Cryptanalyse logique du probleme du logarithme discret sur courbes elliptiques

Monika Trimoska Sorina Ionica Gilles Dequen

MIS, Université de Picardie Jules Verne

Séminaire Caramba
12 mars 2021

Defining discrete log problem

Given a finite cyclic group $(G, +)$ of order N and two elements $g, h \in G$, find $x \in \mathbb{Z}$ such that

$$h = x \cdot g.$$

- Generic attacks - Pollard rho, Baby-step Giant-step, Kangaroo
- Index calculus attack : subexponential in $(\mathbb{Z}/p\mathbb{Z})*$.

Index calculus

1. Finding an appropriate *factor base* $\mathcal{B} = \{g_1, ..., g_k\}$, such that $\mathcal{B} \subseteq G$
2. Relation search phase : find relations of the form

$$[a_i]g \; + \; [b_i]h \; = \; \sum_{j=1}^{k} [c_{ij}]g_j$$

   for random integers a_i,b_i.
3. Linear algebra phase : having matrices $A = (a_i \;\; b_i)$ and $M = (c_{ij})$, find a kernel vector $v = (v_1 ... v_k)$ of the matrix M. Compute solution :

$$x = -(\sum_i a_i v_i)/(\sum_i b_i v_i)$$

Index calculus on binary elliptic curves

Let $\mathbb{F}_{2^n}$ be a finite field and E be an elliptic curve defined by

$$E : y^2 + xy = x^3 + ax^2 + b$$

with $a, b \in \mathbb{F}_{2^n}$ and n prime.

Index calculus on binary elliptic curves

Let $\mathbb{F}_{2^n}$ be a finite field and E be an elliptic curve defined by

$$E : y^2 + xy = x^3 + ax^2 + b$$

with $a, b \in \mathbb{F}_{2^n}$ and n prime.

1. Choice of an appropriate factor base $\mathcal{B}$
2. Point decomposition phase

   Find $P_1, \ldots, P_{m-1} \in \mathcal{B}$, such that, for $R \in E(\mathbb{F}_{2^n})$

   $$R = P_1 + \ldots + P_{m-1}$$

3. Linear algebra

Point Decomposition Problem (PDP)

Semaev's summation polynomials (2004)

$$S_2(X_1, X_2) = X_1 + X_2,$$
$$S_3(X_1, X_2, X_3) = X_1^2 X_2^2 + X_1^2 X_3^2 + X_1 X_2 X_3 + X_2^2 X_3^2 + b,$$

For $m \geq 4$

$$S_m(X_1, \ldots, X_m) =$$
$$Res_X(S_{m-k}(X_1, \ldots, X_{m-k-1}, X), S_{k+2}(X_{m-k}, \ldots, X_m, X))$$

Point Decomposition Problem (PDP)

Semaev's summation polynomials (2004)

$$S_2(X_1, X_2) = X_1 + X_2,$$
$$S_3(X_1, X_2, X_3) = X_1^2X_2^2 + X_1^2X_3^2 + X_1X_2X_3 + X_2^2X_3^2 + b,$$

For $m \geq 4$

$$S_m(X_1, \ldots, X_m) =$$
$$Res_X(S_{m-k}(X_1, \ldots, X_{m-k-1}, X), S_{k+2}(X_{m-k}, \ldots, X_m, X))$$

Reducing the PDP to the problem of finding the roots of S_m

For $R, P_1, \ldots, P_{m-1} \in E(\mathbb{F}_{2^n})$

$$R + P_1 + \ldots + P_{m-1} = \mathcal{O} \iff S_m(\mathbf{x}_R, \mathbf{x}_{P_1}, \ldots, \mathbf{x}_{P_{m-1}}) = 0$$

Index calculus on elliptic curves over extension fields

Gaudry (2008), Diem (2009)

Choice of an appropriate factor base

When E is an elliptic curve defined over $\mathbb{F}_{q^n}$, with n small, the factor base is the set of points whose x-coordinate lies in $\mathbb{F}_q$.

Weil descent

Rewrite the equation $S_{n+1}(\mathbf{x}_R, X_1, \ldots, X_n) = 0$ as a system of n equations over $\mathbb{F}_q$.

Gaudry (2008)

Symmetrization

Rewrite S_m in terms of the elementary symmetric polynomials

$$\begin{aligned}
\mathbf{e}_1 &= \sum_{1 \le i_1 \le m} X_{i_1}, \\
\mathbf{e}_2 &= \sum_{1 \le i_1, i_2 \le m} X_{i_1} X_{i_2}, \\
&\dots \\
\mathbf{e}_m &= \prod_{1 \le i \le m} X_i.
\end{aligned}$$

PDP algebraic model

Yun-Ju *et al.* (2013)

Factor base for elliptic curves defined over $\mathbb{F}_{2^n}$, with n prime

An l-dimensional vector subspace V of $\mathbb{F}_{2^n}/\mathbb{F}_2$. When $l \sim \frac{n}{m}$ the system has a reasonable chance to have a solution.

Let t be a root of a defining polynomial of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

X_i-variables

$$X_1 = c_{1,0} + \ldots + c_{1,l-1}t^{l-1}$$
$$X_2 = c_{2,0} + \ldots + c_{2,l-1}t^{l-1}$$
$$\ldots$$
$$X_m = c_{m,0} + \ldots + c_{m,l-1}t^{l-1}$$

e_i-variables

$$e_1 = d_{1,0} + \ldots + d_{1,l-1}t^{l-1}$$
$$e_2 = d_{2,0} + \ldots + d_{2,2l-2}t^{2l-2}$$
$$\ldots$$
$$e_m = d_{m,0} + \ldots + d_{m,m(l-1)}t^{m(l-1)}$$

PDP algebraic model

Two sets of equations

- Equations defining symmetric polynomials

$$d_{1,0} = c_{1,0} + \ldots + c_{m,0}$$
$$d_{1,1} = c_{1,1} + \ldots + c_{m,1}$$
$$\ldots$$
$$d_{m,m(l-1)} = c_{1,l} \cdot \ldots \cdot c_{m,l}.$$

- Equations derived from the Weil descent

PDP algebraic model

Two sets of equations

- Equations defining symmetric polynomials

$$
\begin{aligned}
&d_{1,0} = c_{1,0} + \ldots + c_{m,0} \\
&d_{1,1} = c_{1,1} + \ldots + c_{m,1} \\
&\ldots \\
&d_{m,m(l-1)} = c_{1,l} \cdot \ldots \cdot c_{m,l}.
\end{aligned}
$$

- Equations derived from the Weil descent

The system is commonly solved using Gröbner basis methods.

Logical cryptanalysis

From the algebraic model to the SAT-reasoning model

Using SAT solvers as a cryptanalytic tool requires expressing the cryptographic problem as a Boolean formula in conjunctive normal form (CNF) - a conjunction ($\wedge$) of OR-clauses.

Example.

$$(\neg x_1 \vee x_2) \wedge$$
$$(\neg x_2 \vee x_4 \vee \neg x_5)) \wedge$$
$$(x_5 \vee x_6)$$

From the algebraic model to the SAT-reasoning model

XOR-enabled SAT solvers are adapted to read a formula in CNF-XOR form - a conjunction ($\wedge$) of OR-clauses and XOR-clauses.

Example.

$$(\neg x_1 \vee x_2) \wedge$$
$$(\neg x_2 \vee x_4 \vee \neg x_5)) \wedge$$
$$(x_1 \oplus x_5 \oplus x_6)$$

From the algebraic model to the SAT-reasoning model

Variables in $\mathbb{F}_2$:
$\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_6$.

Propositional variables:
$x_1, x_2, x_3, x_4, x_5, x_6$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_4 + \mathbf{x}_5 \cdot \mathbf{x}_6 + 1 = 0$$
$$\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_4 + \mathbf{x}_5 + 1 = 0$$
$$\mathbf{x}_3 + \mathbf{x}_4 + \mathbf{x}_2 \cdot \mathbf{x}_4 + 1 = 0$$
$$\mathbf{x}_2 + \mathbf{x}_5 + \mathbf{x}_2 \cdot \mathbf{x}_4 + \mathbf{x}_5 \cdot \mathbf{x}_6 + 1 = 0$$
$$\mathbf{x}_3 + \mathbf{x}_4 + \mathbf{x}_6 + 1 = 0$$

$$(x_1 \oplus (x_2 \wedge x_4) \oplus (x_5 \wedge x_6)) \wedge$$
$$(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus (x_2 \wedge x_4)) \wedge$$
$$(x_2 \oplus x_5 \oplus (x_2 \wedge x_4) \oplus (x_5 \wedge x_6)) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$

From the algebraic model to the SAT-reasoning model

Add new variable x_7 to substitute the conjunction $x_2 \wedge x_4$. We have that

$$x_7 \Leftrightarrow (x_2 \wedge x_4)$$

$$\downarrow$$

$$(x_7 \Rightarrow (x_2 \wedge x_4)) \wedge ((x_2 \wedge x_4) \Rightarrow x_7)$$

$$\swarrow \qquad\qquad \searrow$$

$$\neg x_7 \vee (x_2 \wedge x_4) \qquad\qquad \neg(x_2 \wedge x_4) \vee x_7$$

$$\downarrow \qquad\qquad \downarrow$$

$$(\neg x_7 \vee x_2) \wedge (\neg x_7 \vee x_4) \qquad\qquad \neg x_2 \vee \neg x_4 \vee x_7$$

From the algebraic model to the SAT-reasoning model

Add new variable x_7 to substitute the conjunction $x_2 \wedge x_4$. We have that

$$x_7 \Leftrightarrow (x_2 \wedge x_4)$$

$$(x_7 \Rightarrow (x_2 \wedge x_4)) \wedge ((x_2 \wedge x_4) \Rightarrow x_7)$$

$$\neg x_7 \vee (x_2 \wedge x_4) \qquad \neg(x_2 \wedge x_4) \vee x_7$$

$$(\neg x_7 \vee x_2) \wedge (\neg x_7 \vee x_4) \qquad \neg x_2 \vee \neg x_4 \vee x_7$$

From the algebraic model to the SAT-reasoning model

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(x_1 \oplus (x_2 \wedge x_4) \oplus (x_5 \wedge x_6)) \wedge \\
&(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus (x_2 \wedge x_4)) \wedge \\
&(x_2 \oplus x_5 \oplus (x_2 \wedge x_4) \oplus (x_5 \wedge x_6)) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$

$$
\begin{aligned}
&(\neg x_7 \vee x_2) \wedge \\
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_2 \vee \neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_1 \oplus x_7 \oplus x_8) \wedge \\
&(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$

Unit propagation

Assigning literal l to TRUE will lead to :

1. Every clause containing l is removed (since the clause is satisfied).
2. In every clause that contains $\neg l$ this literal is deleted (since it can not contribute to the clause being satisfied).

- Propagation - obtaining a *unit clause* (clause containing a single literal) $\rightarrow$ the remaining literal is set to TRUE.
- Conflict - it exists at least one clause with all literals assigned to FALSE.

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(\neg x_7 \vee x_2) \wedge \\
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_2 \vee \neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_1 \oplus x_7 \oplus x_8) \wedge \\
&(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_7 \vee x_2) \wedge$$
$$(\neg x_7 \vee x_4) \wedge$$
$$(\neg x_2 \vee \neg x_4 \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_1 \oplus x_7 \oplus x_8) \wedge$$
$$(x_1 \oplus x_2 \oplus x_4 \oplus x_5) \wedge$$
$$(x_3 \oplus x_4 \oplus x_7) \wedge$$
$$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(x_3 \oplus x_4 \oplus x_6)$$

Assigned: $x_1 \leftarrow F$;

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_7 \vee x_2) \wedge$

$(\neg x_7 \vee x_4) \wedge$

$(\neg x_2 \vee \neg x_4 \vee x_7) \wedge$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

$(\cancel{x_1} \oplus x_7 \oplus x_8) \wedge$

$(\cancel{x_1} \oplus x_2 \oplus x_4 \oplus x_5) \wedge$

$(x_3 \oplus x_4 \oplus x_7) \wedge$

$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$

$(x_3 \oplus x_4 \oplus x_6)$

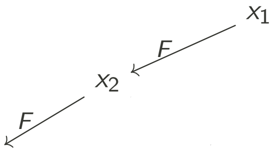
Assigned: $x_1 \leftarrow F$;

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_7 \vee x_2) \wedge$
$(\neg x_7 \vee x_4) \wedge$
$(\neg x_2 \vee \neg x_4 \vee x_7) \wedge$
$(\neg x_8 \vee x_5) \wedge$
$(\neg x_8 \vee x_6) \wedge$
$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$
$(x_7 \oplus x_8) \wedge$
$(x_2 \oplus x_4 \oplus x_5) \wedge$
$(x_3 \oplus x_4 \oplus x_7) \wedge$
$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$
$(x_3 \oplus x_4 \oplus x_6)$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow F$;

Propagation: $x_7 \leftarrow F$;

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_7 \vee x_2) \wedge$

$(\neg x_7 \vee x_4) \wedge$

$(\neg x_2 \vee \neg x_4 \vee x_7) \wedge$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

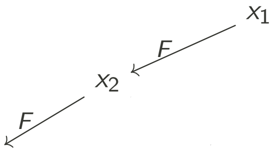
$(x_7 \oplus x_8) \wedge$

$(x_2 \oplus x_4 \oplus x_5) \wedge$

$(x_3 \oplus x_4 \oplus x_7) \wedge$

$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$

$(x_3 \oplus x_4 \oplus x_6)$



Assigned: $x_1 \leftarrow F; x_2 \leftarrow F; x_7 \leftarrow F;$

Propagation: $x_8 \leftarrow T;$

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

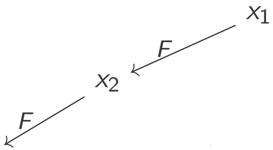
$(x_8) \wedge$

$(x_4 \oplus x_5) \wedge$

$(x_3 \oplus x_4) \wedge$

$(x_5 \oplus x_8) \wedge$

$(x_3 \oplus x_4 \oplus x_6)$



Assigned: $x_1 \leftarrow F; x_2 \leftarrow F; x_7 \leftarrow F;$ $x_8 \leftarrow T;$

Propagation: $x_5 \leftarrow T; x_6 \leftarrow T;$

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

~~$(\neg x_8 \vee x_5) \wedge$~~

~~$(\neg x_8 \vee x_6) \wedge$~~

~~$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$~~

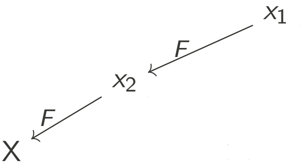
$(\cancel{x_8}\, T) \wedge$

$(x_4 \oplus \cancel{x_5}\, T) \wedge$

$(x_3 \oplus x_4) \wedge$

$(\cancel{x_5}\, T \oplus \cancel{x_8}\, T) \wedge$

$(x_3 \oplus x_4 \oplus \cancel{x_6}\, T)$



Assigned: $x_1 \leftarrow F; x_2 \leftarrow F; x_7 \leftarrow F;$
$x_8 \leftarrow T; x_5 \leftarrow T; x_6 \leftarrow T;$

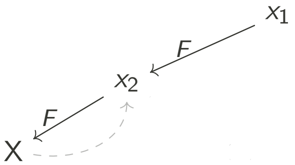
Conflict on fourth XOR-clause.

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(\neg x_7 \vee x_2) \wedge \\
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_2 \vee \neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_7 \oplus x_8) \wedge \\
&(x_2 \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$



Assigned: $x_1 \leftarrow F$;

Backtrack.

Solving process example

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

~~$(\neg x_7 \vee x_2)$~~ $\wedge$

$(\neg x_7 \vee x_4) \wedge$

$($~~$\neg x_2$~~$\vee \neg x_4 \vee x_7) \wedge$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

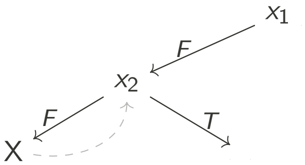
$(x_7 \oplus x_8) \wedge$

$($~~x_2~~$T \oplus x_4 \oplus x_5) \wedge$

$(x_3 \oplus x_4 \oplus x_7) \wedge$

$($~~x_2~~$T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$

$(x_3 \oplus x_4 \oplus x_6)$

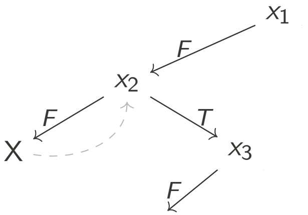


Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$;

Propositional variables:

x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_7 \vee x_4) \wedge$$
$$(\neg x_4 \vee x_7) \wedge$$
$$(\neg x_8 \vee x_5) \wedge$$
$$(\neg x_8 \vee x_6) \wedge$$
$$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$$
$$(x_7 \oplus x_8) \wedge$$
$$(T \oplus x_4 \oplus x_5) \wedge$$
$$(\cancel{x_3} \oplus x_4 \oplus x_7) \wedge$$
$$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$$
$$(\cancel{x_3} \oplus x_4 \oplus x_6)$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow F$;

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_7 \vee \cancel{x_4}) \wedge$

$\cancel{(\neg x_4 \vee x_7)} \wedge$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

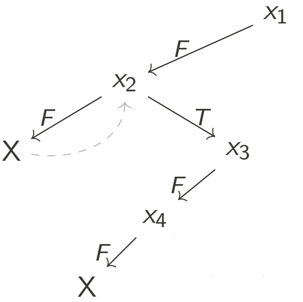
$(x_7 \oplus x_8) \wedge$

$(T \oplus \cancel{x_4} \oplus x_5) \wedge$

$(\cancel{x_4} \oplus x_7) \wedge$

$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$

$(\cancel{x_4} \oplus x_6)$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow F$; $x_4 \leftarrow F$;

Propagation: $x_7 \leftarrow F$; $x_7 \leftarrow T$; Conflict.

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

~~$(\neg x_7 \vee x_4)$~~ $\wedge$

$($~~$\neg x_4$~~ $\vee x_7) \wedge$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

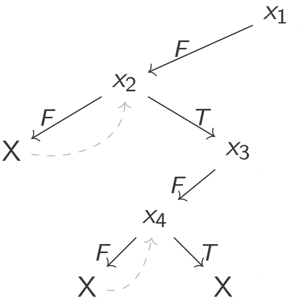
$(x_7 \oplus x_8) \wedge$

$(T \oplus$ ~~x_4~~ $T \oplus x_5) \wedge$

$($~~x_4~~ $T \oplus x_7) \wedge$

$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$

$($~~x_4~~ $T \oplus x_6)$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow F$; $x_4 \leftarrow F$;

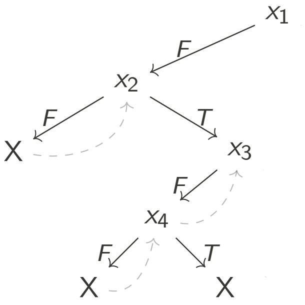
Propagation: $x_7 \leftarrow T$; $x_7 \leftarrow F$; ...
Conflict.

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$
\begin{aligned}
&(\neg x_7 \vee x_4) \wedge \\
&(\neg x_4 \vee x_7) \wedge \\
&(\neg x_8 \vee x_5) \wedge \\
&(\neg x_8 \vee x_6) \wedge \\
&(\neg x_5 \vee \neg x_6 \vee x_8) \wedge \\
&(x_7 \oplus x_8) \wedge \\
&(T \oplus x_4 \oplus x_5) \wedge \\
&(x_3 \oplus x_4 \oplus x_7) \wedge \\
&(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge \\
&(x_3 \oplus x_4 \oplus x_6)
\end{aligned}
$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$;

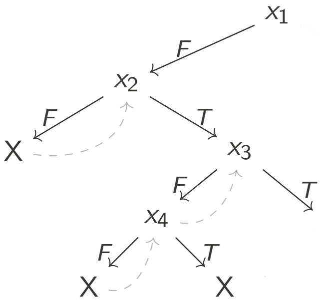
Backtrack

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_7 \lor x_4) \land$
$(\neg x_4 \lor x_7) \land$
$(\neg x_8 \lor x_5) \land$
$(\neg x_8 \lor x_6) \land$
$(\neg x_5 \lor \neg x_6 \lor x_8) \land$
$(x_7 \oplus x_8) \land$
$(T \oplus x_4 \oplus x_5) \land$
$(\cancel{x_3}\, T \oplus x_4 \oplus x_7) \land$
$(T \oplus x_5 \oplus x_7 \oplus x_8) \land$
$(\cancel{x_3}\, T \oplus x_4 \oplus x_6)$



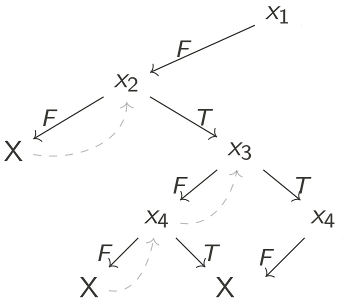
Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$;

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_7 \vee x_4) \wedge$
$(\neg x_4 \vee x_7) \wedge$
$(\neg x_8 \vee x_5) \wedge$
$(\neg x_8 \vee x_6) \wedge$
$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$
$(x_7 \oplus x_8) \wedge$
$(T \oplus x_4 \oplus x_5) \wedge$
$(T \oplus x_4 \oplus x_7) \wedge$
$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$
$(T \oplus x_4 \oplus x_6)$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$;

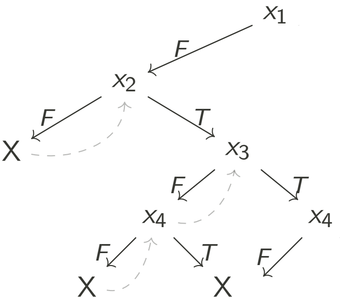
Propagated: $x_7 \leftarrow F$;

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$$(\neg x_8 \lor x_5) \land$$
$$(\neg x_8 \lor x_6) \land$$
$$(\neg x_5 \lor \neg x_6 \lor x_8) \land$$
$$(\cancel{x_7} \oplus x_8) \land$$
$$(T \oplus \cancel{x_4} \oplus x_5) \land$$
$$(T \oplus \cancel{x_4} \oplus \cancel{x_7}) \land$$
$$(T \oplus x_5 \oplus \cancel{x_7} \oplus x_8) \land$$
$$(T \oplus \cancel{x_4} \oplus x_6)$$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$; $x_4 \leftarrow F$; $x_7 \leftarrow F$;

Propagated: $x_8 \leftarrow T$; $x_5 \leftarrow F$; $x_6 \leftarrow F$;

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

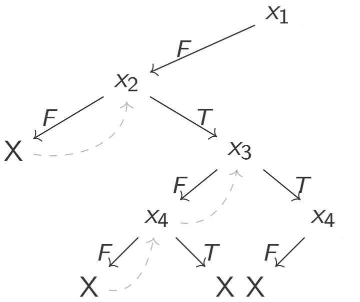
$(x_8 T) \wedge$

$(T \oplus x_5) \wedge$

$(T) \wedge$

$(T \oplus x_5 \oplus x_8 T) \wedge$

$(T \oplus x_6)$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$; $x_4 \leftarrow F$; $x_7 \leftarrow F$; $x_8 \leftarrow T$; $x_5 \leftarrow F$; $x_6 \leftarrow F$;

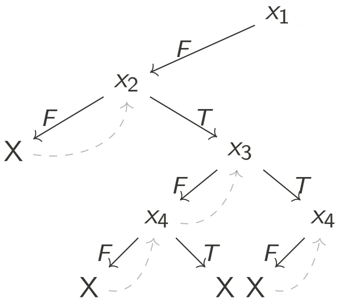
Conflict.

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE, FALSE}\}$

$(\neg x_7 \vee x_4) \wedge$
$(\neg x_4 \vee x_7) \wedge$
$(\neg x_8 \vee x_5) \wedge$
$(\neg x_8 \vee x_6) \wedge$
$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$
$(x_7 \oplus x_8) \wedge$
$(T \oplus x_4 \oplus x_5) \wedge$
$(T \oplus x_4 \oplus x_7) \wedge$
$(T \oplus x_5 \oplus x_7 \oplus x_8) \wedge$
$(T \oplus x_4 \oplus x_6)$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$;

Backtrack.

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$\cancel{(\neg x_7 \lor x_4)} \land$

$(\cancel{\neg x_4} \lor x_7) \land$

$(\neg x_8 \lor x_5) \land$

$(\neg x_8 \lor x_6) \land$

$(\neg x_5 \lor \neg x_6 \lor x_8) \land$

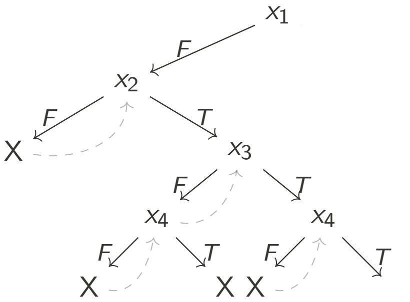
$(\cancel{x_7}\, T \oplus x_8) \land$

$(T \oplus \cancel{x_4}\, T \oplus x_5) \land$

$(T \oplus \cancel{x_4}\, T \oplus \cancel{x_7}\, T) \land$

$(T \oplus x_5 \oplus \cancel{x_7}\, T \oplus x_8) \land$

$(T \oplus \cancel{x_4}\, T \oplus x_6)$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$; $x_4 \leftarrow T$;

Propagation: $x_7 \leftarrow T$; $x_5 \leftarrow T$; $x_6 \leftarrow T$; $x_8 \leftarrow F$;

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

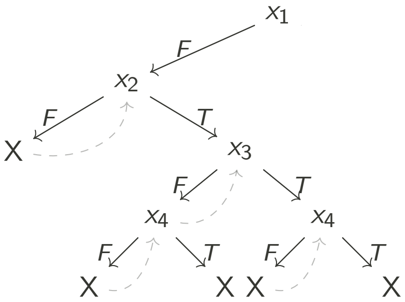
$(T) \wedge$

$(T) \wedge$

$(T) \wedge$

$(T) \wedge$

$(T) \wedge$



Assigned: $x_1 \leftarrow F$; $x_2 \leftarrow T$; $x_3 \leftarrow T$; $x_4 \leftarrow T$; $x_7 \leftarrow T$; $x_5 \leftarrow T$; $x_6 \leftarrow T$; $x_8 \leftarrow F$;

Conflict.

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_7 \vee x_2) \wedge$

$(\neg x_7 \vee x_4) \wedge$

$(\neg x_2 \vee \neg x_4 \vee x_7) \wedge$

$(\neg x_8 \vee x_5) \wedge$

$(\neg x_8 \vee x_6) \wedge$

$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$

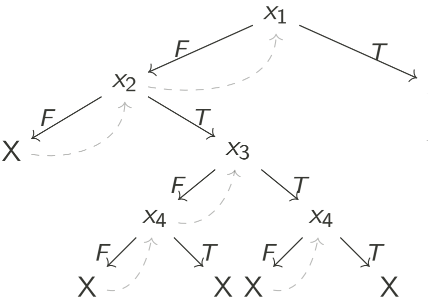
$(\cancel{x_1}\, T \oplus x_7 \oplus x_8) \wedge$

$(\cancel{x_1}\, T \oplus x_2 \oplus x_4 \oplus x_5) \wedge$

$(x_3 \oplus x_4 \oplus x_7) \wedge$

$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \wedge$

$(x_3 \oplus x_4 \oplus x_6)$



Assigned: $x_1 \leftarrow T$;

Solving process example

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_7 \lor x_2) \land$

$(\neg x_7 \lor x_4) \land$

$(\neg x_2 \lor \neg x_4 \lor x_7) \land$

$(\neg x_8 \lor x_5) \land$

$(\neg x_8 \lor x_6) \land$

$(\neg x_5 \lor \neg x_6 \lor x_8) \land$

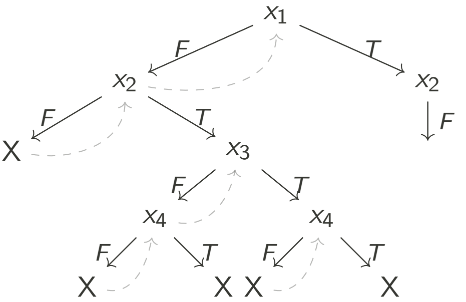
$(T \oplus x_7 \oplus x_8) \land$

$(T \oplus x_2 \oplus x_4 \oplus x_5) \land$

$(x_3 \oplus x_4 \oplus x_7) \land$

$(x_2 \oplus x_5 \oplus x_7 \oplus x_8) \land$

$(x_3 \oplus x_4 \oplus x_6)$



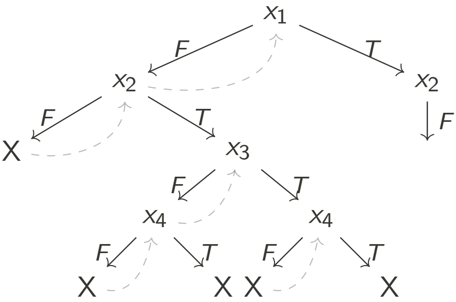
Assigned: $x_1 \leftarrow T$; $x_2 \leftarrow F$;

Propagation: $x_7 \leftarrow F$;

Solving process example

Propositional variables:
$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

$(\neg x_8 \vee x_5) \wedge$
$(\neg x_8 \vee x_6) \wedge$
$(\neg x_5 \vee \neg x_6 \vee x_8) \wedge$
$(T \oplus \cancel{x_7} \oplus x_8) \wedge$
$(T \oplus \cancel{x_2} \oplus x_4 \oplus x_5) \wedge$
$(x_3 \oplus x_4 \oplus \cancel{x_7}) \wedge$
$(\cancel{x_2} \oplus x_5 \oplus \cancel{x_7} \oplus x_8) \wedge$
$(x_3 \oplus x_4 \oplus x_6)$



Assigned: $x_1 \leftarrow T$; $x_2 \leftarrow F$; $x_7 \leftarrow F$;

Propagation: $x_8 \leftarrow F$;

Propositional variables:

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ with truth values in $\{\text{TRUE}, \text{FALSE}\}$

~~$(\neg x_8 \vee x_5) \wedge$~~

~~$(\neg x_8 \vee x_6) \wedge$~~

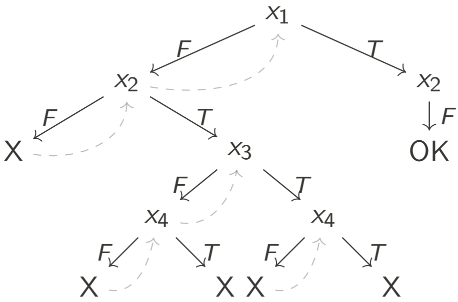
$(\neg x_5 \vee \neg x_6 \vee \cancel{x_8}) \wedge$

$(T \oplus x_4 \oplus x_5) \wedge$

$(x_3 \oplus x_4) \wedge$

$(x_5 \oplus \cancel{x_8}) \wedge$

$(x_3 \oplus x_4 \oplus x_6)$



Assigned: $x_1 \leftarrow T$; $x_2 \leftarrow F$; $x_7 \leftarrow F$; $x_8 \leftarrow F$;

Propagation: $x_5 \leftarrow T$; ... $x_4 \leftarrow T$; ... $x_3 \leftarrow F$; ... $x_6 \leftarrow F$;

DPLL algorithm

Davis-Putnam-Logemann-Loveland (DPLL) algorithm

Building a binary search-tree of height equivalent (at worst) to the number of variables.

WDSat solver

- DPLL-based.
- Composed of three reasoning modules: CNF module, XORSET module and XORGAUSS module.

Branching variables

1. Our DPLL-based algorithm only makes assignments on variables that are present in the initial Boolean polynomial system. Substitution variables are propagated as a consequence.

Branching variables

1. Our DPLL-based algorithm only makes assignments on variables that are present in the initial Boolean polynomial system. Substitution variables are propagated as a consequence.
2. We only reason on X_i-variables. e_i-variables are propagated.

X_i-variables

$$X_1 = c_{1,0} + \ldots + c_{1,l-1} t^{l-1}$$
$$X_2 = c_{2,0} + \ldots + c_{2,l-1} t^{l-1}$$
$$\ldots$$
$$X_m = c_{m,0} + \ldots + c_{m,l-1} t^{l-1}$$

e_i-variables

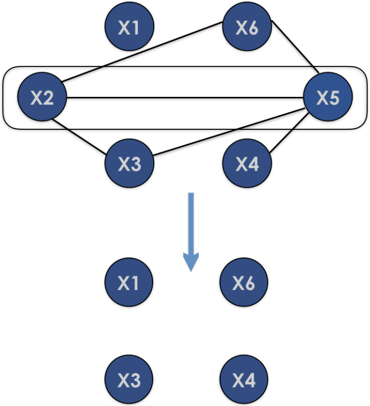
$$e_1 = d_{1,0} + \ldots + d_{1,l-1} t^{l-1}$$
$$e_2 = d_{2,0} + \ldots + d_{2,2l-2} t^{2l-2}$$
$$\ldots$$
$$e_m = d_{m,0} + \ldots + d_{m,m(l-1)} t^{m(l-1)}$$

MVC preprocessing technique

$$\mathbf{x}_1 + \mathbf{x}_2\mathbf{x}_3 + \mathbf{x}_4 + \mathbf{x}_4\mathbf{x}_5 = 0$$
$$\mathbf{x}_1 + \mathbf{x}_2\mathbf{x}_3 = 0$$
$$\mathbf{x}_1 + \mathbf{x}_3\mathbf{x}_5 + \mathbf{x}_6 = 0$$
$$\mathbf{x}_1 + \mathbf{x}_2\mathbf{x}_5\mathbf{x}_6 + \mathbf{x}_6 = 0$$

↓

$$\mathbf{x}_1 + \mathbf{x}_3 = 0$$
$$\mathbf{x}_1 + \mathbf{x}_3 + \mathbf{x}_6 = 0$$
$$\mathbf{x}_1 = 0.$$



MVC of third summation polynomial

$$S_3(X_1, X_2, X_3) = X_1^2 X_2^2 + X_1^2 X_3^2 + X_1 X_2 X_3 + X_2^2 X_3^2 + 1,$$

$$X_1 = c_{1,0} + \ldots + c_{1,l-1} t^{l-1}$$
$$X_2 = c_{2,0} + \ldots + c_{2,l-1} t^{l-1}$$
X_3 is a constant

MVC of third summation polynomial

$$S_3(X_1, X_2, X_3) = X_1^2 X_2^2 + X_1^2 X_3^2 + X_1 X_2 X_3 + X_2^2 X_3^2 + 1,$$

	1	2	3	4	5	6	7	8	9	0
1	○	○	○	○	○	●	●	●	●	●
2	○	○	○	○	○	●	●	●	●	●
3	○	○	○	○	○	●	●	●	●	●
4	○	○	○	○	○	●	●	●	●	●
5	○	○	○	○	○	●	●	●	●	●
6	●	●	●	●	●	○	○	○	○	○
7	●	●	●	●	●	○	○	○	○	○
8	●	●	●	●	●	○	○	○	○	○
9	●	●	●	●	●	○	○	○	○	○
0	●	●	●	●	●	○	○	○	○	○

Figure: Monomials connectivity graph derived from the model of S_3 when $l = 5$

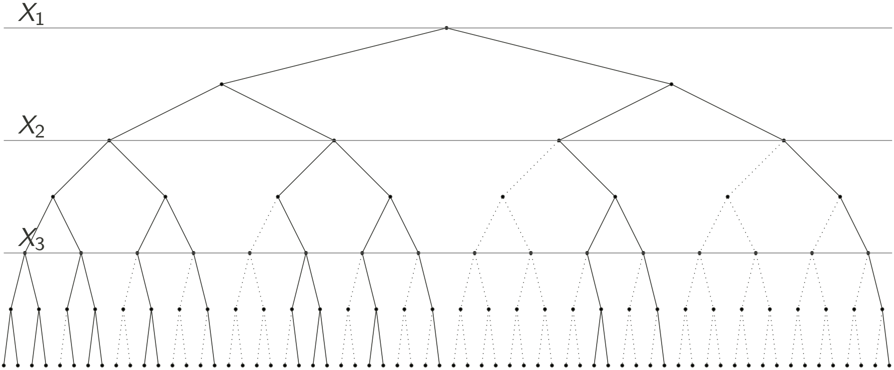
MVC of third summation polynomial

$$S_3(X_1, X_2, X_3) = X_1^2 X_2^2 + X_1^2 X_3^2 + X_1 X_2 X_3 + X_2^2 X_3^2 + 1,$$

- MVC is $\{c_{1,0}, \ldots, c_{1,l-1}\}$ or $\{c_{2,0}, \ldots, c_{2,l-1}\}$.
- Using the MVC preprocessing technique, the complexity of a point decomposition drops from $O(2^{2l})$ to $O(2^l)$.
- Unfortunately, we do not observe this with higher degree summation polynomials.

- Exploit the symmetry of Semaev's summation polynomials: when $X_1, ..., X_m$ is a solution, all permutations of this set are a solution as well.
- Establish the following constraint $X_1 \leq X_2 \leq \ldots \leq X_m$.
- Implement constraint in the solver using a tree-pruning-like technique.
- Optimize the complexity by a factor of $m!$.

WDSat - breaking symmetry



Experimental results

Third summation polynomial
$n = 41,\ l = 20$

Solving approach	SAT		UNSAT	
	Runtime (s)	#Conflicts	Runtime (s)	#Conflicts
Gröbner	16.8	*N/A*	18.7	*N/A*
MiniSat	> 600		> 600	
Glucose	> 600		> 600	
MapleLCMDistChronoBT	> 600		> 600	
CaDiCaL	> 600		> 600	
CryptoMiniSat	29.0	226668	84.3	627539
WDSat+XG-EXT+MVC	**4.2**	**27684**	**13.5**	**86152**

Table: Comparing Gröbner basis and SAT-based approaches for solving the PDP. Running times are in seconds.

Experimental results

Fourth summation polynomial

			SATisfiable			UNSATisfiable		
Approach	l	n	Runtime	#Conflicts	Memory	Runtime	#Conflicts	Memory
Gröbner basis	6	17	207.220	NA	3601	142.119	NA	3291
		19	215.187	NA	3940	155.765	NA	4091
	7	19	3854.708	NA	38763	2650.696	NA	38408
		23	3128.844	NA	35203	2286.136	NA	35162
WDSat	6	17	.601	49117	1.4	3.851	254686	1.4
		19	.470	38137	1.4	3.913	255491	1.4
	7	19	9.643	534867	16.7	44.107	2073089	16.7
		23	9.303	477632	16.7	47.347	2067168	16.7
WDSat breaking-sym	6	17	.220	17792	1.4	.605	43875	1.4
		19	.243	19166	1.4	.639	44034	1.4
	7	19	2.205	130062	1.4	6.859	351353	1.4
		23	3.555	189940	1.4	7.478	350257	1.4

Table: Comparing the WDSat approach with the Gröbner basis approach for solving the PDP. Running times are in seconds and memory is in MB.

Conclusion

- When solving the PDP for prime degree extension fields of $\mathbb{F}_2$, Gröbner basis methods should be replaced with a SAT-based approach.
- Our CNF-XOR model with the dedicated SAT-solver, WDSAT, yields significantly faster running times than all other algebraic and SAT-based approaches.
- Extending the WDSAT solver with our symmetry breaking technique optimizes the resolution of the PDP by a factor of m!.

Papers and open source code

1. **Parity (XOR) Reasoning for the Index Calculus Attack** (CP 2020)

   https://arxiv.org/abs/2001.11229

   https://github.com/mtrimoska/WDSat

2. **A SAT-Based Approach for Index Calculus on Binary Elliptic Curves** (AfricaCrypt 2020)

   https://eprint.iacr.org/2019/313

   https://github.com/mtrimoska/EC-Index-Calculus-Benchmarks