ETH zürich

Foundations of Cryptography
foc.ethz.ch

Worst-Case Subexponential Attacks on PRGs of Constant Degree or Constant Locality

Akın Ünal
akin.uenal@inf.ethz.ch
24.04.2023

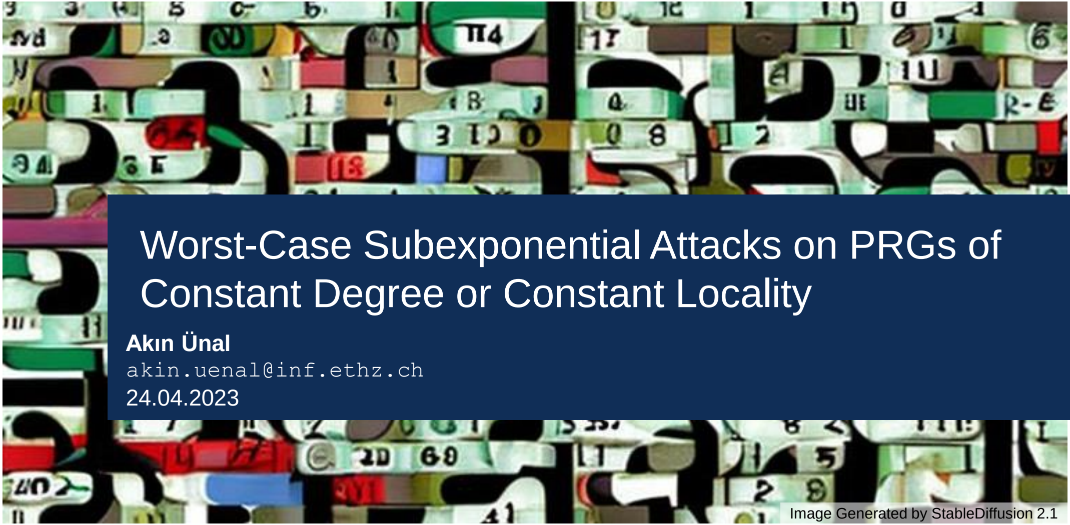


Image Generated by StableDiffusion 2.1

Motivation

Gay-Pass STOC`21
subexp. LWE
+
circular Shielded Randomness
Leakage-security of GSW

Jain-Lin-Sahai EC`22
LPN over $\mathbb{Z}_p$
+
Pairings
+
Local PRGs $F : \{0,1\}^n \rightarrow \{0,1\}^{n^{1+e}}$

Motivation

Gay-Pass STOC`21
subexp. LWE
+
circular Shielded Randomness
Leakage-security of GSW

Jain-Lin-Sahai EC`22
LPN over $\mathbb{Z}_p$
+
Pairings
+
Local PRGs $F : \{0,1\}^n \to \{0,1\}^{n^{1+e}}$

They need *subexponential security*
i.e. each ppt adversary must have an advantage of
$\leq 2^{-\lambda^c}$ for some $c > 0$.

Pseudorandom Number Generators (PRGs)

$$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$$

$m \geq n^{1+e}$, $e > 0$ constant

Pseudorandom Number Generators (PRGs)

$$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$$

$m \geq n^{1+e}$, $e > 0$ constant

Attack distinguishes pseudorandomness

$F(x)$ for $x \leftarrow \mathbb{Z}_p^n$

from true randomness

$y \leftarrow \mathbb{Z}_p^m$.

Pseudorandom Number Generators (PRGs)

$$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$$

$m \geq n^{1+e}$, $e > 0$ constant

For $p = 2$, we have normal binary PRGs
$F: \{0,1\}^n \to \{0,1\}^m$.

Attack distinguishes pseudorandomness
$F(x)$ for $x \leftarrow \mathbb{Z}_p^n$
from true randomness
$y \leftarrow \mathbb{Z}_p^m$.

Pseudorandom Number Generators (PRGs)

$$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$$

$m \geq n^{1+e}$, $e > 0$ constant

For $p = 2$, we have normal binary PRGs $F: \{0,1\}^n \to \{0,1\}^m$.

Attack distinguishes pseudorandomness

$F(x)$ for $x \leftarrow \mathbb{Z}_p^n$

from true randomness

$y \leftarrow \mathbb{Z}_p^m$.

Convention

f_i is the function that computes the i-th output value of F.

I.e. $F(x) = \big(f_1(x), \dots, f_m(x)\big)$

Local and Polynomial PRGs

$F: \{0,1\}^n \to \{0,1\}^m$ has **locality** d

iff

each $f_i(x)$ only depends on d bits of $x \in \{0,1\}^n$.

Local and Polynomial PRGs

$F\colon \{0,1\}^n \to \{0,1\}^m$ has **locality** d

iff

each $f_i(x)$ only depends on d bits of $x \in \{0,1\}^n$.

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ has **degree** d

iff

each $f_i(X)$ is a polynomial in $\mathbb{Z}_p[X_1, \dots, X_n]$ of total degree d.

Results – Overview

Subexponential Attack on PRGs

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$

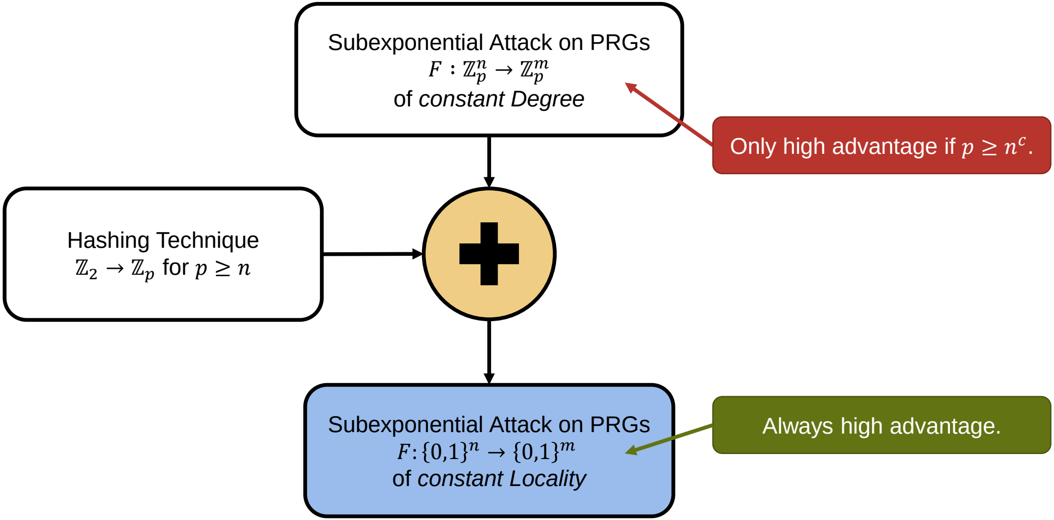
of *constant Degree*

Results – Overview

Subexponential Attack on PRGs
$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$
of *constant Degree*

Only high advantage if $p \geq n^c$.

Results – Overview



Algebraic Attack

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ PRG of degree d

Each $f_i(X_1, \ldots, X_n)$ is a polynomial in $\mathbb{Z}_p[X_1, \ldots, X_n]$ of degree d

How to distinguish $F(x)$, $x \leftarrow \mathbb{Z}_p^n$, from $y \leftarrow \mathbb{Z}_p^m$?

Algebraic Attack

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ PRG of degree d

Each $f_i(X_1, \ldots, X_n)$ is a polynomial in $\mathbb{Z}_p[X_1, \ldots, X_n]$ of degree d

How to distinguish $F(x)$, $x \leftarrow \mathbb{Z}_p^n$, from $y \leftarrow \mathbb{Z}_p^m$?

First Idea
Assume we have a *linear relationship* between $f_1(X), \ldots, f_m(X)$.

Algebraic Attack: Linear Relationship

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ PRG computed by degree-d polynomials $f_1, \dots, f_m \in \mathbb{Z}_p[X_1, \dots, X_n]$.

Let $v \in \mathbb{Z}_p^m, v \neq 0$, be a linear relationship of $f_1, \dots, f_m$ i.e.

$$v_1 \cdot f_1(X) + \cdots + v_m \cdot f_m(X) = 0$$

Algebraic Attack: Linear Relationship

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ PRG computed by degree-d polynomials $f_1, \dots, f_m \in \mathbb{Z}_p[X_1, \dots, X_n]$.

Let $v \in \mathbb{Z}_p^m, v \neq 0$, be a linear relationship of $f_1, \dots, f_m$ i.e.

$$v_1 \cdot f_1(X) + \cdots + v_m \cdot f_m(X) = 0$$

We can use v to distinguish $F(x)$ from y:

For all $x \in \mathbb{Z}_p^n$, we have

$$v_1 \cdot f_1(x) + \cdots + v_m \cdot f_m(x) = 0$$

For $y \leftarrow \mathbb{Z}_p^m$, we have

$$\Pr[v_1 \cdot y_1 + \cdots + v_m \cdot y_m = 0] = \frac{1}{p}$$

Algebraic Attack: Linear Relationship

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ PRG computed by degree-d polynomials $f_1, \dots, f_m \in \mathbb{Z}_p[X_1, \dots, X_n]$.

Let $v \in \mathbb{Z}_p^m, v \neq 0$, be a linear relationship of $f_1, \dots, f_m$ i.e.

$$v_1 \cdot f_1(X) + \cdots + v_m \cdot f_m(X) = 0$$

We can use v to distinguish $F(x)$ from y:

For all $x \in \mathbb{Z}_p^n$, we have

$$v_1 \cdot f_1(x) + \cdots + v_m \cdot f_m(x) = 0$$

For $y \leftarrow \mathbb{Z}_p^m$, we have

$$\Pr[v_1 \cdot y_1 + \cdots + v_m \cdot y_m = 0] = \frac{1}{p}$$

This attack has an advantage of $1 - \frac{1}{p}$

Algebraic Attack: Linear Relationship

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ PRG computed by degree-d polynomials $f_1, \dots, f_m \in \mathbb{Z}_p[X_1, \dots, X_n]$.

Let $v \in \mathbb{Z}_p^m, v \neq 0$, be a linear relationship of $f_1, \dots, f_m$ i.e.

Problem
In general, $f_1, \dots, f_m$ will not be linearly dependent

We can use v to distinguish $F(x)$ from y:

For all $x \in \mathbb{Z}_p^n$, we have

$$v_1 \cdot f_1(x) + \cdots + v_m \cdot f_m(x) = 0$$

For $y \leftarrow \mathbb{Z}_p^m$, we have

$$\Pr[v_1 \cdot y_1 + \cdots + v_m \cdot y_m = 0] = \frac{1}{p}$$

This attack has an advantage of $1 - \frac{1}{p}$

Algebraic Attack: Algebraic Relationship (Zichron 2017)

Idea: Generalize concept of a Linear Relationship

Algebraic Attack: Algebraic Relationship (Zichron 2017)

Idea: Generalize concept of a Linear Relationship

An **algebraic relationship** of $f_1(X), \dots, f_m(X) \in \mathbb{Z}_p[X_1, \dots, X_n]$ is a polynomial $h \in \mathbb{Z}_p[Y_1, \dots, Y_m]$ s.t.

1. $h(Y) \neq 0$
2. $h\big(f_1(X), \dots, f_m(X)\big) = 0$

Algebraic Attack: Algebraic Relationship (Zichron 2017)

Idea: Generalize concept of a Linear Relationship

An **algebraic relationship** of $f_1(X), \dots, f_m(X) \in \mathbb{Z}_p[X_1, \dots, X_n]$ is a polynomial $h \in \mathbb{Z}_p[Y_1, \dots, Y_m]$ s.t.

1. $h(Y) \neq 0$
2. $h\big(f_1(X), \dots, f_m(X)\big) = 0$

We can use h to distinguish $F(x)$ from y:

For all $x \in \mathbb{Z}_p^n$, we have

$$h\big(f_1(x), \dots, f_m(x)\big) = h\big(f_1(X), \dots, f_m(X)\big)(x) = 0$$

For $y \leftarrow \mathbb{Z}_p^m$, we have

$$\Pr[h(y) = 0] \leq \frac{\deg h}{p}$$

Algebraic Attack: Algebraic Relationship (Zichron 2017)

Idea: Generalize concept of a Linear Relationship

An **algebraic relationship** of $f_1(X), \ldots, f_m(X) \in \mathbb{Z}_p[X_1, \ldots, X_n]$ is a polynomial $h \in \mathbb{Z}_p[Y_1, \ldots, Y_m]$ s.t.

1. $h(Y) \neq 0$
2. $h\big(f_1(X), \ldots, f_m(X)\big) = 0$

We can use h to distinguish $F(x)$ from y:

For all $x \in \mathbb{Z}_p^n$, we have

$$h\big(f_1(x), \ldots, f_m(x)\big) = h\big(f_1(X), \ldots, f_m(X)\big)(x) = 0$$

For $y \leftarrow \mathbb{Z}_p^m$, we have

$$\Pr[h(y) = 0] \leq \frac{\deg h}{p}$$

Schwartz-Zippel Lemma

Algebraic Attack: Algebraic Relationship (Zichron 2017)

Idea: Generalize concept of a Linear Relationship

An **algebraic relationship** of $f_1(X), \ldots, f_m(X) \in \mathbb{Z}_p[X_1, \ldots, X_n]$ is a polynomial $h \in \mathbb{Z}_p[Y_1, \ldots, Y_m]$ s.t.

1. $h(Y) \neq 0$
2. $h\big(f_1(X), \ldots, f_m(X)\big) = 0$

We can use h to distinguish $F(x)$ from y:

For all $x \in \mathbb{Z}_p^n$, we have

$$h\big(f_1(x), \ldots, f_m(x)\big) = h\big(f_1(X), \ldots, f_m(X)\big)(x) = 0$$

For $y \leftarrow \mathbb{Z}_p^m$, we have

$$\Pr[h(y) = 0] \leq \frac{\deg h}{p}$$

Schwartz-Zippel Lemma

1. How can we compute h?
2. What is an upper bound for $\deg h$?

Bound Degree of Algebraic Relationship h

$$\phi: \mathbb{Z}_p[Y_1, \dots, Y_m] \to \mathbb{Z}_p[X_1, \dots, X_n]$$
$$g(Y_1, \dots, Y_m) \mapsto g\big(f_1(X), \dots, f_m(X)\big)$$

- ϕ is ring homomorphism

Bound Degree of Algebraic Relationship h

$$\phi: \mathbb{Z}_p[Y_1, \dots, Y_m] \to \mathbb{Z}_p[X_1, \dots, X_n]$$
$$g(Y_1, \dots, Y_m) \mapsto g\big(f_1(X), \dots, f_m(X)\big)$$

- ϕ is ring homomorphism
- $\ker \phi$ contains all algebraic relationships of $f_1, \dots, f_m$

Bound Degree of Algebraic Relationship h

$$\phi_L : \mathbb{Z}_p[Y_1, \dots, Y_m]^{\leq L} \to \mathbb{Z}_p[X_1, \dots, X_n]^{\leq dL}$$
$$g(Y_1, \dots, Y_m) \mapsto g\big(f_1(X), \dots, f_m(X)\big)$$

- ϕ_L is linear homomorphism
- $\ker \phi_L$ contains all algebraic relationships of $f_1, \dots, f_m$ of degree $\leq L$
- $\mathbb{Z}_p[Y_1, \dots, Y_m]^{\leq L} = \{g \in \mathbb{Z}_p[Y_1, \dots, Y_m] : \deg g \leq L\}$
- $\mathbb{Z}_p[X_1, \dots, X_n]^{\leq dL} = \{g \in \mathbb{Z}_p[X_1, \dots, X_n] : \deg g \leq dL\}$

Bound Degree of Algebraic Relationship h

$$\phi_L : \mathbb{Z}_p[Y_1, \dots, Y_m]^{\leq L} \to \mathbb{Z}_p[X_1, \dots, X_n]^{\leq dL}$$
$$g(Y_1, \dots, Y_m) \mapsto g\big(f_1(X), \dots, f_m(X)\big)$$

- ϕ_L is linear homomorphism
- $\ker \phi_L$ contains all algebraic relationships of $f_1, \dots, f_m$ of degree $\leq L$
- $\mathbb{Z}_p[Y_1, \dots, Y_m]^{\leq L} = \{g \in \mathbb{Z}_p[Y_1, \dots, Y_m] : \deg g \leq L\}$
- $\mathbb{Z}_p[X_1, \dots, X_n\,]^{\leq dL} = \{g \in \mathbb{Z}_p[X_1, \dots, X_n] : \deg g \leq dL\}$
- $\dim \ker \phi_L \geq \dim \mathbb{Z}_p[Y_1, \dots, Y_m]^{\leq L} - \dim \mathbb{Z}_p[X_1, \dots, X_n\,]^{\leq dL}$

Dimension Formula for Linear Maps

Bound Degree of Algebraic Relationship h

$$\begin{aligned}\phi_L : \mathbb{Z}_p[Y_1, \dots, Y_m]^{\le L} &\to \mathbb{Z}_p[X_1, \dots, X_n]^{\le dL} \\ g(Y_1, \dots, Y_m) &\mapsto g\big(f_1(X), \dots, f_m(X)\big)\end{aligned}$$

- ϕ_L is linear homomorphism
- $\ker \phi_L$ contains all algebraic relationships of $f_1, \dots, f_m$ of degree $\le L$
- $\mathbb{Z}_p[Y_1, \dots, Y_m]^{\le L} = \{g \in \mathbb{Z}_p[Y_1, \dots, Y_m] : \deg g \le L\}$
- $\mathbb{Z}_p[X_1, \dots, X_n\,]^{\le dL} = \{g \in \mathbb{Z}_p[X_1, \dots, X_n] : \deg g \le dL\}$
- $\dim \ker \phi_L \ge \dim \mathbb{Z}_p[Y_1, \dots, Y_m]^{\le L} - \dim \mathbb{Z}_p[X_1, \dots, X_n\,]^{\le dL} = \binom{m+L}{L} - \binom{n+dL}{dL}$

Bound Degree of Algebraic Relationship h

$$\phi_L : \mathbb{Z}_p[Y_1, \dots, Y_m]^{\leq L} \to \mathbb{Z}_p[X_1, \dots, X_n]^{\leq dL}$$
$$g(Y_1, \dots, Y_m) \mapsto g\big(f_1(X), \dots, f_m(X)\big)$$

- ϕ_L is linear homomorphism
- $\ker \phi_L$ contains all algebraic relationships of $f_1, \dots, f_m$ of degree $\leq L$
- $\mathbb{Z}_p[Y_1, \dots, Y_m]^{\leq L} = \{g \in \mathbb{Z}_p[Y_1, \dots, Y_m] : \deg g \leq L\}$
- $\mathbb{Z}_p[X_1, \dots, X_n]^{\leq dL} = \{g \in \mathbb{Z}_p[X_1, \dots, X_n] : \deg g \leq dL\}$
- $\dim \ker \phi_L \geq \dim \mathbb{Z}_p[Y_1, \dots, Y_m]^{\leq L} - \dim \mathbb{Z}_p[X_1, \dots, X_n]^{\leq dL} = \binom{m+L}{L} - \binom{n+dL}{dL}$

Algebraic Relationship h of degree $\leq L$ exists
$\Leftrightarrow \dim \ker \phi_L > 0$
$\Leftarrow \binom{m+L}{L} > \binom{n+dL}{dL}$

Bound Degree of Algebraic Relationship h

$$\phi_L : \mathbb{Z}_p[Y_1, \ldots, Y_m]^{\leq L} \to \mathbb{Z}_p[X_1, \ldots, X_n]^{\leq dL}$$
$$g(Y_1, \ldots, Y_m) \mapsto g\big(f_1(X), \ldots, f_m(X)\big)$$

- ϕ_L is linear homomorphism
- $\ker \phi_L$ contains all algebraic relationships of $f_1, \ldots, f_m$ of degree $\leq L$
- $\mathbb{Z}_p[Y_1, \ldots, Y_m]^{\leq L} = \{g \in \mathbb{Z}_p[Y_1, \ldots, Y_m] : \deg g \leq L\}$
- $\mathbb{Z}_p[X_1, \ldots, X_n]^{\leq dL} = \{g \in \mathbb{Z}_p[X_1, \ldots, X_n] : \deg g \leq dL\}$
- $\dim \ker \phi_L \geq \dim \mathbb{Z}_p[Y_1, \ldots, Y_m]^{\leq L} - \dim \mathbb{Z}_p[X_1, \ldots, X_n]^{\leq dL} = \binom{m+L}{L} - \binom{n+dL}{dL}$

Algebraic Relationship h of degree $\leq L$ exists
$\Leftrightarrow \dim \ker \phi_L > 0$
$\Leftarrow \binom{m+L}{L} > \binom{n+dL}{dL}$
$\Leftarrow L \geq 2^{\frac{d}{d-1}} \cdot n^{1-\frac{e}{d-1}}$

How to Compute h?

We know that $\ker \phi_L$ contains h for $L = \left\lceil 2^{\frac{d}{d-1}} \cdot n^{1-\frac{e}{d-1}} \right\rceil$.

How to Compute h?

We know that $\ker \phi_L$ contains h for $L = \lceil 2^{\frac{d}{d-1}} \cdot n^{1-\frac{e}{d-1}} \rceil$.

Compute matrix representation of

$$\phi_L: \mathbb{Z}_p[Y_1, \ldots, Y_m]^{\leq L} \to \mathbb{Z}_p[X_1, \ldots, X_n]^{\leq dL}$$

and solve for $\ker \phi_L$ via Gaussian elimination.

Algebraic Attack: Algorithm

Given PRG $F: \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ consisting of $f_1, \dots, f_m \in \mathbb{Z}_p[X_1, \dots, X_n]$ of degree d, $m \geq n^{1+e}$, and $y \in \mathbb{Z}_p^m$.

Decide if $y = \left(f_1(x), \dots, f_m(x)\right)$ or if $y \leftarrow \mathbb{Z}_p^m$.

Algebraic Attack: Algorithm

Given PRG $F: \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ consisting of $f_1, \dots, f_m \in \mathbb{Z}_p[X_1, \dots, X_n]$ of degree d, $m \geq n^{1+e}$, and $y \in \mathbb{Z}_p^m$.

Decide if $y = \left(f_1(x), \dots, f_m(x)\right)$ or if $y \leftarrow \mathbb{Z}_p^m$.

1. Compute $L := \left\lceil 2^{\frac{d}{d-1}} \cdot n^{1-\frac{e}{d-1}} \right\rceil$
2. Compute algebraic relationship $h \in \mathbb{Z}_p[Y_1, \dots, Y_m]$ of degree L
3. If $h(y) = 0$, decide that y is of form $\left(f_1(x), \dots, f_m(x)\right)$
4. Otherwise, decide that y is uniformly random

Algebraic Attack: Algorithm

Given PRG $F: \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ consisting of $f_1, \dots, f_m \in \mathbb{Z}_p[X_1, \dots, X_n]$ of degree d, $m \geq n^{1+e}$, and $y \in \mathbb{Z}_p^m$.

Decide if $y = \left(f_1(x), \dots, f_m(x)\right)$ or if $y \leftarrow \mathbb{Z}_p^m$.

1. Compute $L := \left\lceil 2^{\frac{d}{d-1}} \cdot n^{1-\frac{e}{d-1}} \right\rceil$
2. Compute algebraic relationship $h \in \mathbb{Z}_p[Y_1, \dots, Y_m]$ of degree L
3. If $h(y) = 0$, decide that y is of form $\left(f_1(x), \dots, f_m(x)\right)$
4. Otherwise, decide that y is uniformly random

Time Complexity: $m^{O(\deg h)} = n^{O\left(n^{1-\frac{e}{d-1}}\right)}$

Algebraic Attack: Algorithm

Given PRG $F: \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ consisting of $f_1, \dots, f_m \in \mathbb{Z}_p[X_1, \dots, X_n]$ of degree d, $m \geq n^{1+e}$, and $y \in \mathbb{Z}_p^m$.

Decide if $y = \big(f_1(x), \dots, f_m(x)\big)$ or if $y \leftarrow \mathbb{Z}_p^m$.

1. Compute $L := \left\lceil 2^{\frac{d}{d-1}} \cdot n^{1-\frac{e}{d-1}} \right\rceil$
2. Compute algebraic relationship $h \in \mathbb{Z}_p[Y_1, \dots, Y_m]$ of degree L
3. If $h(y) = 0$, decide that y is of form $\big(f_1(x), \dots, f_m(x)\big)$
4. Otherwise, decide that y is uniformly random

Time Complexity: $m^{O(\deg h)} = n^{O\left(n^{1-\frac{e}{d-1}}\right)}$

Advantage: $1 - O\left(\frac{\deg h}{p}\right) = 1 - O\left(\frac{n^{1-\frac{e}{d-1}}}{p}\right)$

Algebraic Attack: Algorithm

Given PRG $F: \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ consisting of $f_1, \ldots, f_m \in \mathbb{Z}_p[X_1, \ldots, X_n]$ of degree d, $m \geq n^{1+e}$, and $y \in \mathbb{Z}_p^m$.

Decide if $y = (f_1(x), \ldots, f_m(x))$ or if $y \leftarrow \mathbb{Z}_p^m$.

1. Compute $L := \left\lceil 2^{\frac{d}{d-1}} \cdot n^{1-\frac{e}{d-1}} \right\rceil$
2. Compute algebraic relationship $h \in \mathbb{Z}_p[Y_1, \ldots, Y_m]$ of degree L
3. If $h(y) = 0$, decide that y is of form $(f_1(x), \ldots, f_m(x))$
4. Otherwise, decide that y is uniformly random

Time Complexity: $m^{O(\deg h)} = n^{O\left(n^{1-\frac{e}{d-1}}\right)}$

Advantage: $1 - O\left(\frac{\deg h}{p}\right) = 1 - O\left(\frac{n^{1-\frac{e}{d-1}}}{p}\right)$

Good if $p \in \omega\left(n^{1-\frac{e}{d-1}}\right)$.

Bad if $p \in o\left(n^{1-\frac{e}{d-1}}\right)$.

Hashing to Larger Fields

Idea: Convert local PRG $F: \{0,1\}^n \to \{0,1\}^m$ and $y \in \{0,1\}^m$

to a polynomial PRG $G: \{0,1\}^n \to \mathbb{Z}_p^{m'}$ and $y' \in \mathbb{Z}_p^{m'}$

with $p \geq n$ and $m' \approx m$.

Hashing to Larger Fields

Idea: Convert local PRG $F: \{0,1\}^n \to \{0,1\}^m$ and $y \in \{0,1\}^m$ to a polynomial PRG $G: \{0,1\}^n \to \mathbb{Z}_p^{m'}$ and $y' \in \mathbb{Z}_p^{m'}$ with $p \geq n$ and $m' \approx m$.

1. Choose prime $p \geq n$
2. Set $m' = \left\lceil \frac{m}{3 \log p} \right\rceil$
3. Draw $A \leftarrow \mathbb{Z}_p^{m' \times m}$
4. Compute $y' \coloneqq A \cdot y$ for $y \in \{0,1\}^m$
5. Compute $G \coloneqq A \cdot F$

Hashing to Larger Fields

Idea: Convert local PRG $F: \{0,1\}^n \to \{0,1\}^m$ and $y \in \{0,1\}^m$
to a polynomial PRG $G: \{0,1\}^n \to \mathbb{Z}_p^{m'}$ and $y' \in \mathbb{Z}_p^{m'}$
with $p \geq n$ and $m' \approx m$.

1. Choose prime $p \geq n$
2. Set $m' = \left\lfloor \frac{m}{3 \log p} \right\rfloor$
3. Draw $A \leftarrow \mathbb{Z}_p^{m' \times m}$
4. Compute $y' \coloneqq A \cdot y$ for $y \in \{0,1\}^m$
5. Compute $G \coloneqq A \cdot F$

Leftover-Hash-Lemma
y' is close $U(\mathbb{Z}_p^{m'})$ if $y \leftarrow \{0,1\}^m$

Hashing to Larger Fields

Idea: Convert local PRG $F: \{0,1\}^n \to \{0,1\}^m$ and $y \in \{0,1\}^m$
to a polynomial PRG $G: \{0,1\}^n \to \mathbb{Z}_p^{m'}$ and $y' \in \mathbb{Z}_p^{m'}$
with $p \geq n$ and $m' \approx m$.

1. Choose prime $p \geq n$
2. Set $m' = \left\lfloor \frac{m}{3 \log p} \right\rfloor$
3. Draw $A \leftarrow \mathbb{Z}_p^{m' \times m}$
4. Compute $y' \coloneqq A \cdot y$ for $y \in \{0,1\}^m$
5. Compute $G \coloneqq A \cdot F$

What is the algebraic degree of G?

Hashing to Larger Fields

Idea: Convert local PRG $F: \{0,1\}^n \to \{0,1\}^m$ and $y \in \{0,1\}^m$ to a polynomial PRG $G: \{0,1\}^n \to \mathbb{Z}_p^{m'}$ and $y' \in \mathbb{Z}_p^{m'}$ with $p \geq n$ and $m' \approx m$.

1. Choose prime $p \geq n$
2. Set $m' = \left\lfloor \frac{m}{3 \log p} \right\rfloor$
3. Draw $A \leftarrow \mathbb{Z}_p^{m' \times m}$
4. Compute $y' \coloneqq A \cdot y$ for $y \in \{0,1\}^m$
5. Compute $G \coloneqq A \cdot F$

What is the algebraic degree of G?

$\deg G = \operatorname{loc} F$

Hashing + Algebraic Attack on Binary PRGs

Given a PRG $F : \{0,1\}^n \to \{0,1\}^m$ of locality d and a (pseudo-)random bitstring $y \in \{0,1\}^m$, $m \geq n^{1+e}$.

1. Draw $A \leftarrow \mathbb{Z}_p^{\left\lceil \frac{m}{3 \log p} \right\rceil \times m}$ for prime $p \in [n, 2n]$
2. Compute $G \coloneqq A \cdot F: \{0,1\}^n \to \mathbb{Z}_p^{\left\lceil \frac{m}{3 \log p} \right\rceil}$
3. Compute $y' \coloneqq A \cdot y \in \mathbb{Z}_p^{\left\lceil \frac{m}{3 \log p} \right\rceil}$
4. Compute an algebraic relation $h \in \mathbb{Z}_p[Y]$ for G of degree $O\left((\log n)^{\frac{1}{d-1}} \cdot n^{1-\frac{e}{d-1}}\right)$
5. Output 0 if $h(y') = 0$, otherwise 1

Hashing + Algebraic Attack on Binary PRGs

Given a PRG $F: \{0,1\}^n \rightarrow \{0,1\}^m$ of locality d and a (pseudo-)random bitstring $y \in \{0,1\}^m$, $m \geq n^{1+e}$.

1. Draw $A \leftarrow \mathbb{Z}_p^{\left\lceil \frac{m}{3 \log p} \right\rceil \times m}$ for prime $p \in [n, 2n]$
2. Compute $G \coloneqq A \cdot F: \{0,1\}^n \rightarrow \mathbb{Z}_p^{\left\lceil \frac{m}{3 \log p} \right\rceil}$
3. Compute $y' \coloneqq A \cdot y \in \mathbb{Z}_p^{\left\lceil \frac{m}{3 \log p} \right\rceil}$
4. Compute an algebraic relation $h \in \mathbb{Z}_p[Y]$ for G of degree $O\left((\log n)^{\frac{1}{d-1}} \cdot n^{1-\frac{e}{d-1}}\right)$
5. Output 0 if $h(y') = 0$, otherwise 1

Time Complexity:

$$m^{O(\deg h)} = n^{O\left((\log n)^{\frac{1}{d-1}} \cdot n^{1-\frac{e}{d-1}}\right)}$$

Hashing + Algebraic Attack on Binary PRGs

Given a PRG $F : \{0,1\}^n \to \{0,1\}^m$ of locality d and a (pseudo-)random bitstring $y \in \{0,1\}^m$, $m \geq n^{1+e}$.

1. Draw $A \leftarrow \mathbb{Z}_p^{\left\lceil\frac{m}{3\log p}\right\rceil \times m}$ for prime $p \in [n, 2n]$
2. Compute $G \coloneqq A \cdot F : \{0,1\}^n \to \mathbb{Z}_p^{\left\lceil\frac{m}{3\log p}\right\rceil}$
3. Compute $y' \coloneqq A \cdot y \in \mathbb{Z}_p^{\left\lceil\frac{m}{3\log p}\right\rceil}$
4. Compute an algebraic relation $h \in \mathbb{Z}_p[Y]$ for G of degree $O\left((\log n)^{\frac{1}{d-1}} \cdot n^{1-\frac{e}{d-1}}\right)$
5. Output 0 if $h(y') = 0$, otherwise 1

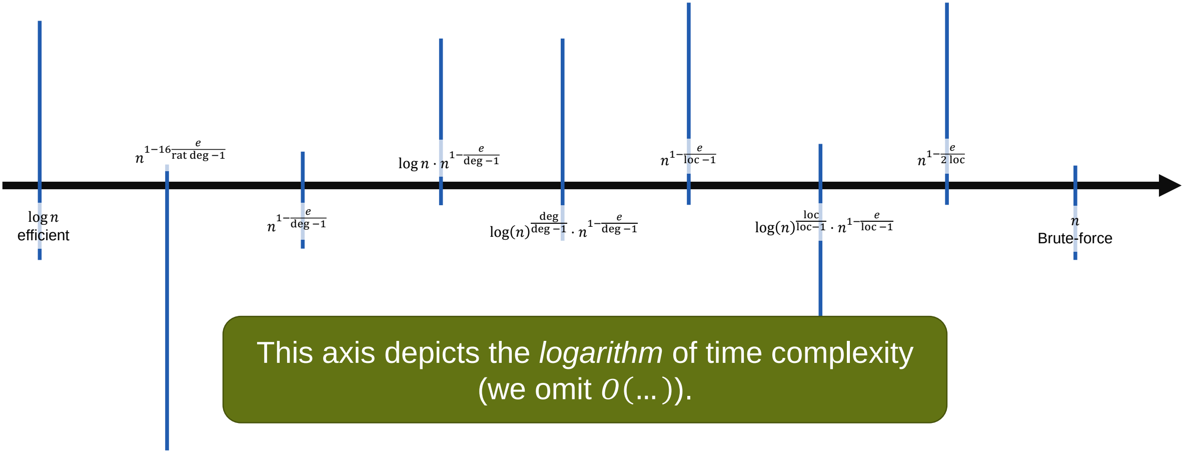
Time Complexity:

$$m^{O(\deg h)} = n^{O\left((\log n)^{\frac{1}{d-1}} \cdot n^{1-\frac{e}{d-1}}\right)}$$

Advantage:

$$1 - O\left(\frac{\deg h}{p}\right) = 1 - O\left(\frac{(\log n)^{\frac{1}{d-1}} \cdot n^{1-\frac{e}{d-1}}}{n}\right) \geq 1 - o(1)$$

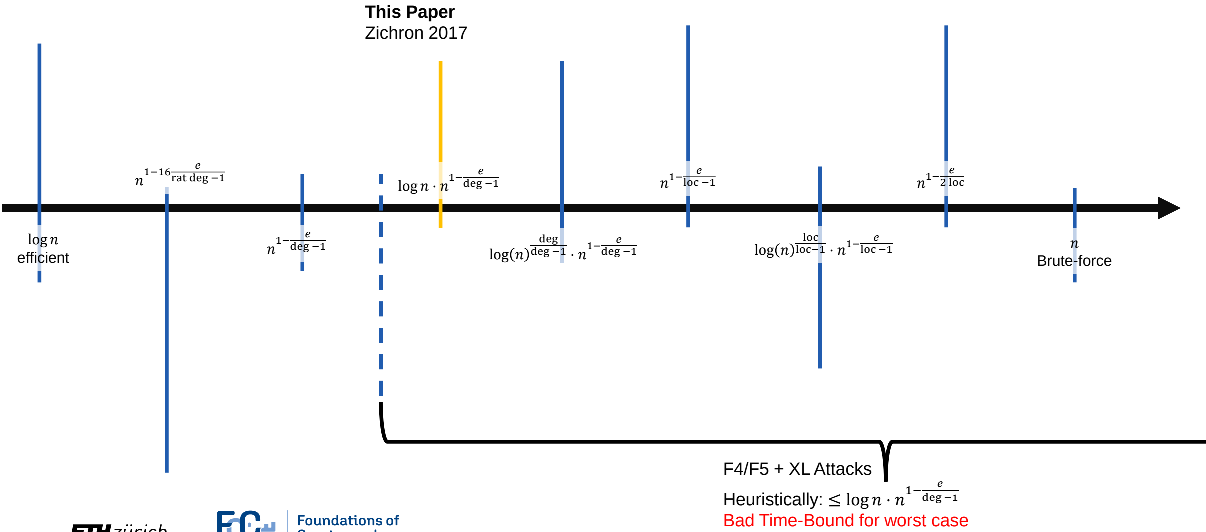
Overview: Attacks on PRGs



This axis depicts the *logarithm* of time complexity (we omit $O(\ldots)$).

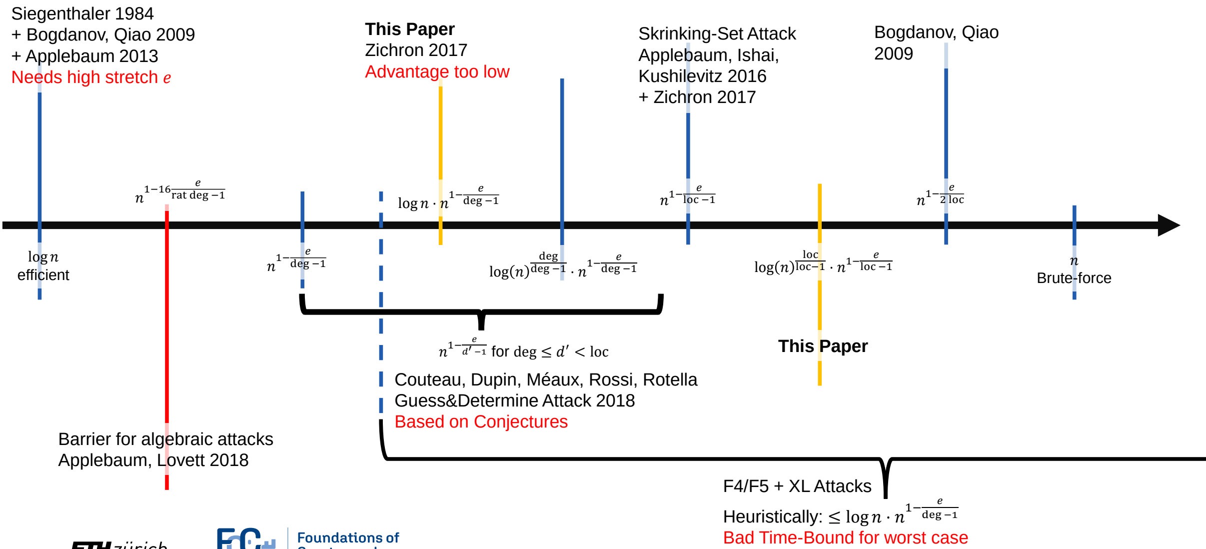
Overview: Attacks on *Constant-Degree* PRGs ($p \geq n^c$)

$$F: \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^{n^{1+e}}$$



Overview: Attacks on *Local* PRGs

$$F: \{0,1\}^n \to \{0,1\}^{n^{1+e}}$$



Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz.
On pseudorandom generators with linear stretch in nc0.
Comput. Complex., 17(1):38–69, apr 2008.

Benny Applebaum and Shachar Lovett.
Algebraic attacks against random local functions and their countermeasures.
SIAM Journal on Computing, 47(1):52–79, 2018.

Benny Applebaum.
Cryptographic hardness of random local functions-survey.
In Amit Sahai, editor, *TCC 2013*, volume 7785 of *LNCS*, page 599. Springer, Heidelberg, March 2013.

Magali Bardet, Jean-Charles Faugère, and Bruno Salvy.
Complexity of Gröbner basis computation for Semi-regular Overdetermined sequences over F_2 with solutions in F_2.
Research Report RR-5049, INRIA, 2003.

Andrej Bogdanov and Youming Qiao.
On the security of goldreich's one-way function.
In Irit Dinur, Klaus Jansen, Joseph Naor, and José Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 392–405, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

Chen-Mou Cheng, Tung Chou, Ruben Niederhagen, and Bo-Yin Yang.
Solving quadratic equations with XL on parallel architectures.
In Emmanuel Prouff and Patrick Schaumont, editors, *CHES 2012*, volume 7428 of *LNCS*, pages 356–373. Springer, Heidelberg, September 2012.

Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Mélissa Rossi, and Yann Rotella.
On the concrete security of Goldreich's pseudorandom generator.
In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 96–124. Springer, Heidelberg, December 2018.

Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir.
Efficient algorithms for solving overdefined systems of multivariate polynomial equations.
In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 392–407. Springer, Heidelberg, May 2000.

Moses Charikar and Anthony Wirth.
Maximizing quadratic programs: Extending Grothendieck's inequality.
In *45th FOCS*, pages 54–60. IEEE Computer Society Press, October 2004.

Jintai Ding, J. Buchmann, M. Mohamed, W. Moahmed, and R. Weinmann.
Mutantxl.
SCC, pages 16–22, 01 2008.

Jean-Charles Faugére.
A new efficient algorithm for computing gröbner bases (f4).
Journal of Pure and Applied Algebra, 139(1):61–88, 1999.

Jean Charles Faugère.
A new efficient algorithm for computing gröbner bases without reduction to zero (f5).
In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ISSAC '02, page 75–83, New York, NY, USA, 2002. Association for Computing Machinery.

Romain Gay and Rafael Pass.
Indistinguishability obfuscation from circular security.
In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2021, 2021.

Michel X. Goemans and David P. Williamson.
Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming.
J. ACM, 42(6):1115–1145, nov 1995.

Aayush Jain, Huijia Lin, and Amit Sahai.
Indistinguishability obfuscation from well-founded assumptions.
In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2021, page 60–73, New York, NY, USA, 2021. Association for Computing Machinery.

Aayush Jain, Huijia Lin, and Amit Sahai.
Indistinguishability obfuscation from lpn over fp, dlin, and prgs in nc0.
In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 670–699, Cham, 2022. Springer International Publishing.

Mohamed Saied Emam Mohamed, Wael Said Abd Elmageed Mohamed, Jintai Ding, and Johannes A. Buchmann.
MXL2: Solving polynomial equations over GF(2) using an improved mutant strategy.
In Johannes Buchmann and Jintai Ding, editors, *Post-quantum cryptography, second international workshop, PQCRYPTO 2008*, pages 203–215. Springer, Heidelberg, October 2008.

T. Siegenthaler.
Correlation-immunity of nonlinear combining functions for cryptographic applications (corresp.).
IEEE Transactions on Information Theory, 30(5):776–780, 1984.

Bo-Yin Yang and Jiun-Ming Chen.
All in the xl family: Theory and practice.
In Choon-sik Park and Seongtaek Chee, editors, *Information Security and Cryptology – ICISC 2004*, pages 67–86, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

Lior Zichron.
Locally computable arithmetic pseudorandom generators, 2017.

Akin Ünal.
Worst-case subexponential attacks on prgs of constant degree or constant locality.
Cryptology ePrint Archive, Paper 2023/119, 2023.
https://eprint.iacr.org/2023/119.

Appendix

How to Bound L

$$\binom{m+L}{L} = \frac{(m+L)\cdots(m+1)}{L\cdots 1} > \frac{(n+dL)\cdots(n+1)}{(dL)\cdots 1} = \binom{n+dL}{dL}$$

$$\Leftrightarrow \quad (m+L)\cdots(m+1)\cdot(dL)\cdots(L+1) > (n+dL)\cdots(n+1)$$

$$\approx \quad m^L \cdot L^{(d-1)L} \geq n^{dL}$$

$$\Leftrightarrow \quad m \cdot L^{d-1} \geq n^d$$

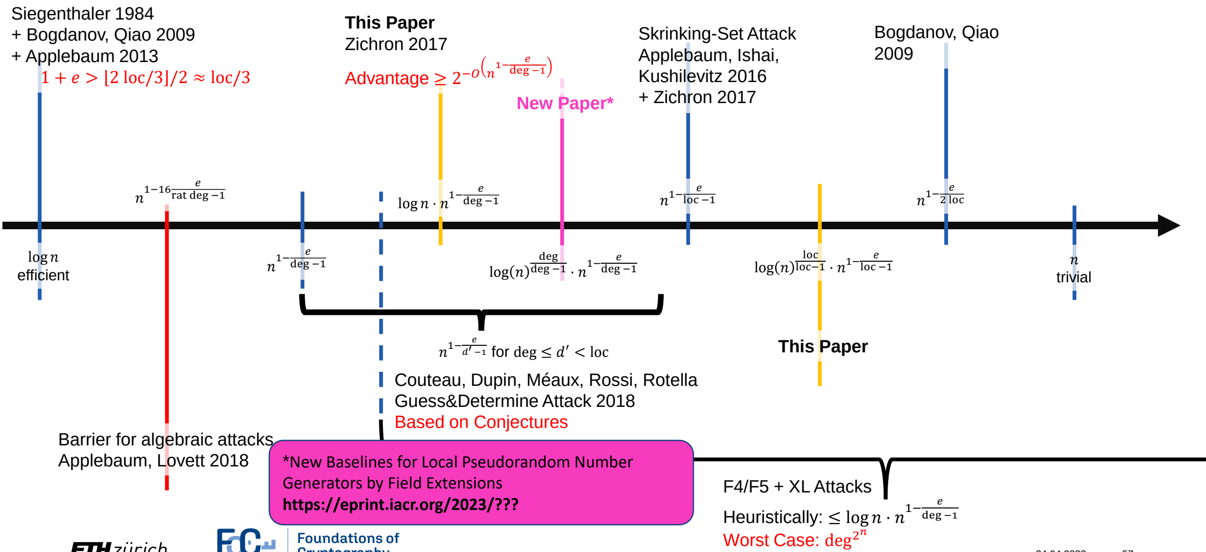
$$\Leftrightarrow \quad L \geq \sqrt[d-1]{n^d/m} \geq n^{1-\frac{e}{d-1}}$$

$(m+L)\cdots(m+1) \approx m^L$
$(dL)\cdots(L+1) \approx L^{(d-1)L}$
$(n+dL)\cdots(n+1) \approx n^{dL}$

Actually $L \geq 2^{\frac{d}{d-1}} \cdot n^{1-\frac{e}{d-1}}$

Overview: Attacks on *Local* PRGs

$$F: \{0,1\}^n \rightarrow \{0,1\}^{n^{1+e}}$$



Hashing Trick: Bad Trade-Off

$F\colon\{0,1\}^n \to \{0,1\}^m$ consists of tri-sum-ands:

$$P \coloneqq (X_1 \wedge X_2) \oplus X_3 \oplus X_4 \oplus X_5 \simeq X_1 \cdot X_2 + X_3 + X_4 + X_5 \bmod 2 \in \mathbb{Z}_2[X_1, \dots, X_5]$$

The same polynomial

$$X_1 \cdot X_2 + X_3 + X_4 + X_5 \bmod p \text{ in } \mathbb{Z}_p[X_1, \dots, X_5]$$

does not compute the same as P over $\{0,1\}^5$:

$$1 \oplus 1 = 1 + 1 = 0 \bmod 2 \qquad\qquad 1 + 1 = 2 \neq 0 \bmod p$$

There is a degree-5 polynomial in $\mathbb{Z}_p[X_1, \dots, X_5]$ that coincides with P on $\{0,1\}^5$:

$$X_1X_2 + X_3 + X_4 + X_5 - X_1X_2X_3 - X_4X_5 - X_1X_2X_4 - X_1X_2X_5 - X_3X_4 - X_3X_5 + X_1X_2X_4X_5 + X_3X_4X_5 + X_1X_2X_3X_4 + X_1X_2X_3X_5 - X_1X_2X_3X_4X_5$$

New Extension Trick

We consider the field extension $GF\left(2^{\lceil \log n \rceil}\right)$ of $\mathbb{Z}_2$.

$$GF\left(2^{\lceil \log n \rceil}\right) \approx \mathbb{Z}_2[\zeta] = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cdot \zeta \oplus \cdots \oplus \mathbb{Z}_2 \cdot \zeta^{\lceil \log n \rceil - 1}$$

We have the bijective map

$$\psi: \{0,1\}^{\lceil \log n \rceil} \to GF\left(2^{\lceil \log n \rceil}\right)$$
$$\left(b_1, \ldots, b_{\lceil \log n \rceil}\right) \mapsto b_1 + b_2 \cdot \zeta + \cdots + b_{\lceil \log n \rceil} \cdot \zeta^{\lceil \log n \rceil - 1}$$

Consider the $m' \times (m' \cdot \lceil \log n \rceil)$-matrix

$$A = I_{m'} \otimes \left(1\ \zeta\ \cdots\ \zeta^{\lceil \log n \rceil - 1}\right) = \begin{pmatrix} 1\ \zeta\ \cdots\ \zeta^{\lceil \log n \rceil - 1} & & \\ & \ddots & \\ & & 1\ \zeta\ \cdots\ \zeta^{\lceil \log n \rceil - 1} \end{pmatrix}$$

For $y \leftarrow \{0,1\}^{m' \cdot \lceil \log n \rceil}$, the vector $A \cdot y$ is a uniformly random element of $GF\left(2^{\lceil \log n \rceil}\right)^{m'}$.

New Extension Trick

We have a natural and homomorphic inclusion of fields $\mathbb{Z}_2 \subset GF\left(2^{\lceil \log n \rceil}\right)$.

This transfers to polynomial rings: $\mathbb{Z}_2[X_1, \dots, X_n] \subset GF\left(2^{\lceil \log n \rceil}\right)[X_1, \dots, X_n]$.

If $f_1, \dots, f_{\lceil \log n \rceil} \in \mathbb{Z}_2[X_1, \dots, X_n]$ are of degree d, then so is

$$f_1(X) + \zeta \cdot f_2(X) + \cdots + \zeta^{\lceil \log n \rceil - 1} \cdot f_{\lceil \log n \rceil}(X)$$

If $F: \{0,1\}^n \to \{0,1\}^{m' \cdot \lceil \log n \rceil}$ is of degree d, then so is $G \coloneqq A \cdot F: \{0,1\}^n \to \{0,1\}^{m'}$.

Degree of new PRG G equals **Degree** of old PRG F.