Boolean Modeling and Analysis of Learning With Rounding

Jules Baudrin, Rachelle Heim Boissier, François-Xavier Standaert

Université Catholique de Louvain

Jan. 2025

Outline

Hard learning problems

Learning With Error (LWE), Learning With Rounding (LWR), Learning Parity with Noise (LPN)

and their ring/module variants.

Central importance in post-quantum cryptography

- Encryption, Key encapsulation mechanisms: CRYSTALS-Kyber, Saber
- Signatures: CRYSTALS-Dilithium, BLISS

and in symmetric cryptography:

- Essentially to build (key homomorphic) PRFs for a variety of applications.
- E.g. distributed PRFs, proxy re-encryption, updatable encryption (Boneh et al., 2013)

Learning With Errors

In a nutshell: solving a noisy linear system over a ring.

Search Learning With Errors (Regev 05)

Parameters: $q \in \mathbb{N}$, $n \in \mathbb{N}^*$, small (Gaussian) distribution χ over $\mathbb{Z}_q$, secret $\boldsymbol{x} \xleftarrow{\$} \mathbb{Z}_q^n$

Given samples from the distribution

$$\mathscr{D}^{\mathsf{LWE}} = \{\ (\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{x} \rangle + e),\ \ \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_q^n,\ \ e \leftarrow \chi\ \}$$

Find $\boldsymbol{x}$.

Learning With Errors

In a nutshell: solving a noisy linear system over a ring.

Search Learning With Errors (Regev 05)

Parameters: $q \in \mathbb{N}$, $n \in \mathbb{N}^*$, small (Gaussian) distribution χ over $\mathbb{Z}_q$, secret $\boldsymbol{x} \xleftarrow{\$} \mathbb{Z}_q^n$

Given samples from the distribution

$$\mathscr{D}^{\mathsf{LWE}} = \{\ (\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{x} \rangle + e),\ \ \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_q^n,\ \ e \leftarrow \chi\ \}$$

Find $\boldsymbol{x}$.

Decision LWE: distinguish from $\mathscr{D}_0 = \{(\boldsymbol{a}, r) \mid \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_q^n, r \xleftarrow{\$} \mathbb{Z}_q\}$

Learning With Errors

In a nutshell: solving a noisy linear system over a ring.

Search Learning With Errors (Regev 05)

Parameters: $q \in \mathbb{N}$, $n \in \mathbb{N}^*$, small (Gaussian) distribution χ over $\mathbb{Z}_q$, secret $\boldsymbol{x} \xleftarrow{\$} \mathbb{Z}_q^n$

Given samples from the distribution

$$\mathscr{D}^{\mathsf{LWE}} = \{\ (\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{x} \rangle + e),\ \ \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_q^n,\ \ e \leftarrow \chi\ \}$$

Find $\boldsymbol{x}$.

Decision LWE: distinguish from $\mathscr{D}_0 = \{(\boldsymbol{a}, r) \mid \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_q^n, r \xleftarrow{\$} \mathbb{Z}_q\}$

- Security level is determined by n, q, and standard deviation σ of χ.
- Drawback: LWE cannot be used to build deterministic primitives such as PRFs.

Learning with Rounding

'A way of partially 'derandomizing' the LWE problem, i.e. generating errors efficiently and deterministically'.

Banerjee, Peikert, Rosen, EC' 2012.

Search Learning With Rounding

Parameters: $q \in \mathbb{N}$, $p, n \in \mathbb{N}^*$, $p < q$, rounding function $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$, secret $\boldsymbol{x} \xleftarrow{\$} \mathbb{Z}_q^n$

Given samples from the distribution

$$\mathscr{D}^{\mathsf{LWR}} = \{\ (\boldsymbol{a}, \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rceil_p),\ \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_q^n\ \}$$

Find $\boldsymbol{x}$.

Today: PQ cryptography (e.g. Saber [B+18]), symmetric cryptography (PRFs indeed).

Power-of-two moduli

Today: Many use-cases rely on LWR with a power-of-two modulus.

Search Learning With Rounding

Parameters: $q \in \mathbb{N}$, $p, n \in \mathbb{N}^*$, $p < q$, rounding function $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$, secret $\boldsymbol{x} \xleftarrow{\$} \mathbb{Z}_q^n$

Given samples from the distribution

$$\mathscr{D}^{\mathrm{LWR}} = \{\ (\boldsymbol{a}, s_{\boldsymbol{a}} = \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rceil_p),\ \ \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_q^n\ \}$$

Find $\boldsymbol{x}$.

Power-of-two moduli

Today: Many use-cases rely on LWR with a power-of-two modulus.

Search Learning With Rounding

Parameters: $q \in \mathbb{N}$, $p, n \in \mathbb{N}^*$, $p < q$, rounding function $\lfloor \cdot \rceil_{2^p} : \mathbb{Z}_{2^q} \to \mathbb{Z}_{2^p}$, secret $\boldsymbol{x} \xleftarrow{\$} \mathbb{Z}_{2^q}^n$

Given samples from the distribution

$$\mathscr{D}^{\mathrm{LWR}} = \{\ (\boldsymbol{a}, s_{\boldsymbol{a}} = \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rceil_p),\ \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_{2^q}^n\ \}$$

Find $\boldsymbol{x}$.

Power-of-two moduli

Today: Many use-cases rely on LWR with a power-of-two modulus.

Search Learning With Rounding

Parameters: $q \in \mathbb{N}$, $p, n \in \mathbb{N}^*$, $p < q$, rounding function $\lfloor \cdot \rceil_{2^p} : \mathbb{Z}_{2^q} \to \mathbb{Z}_{2^p}$, secret $\boldsymbol{x} \xleftarrow{\$} \mathbb{Z}_{2^q}^n$

Given samples from the distribution

$$\mathscr{D}^{\mathrm{LWR}} = \{\ (\boldsymbol{a}, s_{\boldsymbol{a}} = \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rceil_p),\ \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_{2^q}^n\ \}$$

Find $\boldsymbol{x}$.

In this case: the rounding function $\lfloor \cdot \rceil_{2^p}$ simply removes the $q - p$ least significant bits.

- Security level is determined by n, q and $q-p$: noise $\sim$ *Uniform*$[-2^{q-p}, 0)$

e.g. LightSaber: $n = 512, q - p = 3$, dPRF LaKey $n = 256, q - p = 4$.

Power-of-two moduli

Today: Many use-cases rely on LWR with a power-of-two modulus.

Search Learning With Rounding

Parameters: $q \in \mathbb{N}$, $p, n \in \mathbb{N}^*$, $p < q$, rounding function $\lfloor\cdot\rceil_{2^p} : \mathbb{Z}_{2^q} \to \mathbb{Z}_{2^p}$, secret $\boldsymbol{x} \xleftarrow{\$} \mathbb{Z}_{2^q}^n$

Given samples from the distribution

$$\mathscr{D}^{\mathrm{LWR}} = \{\ (\boldsymbol{a}, s_{\boldsymbol{a}} = \lfloor\langle \boldsymbol{a}, \boldsymbol{x}\rangle\rceil_p),\ \boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_{2^q}^n\ \}$$

Find $\boldsymbol{x}$.

In this case: the rounding function $\lfloor\cdot\rceil_{2^p}$ simply removes the $q-p$ least significant bits.

- Security level is determined by n, q and $q-p$: noise $\sim \mathit{Uniform}[-2^{q-p}, 0)$

e.g. LightSaber: $n = 512, q-p = 3$, dPRF LaKey $n = 256, q-p = 4$.

Hardness

Theory

- LWE: Solid theoretical foundations (e.g. Brakerski et al. 13).
- LWR is as hard as LWE (asymptotic reduction, underlying assumptions).

Practice

- Parameter selection driven by best known attacks (Lattice estimator, Albrecht et al.)

> *'The hardness of (ring or module) LWR can be analyzed as an LWE problem, since there is no known attacks that make use of the additional structure offered by these variants'.*
>
> SABER specifications

Open question: what does a deterministic error do to (practical) security?

Linearisation attack by Arora & Ge (2011)

- Low noise, large number of samples (not SABER).

Parameters: $n \in \mathbb{N}^*$, Noise in set E.

Any sample $(\boldsymbol{a}, s_{\boldsymbol{a}} = \langle \boldsymbol{a}, \boldsymbol{x} \rangle + e_0)$, yields the following equation in the secret:

$$\prod_{e \in E} (s_{\boldsymbol{a}} - \langle \boldsymbol{a}, \boldsymbol{x} \rangle - e) = 0. \qquad \text{(degree } |E| \text{ polynomial)}$$

Linearisation: $\binom{n+|E|}{|E|}$ in data, $\binom{n+|E|}{|E|}^{\omega}$ in time, ω linear algebra constant.

And Gröbner? Some asymptotic results for prime or odd moduli (not 2^q).

- **LWE**: Gaussian distribution: bounded noise for a well-chosen number of samples.
- **LWR**: $T = 2^{q-p}$.

Linearisation attack by Arora & Ge (2011)

- Low noise, large number of samples (not SABER).

Parameters: $n \in \mathbb{N}^*$, Noise in set E.

Any sample $(\boldsymbol{a}, s_{\boldsymbol{a}} = \langle \boldsymbol{a}, \boldsymbol{x} \rangle + e_0)$, yields the following equation in the secret:

$$\prod_{e \in E} (s_{\boldsymbol{a}} - \langle \boldsymbol{a}, \boldsymbol{x} \rangle - e) = 0. \qquad \text{(degree } |E| \text{ polynomial)}$$

Linearisation: $\binom{n+|E|}{|E|}$ in data, $\binom{n+|E|}{|E|}^{\omega}$ in time, ω linear algebra constant.

And Gröbner? Some asymptotic results for prime or odd moduli (not 2^q).

- **LWE**: Gaussian distribution: bounded noise for a well-chosen number of samples.
- **LWR**: $T = 2^{q-p}$.

Our main result: in the case of LWR, one can do better.

Outline

A symmetric point of view

Def: A Boolean function is a function $f : \mathbb{F}_2^s \longrightarrow \mathbb{F}_2$.

Ingredients to generate an LWR sample: $(\boldsymbol{a},\ s_{\boldsymbol{a}} = \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rfloor_p)$.

- Inner product $\langle \cdot, \cdot \rangle : \mathbb{Z}_{2^q}^n \times \mathbb{Z}_{2^q}^n \to \mathbb{Z}_{2^q}$
- Rounding function $\lfloor \cdot \rfloor_{2^p} : \mathbb{Z}_{2^q} \to \mathbb{Z}_{2^p}$.

A symmetric point of view

Def: A Boolean function is a function $f : \mathbb{F}_2^s \longrightarrow \mathbb{F}_2$.

Ingredients to generate an LWR sample: $(\boldsymbol{a},\ s_{\boldsymbol{a}} = \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rceil_p)$.

- Inner product $\langle \cdot, \cdot \rangle : \mathbb{Z}_{2^q}^n \times \mathbb{Z}_{2^q}^n \to \mathbb{Z}_{2^q}$
- Rounding function $\lfloor \cdot \rceil_{2^p} : \mathbb{Z}_{2^q} \to \mathbb{Z}_{2^p}$.

Identify $\mathbb{Z}_{2^q}$ with $\mathbb{F}_2^q$.

A symmetric point of view

Def: A Boolean function is a function $f : \mathbb{F}_2^s \longrightarrow \mathbb{F}_2$.

Ingredients to generate an LWR sample: $(\boldsymbol{a},\ s_{\boldsymbol{a}} = \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rfloor_p)$.

- Inner product $\langle \cdot, \cdot \rangle : (\mathbb{F}_2^q)^n \times (\mathbb{F}_2^q)^n \to \mathbb{F}_2^q$
- Rounding function $\lfloor \cdot \rfloor_{2^p} : \mathbb{F}_2^q \to \mathbb{F}_2^p$.

Identify $\mathbb{Z}_{2^q}$ with $\mathbb{F}_2^q$.

A symmetric point of view

Def: A Boolean function is a function $f : \mathbb{F}_2^s \longrightarrow \mathbb{F}_2$.

Ingredients to generate an LWR sample: $(\boldsymbol{a},\ s_{\boldsymbol{a}} = \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rfloor_p)$.

- Inner product $\langle \cdot, \cdot \rangle : (\mathbb{F}_2^q)^n \times (\mathbb{F}_2^q)^n \to \mathbb{F}_2^q$
- Rounding function $\lfloor \cdot \rfloor_{2^p} : \mathbb{F}_2^q \to \mathbb{F}_2^p$.

Identify $\mathbb{Z}_{2^q}$ with $\mathbb{F}_2^q$.

The LWR function $(\boldsymbol{a}, \boldsymbol{x}) \mapsto \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rfloor_{2^p}$ is a vectorial Boolean function.

Symmetric crypto ♡ Boolean functions

The **LWR problem** looks like other symmetric-key problems ($\approx$ Weak-PRF).

Boolean monomials

- $x[i]$ is the bit of index i of x.
- R is the multivariate polynomial ring $\mathbb{F}_2[x[0], \ldots, x[s-1]]$ quotiented by the field equations $x[i]^2 + x[i]$.

Boolean monomial. Let $x, m \in \mathbb{F}_2^s$. x^m denotes the monomial

$$\prod_{i,\ m[i]=1} x[i] \in R\,.$$

Boolean monomials

- $x[i]$ is the bit of index i of x.
- R is the multivariate polynomial ring $\mathbb{F}_2[x[0], \ldots, x[s-1]]$ quotiented by the field equations $x[i]^2 + x[i]$.

Boolean monomial. Let $x, m \in \mathbb{F}_2^s$. x^m denotes the monomial

$$\prod_{i,\ m[i]=1} x[i] \in R\,.$$

Since $3 = (11)_2$, x^3 is the product of the two least significant bits of x, $x[0]x[1]$.

Boolean monomials

- $x[i]$ is the bit of index i of x.
- R is the multivariate polynomial ring $\mathbb{F}_2[x[0], \ldots, x[s-1]]$ quotiented by the field equations $x[i]^2 + x[i]$.

Boolean monomial. Let $x, m \in \mathbb{F}_2^s$. x^m denotes the monomial

$$\prod_{i,\ m[i]=1} x[i] \in R\,.$$

Since $3 = (11)_2$, x^3 is the product of the two least significant bits of x, $x[0]x[1]$.

Since $4 = 2^2 = (100)_2$, x^4 is the third bit of x, $x[2]$.

Boolean monomials

- $x[i]$ is the bit of index i of x.
- R is the multivariate polynomial ring $\mathbb{F}_2[x[0], \ldots, x[s-1]]$ quotiented by the field equations $x[i]^2 + x[i]$.

Boolean monomial. Let $x, m \in \mathbb{F}_2^s$. x^m denotes the monomial

$$\prod_{i,\ m[i]=1} x[i] \in R\,.$$

Since $3 = (11)_2$, x^3 is the product of the two least significant bits of x, $x[0]x[1]$.

Since $4 = 2^2 = (100)_2$, x^4 is the third bit of x, $x[2]$.

Since $2^i = (10\ldots0)_2$, x^{2^i} is the $i+1$th bit of x, $x[i]$.

Symmetric point of view on LWR

The LWR function $(\boldsymbol{a}, \boldsymbol{x}) \mapsto \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rfloor_{2^p}$ is a vectorial Boolean function.

It has domain $\mathbb{Z}_{2^q}^n \times \mathbb{Z}_{2^q}^n$ (or $(\mathbb{F}_2^q)^n \times (\mathbb{F}_2^q)^n$) and co-domain $\mathbb{Z}_{2^p}$ (or $\mathbb{F}_2^p$).

We study the composition of the inner product with a (product of) bit:

$$F^{m,n} : (\boldsymbol{a}, \boldsymbol{x}) \mapsto (\langle \boldsymbol{a}, \boldsymbol{x} \rangle)^m \qquad F_{\boldsymbol{a}}^{m,n} : \boldsymbol{x} \mapsto (\langle \boldsymbol{a}, \boldsymbol{x} \rangle)^m \ .$$

Symmetric point of view on LWR

The LWR function $(\boldsymbol{a}, \boldsymbol{x}) \mapsto \lfloor \langle \boldsymbol{a}, \boldsymbol{x} \rangle \rfloor_{2^p}$ is a vectorial Boolean function.

It has domain $\mathbb{Z}_{2^q}^n \times \mathbb{Z}_{2^q}^n$ (or $(\mathbb{F}_2^q)^n \times (\mathbb{F}_2^q)^n$) and co-domain $\mathbb{Z}_{2^p}$ (or $\mathbb{F}_2^p$).

We study the composition of the inner product with a (product of) bit:

$$F^{m,n} : (\boldsymbol{a}, \boldsymbol{x}) \mapsto (\langle \boldsymbol{a}, \boldsymbol{x} \rangle)^m \qquad F_{\boldsymbol{a}}^{m,n} : \boldsymbol{x} \mapsto (\langle \boldsymbol{a}, \boldsymbol{x} \rangle)^m \ .$$

Most important example:

- $m = 2^{q-p}$. $F^{2^{q-p},n}$ returns the $q - p + 1$th bit of $\langle \boldsymbol{a}, \boldsymbol{x} \rangle$.
  This corresponds to the LSB of the LWR sample.

Algebraic Normal Form

The Algebraic Normal Form (ANF) of $f : \mathbb{F}_2^s \to \mathbb{F}_2$ is the unique multivariate polynomial

$$\sum_{u \in \mathbb{F}_2^s} \alpha_u(f) x^u \in R \qquad \text{s.t.} \qquad \forall x \in \mathbb{F}_2^s, \quad f(x) = \sum_{u \in \mathbb{F}_2^m} \alpha_u(f) x^u \,.$$

Algebraic degree.

$$\deg(f) := \max_{u \in \mathbb{F}_2^m \mid \alpha_u \neq 0} hw(u).$$

Algebraic Normal Form

The Algebraic Normal Form (ANF) of $f : \mathbb{F}_2^s \to \mathbb{F}_2$ is the unique multivariate polynomial

$$\sum_{u \in \mathbb{F}_2^s} \alpha_u(f) x^u \in R \qquad \text{s.t.} \qquad \forall x \in \mathbb{F}_2^s, \quad f(x) = \sum_{u \in \mathbb{F}_2^m} \alpha_u(f) x^u \,.$$

Algebraic degree.

$$\deg(f) := \max_{u \in \mathbb{F}_2^m | \alpha_u \neq 0} hw(u).$$

Example. $f : \mathbb{F}_2^2 \to \mathbb{F}_2$ defined by $f(00) = 0, f(01) = 1, f(10) = 0, f(11) = 0.$

$$f = x[1]x[0] + x[0] = x^3 + x^1 \qquad\qquad \text{degree } 2.$$

Algebraic Normal Form

The Algebraic Normal Form (ANF) of $f : \mathbb{F}_2^s \to \mathbb{F}_2$ is the unique multivariate polynomial

$$\sum_{u \in \mathbb{F}_2^s} \alpha_u(f) x^u \in R \qquad \text{s.t.} \qquad \forall x \in \mathbb{F}_2^s, \quad f(x) = \sum_{u \in \mathbb{F}_2^m} \alpha_u(f) x^u \,.$$

Algebraic degree.

$$\deg(f) := \max_{u \in \mathbb{F}_2^m \mid \alpha_u \neq 0} hw(u).$$

Example. $f : \mathbb{F}_2^2 \to \mathbb{F}_2$ defined by $f(00) = 0, f(01) = 1, f(10) = 0, f(11) = 0.$

$$f = x[1]x[0] + x[0] = x^3 + x^1 \qquad \text{degree } 2.$$

Computing the ANF of a function is a necessary step for algebraic attacks. But it is hard:

- costs $s2^{s-1}$, requires to store the full LUT of size 2^s.
- **LWR:** $s = 2nq > 256$.

Boolean point of view on LWR

$$\begin{aligned} F^{m,n} : (\mathbb{F}_2^q)^n \times (\mathbb{F}_2^q)^n &\longrightarrow \quad \mathbb{F}_2 \\ (a, x) \quad &\longmapsto (\langle a, x \rangle)^m \ . \end{aligned}$$

e.g. $m = 2^{q-p}$ is the LSB of the sample.

Boolean point of view on LWR

$$F^{m,n} : (\mathbb{F}_2^q)^n \times (\mathbb{F}_2^q)^n \longrightarrow \mathbb{F}_2$$
$$(\boldsymbol{a}, \boldsymbol{x}) \longmapsto (\langle \boldsymbol{a}, \boldsymbol{x} \rangle)^m \,.$$

e.g. $m = 2^{q-p}$ is the LSB of the sample.

(Generalised) Boolean monomial. Let $\boldsymbol{u}, \boldsymbol{v} \in (\mathbb{F}_2^q)^n$. $\boldsymbol{a}^{\boldsymbol{u}}\boldsymbol{x}^{\boldsymbol{v}}$ denotes the monomial

$$\boldsymbol{a}^{\boldsymbol{u}}\boldsymbol{x}^{\boldsymbol{v}} = \prod_{i \in [\![0,n]\!]} a_i^{u_i} x_i^{v_i}, \qquad \text{where } a_i^{u_i} x_i^{v_i} \text{ is the Boolean monomial } \prod_{j, u_i[j]=1} a_i[j] \prod_{j, v_i[j]=1} x_i[j] \,.$$

Boolean point of view on LWR

$$\begin{aligned} F^{m,n} : (\mathbb{F}_2^q)^n \times (\mathbb{F}_2^q)^n &\longrightarrow \quad \mathbb{F}_2 \\ (\boldsymbol{a}, \boldsymbol{x}) \quad &\longmapsto ((\langle \boldsymbol{a}, \boldsymbol{x} \rangle))^m . \end{aligned}$$

e.g. $m = 2^{q-p}$ is the LSB of the sample.

(Generalised) Boolean monomial. Let $\boldsymbol{u}, \boldsymbol{v} \in (\mathbb{F}_2^q)^n$. $\boldsymbol{a}^{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{v}}$ denotes the monomial

$$\boldsymbol{a}^{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{v}} = \prod_{i \in [\![0,n]\!]} a_i^{u_i} x_i^{v_i}, \quad \text{where } a_i^{u_i} x_i^{v_i} \text{ is the Boolean monomial } \prod_{j, u_i[j]=1} a_i[j] \prod_{j, v_i[j]=1} x_i[j] .$$

For each random $\boldsymbol{a}$, the function in $\{F_{\boldsymbol{a}}^{m,n} := F^{m,n}(\boldsymbol{a}, \cdot)\}$ is evaluated on the secret $\boldsymbol{x}$ to yield $s_{\boldsymbol{a}}$.

If we can compute the ANF of $F_{\boldsymbol{a}}^{m,n}$, we obtain an equation in the secret $\boldsymbol{x}$:

$$\sum_{\boldsymbol{v} \in (\mathbb{F}_2^q)^n} \alpha_{\boldsymbol{v}}(F_{\boldsymbol{a}}^{m,n})\, \boldsymbol{x}^{\boldsymbol{v}} = (s_{\boldsymbol{a}})^{m/2^{q-p}} .$$

Boolean point of view on LWR

$$F^{m,n} : (\mathbb{F}_2^q)^n \times (\mathbb{F}_2^q)^n \longrightarrow \mathbb{F}_2$$
$$(\mathbf{a}, \mathbf{x}) \longmapsto (\langle \mathbf{a}, \mathbf{x} \rangle)^m \; .$$

e.g. $m = 2^{q-p}$ is the LSB of the sample.

(Generalised) Boolean monomial. Let $\mathbf{u}, \mathbf{v} \in (\mathbb{F}_2^q)^n$. $\mathbf{a}^{\mathbf{u}} \mathbf{x}^{\mathbf{v}}$ denotes the monomial

$$\mathbf{a}^{\mathbf{u}} \mathbf{x}^{\mathbf{v}} = \prod_{i \in [\![0,n]\!]} a_i^{u_i} x_i^{v_i}, \qquad \text{where } a_i^{u_i} x_i^{v_i} \text{ is the Boolean monomial } \prod_{j, u_i[j]=1} a_i[j] \prod_{j, v_i[j]=1} x_i[j] \, .$$

For each random $\mathbf{a}$, the function in $\{F_{\mathbf{a}}^{m,n} := F^{m,n}(\mathbf{a}, \cdot)\}$ is evaluated on the secret $\mathbf{x}$ to yield $s_{\mathbf{a}}$.
If we can compute the ANF of $F_{\mathbf{a}}^{m,n}$, we obtain an equation in the secret $\mathbf{x}$:

$$\sum_{\mathbf{v} \in (\mathbb{F}_2^q)^n} \alpha_{\mathbf{v}}(F_{\mathbf{a}}^{m,n}) \; \mathbf{x}^{\mathbf{v}} = (s_{\mathbf{a}})^{m/2^{q-p}} \, .$$

To do so, we study the ANF of $F^{m,n}$:

$$\sum_{(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_{2^q}^n \times \mathbb{Z}_{2^q}^n} \alpha_{\mathbf{u},\mathbf{v}} \; \mathbf{a}^{\mathbf{u}} \mathbf{x}^{\mathbf{v}} \qquad \text{where } \alpha_{\mathbf{u},\mathbf{v}} \in \mathbb{F}_2, \qquad .$$

Boolean point of view on LWR

$$\begin{aligned} F^{m,n} : (\mathbb{F}_2^q)^n \times (\mathbb{F}_2^q)^n &\longrightarrow \quad \mathbb{F}_2 \\ (\boldsymbol{a}, \boldsymbol{x}) &\longmapsto (\langle \boldsymbol{a}, \boldsymbol{x} \rangle)^m \; . \end{aligned}$$

e.g. $m = 2^{q-p}$ is the LSB of the sample.

(Generalised) Boolean monomial. Let $\boldsymbol{u}, \boldsymbol{v} \in (\mathbb{F}_2^q)^n$. $\boldsymbol{a}^{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{v}}$ denotes the monomial

$$\boldsymbol{a}^{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{v}} = \prod_{i \in [\![0,n]\!]} a_i^{u_i} x_i^{v_i}, \quad \text{where } a_i^{u_i} x_i^{v_i} \text{ is the Boolean monomial } \prod_{j, u_i[j]=1} a_i[j] \prod_{j, v_i[j]=1} x_i[j] \, .$$

For each random $\boldsymbol{a}$, the function in $\{F_{\boldsymbol{a}}^{m,n} := F^{m,n}(\boldsymbol{a}, \cdot)\}$ is evaluated on the secret $\boldsymbol{x}$ to yield $s_{\boldsymbol{a}}$.
If we can compute the ANF of $F_{\boldsymbol{a}}^{m,n}$, we obtain an equation in the secret $\boldsymbol{x}$:

$$\sum_{\boldsymbol{v} \in (\mathbb{F}_2^q)^n} \alpha_{\boldsymbol{v}}(F_{\boldsymbol{a}}^{m,n}) \; \boldsymbol{x}^{\boldsymbol{v}} = (s_{\boldsymbol{a}})^{m/2^{q-p}} \, .$$

To do so, we study the ANF of $F^{m,n}$:

$$\sum_{(\boldsymbol{u},\boldsymbol{v}) \in \mathbb{Z}_{2^q}^n \times \mathbb{Z}_{2^q}^n} \alpha_{\boldsymbol{u},\boldsymbol{v}} \; \boldsymbol{a}^{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{v}} = \sum_{\boldsymbol{v} \in \mathbb{Z}_{2^q}^n} \alpha_{\boldsymbol{v}} \; \boldsymbol{x}^{\boldsymbol{v}} \qquad \text{where } \alpha_{\boldsymbol{u},\boldsymbol{v}} \in \mathbb{F}_2, \; \alpha_{\boldsymbol{v}} = \sum_{\boldsymbol{u} \in \mathbb{Z}_{2^q}^n} \alpha_{\boldsymbol{u},\boldsymbol{v}} \; \boldsymbol{a}^{\boldsymbol{u}} \, .$$

and thus $\alpha_{\boldsymbol{v}}(F^{m,n})(\boldsymbol{a}) = \alpha_{\boldsymbol{v}}(F_{\boldsymbol{a}}^{m,n})$.

Outline

Set of exponents

$$F^{m,n}(\boldsymbol{a},\boldsymbol{x}) = (\langle \boldsymbol{a},\boldsymbol{x}\rangle)^m = \left(\sum a_i \times x_i\right)^m = \sum_{\boldsymbol{v}\in\mathbb{Z}_{\boldsymbol{2}^q}^n} \alpha_{\boldsymbol{v}}\ \boldsymbol{x}^{\boldsymbol{v}}$$ where $\alpha_{\boldsymbol{v}}$ Boolean polynomial in $\boldsymbol{a}$.

Let S_k^n be the set of ordered partitions of length n of k. $|S_k^n| = \binom{n+k-1}{k}$.

Combining results from Braeken and Semaev (FSE, 2005) on the ANF of addition and multiplication:

Theorem (Exponents).

$$\mathrm{Exp}_{\boldsymbol{x}}(F^{m,n}) \subset \bigcup_{i=1}^{m} S_i^n\ .$$

Set of exponents

$$F^{m,n}(\boldsymbol{a}, \boldsymbol{x}) = (\langle \boldsymbol{a}, \boldsymbol{x} \rangle)^m = \left(\sum a_i \times x_i\right)^m = \sum_{\boldsymbol{v} \in \mathbb{Z}_{2^q}^n} \alpha_{\boldsymbol{v}} \, \boldsymbol{x}^{\boldsymbol{v}} \text{ where } \alpha_{\boldsymbol{v}} \text{ Boolean polynomial in } \boldsymbol{a}\,.$$

Let S_k^n be the set of ordered partitions of length n of k. $|S_k^n| = \binom{n+k-1}{k}$.

Combining results from Braeken and Semaev (FSE, 2005) on the ANF of addition and multiplication:

Theorem (Exponents).

$$\mathrm{Exp}_{\boldsymbol{x}}(F^{m,n}) \subset \bigcup_{i=1}^{m} S_i^n\,.$$

Let us look at $\mathrm{Exp}_{\boldsymbol{x}}(F^{2,4})$.

$$S_2^4 = \{(2,0,0,0), (0,2,0,0), (0,0,2,0), (0,0,0,2), (1,1,0,0),$$
$$(1,0,1,0), (1,0,0,1), (0,1,1,0), (0,1,0,1), (0,0,1,1)\}$$
$$S_1^4 = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\}\,.$$

Thus possible $\boldsymbol{x}^{\boldsymbol{v}}$: $x_0^2 = x_0[1]$, $x_1^2 = x_1[1]$, . . . , $x_0^1 x_1^1 = x_0[0]x_1[0]$ . . .

Comparison with Arora-Ge

Recall $\mathrm{Exp}_{x}(F^{m,n}) \subset \bigcup_{i=1}^{m} S_i^n$. **Conjecture**: $\mathrm{Exp}_{x}(F^{m,n}) = \bigcup_{i=1}^{m} S_i^n$ when m is a power of two.

Comparison with Arora-Ge

Recall $\mathrm{Exp}_x(F^{m,n}) \subset \bigcup_{i=1}^m S_i^n$. **Conjecture**: $\mathrm{Exp}_x(F^{m,n}) = \bigcup_{i=1}^m S_i^n$ when m is a power of two.

Important corollaries:

- **Degree.** $\deg(F^{m,n}) \leq m$. If $m \leq n$, we can also show $\deg_x(F^{m,n}) = m$.
- **Number of monomials.** $|\mathrm{Exp}_x(F^{m,n})| \leq \binom{n+m}{m}$. Conjectured equality when m is a power of two.

Comparison with Arora-Ge

Recall $\mathrm{Exp}_x(F^{m,n}) \subset \bigcup_{i=1}^m S_i^n$. **Conjecture**: $\mathrm{Exp}_x(F^{m,n}) = \bigcup_{i=1}^m S_i^n$ when m is a power of two.

Important corollaries:

- **Degree.** $\deg(F^{m,n}) \leq m$. If $m \leq n$, we can also show $\deg_x(F^{m,n}) = m$.
- **Number of monomials.** $|\mathrm{Exp}_x(F^{m,n})| \leq \binom{n+m}{m}$. Conjectured equality when m is a power of two.

- If we use the LSB of the sample ($m = 2^{q-p}$), same number of monomials (Surprising!)

Comparison with Arora-Ge

Recall $\mathrm{Exp}_{x}(F^{m,n}) \subset \bigcup_{i=1}^{m} S_i^n$. **Conjecture**: $\mathrm{Exp}_{x}(F^{m,n}) = \bigcup_{i=1}^{m} S_i^n$ when m is a power of two.

Important corollaries:

- **Degree.** $\deg(F^{m,n}) \leq m$. If $m \leq n$, we can also show $\deg_{x}(F^{m,n}) = m$.
- **Number of monomials.** $|\mathrm{Exp}_{x}(F^{m,n})| \leq \binom{n+m}{m}$. Conjectured equality when m is a power of two.

- If we use the LSB of the sample ($m = 2^{q-p}$), same number of monomials (Surprising!)
- Once the $q-p$ LSBs are recovered, the cost of recovering the full secret is negligible.

Comparison with Arora-Ge

Recall $\mathrm{Exp}_{\mathbf{x}}(F^{m,n}) \subset \bigcup_{i=1}^{m} S_i^n$. **Conjecture**: $\mathrm{Exp}_{\mathbf{x}}(F^{m,n}) = \bigcup_{i=1}^{m} S_i^n$ when m is a power of two.

Important corollaries:

- **Degree.** $\deg(F^{m,n}) \leq m$. If $m \leq n$, we can also show $\deg_{\mathbf{x}}(F^{m,n}) = m$.
- **Number of monomials.** $|\mathrm{Exp}_{\mathbf{x}}(F^{m,n})| \leq \binom{n+m}{m}$. Conjectured equality when m is a power of two.

- If we use the LSB of the sample ($m = 2^{q-p}$), same number of monomials (Surprising!)
- Once the $q - p$ LSBs are recovered, the cost of recovering the full secret is negligible.
- Benefit of working over $\mathbb{F}_2$ rather than $\mathbb{Z}_{2^q}$:
  1. operations are cheaper (we gain at least q).
  2. it's a field.

Comparison with Arora-Ge

Recall $\mathrm{Exp}_{x}(F^{m,n}) \subset \bigcup_{i=1}^{m} S_i^n$. **Conjecture**: $\mathrm{Exp}_{x}(F^{m,n}) = \bigcup_{i=1}^{m} S_i^n$ when m is a power of two.

Important corollaries:

- **Degree.** $\deg(F^{m,n}) \leq m$. If $m \leq n$, we can also show $\deg_{x}(F^{m,n}) = m$.
- **Number of monomials.** $|\mathrm{Exp}_{x}(F^{m,n})| \leq \binom{n+m}{m}$. Conjectured equality when m is a power of two.

- If we use the LSB of the sample ($m = 2^{q-p}$), same number of monomials (Surprising!)
- Once the $q - p$ LSBs are recovered, the cost of recovering the full secret is negligible.
- Benefit of working over $\mathbb{F}_2$ rather than $\mathbb{Z}_{2^q}$:
  1. operations are cheaper (we gain at least q).
  2. it's a field.

A remaining issue

Computing the ANF is the bottleneck.

Möbius transform costs $s2^{s-1}$ in time and 2^s in memory where s is the number of variables.

- **Number of variables.** $F^{m,n}$ depends on at most $s = n \cdot (\lfloor \log_2(m) \rfloor + 1)$ variables of $\boldsymbol{x}$.

NB: this simply comes from the fact that the ith bit of the sum depends only on the i-1 LSBs of the terms.

Outline

Overview

1. The ANF can be computed for arbitrary large n and for m up to 16.
   - NB: used in practice! $m = 8$ for SABER, $m = 16$ for LaKEY.
2. Our methods allows to compute additional relevant metrics of the linearised system.
   - (upper bound on the) rank, relevant change of basis, sparsity.

Overview

1. The ANF can be computed for arbitrary large n and for m up to 16.
   - NB: used in practice! $m = 8$ for SABER, $m = 16$ for LaKEY.
2. Our methods allows to compute additional relevant metrics of the linearised system.
   - (upper bound on the) rank, relevant change of basis, sparsity.

More precisely, we reduce

- the study of the ANF of $F^{m,n}$ to the study of a relevant system of representatives;
- the study of $F^{m,n}$ for all values $n \geq m$ to the study of $F^{m,m}$.

Overview

1. The ANF can be computed for arbitrary large n and for m up to 16.
   - NB: used in practice! $m = 8$ for SABER, $m = 16$ for LaKEY.
2. Our methods allows to compute additional relevant metrics of the linearised system.
   - (upper bound on the) rank, relevant change of basis, sparsity.

More precisely, we reduce

- the study of the ANF of $F^{m,n}$ to the study of a relevant system of representatives;
- the study of $F^{m,n}$ for all values $n \geq m$ to the study of $F^{m,m}$.

How? Most our results stem from the commutativity of modular addition...

Overview

1. The ANF can be computed for arbitrary large n and for m up to 16.
   - NB: used in practice! $m = 8$ for SABER, $m = 16$ for LaKEY.
2. Our methods allows to compute additional relevant metrics of the linearised system.
   - (upper bound on the) rank, relevant change of basis, sparsity.

More precisely, we reduce

- the study of the ANF of $F^{m,n}$ to the study of a relevant system of representatives;
- the study of $F^{m,n}$ for all values $n \geq m$ to the study of $F^{m,m}$.

How? Most our results stem from the commutativity of modular addition...

... formalised using group actions.

Group actions (1)

A (left) **group action** of a group $(\mathbb{G}, \circ)$ on a set E is a function $\mathbb{G} \times E \longrightarrow E, (\sigma, x) \longmapsto \sigma \cdot x$ such that

- For all $x \in E$, $\mathrm{id} \cdot x = x$;
- For all $\sigma, \tau \in \mathbb{G}$, $x \in E$, $\sigma \cdot (\tau \cdot x) = (\sigma \circ \tau) \cdot x$.

The symmetric group $(\mathfrak{S}_n, \circ)$ acts on:

- vectors of size n. $(\sigma, \boldsymbol{u}) \longmapsto \sigma \cdot \boldsymbol{u} := (u_{\sigma^{-1}(0)}, \ldots, u_{\sigma^{-1}(n-1)})$
- ordered pairs of vectors. $(\sigma, (\boldsymbol{u}, \boldsymbol{v})) \longmapsto \sigma \cdot (\boldsymbol{u}, \boldsymbol{v}) = (\sigma \cdot \boldsymbol{u}, \sigma \cdot \boldsymbol{v})$.
- Boolean monomials

$$(\sigma, \boldsymbol{x}^{\boldsymbol{v}}) \mapsto \sigma \cdot (\boldsymbol{x}^{\boldsymbol{v}}) := \boldsymbol{x}^{\sigma^{-1} \cdot \boldsymbol{v}} \quad \text{and} \quad (\sigma, \boldsymbol{a}^{\boldsymbol{u}}\boldsymbol{x}^{\boldsymbol{v}}) \mapsto \sigma \cdot (\boldsymbol{a}^{\boldsymbol{u}}\boldsymbol{x}^{\boldsymbol{v}}) := \boldsymbol{a}^{\sigma^{-1} \cdot \boldsymbol{u}} \boldsymbol{x}^{\sigma^{-1} \cdot \boldsymbol{v}} .$$

Example. Let $\boldsymbol{u} = (2, 0, 0, 0)$, $\boldsymbol{v} = (3, 0, 1, 1)$, $\sigma = (0\ 2\ 1) \in \mathfrak{S}_4$. Since

$$\sigma^{-1} \cdot \boldsymbol{u} = (0, 0, 2, 0) \quad \text{and} \quad \sigma^{-1} \cdot \boldsymbol{v} = (0, 1, 3, 1) ,$$

it comes that $\sigma \cdot (\boldsymbol{a}^{\boldsymbol{u}}\boldsymbol{x}^{\boldsymbol{v}}) = \boldsymbol{a}^{\sigma^{-1} \cdot \boldsymbol{v}} \boldsymbol{x}^{\sigma^{-1} \cdot \boldsymbol{v}} = a_2^2 x_1^1 x_2^3 x_3^1 = a_2[1] x_1[0] x_2[0] x_2[1] x_3[0]$.

Group actions (2)

Let $(\mathbb{G}, \circ)$ a group, E a set, $(\sigma, x) \longmapsto \sigma \cdot x$ a group action.

- **Orbit.** For any $x \in E$, $\mathrm{Orb}(x) = \{\sigma \cdot x,\ \sigma \in \mathbb{G}\} \subset E$.
- **Stabilizer.** For any $x \in E$, $\mathrm{Stab}(x) = \{\sigma,\ \sigma \cdot x = x\}$ subgroup of $\mathbb{G}$.

Example. Let $\boldsymbol{v} = (3, 1, 1)$, $\mathfrak{S}_3 = \{\mathrm{id}, (0\ 1), (0\ 2), (2\ 1), (0\ 1\ 2), (0\ 2\ 1)\}$.

- $\mathrm{Orb}(\boldsymbol{v}) = \{(3, 1, 1), (1, 3, 1), (1, 1, 3)\}$.
- $\mathrm{Stab}(\boldsymbol{v}) = \{\mathrm{id}, (1\ 2)\}$.

Important properties

- The set of orbits $\{\mathrm{Orb}(x),\ x \in E\}$ is a partition of E.
- It thus induces an equivalence relation $\sim$ defined as $x \sim x'$ if and only if $x' \in \mathrm{Orb}(x)$.
- For any $x \in E$,

$$|\mathrm{Orb}(x)| \cdot |\mathrm{Stab}(x)| = |\mathbb{G}| \ .$$

$\mathfrak{S}_n$-invariant Boolean functions

The action on monomials extends linearly to **Boolean functions**. (since $\sigma \cdot (\boldsymbol{a}^{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{v}}) = (\sigma \cdot \boldsymbol{a})^{\boldsymbol{u}} (\sigma \cdot \boldsymbol{x})^{\boldsymbol{v}}$)

Let $f \in \mathbb{Z}_{2^q}^n \to \mathbb{F}_2$, $F : \mathbb{Z}_{2^q}^n \times \mathbb{Z}_{2^q}^n \to \mathbb{F}_2$. We define $\sigma \cdot f$ and $\sigma \cdot F$ as:

$$\sigma \cdot f(\boldsymbol{x}) = f(\sigma \cdot \boldsymbol{x}) \quad \text{and} \quad \sigma \cdot F(\boldsymbol{a}, \boldsymbol{x}) \coloneqq F(\sigma \cdot \boldsymbol{a}, \sigma \cdot \boldsymbol{x}) \,.$$

To formalise the symmetries of $F^{m,n}$, we introduce the notion of **$\mathbb{G}$-invariance**.

Let $\mathbb{G}$ be a subgroup of $\mathfrak{S}_n$. The function f (resp. F) is $\mathbb{G}$-invariant if it satisfies:

$$\forall \sigma \in \mathbb{G}, \quad \sigma \cdot f = f \quad (\text{resp.} \quad \forall \sigma \in \mathbb{G}, \quad \sigma \cdot F = F) \,.$$

Example. The function $f : \boldsymbol{x} = (x_0, x_1) \longmapsto x_{0,0} x_{0,1} + x_{1,0} x_{1,1}$ is $\mathfrak{S}_n$-invariant since

$$f(\boldsymbol{x}) = x_0^3 + x_1^3 = x_1^3 + x_0^3 = (0\ 1) \cdot f(\boldsymbol{x}) \,.$$

NB: it is however not symmetric since $f(x_{0,1}, x_{0,0}, x_{1,1}, x_{1,0}) \neq f(x_{1,1}, x_{0,0}, x_{0,1}, x_{1,0})$.

Reduction to a system of representatives

Let $F : \mathbb{Z}_{2q}^n \times \mathbb{Z}_{2q}^n \longmapsto \mathbb{F}_2^n$. Recall

$$F(\boldsymbol{a}, \boldsymbol{x}) = \sum_{(\boldsymbol{u},\boldsymbol{v}) \in \mathbb{Z}_{2q}^n \times \mathbb{Z}_{2q}^n} \alpha_{(\boldsymbol{u},\boldsymbol{v})}(F)\boldsymbol{a}^{\boldsymbol{u}}\boldsymbol{x}^{\boldsymbol{v}} = \sum_{\boldsymbol{v} \in \mathbb{Z}_{2q}^n} \alpha_{\boldsymbol{v}}(F)\boldsymbol{x}^{\boldsymbol{v}} \quad \text{where} \quad \alpha_{\boldsymbol{v}}(F) = \sum_{\boldsymbol{u} \in \mathbb{Z}_{2q}^n} \alpha_{\boldsymbol{u},\boldsymbol{v}}(F)\boldsymbol{a}^{\boldsymbol{u}}.$$

Reduction to a system of representatives

Let $F : \mathbb{Z}_{2q}^n \times \mathbb{Z}_{2q}^n \longmapsto \mathbb{F}_2^n$. Recall

$$F(\mathbf{a}, \mathbf{x}) = \sum_{(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_{2q}^n \times \mathbb{Z}_{2q}^n} \alpha_{(\mathbf{u},\mathbf{v})}(F) \mathbf{a}^{\mathbf{u}} \mathbf{x}^{\mathbf{v}} = \sum_{\mathbf{v} \in \mathbb{Z}_{2q}^n} \alpha_{\mathbf{v}}(F) \mathbf{x}^{\mathbf{v}} \quad \text{where} \quad \alpha_{\mathbf{v}}(F) = \sum_{\mathbf{u} \in \mathbb{Z}_{2q}^n} \alpha_{\mathbf{u},\mathbf{v}}(F) \mathbf{a}^{\mathbf{u}}.$$

Let $\mathbb{G}$ be a subgroup of $\mathfrak{S}_n$. The following statements are equivalent:

(i) F is $\mathbb{G}$-invariant.

(ii) $\forall \sigma \in \mathbb{G}, \forall \mathbf{u} \in \mathbb{Z}_{2q}^n, \forall \mathbf{v} \in \mathbb{Z}_{2q}^n, \quad \alpha_{\sigma \cdot (\mathbf{u},\mathbf{v})}(F) = \alpha_{(\mathbf{u},\mathbf{v})}(F)$.

(iii) $\forall \sigma \in \mathbb{G}, \forall \mathbf{v} \in \mathbb{Z}_{2q}^n, \quad \sigma \cdot \alpha_{\mathbf{v}}(F) = \alpha_{\sigma^{-1} \cdot \mathbf{v}}(F)$.

Reduction to a system of representatives

Let $F : \mathbb{Z}_{2q}^n \times \mathbb{Z}_{2q}^n \longmapsto \mathbb{F}_2^n$. Recall

$$F(\boldsymbol{a}, \boldsymbol{x}) = \sum_{(\boldsymbol{u},\boldsymbol{v}) \in \mathbb{Z}_{2q}^n \times \mathbb{Z}_{2q}^n} \alpha_{(\boldsymbol{u},\boldsymbol{v})}(F) \boldsymbol{a}^{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{v}} = \sum_{\boldsymbol{v} \in \mathbb{Z}_{2q}^n} \alpha_{\boldsymbol{v}}(F) \boldsymbol{x}^{\boldsymbol{v}} \quad \text{where} \quad \alpha_{\boldsymbol{v}}(F) = \sum_{\boldsymbol{u} \in \mathbb{Z}_{2q}^n} \alpha_{\boldsymbol{u},\boldsymbol{v}}(F) \boldsymbol{a}^{\boldsymbol{u}}.$$

Let $\mathbb{G}$ be a subgroup of $\mathfrak{S}_n$. The following statements are equivalent:

(i) F is $\mathbb{G}$-invariant.

(ii) $\forall \sigma \in \mathbb{G}, \forall \boldsymbol{u} \in \mathbb{Z}_{2q}^n, \forall \boldsymbol{v} \in \mathbb{Z}_{2q}^n, \quad \alpha_{\sigma \cdot (\boldsymbol{u},\boldsymbol{v})}(F) = \alpha_{(\boldsymbol{u},\boldsymbol{v})}(F)$.

(iii) $\forall \sigma \in \mathbb{G}, \forall \boldsymbol{v} \in \mathbb{Z}_{2q}^n, \quad \sigma \cdot \alpha_{\boldsymbol{v}}(F) = \alpha_{\sigma^{-1} \cdot \boldsymbol{v}}(F)$.

By commutativity of modular addition:

$F^{m,n}$ is $\mathfrak{S}_n$-invariant.

Reduction to a system of representatives

Let $F : \mathbb{Z}_{2q}^n \times \mathbb{Z}_{2q}^n \longmapsto \mathbb{F}_2^n$. Recall

$$F(\mathbf{a}, \mathbf{x}) = \sum_{(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_{2q}^n \times \mathbb{Z}_{2q}^n} \alpha_{(\mathbf{u},\mathbf{v})}(F)\mathbf{a}^{\mathbf{u}}\mathbf{x}^{\mathbf{v}} = \sum_{\mathbf{v} \in \mathbb{Z}_{2q}^n} \alpha_{\mathbf{v}}(F)\mathbf{x}^{\mathbf{v}} \quad \text{where} \quad \alpha_{\mathbf{v}}(F) = \sum_{\mathbf{u} \in \mathbb{Z}_{2q}^n} \alpha_{\mathbf{u},\mathbf{v}}(F)\mathbf{a}^{\mathbf{u}}.$$

Let $\mathbb{G}$ be a subgroup of $\mathfrak{S}_n$. The following statements are equivalent:

(i) F is $\mathbb{G}$-invariant.

(ii) $\forall \sigma \in \mathbb{G}, \forall \mathbf{u} \in \mathbb{Z}_{2q}^n, \forall \mathbf{v} \in \mathbb{Z}_{2q}^n, \quad \alpha_{\sigma\cdot(\mathbf{u},\mathbf{v})}(F) = \alpha_{(\mathbf{u},\mathbf{v})}(F)$.

(iii) $\forall \sigma \in \mathbb{G}, \forall \mathbf{v} \in \mathbb{Z}_{2q}^n, \quad \sigma \cdot \alpha_{\mathbf{v}}(F) = \alpha_{\sigma^{-1}\cdot\mathbf{v}}(F)$.

By commutativity of modular addition:

$F^{m,n}$ is $\mathfrak{S}_n$-invariant.

- We can study $\{\alpha_{\mathbf{u},\mathbf{v}}(F^{m,n})\}$ using one element per orbit.
- Coefficients $\alpha_{\mathbf{v}}(F^{m,n})$ and $\alpha_{\mathbf{v}'}(F^{m,n})$ such that $\mathbf{v} \sim \mathbf{v}'$ can computed one from the other.

Scaling

Let $m \in \mathbb{N}^\star$ and $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}^d$. For any $n \geq d$, $\sigma \in \mathfrak{S}_n$,

$$\alpha_{(\boldsymbol{u},\boldsymbol{v})}(F^{m,d}) = \alpha_{\sigma\cdot(\tilde{\boldsymbol{u}},\tilde{\boldsymbol{v}})}(F^{m,n}),$$

where

$$\tilde{\boldsymbol{u}} = \big(u_0, \ldots, u_{d-1}, \underbrace{0, \ldots, 0}_{n-d \text{ zeros}}\big) \qquad \tilde{\boldsymbol{v}} = \big(v_0, \ldots, v_{d-1}, \underbrace{0, \ldots, 0}_{n-d \text{ zeros}}\big).$$

Scaling

Let $m \in \mathbb{N}^\star$ and $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}^d$. For any $n \geq d$, $\sigma \in \mathfrak{S}_n$,

$$\alpha_{(\boldsymbol{u},\boldsymbol{v})}(F^{m,d}) = \alpha_{\sigma\cdot(\tilde{\boldsymbol{u}},\tilde{\boldsymbol{v}})}(F^{m,n}),$$

where

$$\tilde{\boldsymbol{u}} = \big(u_0, \ldots, u_{d-1}, \underbrace{0, \ldots, 0}_{n-d \text{ zeros}}\big) \qquad \tilde{\boldsymbol{v}} = \big(v_0, \ldots, v_{d-1}, \underbrace{0, \ldots, 0}_{n-d \text{ zeros}}\big).$$

- $F^{m,m}$ allows to understand $F^{m,n}$ for all $n \geq m$.

Scaling

Let $m \in \mathbb{N}^\star$ and $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}^d$. For any $n \geq d$, $\sigma \in \mathfrak{S}_n$,

$$\alpha_{(\boldsymbol{u},\boldsymbol{v})}(F^{m,d}) = \alpha_{\sigma\cdot(\tilde{\boldsymbol{u}},\tilde{\boldsymbol{v}})}(F^{m,n}),$$

where

$$\tilde{\boldsymbol{u}} = (u_0, \ldots, u_{d-1}, \underbrace{0, \ldots, 0}_{n-d \text{ zeros}}) \qquad \tilde{\boldsymbol{v}} = (v_0, \ldots, v_{d-1}, \underbrace{0, \ldots, 0}_{n-d \text{ zeros}}).$$

- $F^{m,m}$ allows to understand $F^{m,n}$ for all $n \geq m$.
- Any term of $F^{m,n}$ with a support of size d can be derived from $F^{m,d}$.

Scaling

Let $m \in \mathbb{N}^\star$ and $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}^d$. For any $n \geq d$, $\sigma \in \mathfrak{S}_n$,

$$\alpha_{(\boldsymbol{u},\boldsymbol{v})}(F^{m,d}) = \alpha_{\sigma\cdot(\tilde{\boldsymbol{u}},\tilde{\boldsymbol{v}})}(F^{m,n}) \,,$$

where

$$\tilde{\boldsymbol{u}} = \big(u_0, \ldots, u_{d-1}, \underbrace{0, \ldots, 0}_{n-d \text{ zeros}}\big) \qquad \tilde{\boldsymbol{v}} = \big(v_0, \ldots, v_{d-1}, \underbrace{0, \ldots, 0}_{n-d \text{ zeros}}\big) \,.$$

- $F^{m,m}$ allows to understand $F^{m,n}$ for all $n \geq m$.
- Any term of $F^{m,n}$ with a support of size d can be derived from $F^{m,d}$.

Underlying assumption: for all $\boldsymbol{u}, \boldsymbol{v}$ such that $\alpha_{\boldsymbol{u},\boldsymbol{v}} \neq 0$, $\mathrm{Supp}(\boldsymbol{u}) = \mathrm{Supp}(\boldsymbol{v})$. Stems from:

$$F^{m,n}(\boldsymbol{a}, \boldsymbol{x}) = (\langle \boldsymbol{a}, \boldsymbol{x} \rangle)^m = \left(\sum a_i x_i\right)^m \,.$$

Effective computation of the ANF

Recall: S_m^n ordered partitions of length n of m. Let $\mathscr{C}_m^n$ be a system of representatives (unordered partitions).

$$F^{m,n}(\boldsymbol{a}, \boldsymbol{x}) = \sum_{\boldsymbol{c} \in \mathscr{C}_m^n} \sum_{\boldsymbol{c}' \in \mathrm{Orb}(\boldsymbol{c})} \prod_{i=0}^{n-1} (a_i \times x_i)^{c_i'} = \sum_{\boldsymbol{c} \in \mathscr{C}_m^n} \sum_{\boldsymbol{c}' \in \mathrm{Orb}(\boldsymbol{c})} H_{\boldsymbol{c}'}(\boldsymbol{a}, \boldsymbol{x}) = \sum_{\boldsymbol{c} \in \mathscr{C}_m^n} G_{\boldsymbol{c}}(\boldsymbol{a}, \boldsymbol{x}) \,.$$

Effective computation of the ANF

Recall: S_m^n ordered partitions of length n of m. Let $\mathscr{C}_m^n$ be a system of representatives (unordered partitions).

$$F^{m,n}(\boldsymbol{a},\boldsymbol{x}) = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} \sum_{\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})} \prod_{i=0}^{n-1} (a_i \times x_i)^{c_i'} = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} \sum_{\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})} H_{\boldsymbol{c}'}(\boldsymbol{a},\boldsymbol{x}) = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} G_{\boldsymbol{c}}(\boldsymbol{a},\boldsymbol{x})\,.$$

Effective computation of the ANF

Recall: S_m^n ordered partitions of length n of m. Let $\mathscr{C}_m^n$ be a system of representatives (unordered partitions).

$$F^{m,n}(\boldsymbol{a},\boldsymbol{x}) = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} \sum_{\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})} \prod_{i=0}^{n-1} (a_i \times x_i)^{c_i'} = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} \sum_{\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})} H_{\boldsymbol{c}'}(\boldsymbol{a},\boldsymbol{x}) = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} G_{\boldsymbol{c}}(\boldsymbol{a},\boldsymbol{x})\,.$$

Theorem. Let $\boldsymbol{c} \in \mathbb{Z}_{2^q}^n$, $(\boldsymbol{u},\boldsymbol{v}) \in \mathbb{Z}_{2^q}^n \times \mathbb{Z}_{2^q}^n$. Define $E_{\boldsymbol{c}}(\boldsymbol{u},\boldsymbol{v}) \coloneqq \mathrm{Exp}(H_{\boldsymbol{c}}) \cap \mathrm{Orb}(\boldsymbol{u},\boldsymbol{v})$. For any $\sigma \in \mathfrak{S}_n$,

$$\alpha_{\sigma\cdot(\boldsymbol{u},\boldsymbol{v})}(G_{\boldsymbol{c}}) = \alpha_{(\boldsymbol{u},\boldsymbol{v})}(G_{\boldsymbol{c}}) = \frac{|E_{\boldsymbol{c}}(\boldsymbol{u},\boldsymbol{v})|\; n!}{|\mathrm{Stab}(\boldsymbol{c})|\,|\mathrm{Orb}(\boldsymbol{u},\boldsymbol{v})|} \mod 2\,.$$

Effective computation of the ANF

Recall: S_m^n ordered partitions of length n of m. Let $\mathscr{C}_m^n$ be a system of representatives (unordered partitions).

$$F^{m,n}(\boldsymbol{a},\boldsymbol{x}) = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} \sum_{\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})} \prod_{i=0}^{n-1} (a_i \times x_i)^{c_i'} = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} \sum_{\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})} H_{\boldsymbol{c}'}(\boldsymbol{a},\boldsymbol{x}) = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} G_{\boldsymbol{c}}(\boldsymbol{a},\boldsymbol{x})\,.$$

Theorem. Let $\boldsymbol{c} \in \mathbb{Z}_{2^q}^n$, $(\boldsymbol{u},\boldsymbol{v}) \in \mathbb{Z}_{2^q}^n \times \mathbb{Z}_{2^q}^n$. Define $E_{\boldsymbol{c}}(\boldsymbol{u},\boldsymbol{v}) \coloneqq \mathrm{Exp}(H_{\boldsymbol{c}}) \cap \mathrm{Orb}(\boldsymbol{u},\boldsymbol{v})$. For any $\sigma \in \mathfrak{S}_n$,

$$\alpha_{\sigma\cdot(\boldsymbol{u},\boldsymbol{v})}(G_{\boldsymbol{c}}) = \alpha_{(\boldsymbol{u},\boldsymbol{v})}(G_{\boldsymbol{c}}) = \frac{|E_{\boldsymbol{c}}(\boldsymbol{u},\boldsymbol{v})|\; n!}{|\mathrm{Stab}(\boldsymbol{c})|\,|\mathrm{Orb}(\boldsymbol{u},\boldsymbol{v})|} \mod 2\,.$$

(i) For all canonical $\boldsymbol{c}$, compute $\{(\boldsymbol{u},\boldsymbol{v})^\star, \alpha_{(\boldsymbol{u},\boldsymbol{v})^\star}(G_{\boldsymbol{c}}) = 1\}$ from $H_{\boldsymbol{c}'}$ for some $\boldsymbol{c}' \in \mathrm{Orb}(\boldsymbol{c})$. (Theorem)

Effective computation of the ANF

Recall: S_m^n ordered partitions of length n of m. Let $\mathscr{C}_m^n$ be a system of representatives (unordered partitions).

$$F^{m,n}(\boldsymbol{a},\boldsymbol{x}) = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} \sum_{\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})} \prod_{i=0}^{n-1} (a_i \times x_i)^{c_i'} = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} \sum_{\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})} H_{\boldsymbol{c}'}(\boldsymbol{a},\boldsymbol{x}) = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} G_{\boldsymbol{c}}(\boldsymbol{a},\boldsymbol{x})\,.$$

Theorem. Let $\boldsymbol{c} \in \mathbb{Z}_{2^q}^n$, $(\boldsymbol{u},\boldsymbol{v}) \in \mathbb{Z}_{2^q}^n \times \mathbb{Z}_{2^q}^n$. Define $E_{\boldsymbol{c}}(\boldsymbol{u},\boldsymbol{v}) := \mathrm{Exp}(H_{\boldsymbol{c}}) \cap \mathrm{Orb}(\boldsymbol{u},\boldsymbol{v})$. For any $\sigma \in \mathfrak{S}_n$,

$$\alpha_{\sigma\cdot(\boldsymbol{u},\boldsymbol{v})}(G_{\boldsymbol{c}}) \quad = \quad \alpha_{(\boldsymbol{u},\boldsymbol{v})}(G_{\boldsymbol{c}}) \quad = \quad \frac{|E_{\boldsymbol{c}}(\boldsymbol{u},\boldsymbol{v})|\; n!}{|\mathrm{Stab}(\boldsymbol{c})|\,|\mathrm{Orb}(\boldsymbol{u},\boldsymbol{v})|} \mod 2\,.$$

(i) For all canonical $\boldsymbol{c}$, compute $\{(\boldsymbol{u},\boldsymbol{v})^\star, \alpha_{(\boldsymbol{u},\boldsymbol{v})^\star}(G_{\boldsymbol{c}}) = 1\}$ from $H_{\boldsymbol{c}'}$ for some $\boldsymbol{c}' \in \mathrm{Orb}(\boldsymbol{c})$. (Theorem)

(ii) Compute a SOR of the ANF of $F^{m,n}$ from the $G_{\boldsymbol{c}}$'s i.e. $\{(\boldsymbol{u},\boldsymbol{v})^\star, \alpha_{(\boldsymbol{u},\boldsymbol{v})^\star}(F^{m,n}) = 1\}$.

Effective computation of the ANF

Recall: S_m^n ordered partitions of length n of m. Let $\mathscr{C}_m^n$ be a system of representatives (unordered partitions).

$$F^{m,n}(\boldsymbol{a},\boldsymbol{x}) = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n}\ \sum_{\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})}\ \prod_{i=0}^{n-1}(a_i\times x_i)^{c_i'} = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n}\ \sum_{\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})} H_{\boldsymbol{c}'}(\boldsymbol{a},\boldsymbol{x}) = \sum_{\boldsymbol{c}\in\mathscr{C}_m^n} G_{\boldsymbol{c}}(\boldsymbol{a},\boldsymbol{x})\,.$$

Theorem. Let $\boldsymbol{c}\in\mathbb{Z}_{2^q}^n$, $(\boldsymbol{u},\boldsymbol{v})\in\mathbb{Z}_{2^q}^n\times\mathbb{Z}_{2^q}^n$. Define $E_{\boldsymbol{c}}(\boldsymbol{u},\boldsymbol{v}) := \mathrm{Exp}(H_{\boldsymbol{c}})\cap\mathrm{Orb}(\boldsymbol{u},\boldsymbol{v})$. For any $\sigma\in\mathfrak{S}_n$,

$$\alpha_{\sigma\cdot(\boldsymbol{u},\boldsymbol{v})}(G_{\boldsymbol{c}}) \quad=\quad \alpha_{(\boldsymbol{u},\boldsymbol{v})}(G_{\boldsymbol{c}}) \quad=\quad \frac{|E_{\boldsymbol{c}}(\boldsymbol{u},\boldsymbol{v})|\; n!}{|\mathrm{Stab}(\boldsymbol{c})|\,|\mathrm{Orb}(\boldsymbol{u},\boldsymbol{v})|} \mod 2\,.$$

(i) For all canonical $\boldsymbol{c}$, compute $\{(\boldsymbol{u},\boldsymbol{v})^\star, \alpha_{(\boldsymbol{u},\boldsymbol{v})^\star}(G_{\boldsymbol{c}})=1\}$ from $H_{\boldsymbol{c}'}$ for some $\boldsymbol{c}'\in\mathrm{Orb}(\boldsymbol{c})$. (Theorem)

(ii) Compute a SOR of the ANF of $F^{m,n}$ from the $G_{\boldsymbol{c}}$'s i.e. $\{(\boldsymbol{u},\boldsymbol{v})^\star, \alpha_{(\boldsymbol{u},\boldsymbol{v})^\star}(F^{m,n})=1\}$.

(iii) Compute the multiset $\{\{\alpha_{\boldsymbol{v}^\star}(F^{m,n})\neq 0\}\}$.

NB: $\{\alpha_{\boldsymbol{v}^\star}(F^{m,n})\neq 0\}$ is not a SOR of $\{\alpha_{\boldsymbol{v}}(F^{m,n})\neq 0\}/\sim$.

Effective computation of the number of monomials

Recall. For each random a, the function in $\{F_a^{m,n} := F^{m,n}(a,\cdot)\}$ is evaluated on the secret x to yield s_a.

If we can compute the ANF of $F_a^{m,n}$, we obtain an equation in the secret x:

$$\sum_{\mathbf{v}\in(\mathbb{F}_2^q)^n} \alpha_{\mathbf{v}}(F_a^{m,n})\ x^{\mathbf{v}} = \sum_{\mathbf{v}\in(\mathbb{F}_2^q)^n} \alpha_{\mathbf{v}}(F^{m,n})(a)\ x^{\mathbf{v}} = (s_a)^{m/2^{q-p}}\,.$$

Effective computation of the number of monomials

Recall. For each random $\boldsymbol{a}$, the function in $\{F_{\boldsymbol{a}}^{m,n} := F^{m,n}(\boldsymbol{a}, \cdot)\}$ is evaluated on the secret $\boldsymbol{x}$ to yield $s_{\boldsymbol{a}}$.

If we can compute the ANF of $F_{\boldsymbol{a}}^{m,n}$, we obtain an equation in the secret $\boldsymbol{x}$:

$$\sum_{\boldsymbol{v} \in (\mathbb{F}_2^q)^n} \alpha_{\boldsymbol{v}}(F_{\boldsymbol{a}}^{m,n})\ \boldsymbol{x}^{\boldsymbol{v}} = \sum_{\boldsymbol{v} \in (\mathbb{F}_2^q)^n} \alpha_{\boldsymbol{v}}(F^{m,n})(\boldsymbol{a})\ \boldsymbol{x}^{\boldsymbol{v}} = (s_{\boldsymbol{a}})^{m/2^{q-p}} .$$

NB: Number of monomials in the system:

$$\left| \bigcup_{\boldsymbol{a} \in \mathbb{Z}_{2^q}^n} \{\boldsymbol{v}, \alpha_{\boldsymbol{v}}(F_{\boldsymbol{a}}^{m,n}) \neq 0\} \right| = \left|\{\boldsymbol{v}, \alpha_{\boldsymbol{v}}(F^{m,n}) \neq 0\}\right| .$$

Effective computation of the number of monomials

Recall. For each random a, the function in $\{F_a^{m,n} := F^{m,n}(a,\cdot)\}$ is evaluated on the secret x to yield s_a.

If we can compute the ANF of $F_a^{m,n}$, we obtain an equation in the secret x:

$$\sum_{\boldsymbol{v}\in(\mathbb{F}_2^q)^n} \alpha_{\boldsymbol{v}}(F_a^{m,n})\ x^{\boldsymbol{v}} = \sum_{\boldsymbol{v}\in(\mathbb{F}_2^q)^n} \alpha_{\boldsymbol{v}}(F^{m,n})(a)\ x^{\boldsymbol{v}} = (s_a)^{m/2^{q-p}}\,.$$

NB: Number of monomials in the system:

$$\left|\bigcup_{\boldsymbol{a}\in\mathbb{Z}_{2^q}^n} \{\boldsymbol{v}, \alpha_{\boldsymbol{v}}(F_{\boldsymbol{a}}^{m,n}) \neq 0\}\right| = \left|\{\boldsymbol{v}, \alpha_{\boldsymbol{v}}(F^{m,n}) \neq 0\}\right|\,.$$

- Our algorithm returned the multiset $\{\{\alpha_{\boldsymbol{v}^\star}(F^{m,n}) \neq 0\}\}$, which has cardinal equal to $\left|\{\boldsymbol{v}^\star, \alpha_{\boldsymbol{v}^\star}\} \neq 0\right|$.

  Nr of monomials $= \left|\{\boldsymbol{v}, \alpha_{\boldsymbol{v}} \neq 0\}\right| = \sum_{\boldsymbol{v}^\star,\alpha_{\boldsymbol{v}^\star}\neq 0} \mathrm{Orb}(\alpha_{\boldsymbol{v}^\star})\binom{n}{|\mathrm{Supp}(\boldsymbol{v}^\star)|}$

Effective computation of the number of monomials

Recall. For each random a, the function in $\{F_a^{m,n} := F^{m,n}(a,\cdot)\}$ is evaluated on the secret x to yield s_a.
If we can compute the ANF of $F_a^{m,n}$, we obtain an equation in the secret x:

$$\sum_{\boldsymbol{v}\in(\mathbb{F}_2^q)^n} \alpha_{\boldsymbol{v}}(F_a^{m,n})\ x^{\boldsymbol{v}} = \sum_{\boldsymbol{v}\in(\mathbb{F}_2^q)^n} \alpha_{\boldsymbol{v}}(F^{m,n})(a)\ x^{\boldsymbol{v}} = (s_a)^{m/2^{q-p}}\,.$$

NB: Number of monomials in the system:

$$\left|\bigcup_{\boldsymbol{a}\in\mathbb{Z}_{2^q}^n} \{\boldsymbol{v}, \alpha_{\boldsymbol{v}}(F_{\boldsymbol{a}}^{m,n}) \neq 0\}\right| = \left|\{\boldsymbol{v}, \alpha_{\boldsymbol{v}}(F^{m,n}) \neq 0\}\right|\,.$$

- Our algorithm returned the multiset $\{\{\alpha_{\boldsymbol{v}^\star}(F^{m,n}) \neq 0\}\}$, which has cardinal equal to $\left|\{\boldsymbol{v}^\star, \alpha_{\boldsymbol{v}^\star\}} \neq 0\right|$.

$$\text{Nr of monomials } = |\{\boldsymbol{v}, \alpha_{\boldsymbol{v}} \neq 0\}| = \textstyle\sum_{\boldsymbol{v}^\star, \alpha_{\boldsymbol{v}^\star}\neq 0} \mathrm{Orb}(\alpha_{\boldsymbol{v}^\star})\binom{n}{|\mathsf{Supp}(\boldsymbol{v}^\star)|}$$

In practice, when m is a power of two, this is always equal to the upper bound $\binom{n+m}{m} - 1$.

Effective computation of other parameters

By default, linearisation basis is the set of monomials. **One can do better.**

Example. Assume two monomials x^{v_1} and x^{v_2} always appear together in the system.

- It is interesting to replace these monomials by $x^{v_1} + x^{v_2}$ in the linearisation basis.
- Less variables: improved cost of solving the linear system.
- Ideal situation: being able to compute the rank and relevant basis (not there yet).

Our approach allows us to compute

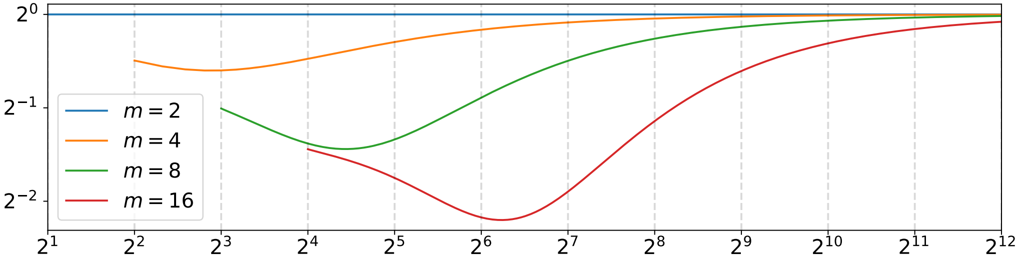
- The set

$$Q^{m,n} = \{Q_\alpha, \alpha \in \mathrm{Coefficients}_{\boldsymbol{x}}(F^{m,n})\}, \text{ where } \forall\alpha,\ Q_\alpha := \sum_{\boldsymbol{v}\in\mathbb{N}^n \mid \alpha_{\boldsymbol{v}}(F^{m,n})=\alpha} \boldsymbol{x}^{\boldsymbol{v}} \in \mathbb{F}_2[\boldsymbol{x}].$$

- The average sparsity in both generating families (monomials, $Q^{m,n}$).
- The rank is a WIP

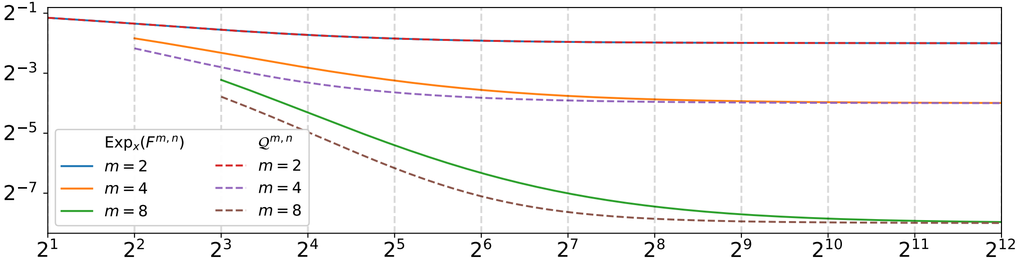
Our results: Upper bound on the rank

Ratio $\left|Q^{m,n}\right| / \binom{n+m}{m} - 1$ **as a function of** n**, for** $n \in [\![m, 4096]\!]$.



Our results: Sparsity

Average fraction of terms in a random equation $F_{\boldsymbol{a}}^{m,n}(\boldsymbol{x})$ as a function of n.



Improvements over Arora-Ge

Comparison to the linearisation attack by Arora & Ge using $\omega = 3$.

and cost of modular addition/multiplication $\approx q - p$.

$m = 2^{q-p}$	n	Arora-Ge	Our work ($\leq$ rank only)	Our work ($\leq$ rank and sparsity)
8	64	$2^{106.4}$	$2^{97.8}$	$2^{87.2}$
	128	$2^{129.3}$	$2^{121.8}$	$2^{110.8}$
	256	$2^{152.7}$	$2^{145.9}$	$2^{134.7}$
16	64	$2^{170.7}$	$2^{157.2}$	Non-available
	128	$2^{214.6}$	$2^{202.00}$	Non-available
	256	$2^{260.5}$	$2^{250.1}$	Non-available

Conclusion and open problems

Resolution techniques

Other observations (see the paper): Surrepresentation of LSBs (of $\boldsymbol{a}$ and $\boldsymbol{x}$).

- In guess-and-solve strategies: it makes sense to guess LSBs first.
- Time-data trade-offs: wait for $\boldsymbol{a}$ with many even a_i's.

Would love some help with resolution techniques

Remaining mathematical open problems such as proving the nr of monomials.

Other applications of group actions in symmetric crypto.