbb{F}_p^*$), set

$$C_\alpha(\eta) = B_k(\eta[\alpha]_1 + [\alpha]_0). \tag{1}$$

Unfortunately, the above code in (1) is not *multiplicative*. In particular, this makes it hard to prove concentration and recoverability. This is why FGPS considered defining the Partial-CDH problem over $\mathbb{F}_{p^2}$ as outputting the coefficient of the degree 1 term of g^{ab}, instead of the coefficient of the degree 0 term. More generally, the list decoding approach has only been proven successful for multiplicative codes so far [1, 8, 16]. One natural question is if it is (even) possible to apply list decoding approach to the case of non-multiplicative codes.

With a careful analysis, we are still able to show that the code in (1) is concentrated and recoverable. Concentration will follow from the key observation that the Fourier transform of the code in (1) is equal to that of a multiplication code (to be defined shortly) up to a factor of a character (as will be proved in Lemma 4). Hence, the l_2-norm of the Fourier transform of the code is equal to that of the multiplication code. That is, the code in (1) is concentrated if and only if the multiplication code is. Note that it is easy to argue that the multiplication code is concentrated.

The goal of recoverability is to recover the secret value from the heavy characters of the code C_α. We find that a character χ_β is heavy for C_α if and only if χ_β is heavy for a multiplicative code C'_α. The associated constant of a heavy character χ_β for the multiplicative code C'_α equals the product of the secret value and an (easily determined) factor. Therefore, one can recover the secret value with a heavy character. We begin by proving Lemma 4.

Lemma 4 *Let F_1, F_2 be functions mapping $\mathbb{Z}_n$ to $\mathbb{C}$. If for any y, $F_2(y) = F_1(y - \sigma)$, where σ is a constant in $\mathbb{Z}_n$, then we have for $\alpha \in \mathbb{Z}_n$, $\widehat{F_2}(\alpha) = \chi_\alpha(\sigma)\widehat{F_1}(\alpha)$.*

Proof of Lemma 4: By the definition of Fourier transform and $F_2(y) = F_1(y - \sigma)$, we have

$$\widehat{F_2}(\alpha) = 1/n \sum_{y \in \mathbb{Z}_n} \overline{F_1(y - \sigma)} \chi_\alpha(y). \tag{2}$$

It is easily seen that if y traverses the complete residue system modulo n then so does $y - \sigma$. Hence, we have $\{y - \sigma\}_{y \in \mathbb{Z}_n} = \mathbb{Z}_n$. Equation (2) can be re-written as

$$\widehat{F_2}(\alpha) = 1/n \sum_{y \in \mathbb{Z}_n} \overline{F_1(y)} \chi_\alpha(y + \sigma). \tag{3}$$

Since $\chi_\alpha(y + \sigma) = \chi_\alpha(\sigma)\chi_\alpha(y)$, equation (3) becomes

$$\widehat{F_2}(\alpha) = 1/n \sum_{y \in \mathbb{Z}_n} \overline{F_1(y)} \chi_\alpha(y)\chi_\alpha(\sigma).$$

It thus follows that $\widehat{F_2}(\alpha) = \chi_\alpha(\sigma)\widehat{F_1}(\alpha)$. This completes the proof the lemma. □

Hard-core predicates for the CDH problem over $\mathbb{F}_{p^2}$. Note that for a given $h \in I_2(p)$, any element $\alpha \in \mathbb{F}_{p^2}$ of length $2l$ can be written as $[\alpha]_1 x + [\alpha]_0$, *i.e.,* $[\alpha]_1$ and $[\alpha]_0$ are the leftmost and

rightmost l bits value of α, respectively. Let $\widetilde{B}_k \colon \mathbb{F}_{p^2} \to \{\pm 1\}$ denote the k-th bit predicate (where $1 \le k \le 2l$) and let β_k be the bias of $\widetilde{B}_k$. In the following, we prove that given an oracle $\mathcal{O}$ that predicts the k-th bit of the CDH value over a random representation of the field $\mathbb{F}_{p^2}$ with non-negligible advantage, we can solve the *regular* CDH problem over $\mathbb{F}_{p^2}$ with non-negligible probability.

Theorem 3 *Under the CDH assumption over $\mathbb{F}_{p^2}$ (i.e., Assumption 1), for any PPT adversary $\mathcal{O}$, we have that for all $h \in I_2(p)$ the following quantity is negligible in l:*

$$\left| \Pr\left[\mathcal{O}(h, \widehat{h}, g, g^a, g^b) = \widetilde{B}_k\big(\phi_{h,\widehat{h}}(g^{ab})\big) \middle| \widehat{h} \xleftarrow{\$} I_2(p); a, b \xleftarrow{\$} \{1, \cdots, p^2 - 1\}\right] - \beta_k \right|.$$

Proof Sketch: For an element $\alpha \in \mathbb{F}_{p^2}$ and a given $h \in I_2(p)$, we define a codeword as follows: $C_\alpha(\widehat{h}) = \widetilde{B}_k(\phi_{h,\widehat{h}}(\alpha))$. If $k \le l$, we have $\widetilde{B}_k(\phi_{h,\widehat{h}}(\alpha)) = B_k([\phi_{h,\widehat{h}}(\alpha)]_0)$. Otherwise if $k > l$, we have $\widetilde{B}_k(\phi_{h,\widehat{h}}(\alpha)) = B_{k-l}([\phi_{h,\widehat{h}}(\alpha)]_1)$. Along the same lines as the proofs of [10, Theorem 5.2] and Theorem 2, predicting any individual bit of the secret CDH value defined above can break the Partial-CDH assumption over $\mathbb{F}_{p^2}$, and hence break the CDH assumption over $\mathbb{F}_{p^2}$, as shown in Theorem 1. ∎

4 Almost All Bits Security of the CDH Problems over $\mathbb{F}_{p^t}$ for $t > 1$

4.1 Hardness of the d-th CDH Assumption over $\mathbb{F}_{p^t}$

We begin with the definition of the the d-th CDH problem over $\mathbb{F}_{p^t}$. For a given prime p, there are many different fields $\mathbb{F}_{p^t}$, but they are all isomorphic to each other. Let $h(x) = x^t + h_{t-1}x^{t-1} + \cdots + h_1 x + h_0$ be a monic irreducible polynomial of degree t in $\mathbb{F}_p$. It is well known that $\mathbb{F}_{p^t}$ is isomorphic to the field $\mathbb{F}_p[x]/(h)$, where $(h(x))$ is a principal ideal in the polynomial ring $\mathbb{F}_p[x]$ and therefore elements of $\mathbb{F}_{p^t}$ can be written as polynomials of degree $t-1$, *i.e.,* if $g \in \mathbb{F}_{p^t}$ then $g = g_{t-1}x^{t-1} + g_{t-2}x^{t-2} + \cdots + g_1 x + g_0$ and addition and multiplication are performed as polynomial operations modulo h. In the following, given $g \in \mathbb{F}_{p^t}$ we denote by $[g]_i$ the coefficient of the degree-i term, *i.e.,* $g_i = [g]_i$. Let $I_t(p)$ be the set of monic irreducible polynomials of degree t in $\mathbb{F}_p$, and let g be a generator of the multiplicative group of $\mathbb{F}_{p^t}$. First, the CDH problem can be easily extended to the case of finite fields $\mathbb{F}_{p^t}$ for $t > 1$.

Assumption 3 (The CDH assumption over $\mathbb{F}_{p^t}$). *We say that the CDH problem is hard in $\mathbb{F}_{p^t}$ for $t > 1$ if for any PPT adversary $\mathcal{A}$, his CDH advantage*

$$\mathbf{Adv}^{\mathrm{cdh}}_{\mathcal{A},\mathbb{F}_{p^t}} \coloneqq \Pr\left[\mathcal{A}(p, g, g^a, g^b) = g^{ab} \middle| p \xleftarrow{\$} \mathcal{G}(1^l); a, b \xleftarrow{\$} \left\{1, \cdots, p^t - 1\right\}\right]$$

is negligible in l.

We say that the *d-th CDH* problem (where $0 \le d \le t-1$) is hard in $\mathbb{F}_{p^t}$ if for all $h \in I_t(p)$ no efficient algorithm given $g, A = g^a, B = g^b \in \mathbb{F}_{p^t}$ can output $\left[g^{ab}\right]_d \in \mathbb{F}_p$. Formally we consider the following assumption:

Assumption 4 (The d-th CDH assumption over $\mathbb{F}_{p^t}$). *We say that the d-th CDH problem (where $0 \le d \le t-1$) is hard in $\mathbb{F}_{p^t}$ (for $t > 1$) if for any PPT adversary $\mathcal{A}$, his d-th CDH advantage for all $h \in I_t(p)$*

$$\mathbf{Adv}^{\mathrm{dcdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}} \coloneqq \Pr\left[\mathcal{A}(p, h, g, g^a, g^b) = \left[g^{ab}\right]_d \middle| p \xleftarrow{\$} \mathcal{G}(1^l); a, b \xleftarrow{\$} \left\{1, \cdots, p^t - 1\right\}\right]$$

is negligible in l.

It is well known that the probability of a random polynomial $h \in \mathbb{F}_p[X]$ of degree t being irreducible is at least $\frac{1}{2t}$. The following theorem asserts that the regular CDH problem over $\mathbb{F}_{p^t}$ with $t > 1$ can be reduced to *any* d-th CDH problem ($0 \leq d \leq t-1$) over a random representation of $\mathbb{F}_{p^t}$. Therefore, all the d-th CDH problems over a random representation of finite fields $\mathbb{F}_{p^t}$ for $t > 1$ are as hard as the regular CDH problem over the same fields.

Theorem 4 *Let $\mathbb{F}_{p^t}$ be a finite filed of size l and $t > 1$. Suppose $\mathcal{A}$ is a d-th CDH adversary that runs in time at most φ and achieves advantage $\mathbf{Adv}^{\mathrm{dcdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}}$ for a monic polynomial $h \xleftarrow{\$} \mathbb{F}_p[X]$ of degree t and $h \in I_t(p)$. Then there exists a CDH adversary $\mathcal{B}$, constructed from $\mathcal{A}$ in a blackbox manner, that runs in time at most $t\varphi$ plus the time to perform poly(l) group operations and achieves advantage $\mathbf{Adv}^{\mathrm{cdh}}_{\mathcal{B},\mathbb{F}_{p^t}} \geq (1-\frac{1}{p})^t \cdot e^{-\frac{2}{p-1}} \cdot (\mathbf{Adv}^{\mathrm{dcdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}})^t$.*

We comment that if an adversary $\mathcal{A}$ can solve the d-th CDH problem over $\mathbb{F}_{p^t}$ with respect to a monic polynomial $h \xleftarrow{\$} \mathbb{F}_p[X]$ of degree t and $h \in I_t(p)$ then we can construct an adversary $\mathcal{B}$ that solves all the d-CDH problems over $\mathbb{F}_{p^t}$ for $0 \leq d \leq t-1$ regarding any $h' \in I_t(p)$. To see this, for $h, h' \in I_t(p)$, we know that there exists an easily computable isomorphism $\phi_{h,h'} \colon \mathbb{F}_p[x]/(h) \to \mathbb{F}_p[x]/(h')$. When adversary $\mathcal{B}$ learns the CDH value with respect to h, it can easily compute all the d-th coordinates under any representation h'.

Theorem 4 proves a slightly weaker result than that of Theorem 1. In Theorem 1, the reduction works for any $h \in I_2(p)$, but in Theorem 4, it works for a random $h \xleftarrow{\$} \mathbb{F}_p[X]$ of degree t and $h \in I_t(p)$. (It could be the case that there exists some $h \in I_t(p)$ such that some d-th CDH problem might not be equivalent to the CDH problem over $\mathbb{F}_{p^t}$, although we conjecture that these two problems are equivalent with respect to any $h \in I_t(p)$.) However, we are able to prove that the 0-th CDH problem and the $(t-1)$-th CDH problem are both strictly equivalent to the CDH problem with respect to any $h \in I_t(p)$, and we have the following theorem:

Theorem 5 *Let $\mathbb{F}_{p^t}$ be a finite filed of size l and $t > 1$. Suppose $\mathcal{A}$ is a 0-th (resp., $(t-1)$-th) CDH adversary that runs in time at most φ and achieves advantage $\mathbf{Adv}^{\mathrm{0cdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}}$ (resp., $\mathbf{Adv}^{(\mathrm{t-1})\mathrm{cdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}}$) for any $h \in I_t(p)$. Then there exists a CDH adversary $\mathcal{B}$, constructed from $\mathcal{A}$ in a blackbox manner, that runs in time at most $t\varphi$ plus the time to perform poly(l) group operations and achieves advantage $\mathbf{Adv}^{\mathrm{cdh}}_{\mathcal{B},\mathbb{F}_{p^t}} \geq e^{-\frac{2}{p-1}} \cdot (\mathbf{Adv}^{\mathrm{0cdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}})^t$ (resp., $\mathbf{Adv}^{\mathrm{cdh}}_{\mathcal{B},\mathbb{F}_{p^t}} \geq e^{-\frac{2}{p-1}} \cdot (\mathbf{Adv}^{(\mathrm{t-1})\mathrm{cdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}})^t$).*

The case of perfect oracles. Applying our approach to the case of perfect oracles, our reduction leads to no security loss and a strict equivalence result. This is in contrast to Verheul's [20], where for many d's, the algorithm can easily have exponential running time in t.

4.2 Bit Security of the CDH Problem over $\mathbb{F}_{p^t}$

We now show the following result: assuming the hardness of the d-th CDH problem over $\mathbb{F}_{p^t}$ with $t > 1$, if $d \neq 0$, we prove the unpredictability of every single bit of the degree-d coordinate of the secret CDH value. Together with the equivalence result, this implies that for the conventional CDH problems over $\mathbb{F}_{p^t}$ for an l-bit prime p and an integer $t > 1$, $(t-1)l$ out of tl secret CDH bits—including every individual bit except that of the degree 0 coordinate—are hard-core.

We begin with the definition of d-th residues modulo p. Let p be a prime and d be an integer. We say that an element $\alpha \in \mathbb{F}_p^*$ is a d-th residue modulo p, if there exists an element $x \in \mathbb{F}_p$ such that

$x^d \equiv \alpha \bmod p$. Let $\mathbb{F}_p^d$ denote the set of the d-th residues modulo p. The following lemma provides a well-known result on d-th residues modulo p:

Lemma 5 *Let p be a prime and $d \in \mathbb{Z}_+$. The number of the d-th residues modulo p is $(p-1)/(d, p-1)$.*

We present a lemma that gives a characterization of the isomorphisms between two representations of the fields $\mathbb{F}_{p^t}$. The isomorphisms generalize that of finite fields $\mathbb{F}_{p^2}$ in FGPS to the case of general finite fields $\mathbb{F}_{p^t}$ for any $t > 1$. More importantly, they simplify that of FGPS in the sense we identify a more restrictive class of isomorphisms. This simplicity turns out to be essential to establishing the bit security for general finite fields.

Lemma 6 *For any $h(x) \in I_t(p)$, there exists a unique function $L_h \colon \mathbb{F}_p^* \to I_t(p)$ which takes λ to the polynomial $\widehat{h}_\lambda = L_h(\lambda) = \frac{h(\lambda x)}{\lambda^t}$ such that λ defines an isomorphism from $\mathbb{F}_p[x]/(h)$ to $\mathbb{F}_p[x]/(\widehat{h}_\lambda)$ that sends*

$$\sum_{i=0}^{t} [\alpha]_i x^i \mapsto \sum_{i=0}^{t} \lambda^i [\alpha]_i x^i.$$

Proof: For any $\lambda \in \mathbb{F}_p^*$, let $\widehat{h}_\lambda(x) = \frac{h(\lambda x)}{\lambda^t}$. It is easy to see that $\widehat{h}_\lambda(x)$ is a monic irreducible polynomial over $\mathbb{F}_p$, *i.e.,* $\widehat{h}_\lambda(x) \in I_t(p)$. Hence, there is an isomorphism from $\mathbb{F}_p[x]/(h)$ to $\mathbb{F}_p[x]/(\widehat{h}_\lambda)$. In order to specify a homomorphism ψ from $\mathbb{F}_p[x]/(h)$ to another field J of characteristic p, it is both necessary and sufficient to choose $\psi(x) = y \in J$ such that $h(y) = 0$ in J. The definition of $\widehat{h}_\lambda$ implies that x sends to λx. The lemma now follows. □

Theorem 6 *Under the d-th CDH assumption over $\mathbb{F}_{p^t}$ for $t > 1$ (i.e., Assumption 4), for any PPT adversary $\mathcal{O}$, if $d \neq 0$, we have that for all $h \in I_t(p)$ the following quantity is negligible:*

$$\left| \Pr\left[\mathcal{O}(h, \lambda, g, g^a, g^b) = B_k\big(\big[\phi_{h,\widehat{h}_\lambda}(g^{ab})\big]_d\big) \middle| \lambda \xleftarrow{\$} \mathbb{F}_p^*; a, b \xleftarrow{\$} \{1, \cdots, p^2 - 1\}\right] - \beta_k \right|.$$

Discussion. It is worth mentioning that Theorem 6 proves what is slightly different in concept from those of FGPS and Theorem 2. In FGPS and Theorem 2, it is shown that any bit prediction oracle must have negligible success probability ranging over *all representations*, whereas Theorem 6 shows that the success probability must be negligible ranging over a restricted class. However, in any application, participants would agree upon some representation that they want to use, and therefore our result does not limit its applicability and it is in fact simpler.[1]

Following from Theorem 4 and Theorem 6, we obtain the following result: almost all individual bits of the CDH value of the traditional CDH problem over finite fields $\mathbb{F}_{p^t}$ for $t > 1$ are hard-core. We require that the underlying field representation h be chosen uniformly at random (just as the generator g). Formally we have the following theorem:

Theorem 7 *Under the CDH assumption over $\mathbb{F}_{p^t}$ for $t > 1$ (i.e., Assumption 3), for any PPT adversary $\mathcal{O}$, if $d \neq 0$, the following quantity is negligible:*

$$\left| \Pr\left[\mathcal{O}(h, \lambda, g, g^a, g^b) = B_k\big(\big[\phi_{h,\widehat{h}_\lambda}(g^{ab})\big]_d\big) \middle| h \xleftarrow{\$} \mathbb{F}_p[x] \text{ and } h \in I_t(p); \lambda \xleftarrow{\$} \mathbb{F}_p^*; a, b \xleftarrow{\$} \{1, \cdots, p^2 - 1\}\right] - \beta_k \right|.$$

[1] The discussion is due to a personal communication with W. E. Skeith III (Aug. 2014).

Following from Theorem 5 and Theorem 6, we have the following theorem which holds for an arbitrary field representation:

Theorem 8 *Under the CDH assumption over $\mathbb{F}_{p^t}$ for $t > 1$ (i.e., Assumption 3), for any PPT adversary $\mathcal{O}$ and any $h \in I_t(p)$; the following quantity is negligible:*

$$\left| \Pr\left[\mathcal{O}(h, \lambda, g, g^a, g^b) = B_k\big(\left[\phi_{h,\widehat{h}_\lambda}(g^{ab})\right]_{t-1}\big) \middle| \lambda \xleftarrow{\$} \mathbb{F}_p^*; a, b \xleftarrow{\$} \{1, \cdots, p^2 - 1\}\right] - \beta_k \right|.$$

5 Conclusion

In this paper, we revisited the d-th CDH problem for any $0 \leq d \leq t-1$ over finite fields $\mathbb{F}_{p^t}$ for $t > 1$ [18, 20]. In contrast to prior work, we considered the most general case of noisy oracles. We proved that all the d-th CDH problems over a random representation of finite fields $\mathbb{F}_{p^t}$ for $t > 1$ are as hard as the regular CDH problem over the same fields. In particular, the 0-th CDH problem and $(t-1)$-th CDH problem given *any* field representation are as hard as the CDH problem. This latter claim applies to the special case of the Partial-CDH and the Dual-Partial CDH problems over $\mathbb{F}_{p^2}$.

We advanced the list decoding approach, and for the first time, we applied it to the case of a non-multiplicative code. We proved that the Partial-CDH problem also admits the hard-core predicates for every individual bit of the other coordinate of the secret CDH value over a random representation of the finite field $\mathbb{F}_{p^2}$. By combining all these, we obtained one of our main results: given an oracle $\mathcal{O}$ that predicts any bit of the CDH value over a random representation of the field $\mathbb{F}_{p^2}$ with non-negligible advantage, we can solve the *regular* CDH problem over $\mathbb{F}_{p^2}$ with non-negligible probability.

We continued to prove that over finite fields $\mathbb{F}_{p^t}$ for any $t > 1$, each d-th CDH problem except $d \neq 0$ admits a large class of hard-core predicates, including every individual bit of d-th coordinate. Hence we proved that almost all bits of the CDH value of the traditional CDH problem over finite fields $\mathbb{F}_{p^t}$ for $t > 1$ are hard-core.

Acknowledgments

We are greatly indebted to past PC members for their valuable comments and for pointing out an error in proving Theorem 2 (now fixed) and an initial idea for proving Theorem 4 on which our algorithm is based. Many thanks to William E. Skeith III for kindly verifying the proofs and for providing insightful corrections, comments, and suggestions. We thank Kai-Min Chung, Alexandre Duc, Matt Franklin, Dimitar Jetchev, Phil Rogaway, Xiaoyun Wang, and Haiyang Xue for helpful comments and discussion. Part of the work was carried out when Mingqiang visited UC Davis.

References

[1] A. Akavia, S. Goldwasser, and S. Safra. Proving hard-core predicates using list decoding. *FOCS 2003*, pp. 146–157, IEEE Computer Society, 2003.

[2] W. Alexi, B. Chor, O. Goldreich, and C. Schnorr. RSA and rabin functions: Certain parts are as hard as the whole. *SIAM Journal on Computing*, 17(2): 194–209, 1988.

[3] M. Ben-Or. Probabilistic algorithms in finite fields. *FOCS 1981*, 11: 394–398, 1981.

[4] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM Journal on Computing*, 13(4): 850–864, 1984.

[5] D. Boneh and I. E. Shparlinski. On the unpredictability of bits of the elliptic curve Diffie-Hellman scheme. *CRYPTO 2001*, LNCS vol. 2139, pp. 201–212, Springer, 2011.

[6] D. Boneh, R. Venkatesan. Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes. *Crypto '96*, LNCS vol. 1109, pp. 129–142, 1996.

[7] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT–22(6): 644–654, 1976.

[8] A. Duc and D. Jetchev. Hardness of computing individual bits for one-way functions on elliptic curves. *CRYPTO 2012*, LNCS vol. 7417, pp. 832–849, 2012.

[9] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, IT–31(4): 469–472, 1985.

[10] N. Fazio, R. Gennaro, I. M. Perera, and W. E. Skeith III. Hard-core predicates for a Diffie-Hellman problem over finite fields. *CRYPTO 2013*, LNCS vol. 8043, pp. 148–165, 2013.

[11] J. von zur Gathen and J. Gerhard. Modern Computer Algebra. *Cambridge University Press*, 1999.

[12] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. *STOC 1989*, pp. 25–32, ACM press, 1989.

[13] S. Goldwasser and S. Micali. Probabilistic encryption. *JCSS*, 28(2):270–299, 1984.

[14] J. Håstad and M. Näslund. The security of individual RSA bits. *FOCS*, pp. 510–521, 1998.

[15] R. Lidl and H. Niederreiter. Finite Fields. *Addison-Wesley*, 1983.

[16] P. Morillo and C. Ràfols. The security of all bits using list decoding. *PKC 2009*, LNCS vol. 5443, pp. 15–33, Springer, 2009.

[17] M. Näslund. All bits in $ax + b \mod p$ are hard. *CRYPTO '96*, pp. 114–128, 1996.

[18] I. E. Shparlinski. Security of polynomial transformations of the Diffie–Hellman key. *Finite Fields and Their Applications*, vol. 10, Issue 1, pp. 123–131, Jan 2014.

[19] A. Slinko. A generalization of Komlós's theorem on random matrices. *New Zealand J. Math.* 30 (1): 81–86, 2001.

[20] E. R. Verheul. Certificates of recoverability with scalable recovery agent security. *PKC 2000*, LNCS vol. 1751, pp. 258–275, 2000.

A. Proof of Theorem 1

Our CDH adversary $\mathcal{B}$ works as follows, given input a random instance of the CDH problem $(g^a, g^b) \in (\mathbb{F}_{p^2})^2$ and given a Partial-CDH adversary $\mathcal{A}$ under the representation determined by any given polynomial $h(x) = x^2 + h_1 x + h_0 \in I_2(p)$.

First, adversary $\mathcal{B}$ chooses two random integers $r, s \xleftarrow{\$} \mathbb{Z}_{p^2-1}$, and computes (g^{a+r}, g^{b+s}). For brevity, let $A = a + r$ and $B = b + s$. Adversary $\mathcal{B}$ then runs the Partial-CDH adversary $\mathcal{A}$ on the generated instance (g^A, g^B) to obtain $\left[g^{AB}\right]_1$. Let $C = as + br + rs$. As $g^{AB} = g^{ab}g^C \bmod h(x)$, we have the following equation

$$(\left[g^C\right]_0 - \left[g^C\right]_1 h_1)\left[g^{ab}\right]_1 + \left[g^C\right]_1\left[g^{ab}\right]_0 = \left[g^{AB}\right]_1. \tag{4}$$

Repeating the above process, adversary $\mathcal{B}$ chooses two random integers $r', s' \xleftarrow{\$} \mathbb{Z}_{p^2-1}$ and gets the following equation

$$(\left[g^{C'}\right]_0 - \left[g^{C'}\right]_1 h_1)\left[g^{ab}\right]_1 + \left[g^{C'}\right]_1\left[g^{ab}\right]_0 = \left[g^{A'B'}\right]_1, \tag{5}$$

where $A' = a + r', B' = b + s'$, and $C' = as' + br' + r's'$.

Combining (4) and (5), we obtain a linear equation set with the unknowns $\left[g^{ab}\right]_1$ and $\left[g^{ab}\right]_0$. If the coefficient matrix of the equation set has full rank then adversary $\mathcal{B}$ can solve the equation set and obtain g^{ab}. The coefficient matrix is of full rank if and only if its determinant is not zero, *i.e.,*

$$(\left[g^C\right]_0 - \left[g^C\right]_1 h_1)\left[g^{C'}\right]_1 - (\left[g^{C'}\right]_0 - \left[g^{C'}\right]_1 h_1)\left[g^C\right]_1 \neq 0. \tag{6}$$

Note that $[g^C]_i$ and $[g^{C'}]_i$ $(i = 0, 1)$ in equation (6) are independently and uniformly distributed at random from $\mathbb{F}_p$. Hence, the probability that the matrix is of full rank is $1 - 1/p$. This completes the proof of this theorem. ∎

B. The Dual-Partial-CDH Problem

We define a *dual* variant of the Partial-CDH problem over $\mathbb{F}_{p^2}$: We say that the *Dual-Partial-CDH* problem is hard in $\mathbb{F}_{p^2}$ if for all $h \in I_2(p)$ no efficient algorithm given $g, A = g^a, B = g^b \in \mathbb{F}_{p^2}$ can output $\left[g^{ab}\right]_0 \in \mathbb{F}_p$. Formally we consider the following assumption:

Assumption 5 (The Dual-Partial-CDH assumption over $\mathbb{F}_{p^2}$). *We say that the Dual-Partial-CDH problem is hard in $\mathbb{F}_{p^2}$ if for any PPT adversary $\mathcal{A}$, his Dual-Partial-CDH advantage for all $h \in I_2(p)$*

$$\mathbf{Adv}^{\mathrm{dpcdh}}_{\mathcal{A},h,\mathbb{F}_{p^2}} := \Pr\left[\mathcal{A}(p, h, g, g^a, g^b) = \left[g^{ab}\right]_0 | p \xleftarrow{\$} \mathcal{G}(1^l); a, b \xleftarrow{\$} \left\{1, \cdots, p^2 - 1\right\}\right]$$

is negligible in l.

The following theorem asserts that the Dual-Partial-CDH problem is also as hard as the conventional CDH problem. Therefore, both the Partial-CDH and Dual-Partial CDH problems are as hard as the conventional CDH problem over $\mathbb{F}_{p^2}$.

Theorem 9 *Suppose $\mathcal{A}$ is a Dual-Partial-CDH adversary that runs in time at most φ and achieves advantage $\mathbf{Adv}^{\mathrm{dpcdh}}_{\mathcal{A},h,\mathbb{F}_{p^2}}$. Then, for all $h \in I_2(p)$, there exists a CDH adversary $\mathcal{B}$, constructed from $\mathcal{A}$ in a blackbox manner, that runs in time at most 2φ plus the time to perform a small constant number of group operations and achieves advantage $\mathbf{Adv}^{\mathrm{cdh}}_{\mathcal{B},\mathbb{F}_{p^2}} \geq (1 - \frac{1}{p}) \cdot (\mathbf{Adv}^{\mathrm{dpcdh}}_{\mathcal{A},h,\mathbb{F}_{p^2}})^2$.*

Proof: The proof is similar to that of Theorem 1. The CDH adversary $\mathcal{B}$ works as follows, given input a random instance of the CDH problem $(g^a, g^b) \in (\mathbb{F}_{p^2})^2$ and given a Dual-Partial-CDH adversary $\mathcal{A}$ under the representation determined by any given polynomial $h(x) = x^2 + h_1 x + h_0 \in I_2(p)$.

First, adversary $\mathcal{B}$ chooses two random integers $r, s \xleftarrow{\$} \mathbb{Z}_{p^2-1}$, and computes (g^{a+r}, g^{b+s}). Let $A = a + r$ and $B = b + s$. Adversary $\mathcal{B}$ then runs the Dual-Partial-CDH adversary $\mathcal{A}$ on the generated instance (g^A, g^B) to obtain $\big[g^{AB}\big]_0$. Let $C = as + br + rs$ and we have $g^{AB} = g^{ab}g^C \bmod h(x)$. Therefore, we have

$$\big[g^C\big]_0\big[g^{ab}\big]_0 - \big[g^C\big]_1 h_0 \big[g^{ab}\big]_1 = \big[g^{AB}\big]_0. \tag{7}$$

Repeating the above process, adversary $\mathcal{B}$ chooses two random integers $r', s' \xleftarrow{\$} \mathbb{Z}_{p^2-1}$ and gets the following equation

$$\big[g^{C'}\big]_0\big[g^{ab}\big]_0 - \big[g^{C'}\big]_1 h_0 \big[g^{ab}\big]_1 = \big[g^{A'B'}\big]_0, \tag{8}$$

where $A' = a + r', B' = b + s'$, and $C' = ar' + bs' + r's'$.

Adversary $\mathcal{B}$ obtains from (7) and (8) a linear equation set with the unknowns $\big[g^{ab}\big]_1$ and $\big[g^{ab}\big]_0$. The coefficient matrix has full rank if and only if

$$\big(\big[g^C\big]_1\big[g^{C'}\big]_0 - \big[g^C\big]_0\big[g^{C'}\big]_1\big) \cdot h_0 \neq 0.$$

It is easy to see that $h_0 \neq 0$, since otherwise $h(x)$ is reducible. Also note that $[g^C]_i$ and $[g^{C'}]_i$ with $i = 0, 1$ are randomly chosen elements from $\mathbb{F}_p$. Therefore, the probability that the coefficient matrix has full rank is $1 - 1/p$. This completes the proof of this theorem. ∎

C. Proof of Theorem 2

Suppose that there exists an oracle $\mathcal{O}$ such that

$$\Big| \Pr_{\eta,a,b}\big[\mathcal{O}(h, \widehat{h}, g, g^a, g^b) = B_k\big(\big[\phi_{h,\widehat{h}}(g^{ab})\big]_0\big)\big] - \beta_k \Big|$$

is larger than a non-negligible quantity ϵ. We construct another oracle $\mathcal{O}'$ that takes as input a base representation $h \in I_2(p)$, a Diffie-Hellman triple $g, g^a, g^b \in \mathbb{F}_{p^2}$, and an element of $\eta \in \mathbb{F}_p$ (instead of $\widehat{h} \in I_2(p)$). The new oracle selects $\lambda \xleftarrow{\$} \mathbb{F}_p^*$, constructs an isomorphism $\widehat{h}$ from the matrix $\left(\begin{smallmatrix} 1 & \eta \\ 0 & \lambda \end{smallmatrix}\right)$ as described in Lemma 3, and returns $\mathcal{O}(h, \widehat{h}, g, g^a, g^b)$. One can then show that

$$\Big| \Pr_{\eta,a,b}\big[\mathcal{O}'(h, \eta, g, g^a, g^b) = B_k\big(\eta\big[g^{ab}\big]_1 + \big[g^{ab}\big]_0\big)\big] - \beta_k \Big|$$

is also larger than a non-negligible quantity.

For any element $\alpha \in \mathbb{F}_{p^2}$, we construct the following encoding of $\eta[\alpha]_1 + [\alpha]_0$ in its polynomial representation for $\mathbb{F}_p[x]/(h)$:

$$C_\alpha \colon \mathbb{F}_p \to \{\pm 1\} \;\text{ such that } C_\alpha(\eta) = B_k(\eta[\alpha]_1 + [\alpha]_0),$$

where, above, $[\alpha]_1$ and $[\alpha]_0$ are under the representation determined by h.

Accessibility. Accessibility proof is the same as that of FGPS. In particular, the oracle $\mathcal{O}'$ allows us to have access to a corrupted codeword $\widetilde{C}_\alpha$ of the above codeword defined as $\widetilde{C}_\alpha = \mathcal{O}'(h, \eta, g, g^a, g^b)$. The code $C_\alpha(\eta)$ is conceptually the same as the code $C_\alpha(\widehat{h})$. Therefore, if the oracle $\mathcal{O}$ has advantage ϵ then we have $|\Pr_\eta[C_\alpha(\eta) = \widetilde{C}_\alpha(\eta)]| \geq \beta_k + \epsilon$. Accessibility of the code C_α follows.

Concentration. We now prove that the codeword C_α is a Fourier concentrated code. To prove so, we define the following related code:

$$C'_\alpha(\eta) = B_k(\eta[\alpha]_1).$$

It is easy to see that $C'_\alpha(\eta) = C_\alpha(\eta - [\alpha]_1^{-1}[\alpha]_0)$. According to Lemma 4, we can obtain

$$\chi_\beta([\alpha]_1^{-1}[\alpha]_0)\widehat{C_\alpha}(\beta) = \widehat{C'_\alpha}(\beta).$$

This immediately implies $|\widehat{C_\alpha}(\beta)| = |\widehat{C'_\alpha}(\beta)|$. Therefore, the code $C_\alpha(\eta)$ is concentrated if and only if the code $C'_\alpha(\eta)$ is. Note that it is easy to argue that $C'_\alpha(\eta)$ is a multiplication code. The proof for concentration of the code $C'_\alpha(\eta)$ is similar to those of [10, 16], and now we describe our proof in some detail.

For $\beta \in \mathbb{F}_p$, if $C'_\alpha(\eta)$ is ϵ-concentrated in $\Gamma_\alpha = \{\chi_\beta\}$ then $B_k(\eta[\alpha]_1)$ is ϵ-concentrated in the set $\{\chi_\eta \colon \eta = \beta[\alpha]_1^{-1}\}$. Thus, we just need to prove the Fourier concentration of $B_k(\eta[\alpha]_1)$. We would need to analyze the Fourier coefficients of $B_k \colon \mathbb{F}_p \to \{\pm 1\}$.

We define $g(x)$ as

$$g(x) = \frac{B_k(x) + B_k(x + 2^k)}{2}.$$

Morillo and Ràfols [16] notice that the Fourier transform of $B_k(x)$ and the Fourier transform of $g(x)$ can be related with the following equation:

$$\widehat{g}(\eta) = \frac{\omega_p^{2^k\eta} + 1}{2}\widehat{B_k}(\eta),$$

where $\eta \in \mathbb{F}_p$ and $\omega_p = e^{2\pi i/p}$.

In particular, assuming $\eta \in [-\frac{p-1}{2}, \frac{p-1}{2}]$, they consider the following two cases for η:

1. $\eta \geq 0$, consider $\delta_{\eta,k} := 2^k\eta - (p-1)/2 \bmod p$ and let $\lambda_{\eta,k} \in [0, 2^{k-1} - 1]$ be the unique integer for which $2^k\eta = (p-1)/2 + \delta_{\eta,k} + p\lambda_{\eta,k}$.

2. $\eta < 0$, consider $\delta_{\eta,k} := 2^k\eta + (p+1)/2 \bmod p$ and let $\lambda_{\eta,k} \in [0, 2^{k-1} - 1]$ be the unique integer for which $2^k\eta = -(p+1)/2 + \delta_{\eta,k} + p\lambda_{\eta,k}$.

For both cases, there are unique integers $\mu_{\eta,k} \in [0, r]$, where r is the largest integer less than $p/2^{k+1}$ and $r_{\eta,k} \in [0, 2^k - 1]$ such that $a_p(2^k\eta - (p-1)/2) = \mu_{\eta,k}2^k + r_{\eta,k}$, where $a_p(x) = \min\{x \bmod p, p - x \bmod p\}$ for $x \bmod p$ being taken in $[0, p-1]$. The definition of Γ_τ in Section 3 is as follows

$$\Gamma_\tau = \{\eta \colon (\lambda_{\eta,k}, \mu_{\eta,k}) \in [0, 1/\tau] \times [0, 1/\tau]\}.$$

Here we select τ such that $1/\tau = poly(\log p)$. Morillo and Ràfols [16] obtain the following upper bound of $\widehat{B_k}(\eta)$:

$$|\widehat{B_k}(\eta)|^2 < O(\frac{1}{\lambda_{\eta,k}^2\mu_{\eta,k}^2}).$$

Now one can conclude that $B_k(\eta[\alpha]_1)$ is Fourier concentrated.

A character χ_β is τ-heavy for C_α if and only if χ_β is τ-heavy for C'_α. Therefore, according to the discussion in FGPS, for a threshold $\tau > 0$, the τ-heavy characters of C_α belong to the set

$$\Gamma_{\alpha,\tau} = \{\chi_\beta \colon \beta = \eta[\alpha]_1 \text{ for } \eta \in \Gamma_\tau\},$$

where Γ_τ is a set containing the τ-heavy coefficients of the function B_k. For each $\eta \in \Gamma_\tau$, there exists a unique integer pair $(\xi_\eta, \varsigma_\eta) \in [0, 1/\tau] \times [0, 1/\tau]$. Note that by [16, Lemma 9], the size of Γ_τ is at most $4\tau^{-2}$.

Recoverability. The proof for recoverability is similar to those of [10, 16]. According to Lemma 1, we know that there exists a threshold τ which is polynomial in the non-negligible quantity ϵ and at least one τ-heavy Fourier character $\chi \neq 0$ for C_α and $\widetilde{C}_\alpha$ such that $\chi \in \mathsf{Heavy}_\tau(C_\alpha) \cap \mathsf{Heavy}_\tau(\widetilde{C}_\alpha)$.

Given a polynomial $h(x) \in I_2(p)$, on input $g, g^a, g^b \in \mathbb{F}_{p^2}$, the following algorithm that has access to $\mathcal{O}$ produces a polynomial size list of elements in $\mathbb{F}_{p^2}$ which contains g^{ab} with probability $1-\delta$.

Let τ be the threshold determined by Lemma 1. We write $\alpha = [\alpha]_1 x + [\alpha]_0$ to denote $g^{ab} \in \mathbb{F}_{p^2}$. Using the learning algorithm of AGS [1] (*i.e.,* the algorithm in Lemma 2), we obtain a polynomial size list L_α of all the τ-heavy Fourier characters for $\widetilde{C}_\alpha$. If χ_β is a non-trivial τ-heavy character for C_α, we have $[\alpha]_1 = \eta^{-1}\beta$. Given $\chi_\beta \in L_\alpha$, we define $L_\beta = \{[\alpha]_1 \colon [\alpha]_1 = \eta^{-1}\beta \text{ for } \eta \in \Gamma_\tau\}$.

Let $L = \bigcup_{\chi_\beta \in L_\alpha} L_\beta$. Note that L is of polynomial size and $\alpha \in L$ with probability $1-\delta$. Since this is a polynomial size set, we can guess a result for $[\alpha]_1$ and hence get $[g^{ab}]_1$. The theorem now follows. ∎

D. Proof of Theorem 4

Before proceeding to the proof, we introduce a useful lemma, which claims that if all the entries in a square matrix are independently and uniformly chosen at random over a large finite field $\mathbb{F}_p$ then there is a good chance that the matrix is nonsingular. Note that we require that the probability depends only on the size of the finite field p, but not on the size of the matrix m. Similar results have been studied in, *e.g.,* [19].[2] For self-containedness, here we include a simpler proof for the lemma (with a better bound).

Lemma 7 *Let M be an $m \times m$ square matrix over the finite field $\mathbb{F}_p$. If every element of the matrix is chosen independently and uniformly at random, then the probability that M is nonsingular is at least $e^{-\frac{2}{p-1}}$.*

Proof: To help understand the proof, we slightly rephrase Lemma 7 in the language of vector space. Let $\mathbb{V}$ be a vector space over the finite field $\mathbb{F}_p$ of dimension m. Let $\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_m}$ be m independent, random vectors in the vector space $\mathbb{V}$. Let the matrix $M = (\boldsymbol{v_1'}, \boldsymbol{v_2'}, \cdots, \boldsymbol{v_m'})$, where $\boldsymbol{v_i'}$ (where $1 \leq i \leq m$) is the transpose of $\boldsymbol{v_i}$. The goal is to show that the probability that the rank of matrix M (*i.e.,*Rank(M)) is m is at least $e^{-\frac{2}{p-1}}$.

Let E_i $(1 \leq i \leq m)$ denote the event that $\boldsymbol{v_i} \notin \text{Span}\{\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_{i-1}}\}$, where Span$\{\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_{i-1}}\}$ is the subspace generated by vectors $\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_{i-1}}$.

It is easy to see that if the events E_i $(1 \leq i \leq m)$ occur simultaneously then the rank of the matrix is m. Hence, we have $\Pr[\text{Rank}(M) = m] \geq \Pr[E_1 E_2 \cdots E_m]$.

Below, we give a lower bound on $\Pr[E_1 E_2 \cdots E_m]$. For random vectors $\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_{i-1}}, \boldsymbol{v_i}$ in vector space $\mathbb{V}$, we actually have that the probability of $\boldsymbol{v_i} \in \text{Span}\{\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_{i-1}}\}$ is at most $\frac{1}{p^{m-i+1}}$. This is because the dimension of vector space $\mathbb{V}$ is m, while the dimension of vector subspace Span$\{\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_{i-1}}\}$ is at most $i-1$. Thus, the probability that E_i occurs is at least $1 - \frac{1}{p^{m-i+1}}$. We now have

$$\Pr[E_1 E_2 \cdots E_m] \geq \prod_{i=1}^{m}(1 - \frac{1}{p^{m-i+1}}) = \prod_{i=1}^{m}(1 - \frac{1}{p^i}) > \prod_{i=1}^{\infty}(1 - \frac{1}{p^i}).$$

[2] There are even more references which study the probability problems with respect to both p and m. The problems, although important, are not our concern here.

It remains to lower bound $\prod_{i=1}^{\infty}(1-\frac{1}{p^i})$. As $\prod_{i=1}^{\infty}(1-\frac{1}{p^i}) = e^{\sum_{i=1}^{\infty}\ln(1-\frac{1}{p^i})}$, we only need to bound the sum $\sum_{i=1}^{\infty}\ln(1-\frac{1}{p^i})$. Using Taylor series expansion, we obtain

$$\sum_{i=1}^{\infty}\ln(1-\frac{1}{p^i}) = -\sum_{i=1}^{\infty}\sum_{n=1}^{\infty}\frac{1}{np^{in}} \geq -\sum_{i=1}^{\infty}\frac{2}{p^i} = -\frac{2}{p-1}.$$

Thus, $\Pr[\mathrm{Rank}(M)=m] \geq \Pr[E_1E_2\cdots E_m] \geq e^{-\frac{2}{p-1}}$. This completes the proof of the lemma. □

Proof of Theorem 4: Let $h(x) = x^t + h_{t-1}x^{t-1} + \cdots + h_x + h_0$ be the irreducible polynomial of degree t over $\mathbb{F}_p$, where its coefficients being uniformly and independently selected at random.

Given a challenge instance $(g^a, g^b) \in (\mathbb{F}_{p^t})^2$ of the CDH problem, our CDH adversary $\mathcal{B}$ works as follows. First, adversary $\mathcal{B}$ chooses t pairs of random integers $(r_\iota, s_\iota) \stackrel{\$}{\leftarrow} (\mathbb{Z}_{p^t-1})^2$ $(\iota = 0, 1, \cdots, t-1)$, and computes $(g^{a+r_\iota}, g^{b+s_\iota})$. For brevity, let $A_\iota = a + r_\iota$ and $B_\iota = b + s_\iota$ for $\iota = 0, 1, \cdots, t-1$. Adversary $\mathcal{B}$ runs the d-th CDH problem under the representation determined by $h(x)$ on each $(g^{A_\iota}, g^{B_\iota})$ to get the d-th coordinate of the CDH value $\left[g^{A_\iota B_\iota}\right]_d$ $(\iota = 0, 1, \cdots, t-1)$.

Adversary $\mathcal{B}$ computes $g^{as_\iota+br_\iota+r_\iota s_\iota} = (g^a)^{s_\iota}(g^b)^{r_\iota}g^{r_\iota s_\iota}$. Let $C_\iota = as_\iota + br_\iota + r_\iota s_\iota$. It is easy to see that $g^{A_\iota B_\iota} = g^{ab}g^{C_\iota} \bmod h(x)$, *i.e.,*

$$\sum_{k=0}^{t-1}[g^{A_\iota B_\iota}]_k x^k \equiv \left(\sum_{i=0}^{t-1}[g^{ab}]_i x^i\right)\left(\sum_{j=0}^{t-1}[g^{C_\iota}]_j x^j\right) \bmod h(x). \tag{9}$$

Therefore $[g^{A_\iota B_\iota}]_d$ can be written as a linear expression with the coordinates of g^{ab} being variables and with some known coefficients $e_{\iota\nu} \in \mathbb{F}_p$ $(0 \leq \iota, \nu \leq t-1)$ such that

$$[g^{A_\iota B_\iota}]_d = \sum_{\nu=0}^{t-1} e_{\iota\nu}[g^{ab}]_\nu, \quad \iota = 0, 1, \cdots, t-1. \tag{10}$$

If the coefficient matrix $(e_{\iota\nu})_{t\times t}$ for the above equation set (10) has full rank, adversary $\mathcal{B}$ can use Gaussian elimination to compute the unknowns and therefore obtain g^{ab}, in polynomial time of l.

Indeed, we will prove in Lemma 8 below that the probability of every element of the coefficient matrix $(e_{\iota\nu})_{t\times t}$ being chosen independently and uniformly at random is at least $(1-\frac{1}{p})^t$, and then according to Lemma 7 we know that the probability of the coefficient matrix being nonsingular is at least $(1-\frac{1}{p})^t \cdot e^{-\frac{2}{p-1}}$.

Therefore, running adversary $\mathcal{A}$ for t times and solving the equation set obtained, adversary $\mathcal{B}$ can compute the desired CDH value, that runs in time at most $t\varphi$ plus the time to perform $poly(l)$ group operations with a non-negligible advantage $(1-\frac{1}{p})^t \cdot e^{-\frac{2}{p-1}} \cdot (\mathbf{Adv}^{\mathrm{dcdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}})^t$. The theorem now follows. ∎

Lemma 8 *The probability of every element of the coefficient matrix $(e_{\iota\nu})_{t\times t}$ being chosen independently and uniformly at random is at least $(1-\frac{1}{p})^t$.*

Proof: Let $\mathcal{E}_\iota = (e_{\iota 0}, e_{\iota 1}, \cdots, e_{\iota(t-1)})$, with $\iota = 0, 1, \cdots, t-1$. We first provide an explicit expression of $\mathcal{E}_\iota$ for equation (9) with $0 \leq \iota \leq t-1$. For brevity, let $x_i = [g^{ab}]_i$ and $y_i = [g^{C_\iota}]_i$ for $0 \leq i \leq t-1$. Then

$$g^{ab} = \sum_{i=0}^{t-1} x_i x^i \quad \text{and} \quad g^{C_\iota} = \sum_{j=0}^{t-1} y_j^{(\iota)} x^j.$$

We observe two simple facts: first, if one can compute all variables x_i $(0 \le i \le t-1)$ then one can recover g^{ab}; second, each variable $y_j^{(\iota)}$ $(0 \le j \le t-1)$ is uniformly and independently chosen at random. Suppose that

$$(\sum_{i=0}^{t-1} x_i x^i)(\sum_{j=0}^{t-1} y_j^{(\iota)} x^j) = \sum_{k=0}^{2t-2} \alpha_k^{(\iota)} x^k.$$

It is easy to see that

$$\alpha_k^{(\iota)} = \sum_{\substack{i+j=k \\ 0 \le i,j \le t-1}} x_i y_j^{(\iota)}.$$

Equation (9) can be written as

$$\sum_{v=0}^{t-1} [g^{A_\iota B_\iota}]_v x^v \equiv \sum_{k=0}^{2t-2} \alpha_k^{(\iota)} x^k \bmod h(x). \tag{11}$$

By a rather complex calculation, we obtain from equation (10) for $0 \le v \le t-1$,

$$[g^{A_\iota B_\iota}]_v = \alpha_v^{(\iota)} - \sum_{i=0}^{v} h_i \beta_{t-1-v+i}^{(\iota)},$$

where we have

$$\beta_1^{(\iota)} = \alpha_{2t-2}^{(\iota)},$$

and for $2 \le k \le t-1$

$$\beta_k^{(\iota)} = \alpha_{2t-k-1}^{(\iota)} - \sum_{i=1}^{k-1} h_{t-k+i} \beta_i^{(\iota)}.$$

In particular, we are interested in the equation for d-th coordinate

$$[g^{A_\iota B_\iota}]_d = \alpha_d^{(\iota)} - \sum_{i=0}^{d} h_i \beta_{t-1-d+i}^{(\iota)}.$$

From the definition of $\beta_i^{(\iota)}$ for $1 \le i \le t-1$, we have

$$[g^{A_\iota B_\iota}]_d = \alpha_d^{(\iota)} + \xi_t \alpha_t^{(\iota)} + \xi_{t+1} \alpha_{t+1}^{(\iota)} + \xi_{t+2} \alpha_{t+2}^{(\iota)} + \cdots \xi_{2t-2} \alpha_{2t-2}^{(\iota)}, \tag{12}$$

where each ξ_z $(t \le z \le 2t-2)$ is a *non-trivial* polynomial of $h_0, h_1, \cdots$, and h_{t-1} (and has the form of $\sum h_0^{i_0} h_1^{i_1} \cdots h_{t-2}^{i_{t-2}} h_{t-1}^{i_{t-1}}$ satisfying $i_0 + i_1 + \cdots + i_{t-1} \le t-1$), and $\deg(\xi_z) = z - t + 1$. It is important to note that $\xi_t = h_d$.

Expanding $\alpha_k^{(\iota)} = \sum_{\substack{i+j=k \\ 0 \le i,j \le t-1}} x_i y_j^{(\iota)}$, equation (12) can be written as

$$[g^{A_\iota B_\iota}]_d = y_d^{(\iota)} x_0 + \sum_{i=1}^{d} \big(y_{d-i}^{(\iota)} + \sum_{j=1}^{i} \xi_{t+j-1} y_{t-i+j-1}^{(\iota)}\big) x_i + \sum_{i=d+1}^{t-1} \big(\sum_{j=1}^{i} \xi_{t+j-1} y_{t-i+j-1}^{(\iota)}\big) x_i. \tag{13}$$

Therefore, $\mathcal{E}_{\iota i}$ $(0 \le i \le t-1)$can be represented as follows:

$$e_{\iota i} = \begin{cases} y_d^{(\iota)}, & (i=0) \\ y_{d-i}^{(\iota)} + \sum_{j=1}^{i} \xi_{t+j-1} y_{t-i+j-1}^{(\iota)}, & (1 \le i \le d) \\ \sum_{j=1}^{i} \xi_{t+j-1} y_{t-i+j-1}^{(\iota)}, & (d+1 \le i \le t-1). \end{cases}$$

(1)All entries are uniformly distributed at random. Recall that all $y_i^{(\iota)}$, $0 \le i \le t-1$, are uniformly distributed at random and $\xi_z, t \le z \le 2t-2$, are polynomials of $h_0, h_1, \cdots, h_{t-1}$.

First, the first $d+1$ entries in $\mathcal{E}_\iota$ (*i.e.,* $e_{\iota 0}, e_{\iota 1}, \cdots, e_{\iota d}$) are clearly uniformly distributed at random, since each $e_{\iota i}$ $(0 \le i \le d)$ contains a term $y_{d-i}^{(\iota)}$.

We now examine the rest $t-1-d$ entries in $\mathcal{E}_\iota$. As $h(x)$ is irreducible, we know at least $h_0 \neq 0$. Denote by h_c $(0 \le c \le d)$ the "last" non-zero element among $h_0, h_1, \cdots, h_d$ such that $h_{c+1} = h_{c+2} = \cdots = h_d = 0$ and $h_c \neq 0$. Hence, according to the equation (11), we have $\xi_t = \cdots = \xi_{t+d-c-1} = 0$ and $\xi_{t+d-c} = h_c$. Since each $e_{\iota i}$ $(d+1 \le i \le t-1)$ contains a term $\xi_{t+d-c} y_{t-i+d-c}^{(\iota)}$ where ξ_{t+d-c} is non-zero and $y_{t-i+d-c}^{(\iota)}$ is uniformly distributed at random, these $t-1-d$ entries of $\mathcal{E}_\iota$ are also uniformly distributed at random.

(2) All entries are linearly independent. We observe that since independently random numbers are used for different rows, any two entries from two different rows are linearly independent. We now prove that with high probability all entries from the same row are *also* linearly independent. Again we consider with loss of generality the first row of the coefficient matrix (*i.e.,* the vector $\mathcal{E}_1$).

Note that each entry of $\mathcal{E}_1$ is a linear combination of $y_0^{(1)}, \cdots, y_{t-1}^{(1)}$. Regarding each such entry as a column vector, we can obtain for the first row a $t \times t$ square matrix—$M_{h,d}$. Denote by γ_i $(0 \le i \le t-1)$ the i-th column vector of matrix $M_{h,d}$, *i.e.,* $e_{1i} = (y_0^{(1)}, \cdots, y_{t-1}^{(1)}) \cdot \gamma_i$.

$$M_{h,d} = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ \\ d-2 \\ d-1 \\ d \\ d+1 \\ \\ t-3 \\ t-2 \\ t-1 \end{array} \begin{array}{c} \begin{array}{ccccccccccccc} 0 & 1 & 2 & & d-2 & d-1 & d & d+1 & & t-3 & t-2 & t-1 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & \xi_t \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 & \xi_t & \xi_{t+1} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & * & \cdots & \xi_{t+d-5} & \xi_{t+d-4} & \xi_{t+d-3} \\ 0 & 1 & 0 & \cdots & 0 & 0 & * & * & \cdots & \xi_{t+d-4} & \xi_{t+d-3} & \xi_{t+d-2} \\ 1 & 0 & 0 & \cdots & 0 & * & * & * & \cdots & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d-1} \\ 0 & 0 & 0 & \cdots & * & * & * & * & \cdots & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \xi_{t+d-5} & \xi_{t+d-4} & \xi_{t+d-3} & \xi_{t+d-2} & \cdots & \xi_{2t-6} & \xi_{2t-5} & \xi_{2t-4} \\ 0 & 0 & \xi_t & \cdots & \xi_{t+d-4} & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d-1} & \cdots & \xi_{2t-5} & \xi_{2t-4} & \xi_{2t-3} \\ 0 & \xi_t & \xi_{t+1} & \cdots & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d-1} & \xi_{t+d} & \cdots & \xi_{2t-4} & \xi_{2t-3} & \xi_{2t-2} \end{pmatrix} \end{array}$$

where we have ξ_{t+i} $(0 \leq i \leq t-2)$ has the following form:

$$\xi_{t+i} = \begin{cases} -h_d, & (i=0) \\ -h_{d-i} - \sum_{j=0}^{i-1} \xi_{t+j} h_{t-i+j}, & (1 \leq i \leq d) \\ -\sum_{j=0}^{i-1} \xi_{t+j} h_{t-i+j}, & (d+1 \leq i \leq t-2). \end{cases}$$

We claim that all ξ_{t+i} $(0 \leq i \leq t-2)$ are independently and uniformly distributed at random. This is because each ξ_{t+i} $(0 \leq i \leq t-2)$ contains a term $h_d h_{t-i}$ and $h_0, \cdots, h_{t-1}$ are uniformly and independently distributed.

It is easy to see that $\gamma_0, \cdots, \gamma_d$ are independently distributed over $\mathbb{F}_p$. We now prove that the probability that $\gamma_0, \cdots, \gamma_d, \gamma_{d+1}$ are also linearly independent over $\mathbb{F}_p$ is $1 - \frac{1}{p}$. Here we consider the case $d > [t/2] + 1$. (The case $d \leq [t/2] + 1$ is simpler.) If $\gamma_0, \cdots, \gamma_d, \gamma_{d+1}$ are linearly dependent over $\mathbb{F}_p$, there exist $a_0, \cdots, a_d \in \mathbb{F}_p$ such that

$$a_0\gamma_0 + a_1\gamma_1 + \cdots + a_d\gamma_d = \gamma_{d+1}.$$

Let $i_0 = 2d - t$ and $j_0 = t - d$. We have the following $d+2$ equations:

$$\begin{array}{lcl} a_d & = & \cdots = a_{i_0+1} = 0, \\ a_{i_0} & = & \xi_t, \\ a_{i_0-1} + a_{d+1}\xi_t & = & \xi_{t+1}, \\ \cdots & \cdots & \cdots \\ a_0 + a_{j_0}\xi_t + \cdots + a_d\xi_{t+d+1-j_0} & = & \xi_{t+d+2-j_0}, \\ a_{j_0-1}\xi_t + \cdots + a_d\xi_{t+d+2-j_0} & = & \xi_{t+d+3-j_0}. \end{array}$$

Note that $a_0, \cdots, a_d$ can be uniquely determined by the first $d+1$ equations. Since $\xi_{t+d+3-j_0}$ is independent from $\xi_t, \cdots, \xi_{t+d+2-j_0}$, the probability that the last equation holds is $\frac{1}{p}$. Hence, we know the probability that $\gamma_0, \cdots, \gamma_d, \gamma_{d+1}$ are independently distributed over $\mathbb{F}_p$ is $1 - \frac{1}{p}$.

We can prove inductively that for any $d+2 \leq k \leq t$ the probability that $\gamma_0, \cdots, \gamma_d, \gamma_{d+1}, \cdots \gamma_k$ are independent over $\mathbb{F}_p$ is $1 - \frac{1}{p}$. We conclude that the probability that $\gamma_0, \cdots, \gamma_d, \gamma_{d+1}, \cdots \gamma_t$ are independently distributed over $\mathbb{F}_p$ is at least $(1 - \frac{1}{p})^t$. This completes the proof of this lemma. □

E. Proof of Theorem 5

The proof is simpler than that of Theorem 4. As in Theorem 4, the crux is to show that each element of the coefficient matrix is independently and uniformly distributed at random. For both 0-th CDH problem and $(t-1)$-th CDH problem, it is easy to argue the uniformity property. Note that this property only depends on (r_i, s_i) but not the coefficients in $h(x)$. Now let's look at the independence property. The matrices $M_{h,0}$ and $M_{h,t-1}$ are of the following form:

$$M_{h,0} = \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & h_0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & h_0 & \xi_{t+1} \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & \xi_{t+d-5} & \xi_{t+d-4} & \xi_{t+d-3} \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & h_0 & \cdots & \xi_{t+d-4} & \xi_{t+d-3} & \xi_{t+d-2} \\
0 & 0 & 0 & \cdots & 0 & 0 & h_0 & * & \cdots & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d-1} \\
0 & 0 & 0 & \cdots & 0 & h_0 & * & * & \cdots & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d} \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & \xi_{t+d-5} & \xi_{t+d-4} & \xi_{t+d-3} & \xi_{t+d-2} & \cdots & \xi_{2t-6} & \xi_{2t-5} & \xi_{2t-4} \\
0 & 0 & h_0 & \cdots & \xi_{t+d-4} & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d-1} & \cdots & \xi_{2t-5} & \xi_{2t-4} & \xi_{2t-3} \\
0 & h_0 & \xi_{t+1} & \cdots & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d-1} & \xi_{t+d} & \cdots & \xi_{2t-4} & \xi_{2t-3} & \xi_{2t-2}
\end{pmatrix}$$

$$M_{h,t-1} = \begin{pmatrix}
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & h_0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 1 & h_0 & \xi_{t+1} \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & \cdots & \xi_{t+d-5} & \xi_{t+d-4} & \xi_{t+d-3} \\
0 & 0 & 0 & \cdots & 0 & 0 & 1 & * & \cdots & \xi_{t+d-4} & \xi_{t+d-3} & \xi_{t+d-2} \\
0 & 0 & 0 & \cdots & 0 & 1 & * & * & \cdots & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d-1} \\
0 & 0 & 0 & \cdots & 1 & * & * & * & \cdots & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d} \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
0 & 0 & 1 & \cdots & \xi_{t+d-5} & \xi_{t+d-4} & \xi_{t+d-3} & \xi_{t+d-2} & \cdots & \xi_{2t-6} & \xi_{2t-5} & \xi_{2t-4} \\
0 & 1 & h_0 & \cdots & \xi_{t+d-4} & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d-1} & \cdots & \xi_{2t-5} & \xi_{2t-4} & \xi_{2t-3} \\
1 & h_0 & \xi_{t+1} & \cdots & \xi_{t+d-3} & \xi_{t+d-2} & \xi_{t+d-1} & \xi_{t+d} & \cdots & \xi_{2t-4} & \xi_{2t-3} & \xi_{2t-2}
\end{pmatrix}$$

For $M_{h,0}$, we know $h_0 \neq 0$, as otherwise h would be reducible. $M_{h,t-1}$ is simply an anti-triangular matrix. It is easy to see that both matrices are of full rank with probability 1. Theorem 5 easily follows.

F. Proof of Theorem 6

For an element $\alpha \in \mathbb{F}_{p^t}$ and a monic irreducible polynomial $h \in I_t(p)$, $\lambda \xleftarrow{\$} \mathbb{F}_p^*$, the prediction oracle $\mathcal{O}$ gives noisy access to the codeword $B_k(\lambda^d[\alpha]_d)$. Note that when $d \neq 1$ the above code is not *multiplicative*. Again, this would make it hard to prove concentration and recoverability. In order to apply the techniques of [1], we would need noisy access to the multiplication code

$$C_\alpha : \mathbb{F}_p \mapsto \{\pm 1\}, \quad \text{defined as} \quad C_\alpha(\lambda) = B_k(\lambda[\alpha]_d) \quad (\text{extended by} \quad C_\alpha(0) = -1).$$

We construct another oracle $\mathcal{O}'$ that takes as input a base representation $h \in I_t(p)$, a Diffie-Hellman triple $g, g^a, g^b \in \mathbb{F}_{p^t}$, and $\lambda \xleftarrow{\$} \mathbb{F}_p^*$, and returns $\mathcal{O}(h, r_\lambda, g, g^a, g^b)$ if λ is a d-th residue modulo p, where $r_\lambda^d \equiv \lambda (\text{mod } p)$, otherwise tosses a β_k-biased coin.

Suppose that there exists an oracle $\mathcal{O}$ such that

$$\Big| \Pr_{\lambda,a,b} \big[\mathcal{O}(h, \lambda, g, g^a, g^b) = B_k\big(\big[\phi_{h,\widehat{h}_\lambda}(g^{ab})\big]_d\big)\big] - \beta_k \Big| \geq \epsilon \tag{14}$$

where ϵ is a non-negligible quantity. Following the technique in Boneh and Shparlinski [5], we now show that

$$\big|\Pr_{\lambda,a,b}\big[\mathcal{O}'(h,\lambda,g,g^a,g^b) = B_k\big(\lambda\big[g^{ab}\big]_d\big)\big] - \beta_k\big| \geq \epsilon/d.$$

Let $E_{g^{ab}}$ be the event that $\mathcal{O}'(h,\lambda,g,g^a,g^b) = B_k\big(\lambda\big[g^{ab}\big]_d\big)$. Note that if λ is uniform in $\mathbb{F}_p^d \setminus \{0\}$ then r_λ is uniform in $\mathbb{F}_p^*$. Therefore, we have

$$\begin{aligned}
\Pr[E_{g^{ab}}] &= \tfrac{1}{(d,p-1)}\Pr[E_{g^{ab}}|\lambda \in \mathbb{F}_p^d] + (1 - \tfrac{1}{(d,p-1)})\Pr[E_{g^{ab}}|\lambda \notin \mathbb{F}_p^d] \quad \text{(according to Lemma 5)} \\
&\geq \tfrac{1}{(d,p-1)}(\beta_k + \epsilon) + (1 - \tfrac{1}{(d,p-1)})\beta_k \quad \text{(according to condition (14))} \\
&= \beta_k + \tfrac{\epsilon}{(d,p-1)} \geq \beta_k + \tfrac{\epsilon}{d}.
\end{aligned}$$

Note that $t > d$ and therefore the above quantity is non-negligible.

Accessibility. The oracle $\mathcal{O}'$ allows us to have access to a corrupted codeword $\widetilde{C}_\alpha$ of the above codeword defined as $\widetilde{C}_\alpha = \mathcal{O}'(h,\lambda,g,g^a,g^b)$. Therefore, if the oracle $\mathcal{O}$ has advantage ϵ then we have $|\Pr[C_\alpha(\lambda) = \widetilde{C}_\alpha(\lambda)]| \geq \beta_k + \epsilon/d$. Accessibility of the code C_α follows.

Concentration. The proof is similar to that of Theorem 2. For a threshold $\tau > 0$, the τ-heavy characters of C_α belong to the set

$$\Gamma_{\alpha,\tau} = \{\chi_\beta \colon \beta = \lambda[\alpha]_d \text{ for } \lambda \in \Gamma_\tau\},$$

where Γ_τ is a set containing the τ-heavy coefficients of the function B_k. For each $\lambda \in \Gamma_\tau$, there exists a unique integer pair $(\xi_\lambda, \varsigma_\lambda) \in [0, 1/\tau] \times [0, 1/\tau]$. As in Theorem 2, the proof for concentration of the code $C_\alpha(\lambda)$ is now similar to those of [10, 16].

Recoverability. First, by Lemma 1 we know that there exists a threshold τ which is polynomial in the non-negligible quantity ϵ and at least one τ-heavy Fourier character $\chi \neq 0$ for C_α and $\widetilde{C}_\alpha$ such that $\chi \in \mathsf{Heavy}_\tau(C_\alpha) \cap \mathsf{Heavy}_\tau(\widetilde{C}_\alpha)$.

Given a polynomial $h(x) \in I_t(p)$, on input $g, g^a, g^b \in \mathbb{F}_{p^t}$, the following algorithm that has access to $\mathcal{O}$ produces a polynomial size list of elements in $\mathbb{F}_{p^t}$ which contains g^{ab} with probability $1 - \delta$.

Let τ be the threshold determined by Lemma 1. We write $\alpha = \sum_{i=0}^{t-1}[\alpha]_i x^i$ to denote $g^{ab} \in \mathbb{F}_{p^t}$. Again using the learning algorithm of AGS [1], we obtain a polynomial size list L_α of all the τ-heavy Fourier characters for $\widetilde{C}_\alpha$. If χ_β is a non-trivial τ-heavy character for C_α, we have $[\alpha]_d = \lambda^{-1}\beta$. Given $\chi_\beta \in L_\alpha$, we define $L_\beta = \{[\alpha]_d \colon [\alpha]_d = \lambda^{-1}\beta \text{ for } \lambda \in \Gamma_\tau\}$.

Let $L = \bigcup_{\chi_\beta \in L_\alpha} L_\beta$, which is a set of polynomial size. Also we have $\alpha \in L$ with probability $1 - \delta$. We can guess a result for $[\alpha]_d$ and hence get $[g^{ab}]_d$. The theorem now follows. ∎