

A Simple Deterministic Algorithm for Systems of Quadratic Polynomials over \mathbb{F}_2

Monika Trimoska

Radboud University, University of Picardie Jules Verne
joint work with Charles Bouillaguet and Claire Delaplace

CROSSFYRE
2 December 2021

The multivariate polynomial problem

Definition

Given m multivariate quadratic polynomials f_1, \dots, f_m of n variables over a finite field \mathbb{F} , find a tuple $\mathbf{w} = (w_1, \dots, w_n)$ in \mathbb{F}^n , such that $f_1(\mathbf{w}) = \dots = f_m(\mathbf{w}) = 0$.

The degree-two case (MQ) is the underlying problem in one of the five families of post-quantum cryptographic schemes.

At the core of algebraic cryptanalysis: finding a solution to the multivariate polynomial system results in recovering the secret key or the plaintext.

Main idea

Example. $f_1 = x_1 + x_1x_3 + x_2x_4 + x_3x_4,$

$$f_2 = x_1 + x_1x_2 + x_3 + x_2x_4 + x_3x_4,$$

$$f_3 = x_1x_2 + x_3 + x_1x_4,$$

$$f_4 = x_2 + x_2x_3 + x_3 + x_4$$

Main idea

Example. $f_1 = x_1 + x_1x_3 + x_2x_4 + x_3x_4,$

$f_2 = x_1 + x_1x_2 + x_3 + x_2x_4 + x_3x_4,$

$f_3 = x_1x_2 + x_3 + x_1x_4,$

$f_4 = x_2 + x_2x_3 + x_3 + x_4$

→ First step: linearization

	x_1	x_1x_2	x_2	x_1x_3	x_2x_3	x_3	x_1x_4	x_2x_4	x_3x_4	x_4
f_1	1	0	0	1	0	0	0	1	1	0
f_2	1	1	0	0	0	1	0	1	1	0
f_3	0	1	0	0	0	1	1	0	0	0
f_4	0	0	1	0	1	1	0	0	0	1

Main idea

- Linearization
- Assign x_4 to 0.

	x_1	x_1x_2	x_2	x_1x_3	x_2x_3	x_3	x_1x_4	x_2x_4	x_3x_4	x_4
f_1	1	0	0	1	0	0				
f_2	1	1	0	0	0	1				
f_3	0	1	0	0	0	1				
f_4	0	0	1	0	1	1				

Main idea

- Linearization
- Assign x_4 to 0.
- Assign x_3 to 0.

	x_1	x_1x_2	x_2	x_1x_3	x_2x_3	x_3	x_1x_4	x_2x_4	x_3x_4	x_4
f_1	1	0	0							
f_2	1	1	0							
f_3	0	1	0							
f_4	0	0	1							

Main idea

- Linearization
- Assign x_4 to 0.
- Assign x_3 to 0.

	x_1	x_1x_2	x_2	x_1x_3	x_2x_3	x_3	x_1x_4	x_2x_4	x_3x_4	x_4
f_1	1	0	0							
f_2	1	1	0							
f_3	0	1	0							
f_4	0	0	1							

- Solve with Gaussian Elimination.

Guess sufficiently many variables so that the remaining polynomial system can be solved by linearization.

Guess **sufficiently many** variables so that the remaining polynomial system can be solved by linearization.

→ A linearized system is overdetermined when the the number of equations is greater than the number of monomials.

$$m \geq \frac{n(n+1)}{2}$$

Guess **sufficiently many** variables so that the remaining polynomial system can be solved by linearization.

→ A linearized system is overdetermined when the the number of equations is greater than the number of monomials.

$$m \geq \frac{n(n+1)}{2}$$

→ Guess the values of all variables except the $\sqrt{2m}$ last ones.

Guess **sufficiently many** variables so that the remaining polynomial system can be solved by linearization.

→ A linearized system is overdetermined when the the number of equations is greater than the number of monomials.

$$m \geq \frac{n(n+1)}{2}$$

→ Guess the values of all variables except the $\sqrt{2m}$ last ones.

$$\mathcal{O}(2^{n-\sqrt{2m}})$$

First refinement - a toy example

$$f_1 = x_1x_5 + x_2x_3 + x_2x_5 + x_3x_4 + x_1 + x_4 + x_5 + 1,$$

$$f_2 = x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_5 + x_4x_5 + x_1 + x_2 + x_4,$$

$$f_3 = x_1x_4 + x_2x_5 + x_3x_4 + x_1 + x_2 + x_4 + 1,$$

$$f_4 = x_1x_2 + x_1x_4 + x_2x_4 + x_2x_5 + x_2 + x_4 + x_5,$$

$$f_5 = x_1x_2 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4 + x_3x_5 + x_4x_5 + x_1 + x_5 + 1$$

→ Write the polynomials in $\mathbb{F}_2[x_1, x_2, x_3][x_4, x_5]$.

First refinement - a toy example

$$f_1 = x_1x_5 + x_2x_3 + x_2x_5 + x_3x_4 + x_1 + x_4 + x_5 + 1,$$

$$f_2 = x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_5 + x_4x_5 + x_1 + x_2 + x_4,$$

$$f_3 = x_1x_4 + x_2x_5 + x_3x_4 + x_1 + x_2 + x_4 + 1,$$

$$f_4 = x_1x_2 + x_1x_4 + x_2x_4 + x_2x_5 + x_2 + x_4 + x_5,$$

$$f_5 = x_1x_2 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4 + x_3x_5 + x_4x_5 + x_1 + x_5 + 1$$

→ Write the polynomials in $\mathbb{F}_2[x_1, x_2, x_3][x_4, x_5]$.

$$\begin{array}{c} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \end{array} \left[\begin{array}{c|cc|c} x_4x_5 & & & 1 \\ \hline 0 & x_3 + 1 & x_1 + x_2 + 1 & x_2x_3 + x_1 + 1 \\ 1 & x_1 + x_2 + 1 & x_1 + x_3 & x_1x_3 + x_2x_3 + x_1 + x_2 \\ 0 & x_1 + x_3 + 1 & x_2 & x_1 + x_2 + 1 \\ 0 & x_1 + x_2 + 1 & x_2 + 1 & x_1x_2 + x_2 \\ 1 & x_2 + x_3 & x_1 + x_3 + 1 & x_1x_2 + x_2x_3 + x_1 + 1 \end{array} \right]$$

First refinement - a toy example

$$\begin{array}{c} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \end{array} \left[\begin{array}{c|c|c|c} x_4 x_5 & x_4 & x_5 & 1 \\ \hline 0 & x_3 + 1 & x_1 + x_2 + 1 & x_2 x_3 + x_1 + 1 \\ \hline 1 & x_1 + x_2 + 1 & x_1 + x_3 & x_1 x_3 + x_2 x_3 + x_1 + x_2 \\ \hline 0 & x_1 + x_3 + 1 & x_2 & x_1 + x_2 + 1 \\ \hline 0 & x_1 + x_2 + 1 & x_2 + 1 & x_1 x_2 + x_2 \\ \hline 1 & x_2 + x_3 & x_1 + x_3 + 1 & x_1 x_2 + x_2 x_3 + x_1 + 1 \end{array} \right]$$

→ Put the columns corresponding to quadratic terms in reduced row echelon form.

First refinement - a toy example

$$\begin{array}{c}
 f_1 \\
 f_2 \\
 f_3 \\
 f_4 \\
 f_5
 \end{array}
 \begin{array}{c}
 x_4 x_5 \\
 x_4 \\
 x_5 \\
 1
 \end{array}
 \left[\begin{array}{c|c|c|c}
 0 & x_3 + 1 & x_1 + x_2 + 1 & x_2 x_3 + x_1 + 1 \\
 1 & x_1 + x_2 + 1 & x_1 + x_3 & x_1 x_3 + x_2 x_3 + x_1 + x_2 \\
 0 & x_1 + x_3 + 1 & x_2 & x_1 + x_2 + 1 \\
 0 & x_1 + x_2 + 1 & x_2 + 1 & x_1 x_2 + x_2 \\
 1 & x_2 + x_3 & x_1 + x_3 + 1 & x_1 x_2 + x_2 x_3 + x_1 + 1
 \end{array} \right]$$

→ Put the columns corresponding to quadratic terms in reduced row echelon form.

$$\begin{array}{c}
 f_2 \\
 f_1 \\
 f_3 \\
 f_4 \\
 f_2 + f_5
 \end{array}
 \begin{array}{c}
 x_4 x_5 \\
 x_4 \\
 x_5 \\
 1
 \end{array}
 \left[\begin{array}{c|c|c|c}
 1 & x_1 + x_2 + 1 & x_1 + x_3 & x_1 x_3 + x_2 x_3 + x_1 + x_2 \\
 0 & x_3 + 1 & x_1 + x_2 + 1 & x_2 x_3 + x_1 + 1 \\
 0 & x_1 + x_3 + 1 & x_2 & x_1 + x_2 + 1 \\
 0 & x_1 + x_2 + 1 & x_2 + 1 & x_1 x_2 + x_2 \\
 0 & x_1 + x_3 + 1 & 1 & x_1 x_2 + x_1 x_3 + x_2 + 1
 \end{array} \right]$$

First refinement - a toy example

	$x_4 x_5$	x_4	x_5	1
f_2	1	$x_1 + x_2 + 1$	$x_1 + x_3$	$x_1 x_3 + x_2 x_3 + x_1 + x_2$
f_1	0	$x_3 + 1$	$x_1 + x_2 + 1$	$x_2 x_3 + x_1 + 1$
f_3	0	$x_1 + x_3 + 1$	x_2	$x_1 + x_2 + 1$
f_4	0	$x_1 + x_2 + 1$	$x_2 + 1$	$x_1 x_2 + x_2$
$f_2 + f_5$	0	$x_1 + x_3 + 1$	1	$x_1 x_2 + x_1 x_3 + x_2 + 1$

→ Create a system by extracting non-pivotal rows.

First refinement - a toy example

	$x_4 x_5$	x_4	x_5	1
f_2	1	$x_1 + x_2 + 1$	$x_1 + x_3$	$x_1 x_3 + x_2 x_3 + x_1 + x_2$
f_1	0	$x_3 + 1$	$x_1 + x_2 + 1$	$x_2 x_3 + x_1 + 1$
f_3	0	$x_1 + x_3 + 1$	x_2	$x_1 + x_2 + 1$
f_4	0	$x_1 + x_2 + 1$	$x_2 + 1$	$x_1 x_2 + x_2$
$f_2 + f_5$	0	$x_1 + x_3 + 1$	1	$x_1 x_2 + x_1 x_3 + x_2 + 1$

→ Create a system by extracting non-pivotal rows.

$$\underbrace{\begin{pmatrix} x_3 + 1 & x_1 + x_2 + 1 \\ x_1 + x_3 + 1 & x_2 \\ x_1 + x_2 + 1 & x_2 + 1 \\ x_1 + x_3 + 1 & 1 \end{pmatrix}}_{L(x_1, x_2, x_3)} \begin{pmatrix} x_4 \\ x_5 \end{pmatrix} = \underbrace{\begin{pmatrix} x_2 x_3 + x_1 + 1 \\ x_1 + x_2 + 1 \\ x_1 x_2 + x_2 \\ x_1 x_2 + x_1 x_3 + x_2 + 1 \end{pmatrix}}_{Q(x_1, x_2, x_3)}$$

First refinement - a toy example

$$\underbrace{\begin{pmatrix} x_3 + 1 & x_1 + x_2 + 1 \\ x_1 + x_3 + 1 & x_2 \\ x_1 + x_2 + 1 & x_2 + 1 \\ x_1 + x_3 + 1 & 1 \end{pmatrix}}_{L(x_1, x_2, x_3)} \begin{pmatrix} x_4 \\ x_5 \end{pmatrix} = \underbrace{\begin{pmatrix} x_2 x_3 + x_1 + 1 \\ x_1 + x_2 + 1 \\ x_1 x_2 + x_2 \\ x_1 x_2 + x_1 x_3 + x_2 + 1 \end{pmatrix}}_{Q(x_1, x_2, x_3)}$$

- Enumerate all the possible values of the variables (x_1, x_2, x_3) .
- For each combination, solve the linear system $L(x_1, x_2, x_3) \cdot (x_4, x_5)^t = Q(x_1, x_2, x_3)$ for (x_4, x_5) .
- Check candidate solutions against f_2 .

Early elimination of inconsistent solutions

For each combination (x_1, x_2, x_3) :

- 1 Check whether the linear system is both full-rank and inconsistent. If this is the case, we can move on.
- 2 Otherwise, compute solution (or a basis of the solution space).

Early elimination of inconsistent solutions

For each combination (x_1, x_2, x_3) :

- 1 Check whether the linear system is both full-rank and inconsistent. If this is the case, we can move on.
- 2 Otherwise, compute solution (or a basis of the solution space).

Other (implementation) refinements

- Faster Polynomial Enumeration Using a Gray Code.
- Vectorization.

- The algorithm is simple - does not rely on sophisticated data structures or complex sub-algorithms such as fast multivariate polynomial multiplication, fast multipoint evaluation/interpolation, Gröbner basis computations or large sparse linear system solvers.
- The memory complexity is negligible.
- The algorithm is trivially parallelizable.
- Our implementation outperforms a competitive implementation of exhaustive search (libfes-lite) for a sufficiently large m (example, $m = 48$ using a single core on a recent laptop).

Overview of related work

Hybridization

Candidate
solutions
(subsystem)

Conflict
search

Extending
to higher
degrees

Computing
a Gröbner
Basis

Simple

FXL

BoolSolve

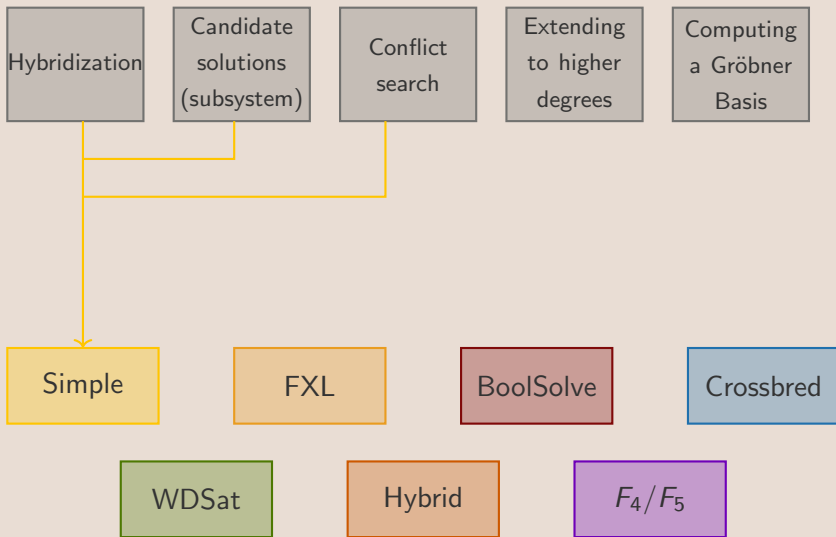
Crossbred

WDSat

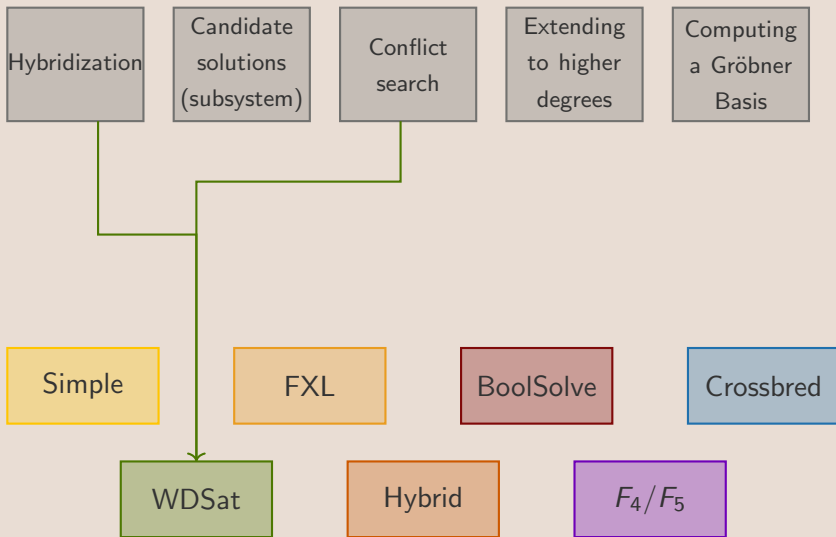
Hybrid

F_4/F_5

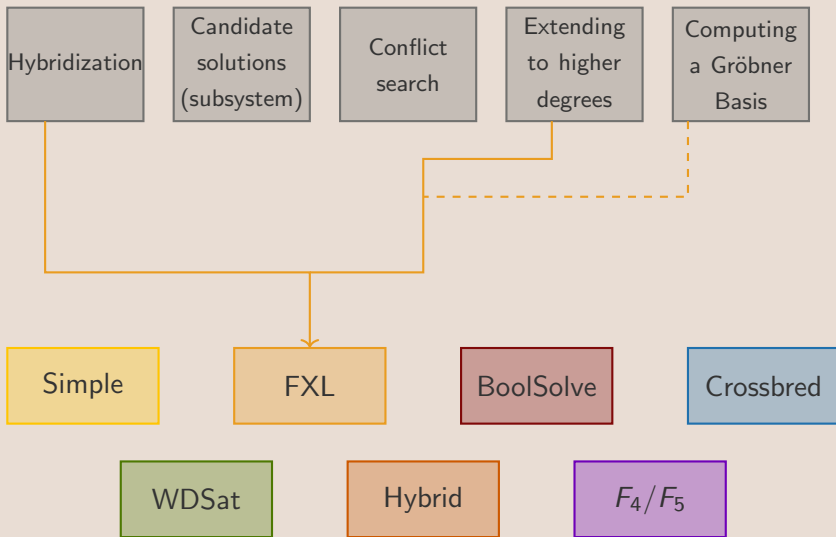
Overview of related work



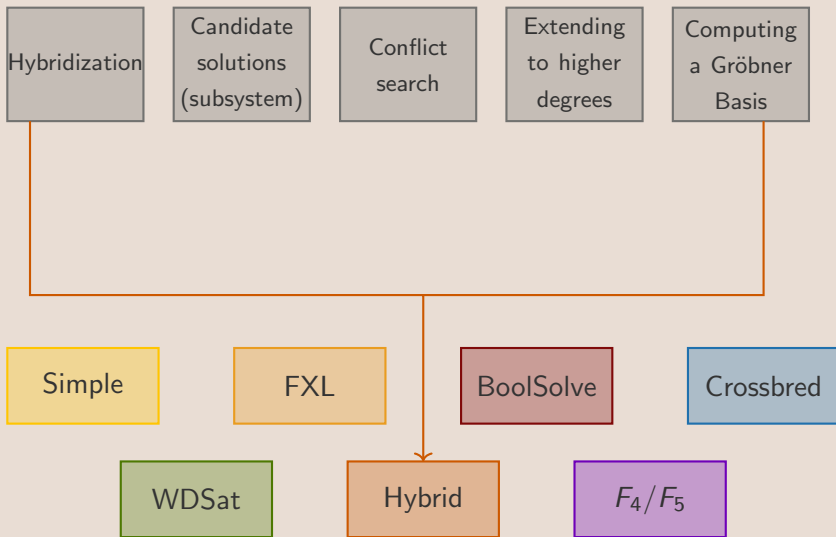
Overview of related work



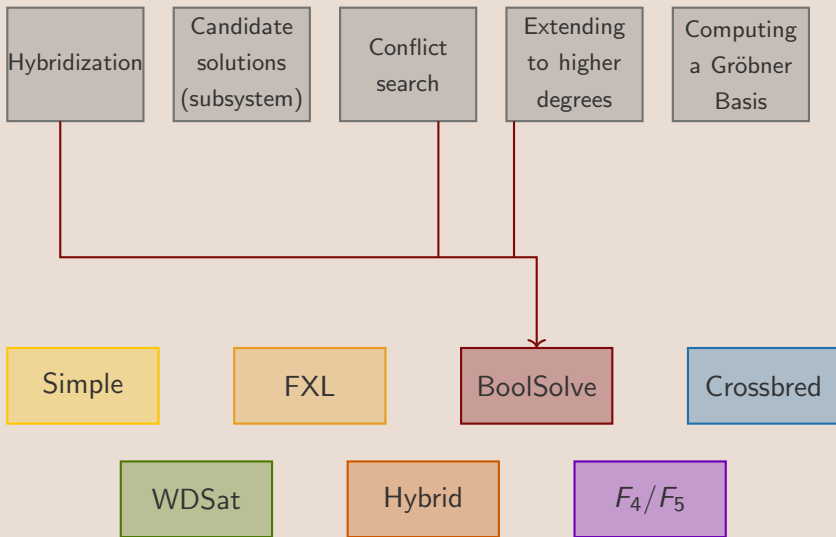
Overview of related work



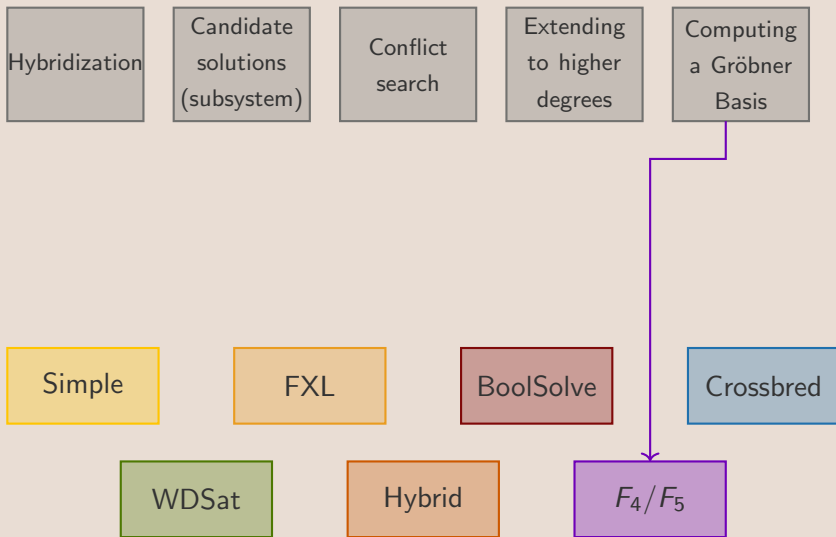
Overview of related work



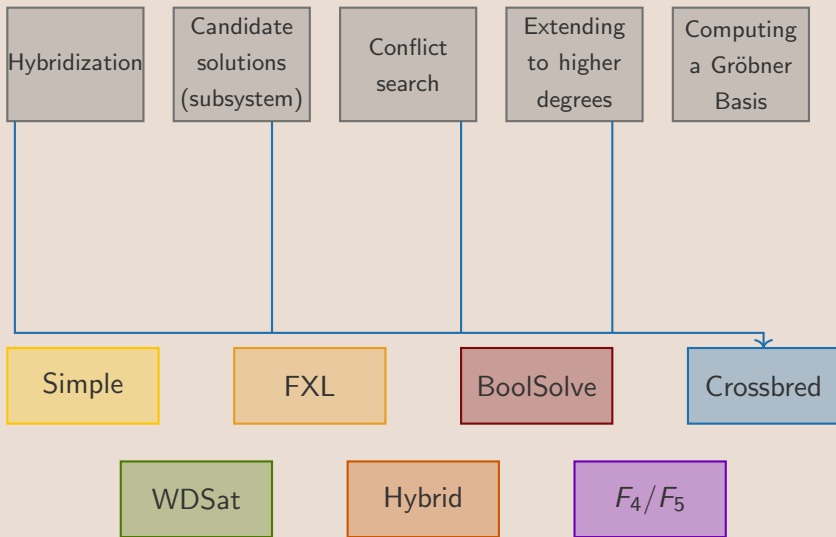
Overview of related work



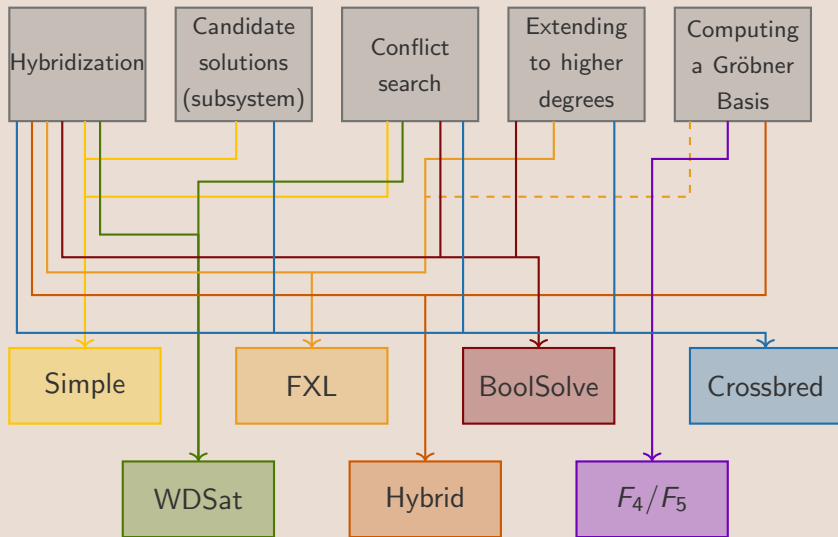
Overview of related work



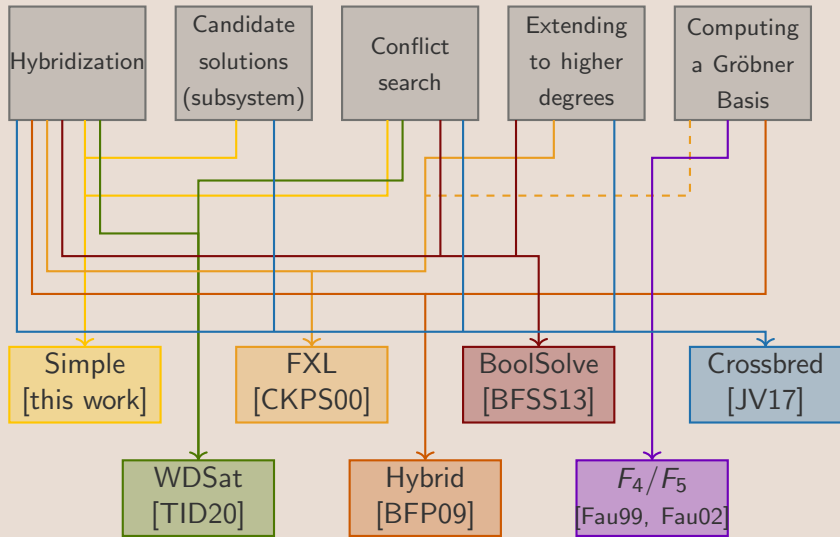
Overview of related work










Overview of related work



Overview of related work



-  Luk Bettale, Jean-Charles Faugère, and Ludovic Perret, *Hybrid approach for solving multivariate systems over finite fields*, J. Math. Cryptol. **3** (2009), no. 3, 177–197.
-  Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Pierre-Jean Spaenlehauer, *On the complexity of solving quadratic boolean systems*, J. Complexity **29** (2013), no. 1, 53–75.
-  Nicolas T. Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir, *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding (Bart Preneel, ed.), Lecture Notes in Computer Science, vol. 1807, Springer, 2000, pp. 392–407.
-  Jean-Charles Faugère, *A new efficient algorithm for computing grobner bases (f4)*, Journal of Pure and Applied Algebra **139** (1999), no. 1-3, 61–68.

-  Jean Charles Faugère, *A new efficient algorithm for computing gröbner bases without reduction to zero (f5)*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ISSAC '02, Association for Computing Machinery, 2002, p. 75–83.
-  Antoine Joux and Vanessa Vitse, *A Crossbred Algorithm for Solving Boolean Polynomial Systems*, NuTMiC, Lecture Notes in Computer Science, vol. 10737, Springer, 2017, <https://eprint.iacr.org/2017/372.pdf>, pp. 3–21.
-  Monika Trimoska, Sorina Ionica, and Gilles Dequen, *Parity (xor) reasoning for the index calculus attack*, Principles and Practice of Constraint Programming (Cham) (Helmut Simonis, ed.), Springer International Publishing, 2020, pp. 774–790.