Bits Security of the CDH Problems over Finite Fields

Mingqiang Wang
Shandong University
wangmingqiang@sdu.edu.cn

Tao Zhan
Shandong University
zhantao@moe.edu.cn

Haibin Zhang
UC Davis
hbzhang@ucdavis.edu

One-Way Functions and Hard-Core Predicates

- One-way function $f : D \rightarrow R$
- Hard-core predicate $P : D \rightarrow \{0,1\}$

For $\forall$ PPT adversary A

$$\Pr[A(f(x)) = P(x)] \leq 1/2 + negl.$$

Generic vs. Specific Approaches for Hard-Core Predicates

- Generic approaches:
  -working for any one-way functions
  -Goldreich-Levin (1989), Näslund (1996)

- Specific approaches:
  -discrete logs (1984)
  -RSA,Rabin (1988)
  ...
  -CDH (finite fields)? A long-standing open problem

FGPS (2013): First Known Results over Finite Fields

- Fazio, Gennaro, Perera, Skeith III, FGPS, Crypto 2013
- Basic Fact: F_{p^2} is isomorphic to $F[x]/(h(x))$

  $g \in F_{p^2}$ can be written as $g_0 + g_1 x$ or (g_0, g_1)

- Partial CDH problem over F_{p^2}

  $$\text{Compute}\,[g^{ab}]_1 \text{ given } g, g^a, g^b \in F_{p^2}$$

- Main result of FGPS: Every single bit in $[g^{ab}]_1$ is hard-core over a random representation of the field F_{p^2}.

Open Problems Remain

- Old open problem:

  1. Specific hard-core predicates over finite fields for regular CDH problems.

- New open problems from FGPS:

  2. hardness of Partial-CDH problem over F_{p^2}

  3. results hold for F_{p^t} (t>1)?

Our Results: Resolving the Open Problems

- 1. Partial-CDH is as hard as CDH over F_{p^2}.
- 2. All CDH bits over F_{p^2} are hard-core.
- 3. Define a generalized class of problems---*d*-th CDH problems over F_{p^t} (t>1) for $0 \le d \le t-1$:

$$\text{Compute } [g^{ab}]_d \text{ given } g, g^a, g^b \in F_{p^t}$$

  We prove they are *all* as hard as CDH.
- 4. Almost all individual bits over F_{p^t} (t>1) are hard-core.

- 5'. Advanced list-decoding approach.

FGPS

- Result: Half the bits in F_{p^2} are hard-core for a weaker CDH problem.
- Question: Hardness of Partial-CDH?
- Question: Hard-core predicates over F_{p^t}?

Ours

- 1.Stronger: All the bits in F_{p^2} are hard-core for regular CDH problem.
- 2. Anwer: Partial-CDH and its generalization (*d*-th CDH) are as hard as CDH.
- 3. Answer: Almost all bits in F_{p^t} are hard-core.

- 1+3: Proving the existence of specific hard-core bits for CDH over finite fields.

Still Two Open Problems

- 1. From "almost all" to "all" bits over F_{p^t} (t>1)?
- 2. CDH hard-core predicates over F_p?

Bits Security of the CDH Problems over Finite Fields

- Currently as a technical report:

  http://csiflabs.cs.ucdavis.edu/~hbzhang/cdh.pdf

- Comments are appreciated! Thank you!