Bit Security of the CDH Problems over Finite Fields

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

[1] Shandong University, Jinan, China
wangmingqiang@sdu.edu.cn, zhantao@moe.edu.cn
[2] University of North Carolina, Chapel Hill, Chapel Hill, USA
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) made 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.

Keywords: 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 [4,14] 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 [13,19], 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 (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 $h(x) = x^2 + h_1 x + h_0$ be a monic

O. Dunkelman and L. Keliher (Eds.): SAC 2015, LNCS 9566, pp. 441–461, 2016.
DOI: 10.1007/978-3-319-31301-6_25

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 $g = g_1 x + g_0$ 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, Sect. 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 $0 \le d \le t-1$. 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 that the hardness of d-th CDH problem had already been studied in [20,22]. Verheul [22, 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 such that the algorithm can have exponential running time in t.

Shparlinski [20] generalized Verheul's result to handle the case of *noisy* oracles (which return correct answers with some probabilities). Shparlinski's reduction uses a strategy that is the same as Verheul's to limit the behavior of the oracle. Namely, the queries given to the d-th CDH oracle have the form of $(g^x, g^y \cdot g^r)$ with uniformly chosen r. In this case, it is not guaranteed that the noisy d-th CDH oracle would answer this type of queries correctly. It might well be the case that a malicious d-th CDH problem oracle (adversary) simply always returns 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 problematic in the sense it failed to prove what's claimed in the presence of noisy oracles. (Note that Verheul's reduction does not suffer from the same problem, as the answers returned by the perfect oracles are always correct.)

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 [22] and Shparlinski [20]. 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 [18] and Duc and Jetchev [8]. Up to now, the list decoding approach has only been proven successful for multiplicative codes [1,8,18]. 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 the 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, Sect. 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 those 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 those 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.

1.2 Further History and Discussion

An earlier version was put online [23]. Galbraith and Shani [11] extended our work to obtain an essentially stronger hard-core result that works for every individual bit for any finite fields $\mathbb{F}_{p^t}$ with *any* t. Thus, as claimed by the authors, this improvement can allow us to consider "the case of large t, and in particular the case of fields with small characteristic" [11, p. 264]. We certainly agree with this point of view, but one may not understand that our reduction approach is inherently defective. The security loss in our reduction only comes from the loss in proving the equivalence between the d-th CDH problem and the conventional CDH problem. If one can find a way to prove their equivalence with no security loss, as what we did for the case of perfect oracles, our result can be equally expressive.

As commented by Galbraith and Shani [11, Remark 25], their approach does not work for the popular polynomial basis, while our approach deals with this case, and therefore our result will be useful when one desires a hard-core bit in its polynomial basis.

Another reason that makes our paper worth attending to is that as discussed earlier, we point out the "problem" of studying the hardness of the d-th CDH problem in prior work by Shparlinski [20]. We regard identifying the problem and providing a more general and correct proof as an important contribution of the paper. However, one may not really deem Verheul's result [22] as being "faulty" or "flawed"; rather, it is that our result provides a stronger result for the problem.

By the same token, with Verheul's result, one may regard that FGPS is actually the first (though they did not notice this) to solve the open problem whether there exists "specific" hard-core bits over finite fields: half of the individual bits of the secret CDH value over $\mathbb{F}_{p^2}$ are unpredictable. If one is uncomfortable about their restricted reduction from CDH to d-th CDH, our result for the case of both perfects oracles and noisy oracles can then come into use.

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 $\epsilon > 0$.

This and subsequent definitions can be readily made *asymptotic* by requiring that ϵ depend on the security parameter.

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 χ_α is τ-heavy if the weight of its corresponding Fourier coefficient is at least τ. The set of all τ-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 the message 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 $\mathcal{C} = \{C_\alpha\colon \mathbb{Z}_n \to \{\pm 1\}\}$ is concentrated if each of its codewords C_α is Fourier concentrated.*

Definition 4 (Recoverable code). *A code $\mathcal{C} = \{C_\alpha\colon \mathbb{Z}_n \to \{\pm 1\}\}$ 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., $\{\alpha \in \mathbb{Z}_n\colon \chi \in \mathsf{Heavy}_\tau(C_\alpha)\}$).*

Lemma 1 below shows that in a concentrated code $\mathcal{C}$, any corrupted ("noisy") versions $\widetilde{C}_\alpha$ 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 $f, g\colon \mathbb{Z}_n \to \{\pm 1\}$ 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 $\chi \neq 0$ which is 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* $w\colon \mathbb{Z}_n \to \{\pm 1\}$, $\tau > 0$ *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 $f\colon \mathcal{D} \to \mathcal{R}$ 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 [13] 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 [18] 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.

Roughly speaking, accessibility is related to both the code and the oracle, while concentration and recoverability concern the code itself. 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 Sect. 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*

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

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 that 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 $\mathbf{Adv}^{\mathrm{cdh}}_{\mathcal{B},h,\mathbb{F}_{p^2}} \geq (1-\frac{1}{p}) \cdot (\mathbf{Adv}^{\mathrm{pcdh}}_{\mathcal{A},h,\mathbb{F}_{p^2}})^2$.*

Proof: 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

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

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

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

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

Combining the above two equations, 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.,*

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

Note that $[g^C]_i$ and $[g^{C'}]_i$ $(i = 0, 1)$ in the above equation 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. ∎

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 our full paper [23]. 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:*

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

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 $\eta \in \mathbb{F}_p$, 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 [1,8,18]. 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. This follows from a (well-known) scaling property of the Fourier transform, as shown in Lemma 4 below. 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 first describe the scaling property of the Fourier transform.

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 Theorem 2: Suppose that there exists an oracle $\mathcal{O}$ such that

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

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

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

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 [10,18], 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 [18] 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 Sect. 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 [18] 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 [18, Lemma 9], the size of Γ_τ is at most $4\tau^{-2}$.

Recoverability. The proof for recoverability is similar to those of [10,18]. 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. ∎

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 $1 \leq k \leq 2l$) 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:*

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

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 $k \leq l$, 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 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*

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

is negligible in l.

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

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

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 $(0 \le d \le t-1)$ 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 field 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 $\mathbf{Adv}^{\mathrm{cdh}}_{\mathcal{B},\mathbb{F}_{p^t}} \ge (1-\frac{1}{p})^t \cdot e^{-\frac{2}{p-1}} \cdot (\mathbf{Adv}^{\mathrm{dcdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}})^t$.*

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. The proof of the lemma is fairly easy and can be found in our full paper [23].

Lemma 5. *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 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 integers $(r_\iota, s_\iota) \xleftarrow{\$} (\mathbb{Z}_{p^t-1})^2$ $(\iota = 0, 1, \cdots, t-1)$, 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.*,

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

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 $e_{\iota\nu} \in \mathbb{F}_p$ $(0 \le \iota, \nu \le t-1)$ such that

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

If the coefficient matrix $(e_{\iota\nu})_{t\times t}$ for the above equation set 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 can show (with the proof in our full paper [23]) 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 5 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. ▮

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 field 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., $\mathbf{Adv}^{\mathrm{(t-1)cdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}}$) 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., $\mathbf{Adv}^{\mathrm{cdh}}_{\mathcal{B},\mathbb{F}_{p^t}} \geq e^{-\frac{2}{p-1}} \cdot (\mathbf{Adv}^{\mathrm{(t-1)cdh}}_{\mathcal{A},h,\mathbb{F}_{p^t}})^t$).*

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 [22], 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 6. *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 7. *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:*

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

Proof: 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

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

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 $r_\lambda^d \equiv \lambda (\bmod\, p)$, otherwise tosses a β_k-biased coin.

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

$$\Big| \Pr_{\lambda,a,b}\big[\mathcal{O}(h,\lambda,g,g^a,g^b) = B_k\big(\big[\phi_{h,\widehat{h}_\lambda}(g^{ab})\big]_d\big)\big] - \beta_k\Big| \geq \epsilon \qquad (2)$$

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 $\mathbb{F}_p^d \backslash \{0\}$ then r_λ is uniform in $\mathbb{F}_p^*$. Therefore, we have

$$\begin{aligned}
\Pr[E_{g^{ab}}] &= \frac{1}{(d,p-1)} \Pr[E_{g^{ab}} | \lambda \in \mathbb{F}_p^d] + (1 - \frac{1}{(d,p-1)}) \Pr[E_{g^{ab}} | \lambda \notin \mathbb{F}_p^d] \quad (\text{Lemma 6}) \\
&\geq \frac{1}{(d,p-1)}(\beta_k + \epsilon) + (1 - \frac{1}{(d,p-1)})\beta_k \quad (\text{condition (2)}) \\
&= \beta_k + \frac{\epsilon}{(d,p-1)} \geq \beta_k + \frac{\epsilon}{d}.
\end{aligned}$$

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 [10,18].

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. ▮

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.

Following from Theorems 4 and 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:*

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

Following from Theorems 5 and 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:*

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

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 $t > 1$ [20,22]. 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. Mingqiang Wang is supported by National 973 Grant 2013CB834205 and NSFC Grant 61272035. Haibin Zhang is supported by NSF CNS 1228828. We are greatly indebted to SAC15 and past PC members for their valuable comments and corrections. Many thanks to William E. Skeith 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.

References

1. Akavia, A., Goldwasser, S., Safra, S.: Proving hard-core predicates using list decoding. In: FOCS, pp. 146–157. IEEE Computer Society (2003)
2. Alexi, W., Chor, B., Goldreich, O., Schnorr, C.: RSA and Rabin functions: certain parts are as hard as the whole. SIAM J. Comput. **17**(2), 194–209 (1988)
3. Ben-Or, M.: Probabilistic algorithms in finite fields. In: FOCS 1981, vol. 11, pp. 394–398 (1981)
4. Blum, M., Micali, S.: How to generate cryptographically strong sequences of pseudorandom bits. SIAM J. Comput. **13**(4), 850–864 (1984)
5. Boneh, D., Shparlinski, I.E.: On the unpredictability of bits of the elliptic curve Diffie-Hellman scheme. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 201–212. Springer, Heidelberg (2001)
6. Boneh, D., Venkatesan, R.: Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 129–142. Springer, Heidelberg (1996)
7. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theor. **22**(6), 644–654 (1976)

8. Duc, A., Jetchev, D.: Hardness of computing individual bits for one-way functions on elliptic curves. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 832–849. Springer, Heidelberg (2012)
9. ElGamal, T.: A public-key cryptosystem, a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theor. **IT–31**(4), 469–472 (1985)
10. Fazio, N., Gennaro, R., Perera, I.M., Skeith III, W.E.: Hard-core predicates for a Diffie-Hellman problem over finite fields. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 148–165. Springer, Heidelberg (2013)
11. Galbraith, S.D., Shani, B.: The multivariate hidden number problem. In: Lehmann, A., Wolf, S. (eds.) ICITS 2015. LNCS, vol. 9063, pp. 250–268. Springer, Heidelberg (2015)
12. von Zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, Cambridge (1999)
13. Goldreich, O., Levin, L.A.: A hard-core predicate for all one-way functions. In: STOC, pp. 25–32. ACM Press (1989)
14. Goldwasser, S., Micali, S.: Probabilistic encryption. JCSS **28**(2), 270–299 (1984)
15. Håstad, J., Näslund, M.: The security of individual RSA bits. In: FOCS, pp. 510–521 (1998)
16. Joux, A.: A new index calculus algorithm with complexity L(1/4 + o(1)) in small characteristic. In: Lange, T., Lauter, K., Lisoněk, P. (eds.) SAC 2013. LNCS, vol. 8282, pp. 355–380. Springer, Heidelberg (2014)
17. Lidl, R., Niederreiter, H.: Finite Fields. Addison-Wesley, Reading (1983)
18. Morillo, P., Ràfols, C.: The security of all bits using list decoding. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 15–33. Springer, Heidelberg (2009)
19. Näslund, M.: All bits in $ax + b$ mod p are hard. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 114–128. Springer, Heidelberg (1996)
20. Shparlinski, I.E.: Security of polynomial transformations of the Diffie-Hellman key. Finite Fields Appl. **10**(1), 123–131 (2014)
21. Slinko, A.: A generalization of Komlós's theorem on random matrices. N. Z. J. Math. **30**(1), 81–86 (2001)
22. Verheul, E.R.: Certificates of recoverability with scalable recovery agent security. In: Imai, H., Zheng, Y. (eds.) PKC 2000. LNCS, vol. 1751, pp. 258–275. Springer, Heidelberg (2000)
23. Wang, M., Zhan, T., Zhang, H.: Bit security of the CDH problems over finite fields. Full version, Cryptology ePrint Archive: Report 2014/685. http://eprint.iacr.org