Where did my RAM go? Using algebraic cryptanalysis in practice

Lars Ran

Monika Trimoska

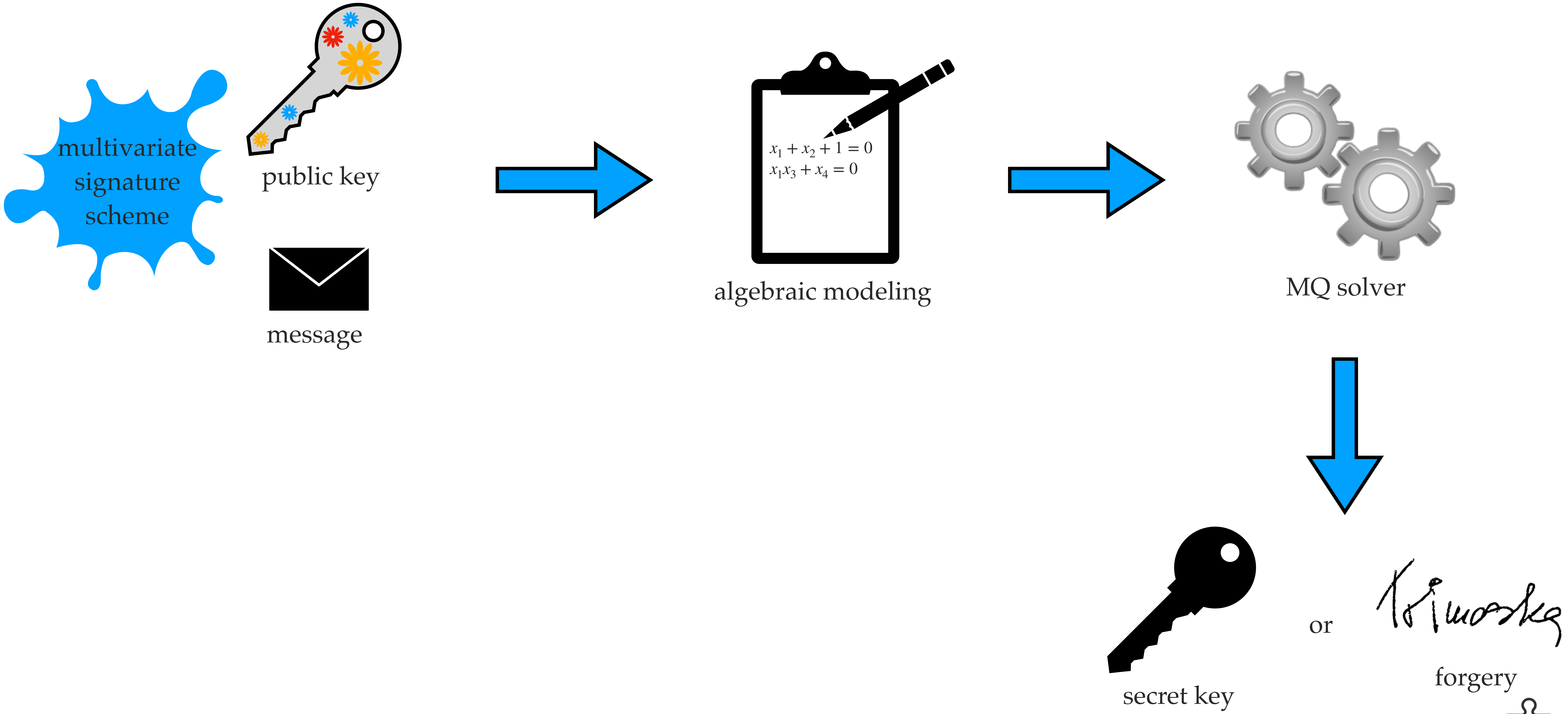
Summer school on RWC and privacy
July 1, Dubrovnik, Croatia

TU/e

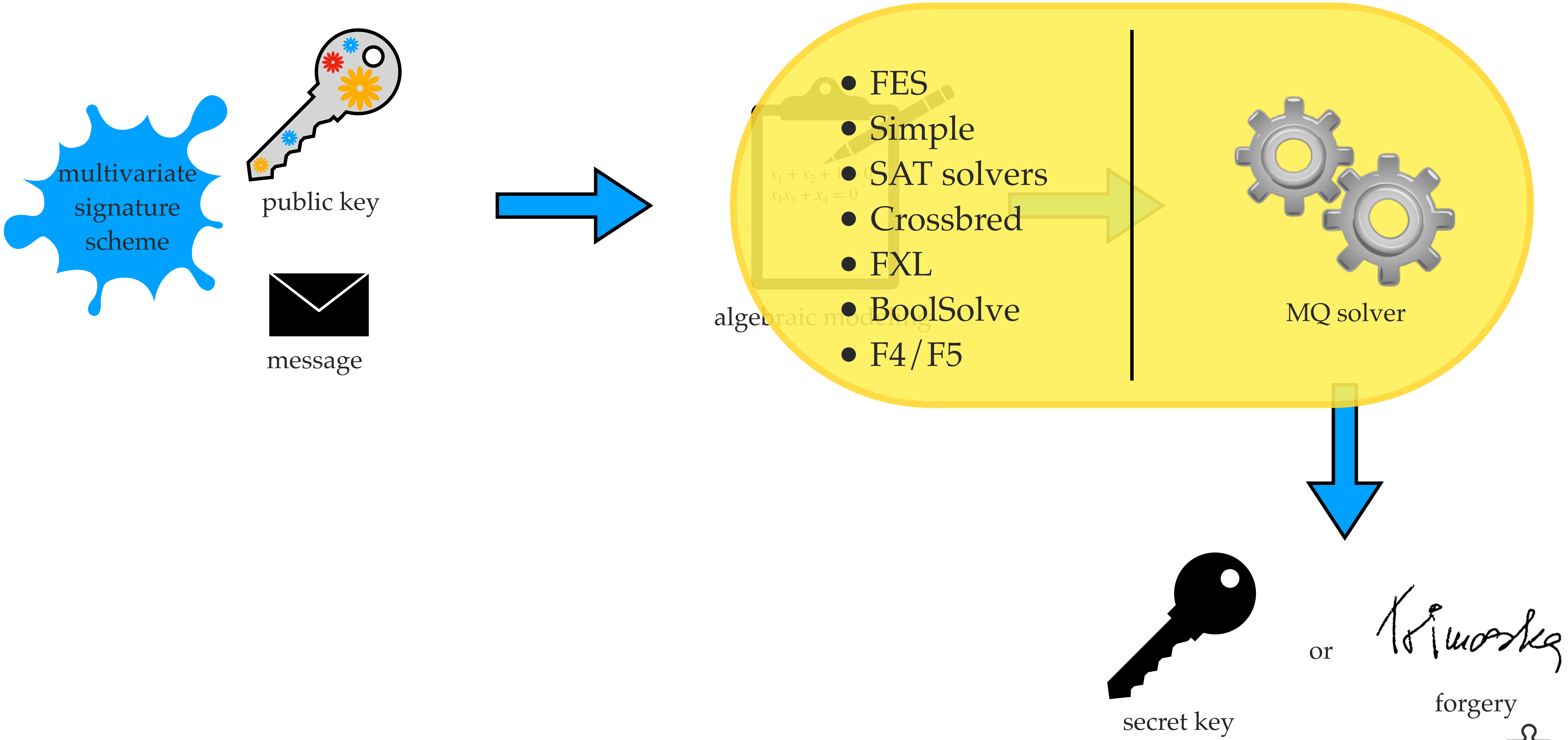
Algebraic cryptanalysis

A type of cryptanalytic methods where the problem of finding the secret key (or any attack goal) is reduced to the problem of finding a solution to a nonlinear multivariate polynomial system of equations.

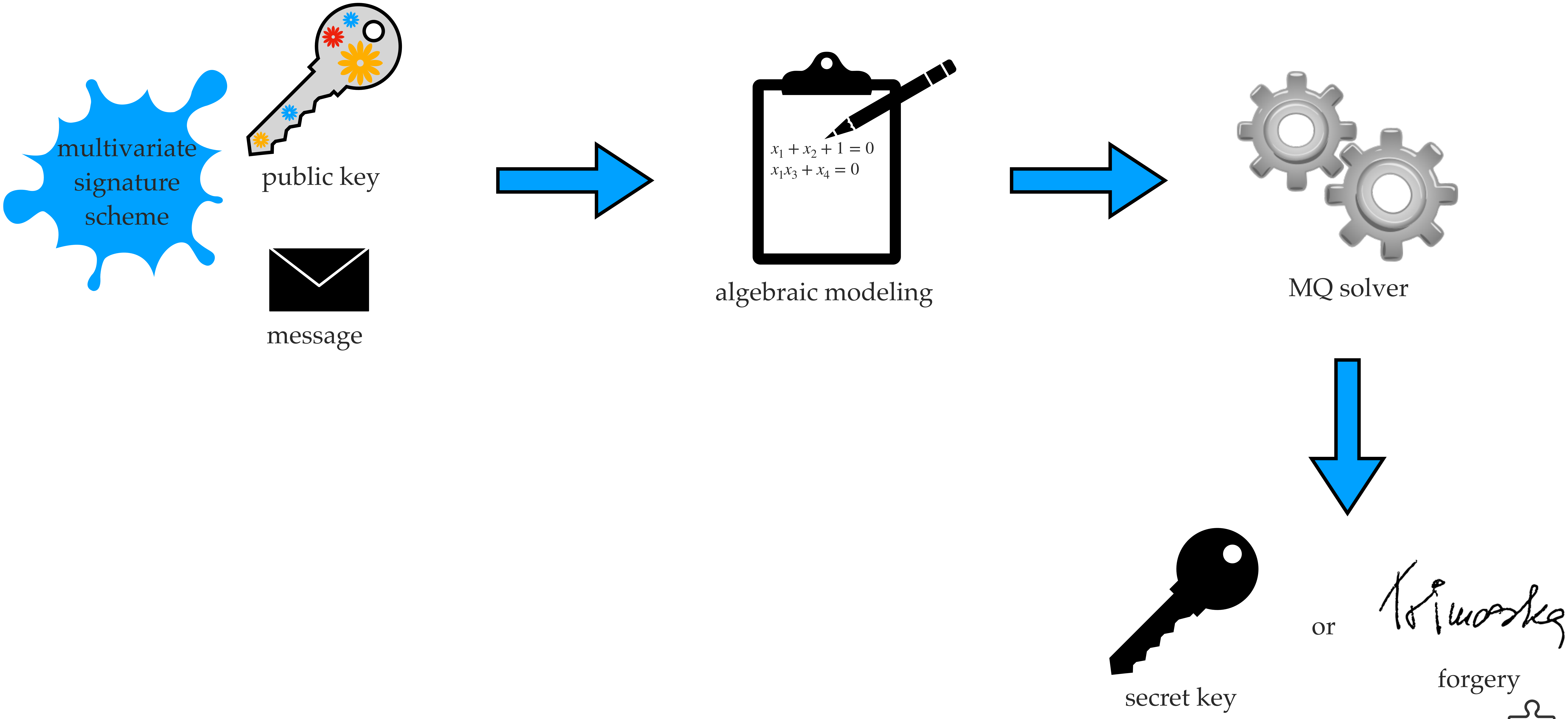
Algebraic cryptanalysis



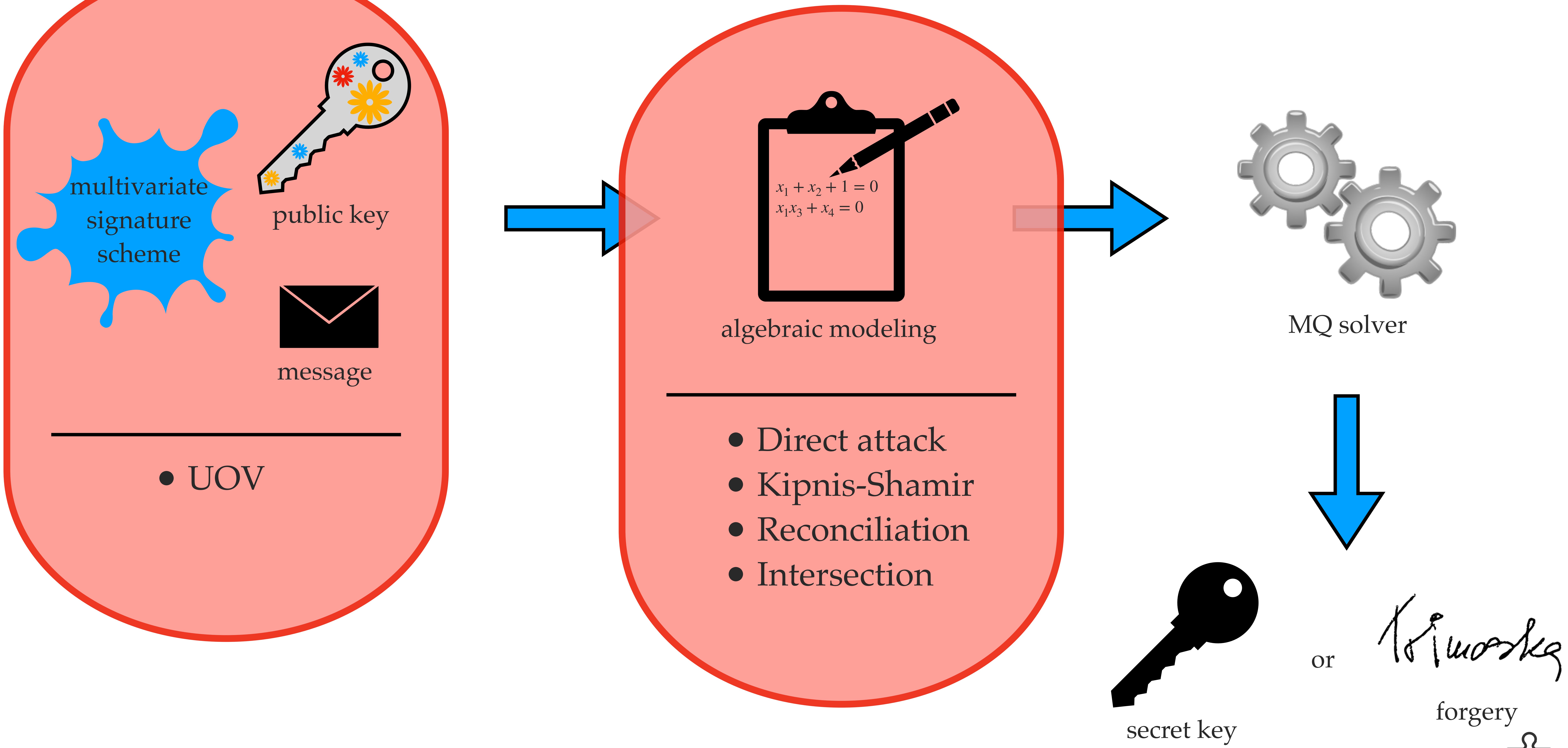
Algebraic cryptanalysis



Algebraic cryptanalysis



Algebraic cryptanalysis



The MQ problem (recall)

The MQ problem

Given m multivariate quadratic polynomials $f_1, \ldots, f_m$ of n variables over a finite field $\mathbb{F}_q$, find a tuple $\mathbf{x} = (x_1, \ldots, x_n)$ in $\mathbb{F}_q^n$, such that $f_1(\mathbf{x}) = \ldots = f_m(\mathbf{x}) = 0$.

Example.

$$
\begin{aligned}
f_1 &: x_1x_3 + x_2x_4 + x_1 + x_3 + x_4 = 0\\
f_2 &: x_2x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_4 = 0\\
f_3 &: x_2x_4 + x_3x_4 + x_1 + x_3 + 1 = 0\\
f_4 &: x_1x_2 + x_1x_3 + x_2x_3 + x_3 + x_4 + 1 = 0\\
f_5 &: x_1x_2 + x_2x_3 + x_1x_4 + x_3 = 0\\
f_6 &: x_1x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_3 + x_4 = 0
\end{aligned}
$$

Algebraic cryptanalysis : modelisation example

Example.

Given matrices $\mathbf{C}_1, \mathbf{C}_2, \mathbf{D}_1, \mathbf{D}_2 \in \mathscr{M}_{n,n}(\mathbb{F}_q)$ (the space of matrices over $\mathbb{F}_q$ of size $n \times n$), find $\mathbf{A}, \mathbf{B} \in \mathrm{GL}_n(\mathbb{F}_q)$ (the space of invertible matrices over $\mathbb{F}_q$ of size $n \times n$), such that

$$\mathbf{D}_1 = \mathbf{A}\mathbf{C}_1\mathbf{B}$$
$$\mathbf{D}_2 = \mathbf{A}\mathbf{C}_2\mathbf{B}$$

Algebraic cryptanalysis : modelisation example

Example. $\mathbf{D}_1 = \mathbf{A}\mathbf{C}_1\mathbf{B}$

$\mathbf{D}_2 = \mathbf{A}\mathbf{C}_2\mathbf{B}$

$$\underbrace{\begin{bmatrix} d_{1,1} & d_{1,2} & d_{1,3} & d_{1,4} & d_{1,5} \\ d_{2,1} & d_{2,2} & d_{2,3} & d_{2,4} & d_{2,5} \\ d_{3,1} & d_{3,2} & d_{3,3} & d_{3,4} & d_{3,5} \\ d_{4,1} & d_{4,2} & d_{4,3} & d_{4,4} & d_{4,5} \\ d_{5,1} & d_{5,2} & d_{5,3} & d_{5,4} & d_{5,5} \end{bmatrix}}_{\mathbf{D}_1} = \underbrace{\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} \\ a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} \end{bmatrix}}_{\mathbf{A}} \underbrace{\begin{bmatrix} c_{1,1} & c_{1,2} & c_{1,3} & c_{1,4} & c_{1,5} \\ c_{2,1} & c_{2,2} & c_{2,3} & c_{2,4} & c_{2,5} \\ c_{3,1} & c_{3,2} & c_{3,3} & c_{3,4} & c_{3,5} \\ c_{4,1} & c_{4,2} & c_{4,3} & c_{4,4} & c_{4,5} \\ c_{5,1} & c_{5,2} & c_{5,3} & c_{5,4} & c_{5,5} \end{bmatrix}}_{\mathbf{C}_1} \underbrace{\begin{bmatrix} b_{1,1} & b_{1,2} & b_{1,3} & b_{1,4} & b_{1,5} \\ b_{2,1} & b_{2,2} & b_{2,3} & b_{2,4} & b_{2,5} \\ b_{3,1} & b_{3,2} & b_{3,3} & b_{3,4} & b_{3,5} \\ b_{4,1} & b_{4,2} & b_{4,3} & b_{4,4} & b_{4,5} \\ b_{5,1} & b_{5,2} & b_{5,3} & b_{5,4} & b_{5,5} \end{bmatrix}}_{\mathbf{B}}$$

Algebraic cryptanalysis : modelisation example

Example. $\mathbf{D}_1 = \mathbf{A}\mathbf{C}_1\mathbf{B}$
$\mathbf{D}_2 = \mathbf{A}\mathbf{C}_2\mathbf{B}$

$$\mathbf{D}_1 = \begin{pmatrix} d_{1,1} & d_{1,2} & d_{1,3} & d_{1,4} & d_{1,5} \\ d_{2,1} & d_{2,2} & d_{2,3} & d_{2,4} & d_{2,5} \\ d_{3,1} & d_{3,2} & d_{3,3} & d_{3,4} & d_{3,5} \\ d_{4,1} & d_{4,2} & d_{4,3} & d_{4,4} & d_{4,5} \\ d_{5,1} & d_{5,2} & d_{5,3} & d_{5,4} & d_{5,5} \end{pmatrix} = \mathbf{A}\mathbf{C}_1\mathbf{B} = \begin{pmatrix} \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,5} \end{pmatrix}$$

Algebraic cryptanalysis : modelisation example

Example. $\mathbf{D}_1 = \mathbf{A}\mathbf{C}_1\mathbf{B}$

$\mathbf{D}_2 = \mathbf{A}\mathbf{C}_2\mathbf{B}$

$$d_{1,1} - \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,1} = 0,$$

$$\underbrace{\begin{bmatrix} d_{1,1} & d_{1,2} & d_{1,3} & d_{1,4} & d_{1,5} \\ d_{2,1} & d_{2,2} & d_{2,3} & d_{2,4} & d_{2,5} \\ d_{3,1} & d_{3,2} & d_{3,3} & d_{3,4} & d_{3,5} \\ d_{4,1} & d_{4,2} & d_{4,3} & d_{4,4} & d_{4,5} \\ d_{5,1} & d_{5,2} & d_{5,3} & d_{5,4} & d_{5,5} \end{bmatrix}}_{\mathbf{D}_1} = \underbrace{\begin{bmatrix} \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,5} \end{bmatrix}}_{\mathbf{A}\mathbf{C}_1\mathbf{B}}$$

Algebraic cryptanalysis : modelisation example

Example.

$$\mathbf{D}_1 = \mathbf{A}\mathbf{C}_1\mathbf{B}$$
$$\mathbf{D}_2 = \mathbf{A}\mathbf{C}_2\mathbf{B}$$

$$d_{1,1} - \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,1} = 0,$$

$$d_{2,1} - \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,1} = 0,$$

$$\mathbf{D}_1 = \begin{pmatrix} d_{1,1} & d_{1,2} & d_{1,3} & d_{1,4} & d_{1,5} \\ d_{2,1} & d_{2,2} & d_{2,3} & d_{2,4} & d_{2,5} \\ d_{3,1} & d_{3,2} & d_{3,3} & d_{3,4} & d_{3,5} \\ d_{4,1} & d_{4,2} & d_{4,3} & d_{4,4} & d_{4,5} \\ d_{5,1} & d_{5,2} & d_{5,3} & d_{5,4} & d_{5,5} \end{pmatrix} = \mathbf{A}\mathbf{C}_1\mathbf{B} = \begin{pmatrix} \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,5} \end{pmatrix}$$

Algebraic cryptanalysis : modelisation example

Example. $\mathbf{D}_1 = \mathbf{A}\mathbf{C}_1\mathbf{B}$

$\mathbf{D}_2 = \mathbf{A}\mathbf{C}_2\mathbf{B}$

$$d_{1,1} - \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,1} = 0, \qquad d_{1,2} - \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,2} = 0, \ldots$$

$$d_{2,1} - \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,1} = 0,$$

$$\underbrace{\begin{array}{|c|c|c|c|c|}\hline d_{1,1} & d_{1,2} & d_{1,3} & d_{1,4} & d_{1,5} \\ \hline d_{2,1} & d_{2,2} & d_{2,3} & d_{2,4} & d_{2,5} \\ \hline d_{3,1} & d_{3,2} & d_{3,3} & d_{3,4} & d_{3,5} \\ \hline d_{4,1} & d_{4,2} & d_{4,3} & d_{4,4} & d_{4,5} \\ \hline d_{5,1} & d_{5,2} & d_{5,3} & d_{5,4} & d_{5,5} \\ \hline \end{array}}_{\mathbf{D}_1} = \underbrace{\begin{array}{|c|c|c|c|c|}\hline \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,5} \\ \hline \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,5} \\ \hline \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,5} \\ \hline \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,5} \\ \hline \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,5} \\ \hline \end{array}}_{\mathbf{A}\mathbf{C}_1\mathbf{B}}$$

Algebraic cryptanalysis : modelisation example

Example.

$$\mathbf{D}_1 = \mathbf{A}\mathbf{C}_1\mathbf{B}$$
$$\mathbf{D}_2 = \mathbf{A}\mathbf{C}_2\mathbf{B}$$

$$d_{1,1} - \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,1} = 0, \qquad d_{1,2} - \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,2} = 0, \ldots$$

$$d_{2,1} - \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,1} = 0, \qquad d_{l,p} - \sum_{i=1}^{n}\sum_{j=1}^{n} a_{l,j}c_{j,i}b_{i,p} = 0$$

$$\overbrace{\begin{bmatrix} d_{1,1} & d_{1,2} & d_{1,3} & d_{1,4} & d_{1,5} \\ d_{2,1} & d_{2,2} & d_{2,3} & d_{2,4} & d_{2,5} \\ d_{3,1} & d_{3,2} & d_{3,3} & d_{3,4} & d_{3,5} \\ d_{4,1} & d_{4,2} & d_{4,3} & d_{4,4} & d_{4,5} \\ d_{5,1} & d_{5,2} & d_{5,3} & d_{5,4} & d_{5,5} \end{bmatrix}}^{\mathbf{D}_1} = \overbrace{\begin{bmatrix} \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{1,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{2,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{3,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{4,j}c_{j,i}b_{i,5} \\ \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,1} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,2} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,3} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,4} & \sum_{i=1}^{n}\sum_{j=1}^{n} a_{5,j}c_{j,i}b_{i,5} \end{bmatrix}}^{\mathbf{A}\mathbf{C}_1\mathbf{B}}$$

Algebraic cryptanalysis : modelisation example

A motivating example: a better idea for modelisation.

Given matrices $\mathbf{C}_1, \mathbf{C}_2, \mathbf{D}_1, \mathbf{D}_2 \in \mathscr{M}_{n,n}(\mathbb{F}_q)$ (the space of matrices over $\mathbb{F}_q$ of size $n \times n$), find $\mathbf{A}, \mathbf{B} \in \mathrm{GL}_n(\mathbb{F}_q)$ (the space of invertible matrices over $\mathbb{F}_q$ of size $n \times n$), such that

$$\mathbf{A}^{-1}\mathbf{D}_1 = \mathbf{C}_1\mathbf{B}$$
$$\mathbf{A}^{-1}\mathbf{D}_2 = \mathbf{C}_2\mathbf{B}$$

Algebraic cryptanalysis : modelisation example

Example. $\mathbf{A}^{-1}\mathbf{D}_1 = \mathbf{C}_1\mathbf{B}$
$\mathbf{A}^{-1}\mathbf{D}_2 = \mathbf{C}_2\mathbf{B}$

$$\underbrace{\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} \\ a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} \end{pmatrix}}_{\mathbf{A}^{-1}} \underbrace{\begin{pmatrix} d_{1,1} & d_{1,2} & d_{1,3} & d_{1,4} & d_{1,5} \\ d_{2,1} & d_{2,2} & d_{2,3} & d_{2,4} & d_{2,5} \\ d_{3,1} & d_{3,2} & d_{3,3} & d_{3,4} & d_{3,5} \\ d_{4,1} & d_{4,2} & d_{4,3} & d_{4,4} & d_{4,5} \\ d_{5,1} & d_{5,2} & d_{5,3} & d_{5,4} & d_{5,5} \end{pmatrix}}_{\mathbf{D}_1} = \underbrace{\begin{pmatrix} c_{1,1} & c_{1,2} & c_{1,3} & c_{1,4} & c_{1,5} \\ c_{2,1} & c_{2,2} & c_{2,3} & c_{2,4} & c_{2,5} \\ c_{3,1} & c_{3,2} & c_{3,3} & c_{3,4} & c_{3,5} \\ c_{4,1} & c_{4,2} & c_{4,3} & c_{4,4} & c_{4,5} \\ c_{5,1} & c_{5,2} & c_{5,3} & c_{5,4} & c_{5,5} \end{pmatrix}}_{\mathbf{C}_1} \underbrace{\begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} & b_{1,4} & b_{1,5} \\ b_{2,1} & b_{2,2} & b_{2,3} & b_{2,4} & b_{2,5} \\ b_{3,1} & b_{3,2} & b_{3,3} & b_{3,4} & b_{3,5} \\ b_{4,1} & b_{4,2} & b_{4,3} & b_{4,4} & b_{4,5} \\ b_{5,1} & b_{5,2} & b_{5,3} & b_{5,4} & b_{5,5} \end{pmatrix}}_{\mathbf{B}}$$

Algebraic cryptanalysis : modelisation example

Example.
$$\mathbf{A}^{-1}\mathbf{D}_1 = \mathbf{C}_1\mathbf{B}$$
$$\mathbf{A}^{-1}\mathbf{D}_2 = \mathbf{C}_2\mathbf{B}$$

$$\underbrace{\begin{pmatrix}
\sum_{i=1}^{n} a_{1,i}d_{i,1} & \sum_{i=1}^{n} a_{1,i}d_{i,2} & \sum_{i=1}^{n} a_{1,i}d_{i,3} & \sum_{i=1}^{n} a_{1,i}d_{i,4} & \sum_{i=1}^{n} a_{1,i}d_{i,5} \\
\sum_{i=1}^{n} a_{2,i}d_{i,1} & \sum_{i=1}^{n} a_{2,i}d_{i,2} & \sum_{i=1}^{n} a_{2,i}d_{i,3} & \sum_{i=1}^{n} a_{2,i}d_{i,4} & \sum_{i=1}^{n} a_{2,i}d_{i,5} \\
\sum_{i=1}^{n} a_{3,i}d_{i,1} & \sum_{i=1}^{n} a_{3,i}d_{i,2} & \sum_{i=1}^{n} a_{3,i}d_{i,3} & \sum_{i=1}^{n} a_{3,i}d_{i,4} & \sum_{i=1}^{n} a_{3,i}d_{i,5} \\
\sum_{i=1}^{n} a_{4,i}d_{i,1} & \sum_{i=1}^{n} a_{4,i}d_{i,2} & \sum_{i=1}^{n} a_{4,i}d_{i,3} & \sum_{i=1}^{n} a_{4,i}d_{i,4} & \sum_{i=1}^{n} a_{4,i}d_{i,5} \\
\sum_{i=1}^{n} a_{5,i}d_{i,1} & \sum_{i=1}^{n} a_{5,i}d_{i,2} & \sum_{i=1}^{n} a_{5,i}d_{i,3} & \sum_{i=1}^{n} a_{5,i}d_{i,4} & \sum_{i=1}^{n} a_{5,i}d_{i,5}
\end{pmatrix}}_{\mathbf{A}^{-1}\mathbf{D}_1}
=
\underbrace{\begin{pmatrix}
\sum_{i=1}^{n} c_{1,i}b_{i,1} & \sum_{i=1}^{n} c_{1,i}b_{i,2} & \sum_{i=1}^{n} c_{1,i}b_{i,3} & \sum_{i=1}^{n} c_{1,i}b_{i,4} & \sum_{i=1}^{n} c_{1,i}b_{i,5} \\
\sum_{i=1}^{n} c_{2,i}b_{i,1} & \sum_{i=1}^{n} c_{2,i}b_{i,2} & \sum_{i=1}^{n} c_{2,i}b_{i,3} & \sum_{i=1}^{n} c_{2,i}b_{i,4} & \sum_{i=1}^{n} c_{2,i}b_{i,5} \\
\sum_{i=1}^{n} c_{3,i}b_{i,1} & \sum_{i=1}^{n} c_{3,i}b_{i,2} & \sum_{i=1}^{n} c_{3,i}b_{i,3} & \sum_{i=1}^{n} c_{3,i}b_{i,4} & \sum_{i=1}^{n} c_{3,i}b_{i,5} \\
\sum_{i=1}^{n} c_{4,i}b_{i,1} & \sum_{i=1}^{n} c_{4,i}b_{i,2} & \sum_{i=1}^{n} c_{4,i}b_{i,3} & \sum_{i=1}^{n} c_{4,i}b_{i,4} & \sum_{i=1}^{n} c_{4,i}b_{i,5} \\
\sum_{i=1}^{n} c_{5,i}b_{i,1} & \sum_{i=1}^{n} c_{5,i}b_{i,2} & \sum_{i=1}^{n} c_{5,i}b_{i,3} & \sum_{i=1}^{n} c_{5,i}b_{i,4} & \sum_{i=1}^{n} c_{5,i}b_{i,5}
\end{pmatrix}}_{\mathbf{C}_1\mathbf{B}}$$

Algebraic cryptanalysis : modelisation example

Example.

$$\mathbf{A}^{-1}\mathbf{D}_1 = \mathbf{C}_1\mathbf{B}$$
$$\mathbf{A}^{-1}\mathbf{D}_2 = \mathbf{C}_2\mathbf{B}$$

$$\sum_{i=1}^{n} a_{1,i}d_{i,1} - \sum_{i=1}^{n} c_{1,i}b_{i,1} = 0,$$

$$\overset{\mathbf{A}^{-1}\mathbf{D}_1}{\begin{bmatrix}
\sum_{i=1}^{n} a_{1,i}d_{i,1} & \sum_{i=1}^{n} a_{1,i}d_{i,2} & \sum_{i=1}^{n} a_{1,i}d_{i,3} & \sum_{i=1}^{n} a_{1,i}d_{i,4} & \sum_{i=1}^{n} a_{1,i}d_{i,5} \\
\sum_{i=1}^{n} a_{2,i}d_{i,1} & \sum_{i=1}^{n} a_{2,i}d_{i,2} & \sum_{i=1}^{n} a_{2,i}d_{i,3} & \sum_{i=1}^{n} a_{2,i}d_{i,4} & \sum_{i=1}^{n} a_{2,i}d_{i,5} \\
\sum_{i=1}^{n} a_{3,i}d_{i,1} & \sum_{i=1}^{n} a_{3,i}d_{i,2} & \sum_{i=1}^{n} a_{3,i}d_{i,3} & \sum_{i=1}^{n} a_{3,i}d_{i,4} & \sum_{i=1}^{n} a_{3,i}d_{i,5} \\
\sum_{i=1}^{n} a_{4,i}d_{i,1} & \sum_{i=1}^{n} a_{4,i}d_{i,2} & \sum_{i=1}^{n} a_{4,i}d_{i,3} & \sum_{i=1}^{n} a_{4,i}d_{i,4} & \sum_{i=1}^{n} a_{4,i}d_{i,5} \\
\sum_{i=1}^{n} a_{5,i}d_{i,1} & \sum_{i=1}^{n} a_{5,i}d_{i,2} & \sum_{i=1}^{n} a_{5,i}d_{i,3} & \sum_{i=1}^{n} a_{5,i}d_{i,4} & \sum_{i=1}^{n} a_{5,i}d_{i,5}
\end{bmatrix}}
=
\overset{\mathbf{C}_1\mathbf{B}}{\begin{bmatrix}
\sum_{i=1}^{n} c_{1,i}b_{i,1} & \sum_{i=1}^{n} c_{1,i}b_{i,2} & \sum_{i=1}^{n} c_{1,i}b_{i,3} & \sum_{i=1}^{n} c_{1,i}b_{i,4} & \sum_{i=1}^{n} c_{1,i}b_{i,5} \\
\sum_{i=1}^{n} c_{2,i}b_{i,1} & \sum_{i=1}^{n} c_{2,i}b_{i,2} & \sum_{i=1}^{n} c_{2,i}b_{i,3} & \sum_{i=1}^{n} c_{2,i}b_{i,4} & \sum_{i=1}^{n} c_{2,i}b_{i,5} \\
\sum_{i=1}^{n} c_{3,i}b_{i,1} & \sum_{i=1}^{n} c_{3,i}b_{i,2} & \sum_{i=1}^{n} c_{3,i}b_{i,3} & \sum_{i=1}^{n} c_{3,i}b_{i,4} & \sum_{i=1}^{n} c_{3,i}b_{i,5} \\
\sum_{i=1}^{n} c_{4,i}b_{i,1} & \sum_{i=1}^{n} c_{4,i}b_{i,2} & \sum_{i=1}^{n} c_{4,i}b_{i,3} & \sum_{i=1}^{n} c_{4,i}b_{i,4} & \sum_{i=1}^{n} c_{4,i}b_{i,5} \\
\sum_{i=1}^{n} c_{5,i}b_{i,1} & \sum_{i=1}^{n} c_{5,i}b_{i,2} & \sum_{i=1}^{n} c_{5,i}b_{i,3} & \sum_{i=1}^{n} c_{5,i}b_{i,4} & \sum_{i=1}^{n} c_{5,i}b_{i,5}
\end{bmatrix}}$$

Algebraic cryptanalysis : modelisation example

Example.

$$\mathbf{A}^{-1}\mathbf{D}_1 = \mathbf{C}_1\mathbf{B}$$
$$\mathbf{A}^{-1}\mathbf{D}_2 = \mathbf{C}_2\mathbf{B}$$

$$\sum_{i=1}^{n} a_{1,i}d_{i,1} - \sum_{i=1}^{n} c_{1,i}b_{i,1} = 0,$$

$$\sum_{i=1}^{n} a_{2,i}d_{i,1} - \sum_{i=1}^{n} c_{2,i}b_{i,1} = 0,$$

$$\overset{\mathbf{A}^{-1}\mathbf{D}_1}{\begin{bmatrix}
\sum_{i=1}^{n} a_{1,i}d_{i,1} & \sum_{i=1}^{n} a_{1,i}d_{i,2} & \sum_{i=1}^{n} a_{1,i}d_{i,3} & \sum_{i=1}^{n} a_{1,i}d_{i,4} & \sum_{i=1}^{n} a_{1,i}d_{i,5} \\
\sum_{i=1}^{n} a_{2,i}d_{i,1} & \sum_{i=1}^{n} a_{2,i}d_{i,2} & \sum_{i=1}^{n} a_{2,i}d_{i,3} & \sum_{i=1}^{n} a_{2,i}d_{i,4} & \sum_{i=1}^{n} a_{2,i}d_{i,5} \\
\sum_{i=1}^{n} a_{3,i}d_{i,1} & \sum_{i=1}^{n} a_{3,i}d_{i,2} & \sum_{i=1}^{n} a_{3,i}d_{i,3} & \sum_{i=1}^{n} a_{3,i}d_{i,4} & \sum_{i=1}^{n} a_{3,i}d_{i,5} \\
\sum_{i=1}^{n} a_{4,i}d_{i,1} & \sum_{i=1}^{n} a_{4,i}d_{i,2} & \sum_{i=1}^{n} a_{4,i}d_{i,3} & \sum_{i=1}^{n} a_{4,i}d_{i,4} & \sum_{i=1}^{n} a_{4,i}d_{i,5} \\
\sum_{i=1}^{n} a_{5,i}d_{i,1} & \sum_{i=1}^{n} a_{5,i}d_{i,2} & \sum_{i=1}^{n} a_{5,i}d_{i,3} & \sum_{i=1}^{n} a_{5,i}d_{i,4} & \sum_{i=1}^{n} a_{5,i}d_{i,5}
\end{bmatrix}}
=
\overset{\mathbf{C}_1\,\mathbf{B}}{\begin{bmatrix}
\sum_{i=1}^{n} c_{1,i}b_{i,1} & \sum_{i=1}^{n} c_{1,i}b_{i,2} & \sum_{i=1}^{n} c_{1,i}b_{i,3} & \sum_{i=1}^{n} c_{1,i}b_{i,4} & \sum_{i=1}^{n} c_{1,i}b_{i,5} \\
\sum_{i=1}^{n} c_{2,i}b_{i,1} & \sum_{i=1}^{n} c_{2,i}b_{i,2} & \sum_{i=1}^{n} c_{2,i}b_{i,3} & \sum_{i=1}^{n} c_{2,i}b_{i,4} & \sum_{i=1}^{n} c_{2,i}b_{i,5} \\
\sum_{i=1}^{n} c_{3,i}b_{i,1} & \sum_{i=1}^{n} c_{3,i}b_{i,2} & \sum_{i=1}^{n} c_{3,i}b_{i,3} & \sum_{i=1}^{n} c_{3,i}b_{i,4} & \sum_{i=1}^{n} c_{3,i}b_{i,5} \\
\sum_{i=1}^{n} c_{4,i}b_{i,1} & \sum_{i=1}^{n} c_{4,i}b_{i,2} & \sum_{i=1}^{n} c_{4,i}b_{i,3} & \sum_{i=1}^{n} c_{4,i}b_{i,4} & \sum_{i=1}^{n} c_{4,i}b_{i,5} \\
\sum_{i=1}^{n} c_{5,i}b_{i,1} & \sum_{i=1}^{n} c_{5,i}b_{i,2} & \sum_{i=1}^{n} c_{5,i}b_{i,3} & \sum_{i=1}^{n} c_{5,i}b_{i,4} & \sum_{i=1}^{n} c_{5,i}b_{i,5}
\end{bmatrix}}$$

Algebraic cryptanalysis : modelisation example

Example.

$$\mathbf{A}^{-1}\mathbf{D}_1 = \mathbf{C}_1\mathbf{B}$$
$$\mathbf{A}^{-1}\mathbf{D}_2 = \mathbf{C}_2\mathbf{B}$$

$$\sum_{i=1}^{n} a_{1,i}d_{i,1} - \sum_{i=1}^{n} c_{1,i}b_{i,1} = 0, \quad \sum_{i=1}^{n} a_{1,i}d_{i,2} - \sum_{i=1}^{n} c_{1,i}b_{i,2} = 0, \ldots$$

$$\sum_{i=1}^{n} a_{2,i}d_{i,1} - \sum_{i=1}^{n} c_{2,i}b_{i,1} = 0,$$

$$\mathbf{A}^{-1}\mathbf{D}_1 = \begin{bmatrix} \sum_{i=1}^{n} a_{1,i}d_{i,1} & \sum_{i=1}^{n} a_{1,i}d_{i,2} & \sum_{i=1}^{n} a_{1,i}d_{i,3} & \sum_{i=1}^{n} a_{1,i}d_{i,4} & \sum_{i=1}^{n} a_{1,i}d_{i,5} \\ \sum_{i=1}^{n} a_{2,i}d_{i,1} & \sum_{i=1}^{n} a_{2,i}d_{i,2} & \sum_{i=1}^{n} a_{2,i}d_{i,3} & \sum_{i=1}^{n} a_{2,i}d_{i,4} & \sum_{i=1}^{n} a_{2,i}d_{i,5} \\ \sum_{i=1}^{n} a_{3,i}d_{i,1} & \sum_{i=1}^{n} a_{3,i}d_{i,2} & \sum_{i=1}^{n} a_{3,i}d_{i,3} & \sum_{i=1}^{n} a_{3,i}d_{i,4} & \sum_{i=1}^{n} a_{3,i}d_{i,5} \\ \sum_{i=1}^{n} a_{4,i}d_{i,1} & \sum_{i=1}^{n} a_{4,i}d_{i,2} & \sum_{i=1}^{n} a_{4,i}d_{i,3} & \sum_{i=1}^{n} a_{4,i}d_{i,4} & \sum_{i=1}^{n} a_{4,i}d_{i,5} \\ \sum_{i=1}^{n} a_{5,i}d_{i,1} & \sum_{i=1}^{n} a_{5,i}d_{i,2} & \sum_{i=1}^{n} a_{5,i}d_{i,3} & \sum_{i=1}^{n} a_{5,i}d_{i,4} & \sum_{i=1}^{n} a_{5,i}d_{i,5} \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{n} c_{1,i}b_{i,1} & \sum_{i=1}^{n} c_{1,i}b_{i,2} & \sum_{i=1}^{n} c_{1,i}b_{i,3} & \sum_{i=1}^{n} c_{1,i}b_{i,4} & \sum_{i=1}^{n} c_{1,i}b_{i,5} \\ \sum_{i=1}^{n} c_{2,i}b_{i,1} & \sum_{i=1}^{n} c_{2,i}b_{i,2} & \sum_{i=1}^{n} c_{2,i}b_{i,3} & \sum_{i=1}^{n} c_{2,i}b_{i,4} & \sum_{i=1}^{n} c_{2,i}b_{i,5} \\ \sum_{i=1}^{n} c_{3,i}b_{i,1} & \sum_{i=1}^{n} c_{3,i}b_{i,2} & \sum_{i=1}^{n} c_{3,i}b_{i,3} & \sum_{i=1}^{n} c_{3,i}b_{i,4} & \sum_{i=1}^{n} c_{3,i}b_{i,5} \\ \sum_{i=1}^{n} c_{4,i}b_{i,1} & \sum_{i=1}^{n} c_{4,i}b_{i,2} & \sum_{i=1}^{n} c_{4,i}b_{i,3} & \sum_{i=1}^{n} c_{4,i}b_{i,4} & \sum_{i=1}^{n} c_{4,i}b_{i,5} \\ \sum_{i=1}^{n} c_{5,i}b_{i,1} & \sum_{i=1}^{n} c_{5,i}b_{i,2} & \sum_{i=1}^{n} c_{5,i}b_{i,3} & \sum_{i=1}^{n} c_{5,i}b_{i,4} & \sum_{i=1}^{n} c_{5,i}b_{i,5} \end{bmatrix} = \mathbf{C}_1\mathbf{B}$$

Algebraic cryptanalysis : modelisation example

Example.
$$\mathbf{A}^{-1}\mathbf{D}_1 = \mathbf{C}_1\mathbf{B}$$
$$\mathbf{A}^{-1}\mathbf{D}_2 = \mathbf{C}_2\mathbf{B}$$

$$\sum_{i=1}^{n} a_{1,i}d_{i,1} - \sum_{i=1}^{n} c_{1,i}b_{i,1} = 0, \quad \sum_{i=1}^{n} a_{1,i}d_{i,2} - \sum_{i=1}^{n} c_{1,i}b_{i,2} = 0, \ldots$$

$$\sum_{i=1}^{n} a_{2,i}d_{i,1} - \sum_{i=1}^{n} c_{2,i}b_{i,1} = 0, \quad \sum_{i=1}^{n} a_{l,i}d_{i,p} - \sum_{i=1}^{n} c_{l,i}b_{i,p} = 0$$

$$\underbrace{\begin{bmatrix}
\sum_{i=1}^{n} a_{1,i}d_{i,1} & \sum_{i=1}^{n} a_{1,i}d_{i,2} & \sum_{i=1}^{n} a_{1,i}d_{i,3} & \sum_{i=1}^{n} a_{1,i}d_{i,4} & \sum_{i=1}^{n} a_{1,i}d_{i,5} \\
\sum_{i=1}^{n} a_{2,i}d_{i,1} & \sum_{i=1}^{n} a_{2,i}d_{i,2} & \sum_{i=1}^{n} a_{2,i}d_{i,3} & \sum_{i=1}^{n} a_{2,i}d_{i,4} & \sum_{i=1}^{n} a_{2,i}d_{i,5} \\
\sum_{i=1}^{n} a_{3,i}d_{i,1} & \sum_{i=1}^{n} a_{3,i}d_{i,2} & \sum_{i=1}^{n} a_{3,i}d_{i,3} & \sum_{i=1}^{n} a_{3,i}d_{i,4} & \sum_{i=1}^{n} a_{3,i}d_{i,5} \\
\sum_{i=1}^{n} a_{4,i}d_{i,1} & \sum_{i=1}^{n} a_{4,i}d_{i,2} & \sum_{i=1}^{n} a_{4,i}d_{i,3} & \sum_{i=1}^{n} a_{4,i}d_{i,4} & \sum_{i=1}^{n} a_{4,i}d_{i,5} \\
\sum_{i=1}^{n} a_{5,i}d_{i,1} & \sum_{i=1}^{n} a_{5,i}d_{i,2} & \sum_{i=1}^{n} a_{5,i}d_{i,3} & \sum_{i=1}^{n} a_{5,i}d_{i,4} & \sum_{i=1}^{n} a_{5,i}d_{i,5}
\end{bmatrix}}_{\mathbf{A}^{-1}\mathbf{D}_1}
=
\underbrace{\begin{bmatrix}
\sum_{i=1}^{n} c_{1,i}b_{i,1} & \sum_{i=1}^{n} c_{1,i}b_{i,2} & \sum_{i=1}^{n} c_{1,i}b_{i,3} & \sum_{i=1}^{n} c_{1,i}b_{i,4} & \sum_{i=1}^{n} c_{1,i}b_{i,5} \\
\sum_{i=1}^{n} c_{2,i}b_{i,1} & \sum_{i=1}^{n} c_{2,i}b_{i,2} & \sum_{i=1}^{n} c_{2,i}b_{i,3} & \sum_{i=1}^{n} c_{2,i}b_{i,4} & \sum_{i=1}^{n} c_{2,i}b_{i,5} \\
\sum_{i=1}^{n} c_{3,i}b_{i,1} & \sum_{i=1}^{n} c_{3,i}b_{i,2} & \sum_{i=1}^{n} c_{3,i}b_{i,3} & \sum_{i=1}^{n} c_{3,i}b_{i,4} & \sum_{i=1}^{n} c_{3,i}b_{i,5} \\
\sum_{i=1}^{n} c_{4,i}b_{i,1} & \sum_{i=1}^{n} c_{4,i}b_{i,2} & \sum_{i=1}^{n} c_{4,i}b_{i,3} & \sum_{i=1}^{n} c_{4,i}b_{i,4} & \sum_{i=1}^{n} c_{4,i}b_{i,5} \\
\sum_{i=1}^{n} c_{5,i}b_{i,1} & \sum_{i=1}^{n} c_{5,i}b_{i,2} & \sum_{i=1}^{n} c_{5,i}b_{i,3} & \sum_{i=1}^{n} c_{5,i}b_{i,4} & \sum_{i=1}^{n} c_{5,i}b_{i,5}
\end{bmatrix}}_{\mathbf{C}_1\mathbf{B}}$$

Algebraic cryptanalysis : modelisation example

A motivating example: a better idea for modelisation.

Given matrices $\mathbf{C}_1, \mathbf{C}_2, \mathbf{D}_1, \mathbf{D}_2 \in \mathscr{M}_{n,n}(\mathbb{F}_q)$ (the space of matrices over $\mathbb{F}_q$ of size $n \times n$), find $\mathbf{A}, \mathbf{B} \in \mathrm{GL}_n(\mathbb{F}_q)$ (the space of invertible matrices over $\mathbb{F}_q$ of size $n \times n$), such that

$$\mathbf{A}^{-1}\mathbf{D}_1 = \mathbf{C}_1\mathbf{B}$$
$$\mathbf{A}^{-1}\mathbf{D}_2 = \mathbf{C}_2\mathbf{B}$$

Algebraic cryptanalysis : modelisation example

A motivating example: a better idea for modelisation.

Given matrices $\mathbf{C}_1, \mathbf{C}_2, \mathbf{D}_1, \mathbf{D}_2 \in \mathscr{M}_{n,n}(\mathbb{F}_q)$ (the space of matrices over $\mathbb{F}_q$ of size $n \times n$), find $\mathbf{A}, \mathbf{B} \in \mathrm{GL}_n(\mathbb{F}_q)$ (the space of invertible matrices over $\mathbb{F}_q$ of size $n \times n$), such that

$$\mathbf{A}^{-1}\mathbf{D}_1 = \mathbf{C}_1\mathbf{B}$$
$$\mathbf{A}^{-1}\mathbf{D}_2 = \mathbf{C}_2\mathbf{B}$$

→ Results in a linear system with the same number of variables and equations.

Algebraic cryptanalysis : modelisation example

A motivating example: a better idea for modelisation.

Given matrices $\mathbf{C}_1, \mathbf{C}_2, \mathbf{D}_1, \mathbf{D}_2 \in \mathscr{M}_{n,n}(\mathbb{F}_q)$ (the space of matrices over $\mathbb{F}_q$ of size $n \times n$), find $\mathbf{A}, \mathbf{B} \in \mathrm{GL}_n(\mathbb{F}_q)$ (the space of invertible matrices over $\mathbb{F}_q$ of size $n \times n$), such that

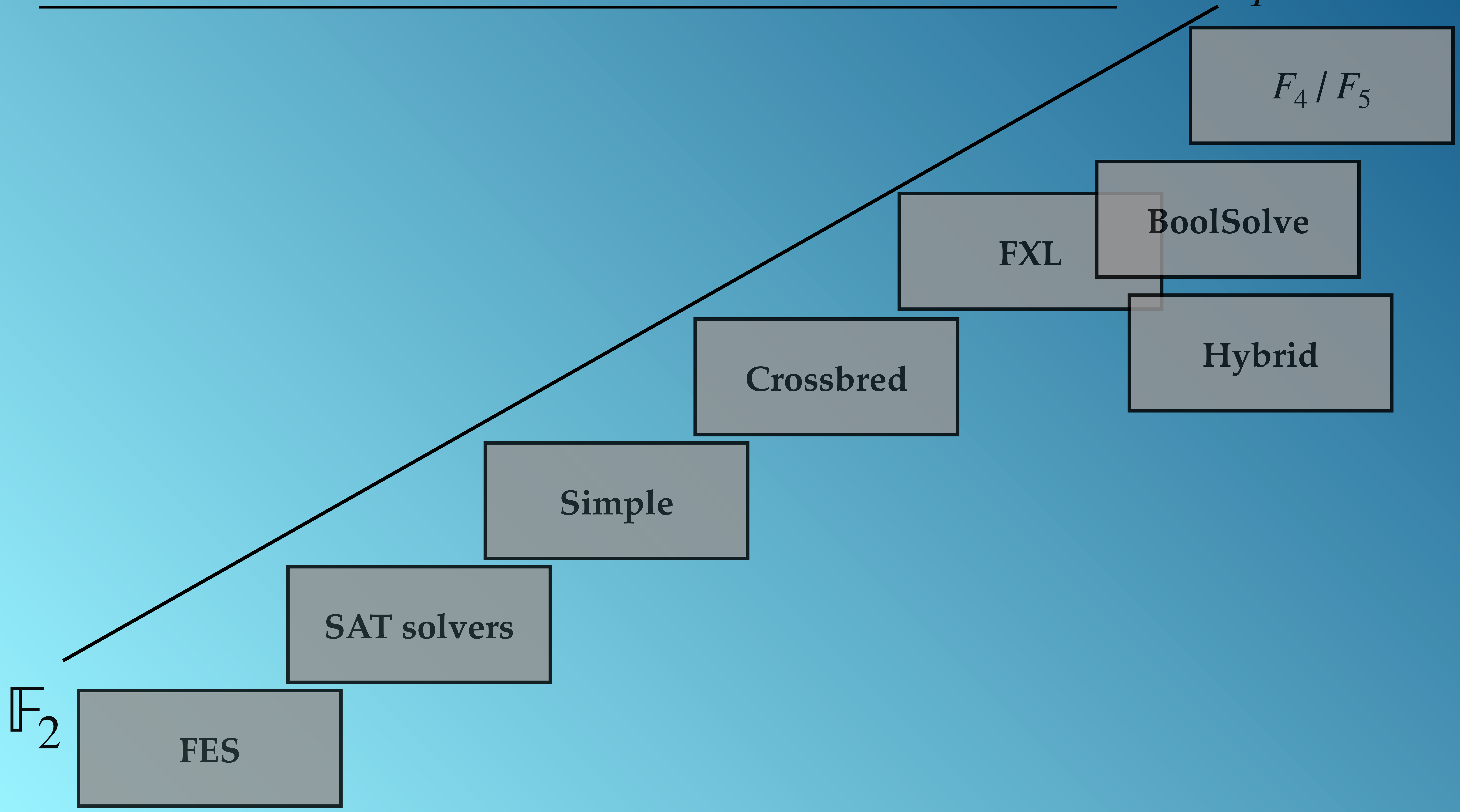
$$\mathbf{A}^{-1}\mathbf{D}_1 = \mathbf{C}_1\mathbf{B}$$
$$\mathbf{A}^{-1}\mathbf{D}_2 = \mathbf{C}_2\mathbf{B}$$

→ Results in a linear system with the same number of variables and equations.

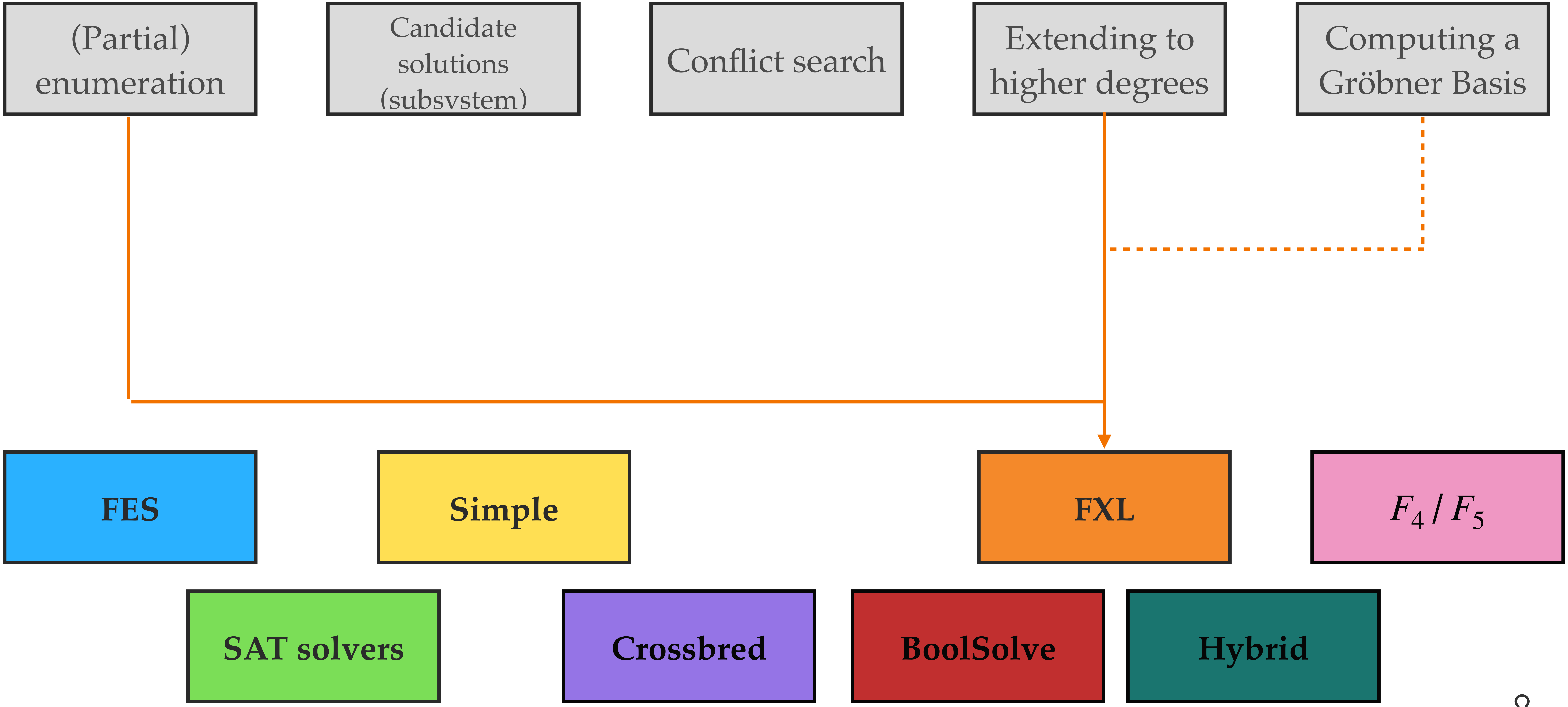
→ If $\mathbf{C}_1, \mathbf{C}_2, \mathbf{D}_1, \mathbf{D}_2$ are all full rank, we should have a unique solution.

→ We can easily recover $\mathbf{A}$ from $\mathbf{A}^{-1}$.

Overview of solvers



Summary


(Partial) enumeration
Candidate solutions (subsystem)
Conflict search
Extending to higher degrees
Computing a Gröbner Basis
FES
Simple
FXL
F_4 / F_5
SAT solvers
Crossbred
BoolSolve
Hybrid

Summary

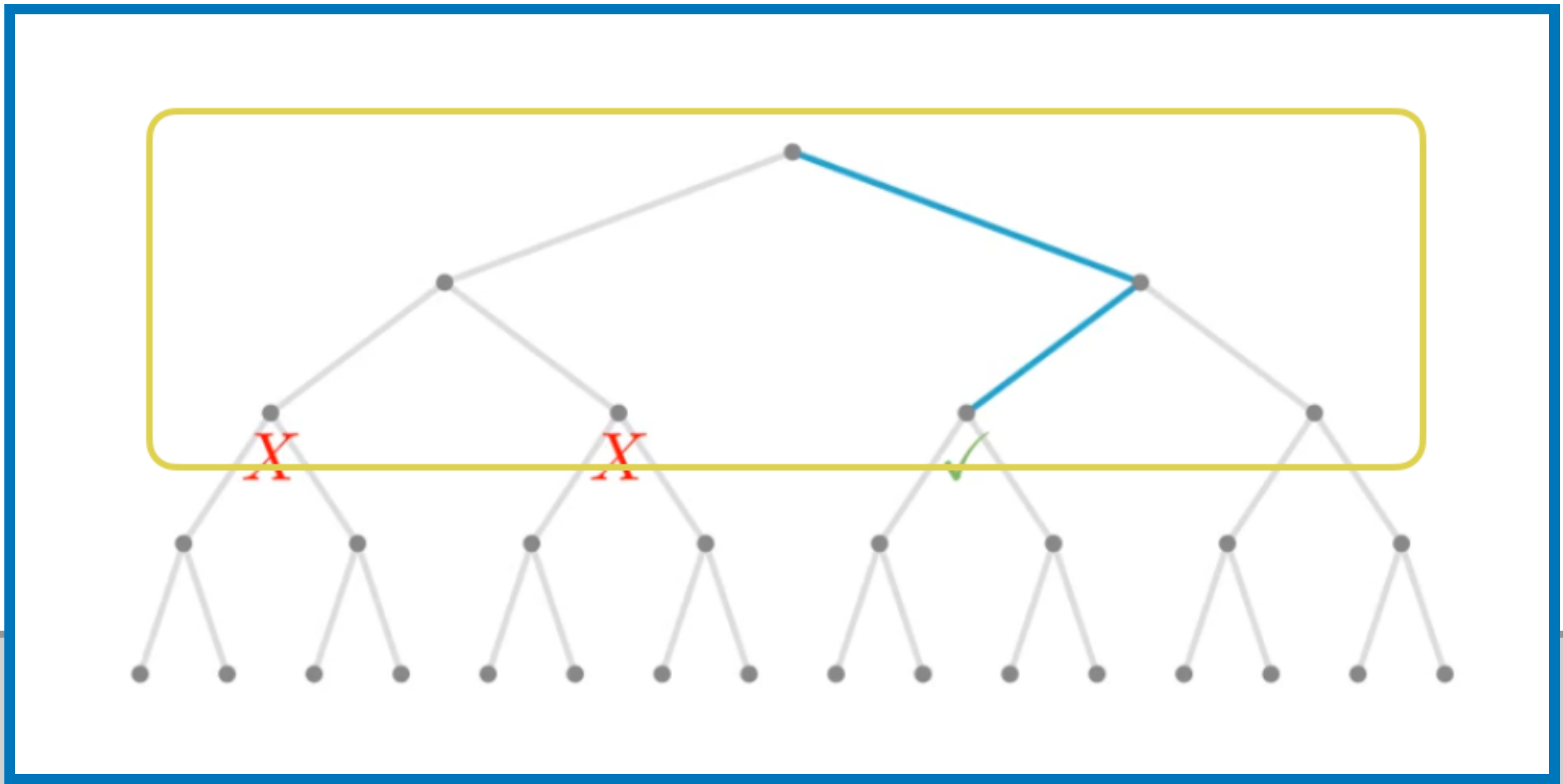
(Partial) enumeration

Candidate solutions (subsystem)

Conflict search

Extending to higher degrees

Computing a Gröbner Basis



FES

F_4 / F_5

SAT solvers

Crossbred

BoolSolve

Hybrid

Summary

(Partial) enumeration

Candidate solutions

Conflict search

Extending to higher degrees

Computing a Gröbner Basis

	x_1x_2	x_1x_3	x_1x_4	x_1	x_2x_3	x_2x_4	x_2	x_3x_4	x_3	x_4	1	$x_1x_2x_3$	$x_1x_2x_4$	$x_1x_3x_4$	$x_2x_3x_4$	$x_1x_2x_3x_4$
f_1	0	1	0	1	0	1	0	0	1	1	0					
f_2	0	0	1	1	1	0	1	1	0	1	0					
f_3	0	0	0	1	0	1	0	1	1	0	1					
f_4	1	1	0	1	1	0	0	0	1	1	1					
f_5	1	0	1	1	1	0	0	0	1	0	0					
f_6	0	1	1	1	0	0	1	1	1	1	0					
x_1f_1																
x_2f_1																
$\cdots$																
$x_1x_2f_1$																
$x_1x_3f_1$																

FES

F_4 / F_5

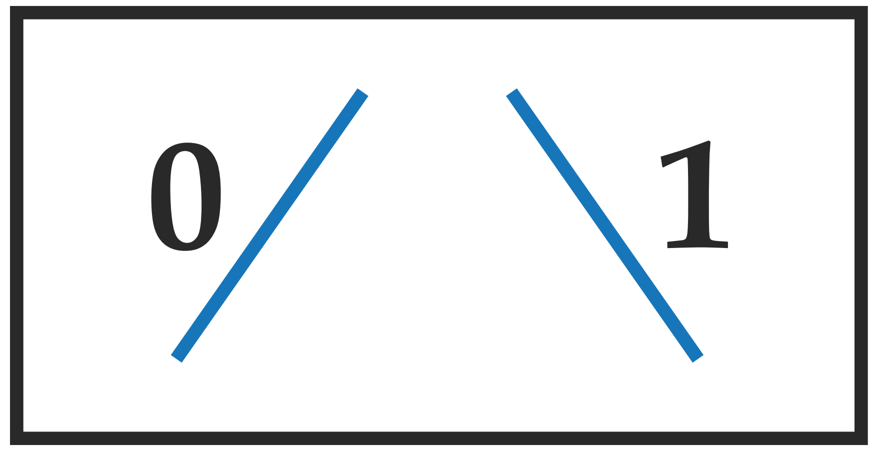
SAT solvers

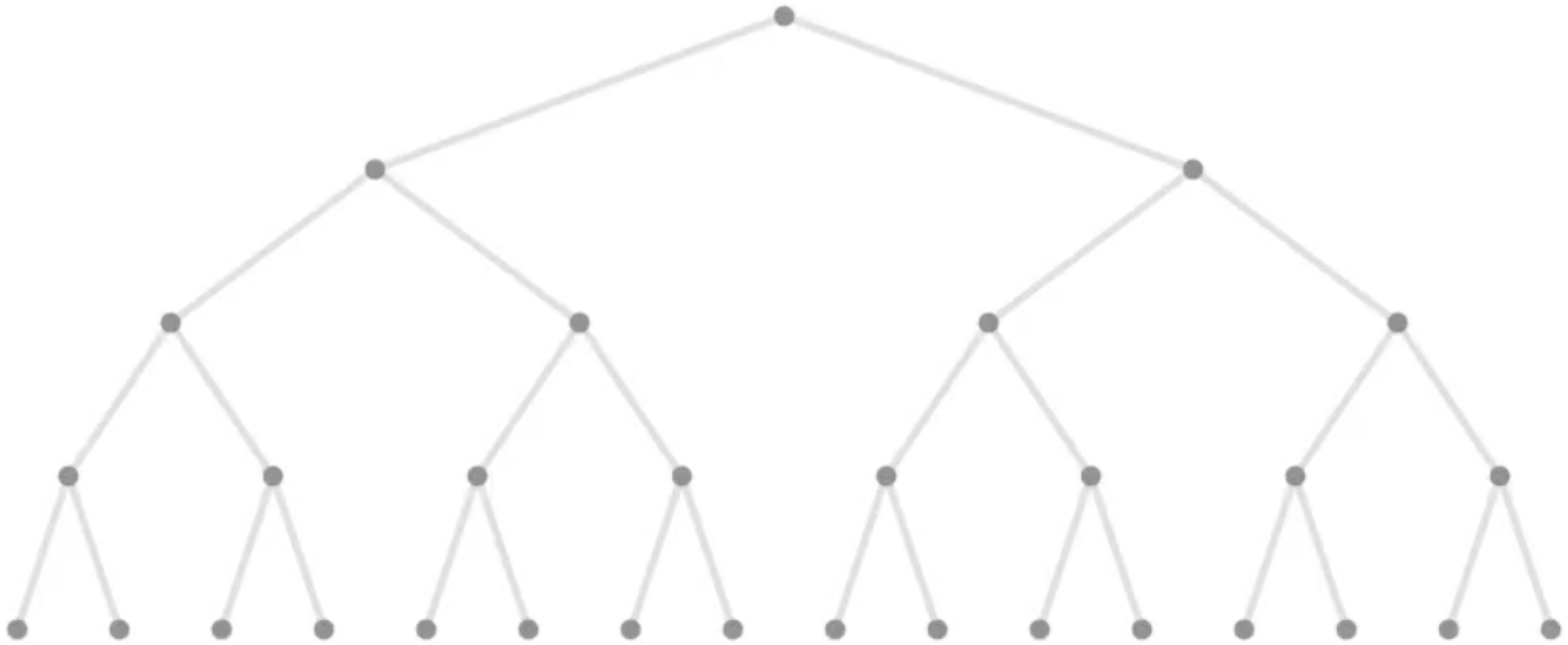
Crossbred

BoolSolve

Hybrid

Exhaustive Search





Binary search tree

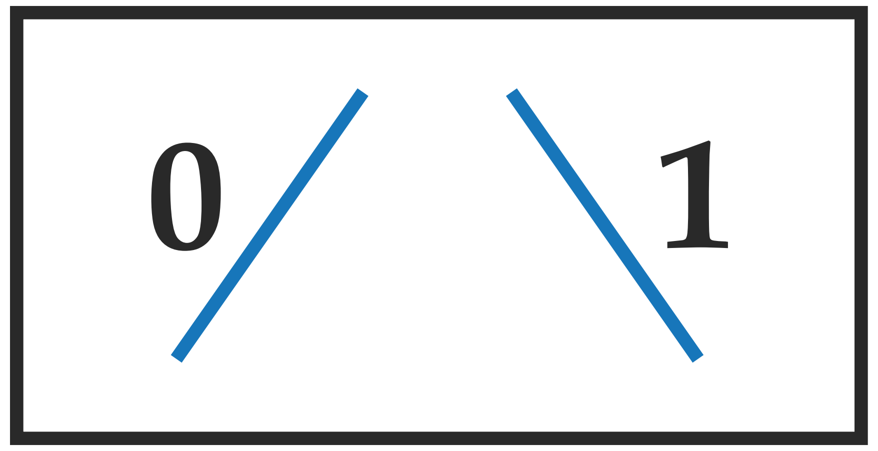
$$x_1 \cdot x_2 + x_1 \cdot x_3 + x_3 \cdot x_4 + x_3 = 0$$

$$x_2 \cdot x_3 + x_2 \cdot x_4 + x_1 + x_2 + 1 = 0$$

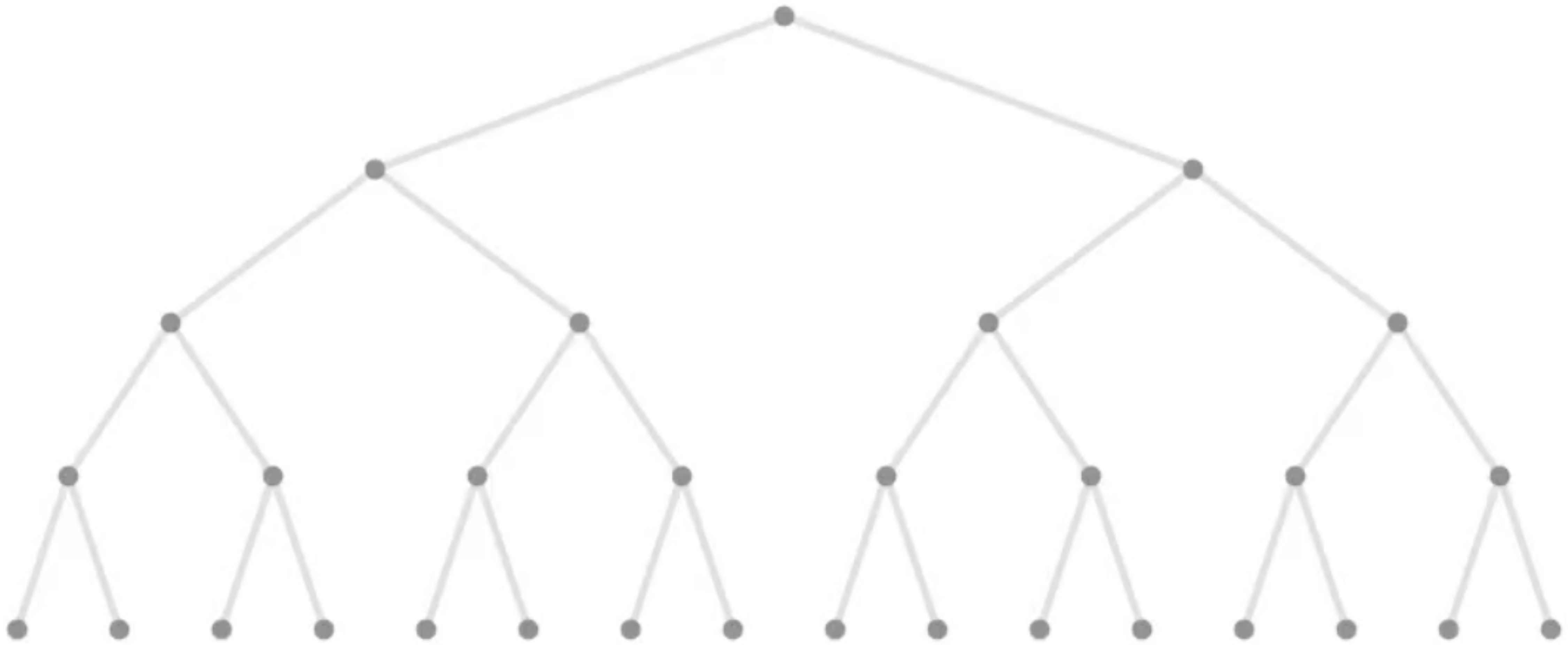
$$x_1 \cdot x_2 + x_2 \cdot x_3 + x_2 \cdot x_4 + x_1 + x_4 = 0$$

$$x_1 \cdot x_4 + x_2 \cdot x_3 + x_2 + x_3 + x_4 = 0$$

Exhaustive Search



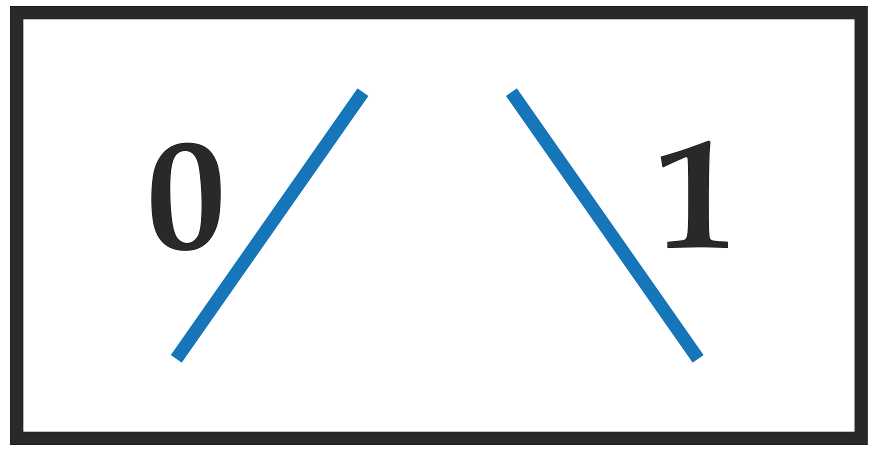
Worst-case complexity: $\mathcal{O}(2^n)$

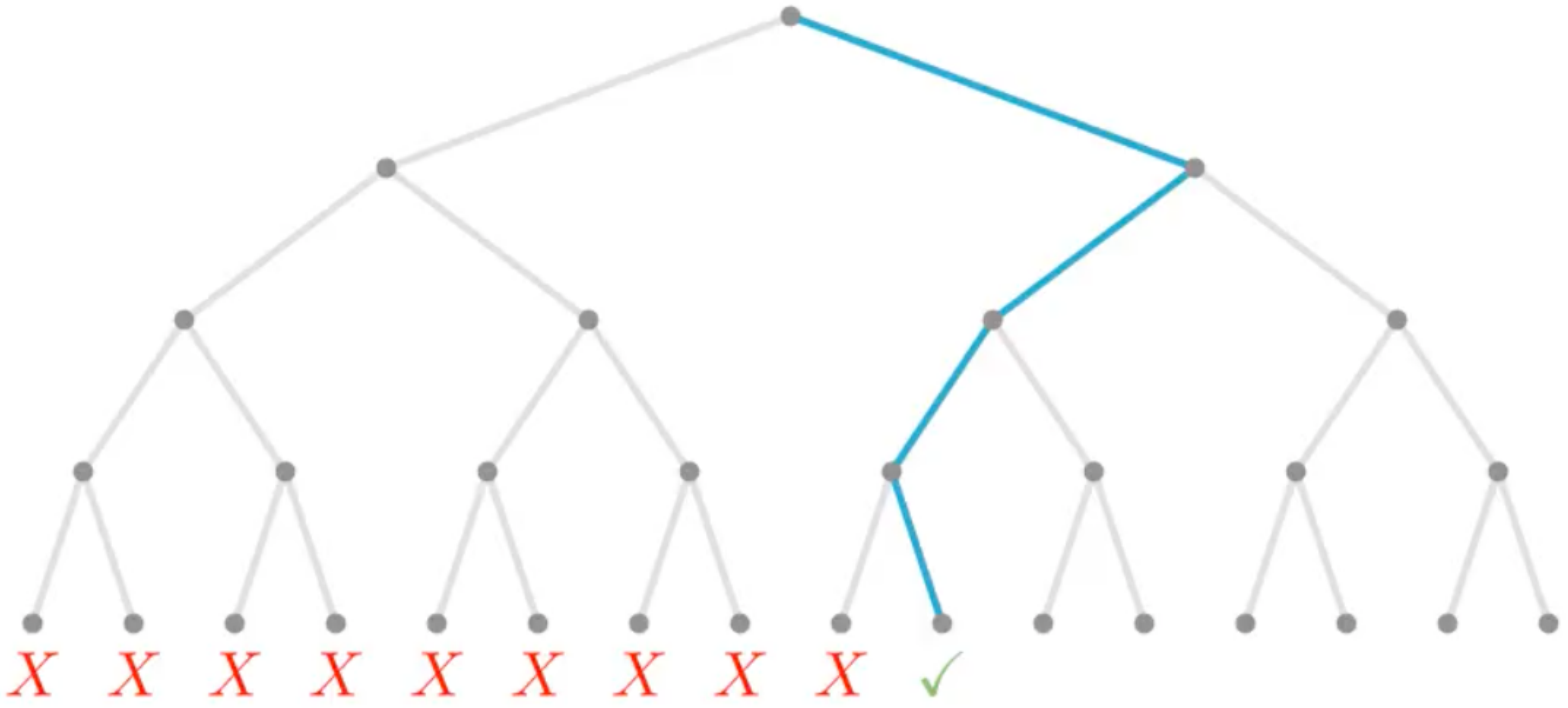


$$x_1 \cdot x_2 + x_1 \cdot x_3 + x_3 \cdot x_4 + x_3 = 0$$
$$x_2 \cdot x_3 + x_2 \cdot x_4 + x_1 + x_2 + 1 = 0$$
$$x_1 \cdot x_2 + x_2 \cdot x_3 + x_2 \cdot x_4 + x_1 + x_4 = 0$$
$$x_1 \cdot x_4 + x_2 \cdot x_3 + x_2 + x_3 + x_4 = 0$$

Binary search tree

Exhaustive Search

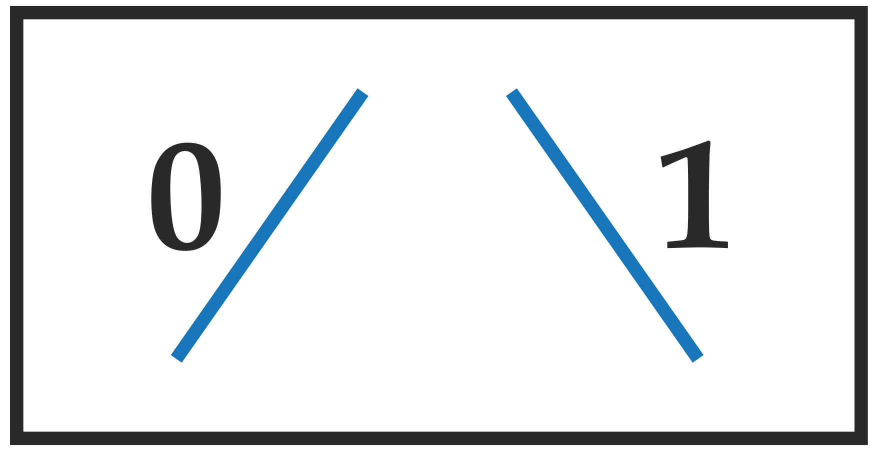




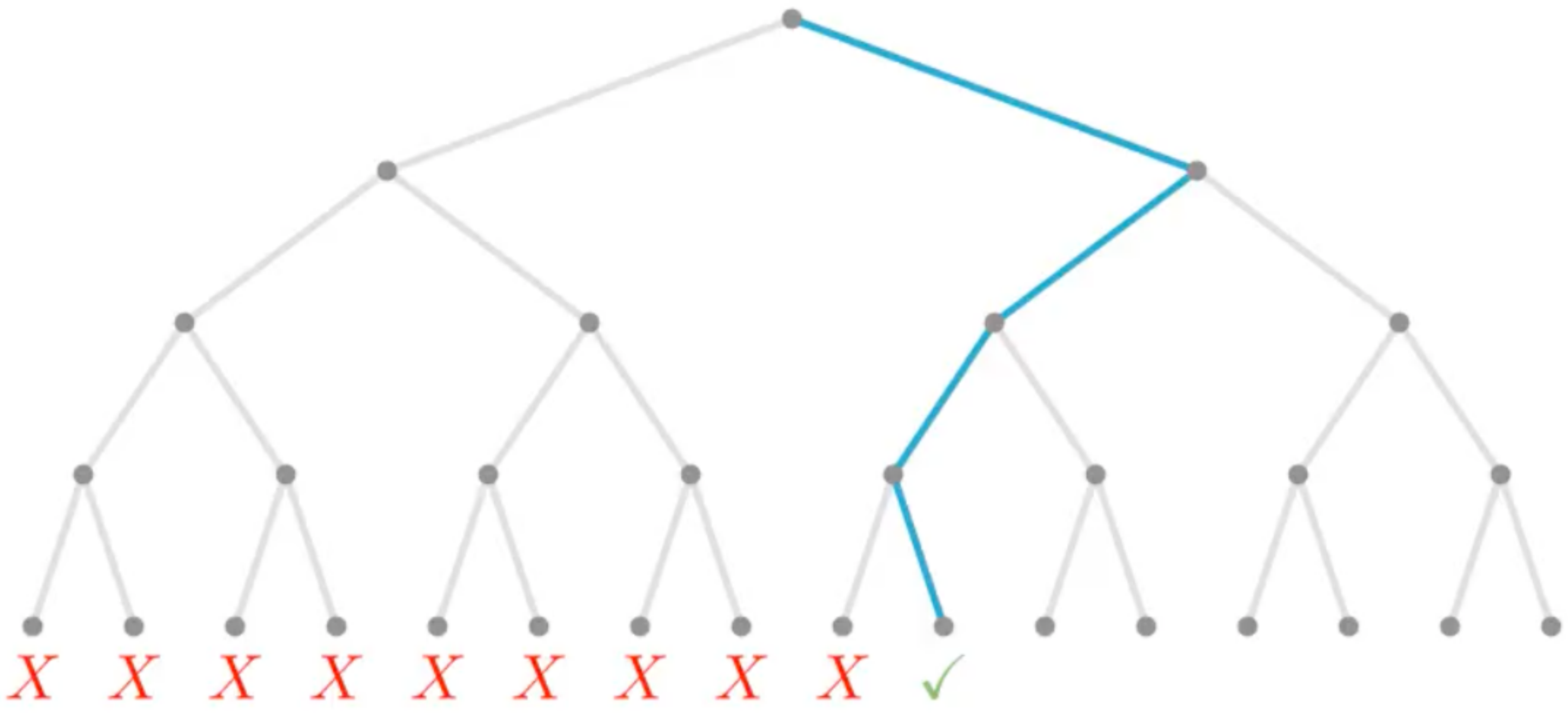
$$1 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 + 0 = 0$$
$$0 \cdot 0 + 0 \cdot 1 + 1 + 0 + 1 = 0$$
$$1 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 + 1 + 1 = 0$$
$$1 \cdot 1 + 0 \cdot 0 + 0 + 0 + 1 = 0$$

Binary search tree

Exhaustive Search



Worst-case complexity: $\mathcal{O}(2^n)$



Binary search tree

$$1 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 + 0 = 0$$
$$0 \cdot 0 + 0 \cdot 1 + 1 + 0 + 1 = 0$$
$$1 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 + 1 + 1 = 0$$
$$1 \cdot 1 + 0 \cdot 0 + 0 + 0 + 1 = 0$$

Macaulay matrix

Linearisation

Linear systems are easy to solve, nonlinear systems are hard.

Linearisation

Linear systems are easy to solve, nonlinear systems are hard.

Linearisation: for each nonlinear monomial, replace all of its occurrences by a new variable.

Linearisation

Linear systems are easy to solve, nonlinear systems are hard.

Linearisation: for each nonlinear monomial, replace all of its occurrences by a new variable.

Example.

$$\begin{aligned}
f_1 &: x_1x_3 + x_2x_4 + x_1 + x_3 + x_4 = 0\\
f_2 &: x_2x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_4 = 0\\
f_3 &: x_2x_4 + x_3x_4 + x_1 + x_3 + 1 = 0\\
f_4 &: x_1x_2 + x_1x_3 + x_2x_3 + x_3 + x_4 + 1 = 0\\
f_5 &: x_1x_2 + x_2x_3 + x_1x_4 + x_3 = 0\\
f_6 &: x_1x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_3 + x_4 = 0
\end{aligned}
\longrightarrow
\begin{aligned}
f_1 &: y_2 + y_5 + x_1 + x_3 + x_4 = 0\\
f_2 &: y_4 + y_3 + y_6 + x_1 + x_2 + x_4 = 0\\
f_3 &: y_5 + y_6 + x_1 + x_3 + 1 = 0\\
f_4 &: y_1 + y_2 + y_4 + x_3 + x_4 + 1 = 0\\
f_5 &: y_1 + y_4 + y_3 + x_3 = 0\\
f_6 &: y_2 + y_3 + y_6 + x_1 + x_2 + x_3 + x_4 = 0
\end{aligned}$$

Linearisation

Linear systems are easy to solve, nonlinear systems are hard.

Linearisation: for each nonlinear monomial, replace all of its occurrences by a new variable.

Example.

$$
\begin{aligned}
f_1 &: x_1x_3 + x_2x_4 + x_1 + x_3 + x_4 = 0\\
f_2 &: x_2x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_4 = 0\\
f_3 &: x_2x_4 + x_3x_4 + x_1 + x_3 + 1 = 0\\
f_4 &: \boxed{x_1x_2} + x_1x_3 + x_2x_3 + x_3 + x_4 + 1 = 0\\
f_5 &: \boxed{x_1x_2} + x_2x_3 + x_1x_4 + x_3 = 0\\
f_6 &: x_1x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_3 + x_4 = 0
\end{aligned}
\quad\longrightarrow\quad
\begin{aligned}
f_1 &: y_2 + y_5 + x_1 + x_3 + x_4 = 0\\
f_2 &: y_4 + y_3 + y_6 + x_1 + x_2 + x_4 = 0\\
f_3 &: y_5 + y_6 + x_1 + x_3 + 1 = 0\\
f_4 &: \boxed{y_1} + y_2 + y_4 + x_3 + x_4 + 1 = 0\\
f_5 &: \boxed{y_1} + y_4 + y_3 + x_3 = 0\\
f_6 &: y_2 + y_3 + y_6 + x_1 + x_2 + x_3 + x_4 = 0
\end{aligned}
$$

Linearisation

<u>Linearisation adds solutions</u>: a *random* quadratic system of m equations in n variables, when $n = m$, is expected to have one solution (probability is $\sim \frac{1}{q}$ for systems over $\mathbb{F}_q$). The corresponding linearised system has a solution space of dimension $\binom{n+1}{2} - m$.

$\binom{n}{2}$ quadratic plus n linear monomials

Linearisation

<u>Linearisation adds solutions</u>: a *random* quadratic system of m equations in n variables, when $n = m$, is expected to have one solution (probability is $\sim \frac{1}{q}$ for systems over $\mathbb{F}_q$). The corresponding linearised system has a solution space of dimension $\binom{n+1}{2} - m$.

$\binom{n}{2}$ quadratic plus n linear monomials

<u>Loss of information</u>: e.g. assignment $x_1 = 1; x_2 = 0; y_1 = 1;$ is part of a valid solution to the linearised system, but $x_1 x_2 \neq y_1$.

Macaulay matrix

Monomials →

Equations ↓

	x_1x_2	x_1x_3	x_1x_4	x_1	x_2x_3	x_2x_4	x_2	x_3x_4	x_3	x_4	1
f_1											
f_2											
f_3											
f_4											
f_5											
f_6											

$$f_1 : x_1x_3 + x_2x_4 + x_1 + x_3 + x_4 = 0$$
$$f_2 : x_2x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_4 = 0$$
$$f_3 : x_2x_4 + x_3x_4 + x_1 + x_3 + 1 = 0$$
$$f_4 : x_1x_2 + x_1x_3 + x_2x_3 + x_3 + x_4 + 1 = 0$$
$$f_5 : x_1x_2 + x_2x_3 + x_1x_4 + x_3 = 0$$
$$f_6 : x_1x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_3 + x_4 = 0$$

Macaulay matrix

Monomials →

Equations ↓

	x_1x_2	x_1x_3	x_1x_4	x_1	x_2x_3	x_2x_4	x_2	x_3x_4	x_3	x_4	1
f_1	0	1	0	1	0	1	0	0	1	1	0
f_2	0	0	1	1	1	0	1	1	0	1	0
f_3	0	0	0	1	0	1	0	1	1	0	1
f_4	1	1	0	1	1	0	0	0	1	1	1
f_5	1	0	1	1	1	0	0	0	1	0	0
f_6	0	1	1	1	0	0	1	1	1	1	0

$$f_1 : x_1x_3 + x_2x_4 + x_1 + x_3 + x_4 = 0$$
$$f_2 : x_2x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_4 = 0$$
$$f_3 : x_2x_4 + x_3x_4 + x_1 + x_3 + 1 = 0$$
$$f_4 : x_1x_2 + x_1x_3 + x_2x_3 + x_3 + x_4 + 1 = 0$$
$$f_5 : x_1x_2 + x_2x_3 + x_1x_4 + x_3 = 0$$
$$f_6 : x_1x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_3 + x_4 = 0$$

Gröbner basis algorithms

[Buchberger, 1965]

[Lazard, 1983]

F_4/F_5 [Faugère, 1999/2002]

(XL [Courtois, Klimov, Patarin, Shamir, 2000])

Gröbner basis algorithms (intuition)

*We are essentially describing the XL algorithm.

Gröbner basis algorithms (intuition)

*We are essentially describing the XL algorithm.

	x_1x_2	x_1x_3	x_1x_4	x_1	x_2x_3	x_2x_4	x_2	x_3x_4	x_3	x_4	1
f_1	0	1	0	1	0	1	0	0	1	1	0
f_2	0	0	1	1	1	0	1	1	0	1	0
f_3	0	0	0	1	0	1	0	1	1	0	1
f_4	1	1	0	1	1	0	0	0	1	1	1
f_5	1	0	1	1	1	0	0	0	1	0	0
f_6	0	1	1	1	0	0	1	1	1	1	0

Gröbner basis algorithms (intuition)

*We are essentially describing the XL algorithm.

$f_1 : x_1x_3 + x_2x_4 + x_1 + x_3 + x_4 = 0$

$f_2 : x_2x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_4 = 0$

$f_3 : x_2x_4 + x_3x_4 + x_1 + x_3 + 1 = 0$

$f_4 : x_1x_2 + x_1x_3 + x_2x_3 + x_3 + x_4 + 1 = 0$

$f_5 : x_1x_2 + x_2x_3 + x_1x_4 + x_3 = 0$

$f_6 : x_1x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_3 + x_4 = 0$

	x_1x_2	x_1x_3	x_1x_4	x_1	x_2x_3	x_2x_4	x_2	x_3x_4	x_3	x_4	1
f_1	0	1	0	1	0	1	0	0	1	1	0
f_2	0	0	1	1	1	0	1	1	0	1	0
f_3	0	0	0	1	0	1	0	1	1	0	1
f_4	1	1	0	1	1	0	0	0	1	1	1
f_5	1	0	1	1	1	0	0	0	1	0	0
f_6	0	1	1	1	0	0	1	1	1	1	0

Gröbner basis algorithms (intuition)

*We are essentially describing the XL algorithm.

$\boxed{D = 3}$

$$f_1 : x_1x_3 + x_2x_4 + x_1 + x_3 + x_4 = 0$$
$$f_2 : x_2x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_4 = 0$$
$$f_3 : x_2x_4 + x_3x_4 + x_1 + x_3 + 1 = 0$$
$$f_4 : x_1x_2 + x_1x_3 + x_2x_3 + x_3 + x_4 + 1 = 0$$
$$f_5 : x_1x_2 + x_2x_3 + x_1x_4 + x_3 = 0$$
$$f_6 : x_1x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_3 + x_4 = 0$$

	x_1x_2	x_1x_3	x_1x_4	x_1	x_2x_3	x_2x_4	x_2	x_3x_4	x_3	x_4	1	$x_1x_2x_3$	$x_1x_2x_4$	$x_1x_3x_4$	$x_2x_3x_4$
f_1	0	1	0	1	0	1	0	0	1	1	0				
f_2	0	0	1	1	1	0	1	1	0	1	0				
f_3	0	0	0	1	0	1	0	1	1	0	1				
f_4	1	1	0	1	1	0	0	0	1	1	1				
f_5	1	0	1	1	1	0	0	0	1	0	0				
f_6	0	1	1	1	0	0	1	1	1	1	0				
x_1f_1															
x_2f_1															
$\cdots$															

Gröbner basis algorithms (intuition)

*We are essentially describing the XL algorithm.

$f_1 : x_1x_3 + x_2x_4 + x_1 + x_3 + x_4 = 0$

$f_2 : x_2x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_4 = 0$

$f_3 : x_2x_4 + x_3x_4 + x_1 + x_3 + 1 = 0$

$f_4 : x_1x_2 + x_1x_3 + x_2x_3 + x_3 + x_4 + 1 = 0$

$f_5 : x_1x_2 + x_2x_3 + x_1x_4 + x_3 = 0$

$f_6 : x_1x_3 + x_1x_4 + x_3x_4 + x_1 + x_2 + x_3 + x_4 = 0$

$\boxed{D = 4}$

	x_1x_2	x_1x_3	x_1x_4	x_1	x_2x_3	x_2x_4	x_2	x_3x_4	x_3	x_4	1	$x_1x_2x_3$	$x_1x_2x_4$	$x_1x_3x_4$	$x_2x_3x_4$	$x_1x_2x_3x_4$
f_1	0	1	0	1	0	1	0	0	1	1	0					
f_2	0	0	1	1	1	0	1	1	0	1	0					
f_3	0	0	0	1	0	1	0	1	1	0	1					
f_4	1	1	0	1	1	0	0	0	1	1	1					
f_5	1	0	1	1	1	0	0	0	1	0	0					
f_6	0	1	1	1	0	0	1	1	1	1	0					
x_1f_1																
x_2f_1																
$\dots$																
$x_1x_2f_1$																
$x_1x_3f_1$																

XL / Gröbner basis algorithms: complexity

XL/Gröbner basis algorithms: complexity

$$\mathcal{O}\left(mD_{reg}\binom{n+D_{reg}-1}{D_{reg}}^{\omega}\right)$$

XL/Gröbner basis algorithms: complexity

$$\mathcal{O}\left(mD_{reg} \binom{n + D_{reg} - 1}{D_{reg}}^{\omega} \right)$$

D_{reg}: degree of regularity

the power of the first non-positive coefficient in the expansion of $$\frac{(1-t^2)^m}{(1-t)^n}$$

XL/Gröbner basis algorithms: complexity

D_{reg}: degree of regularity

the power of the first non-positive coefficient in the expansion of $$\frac{(1-t^2)^m}{(1-t)^n}$$

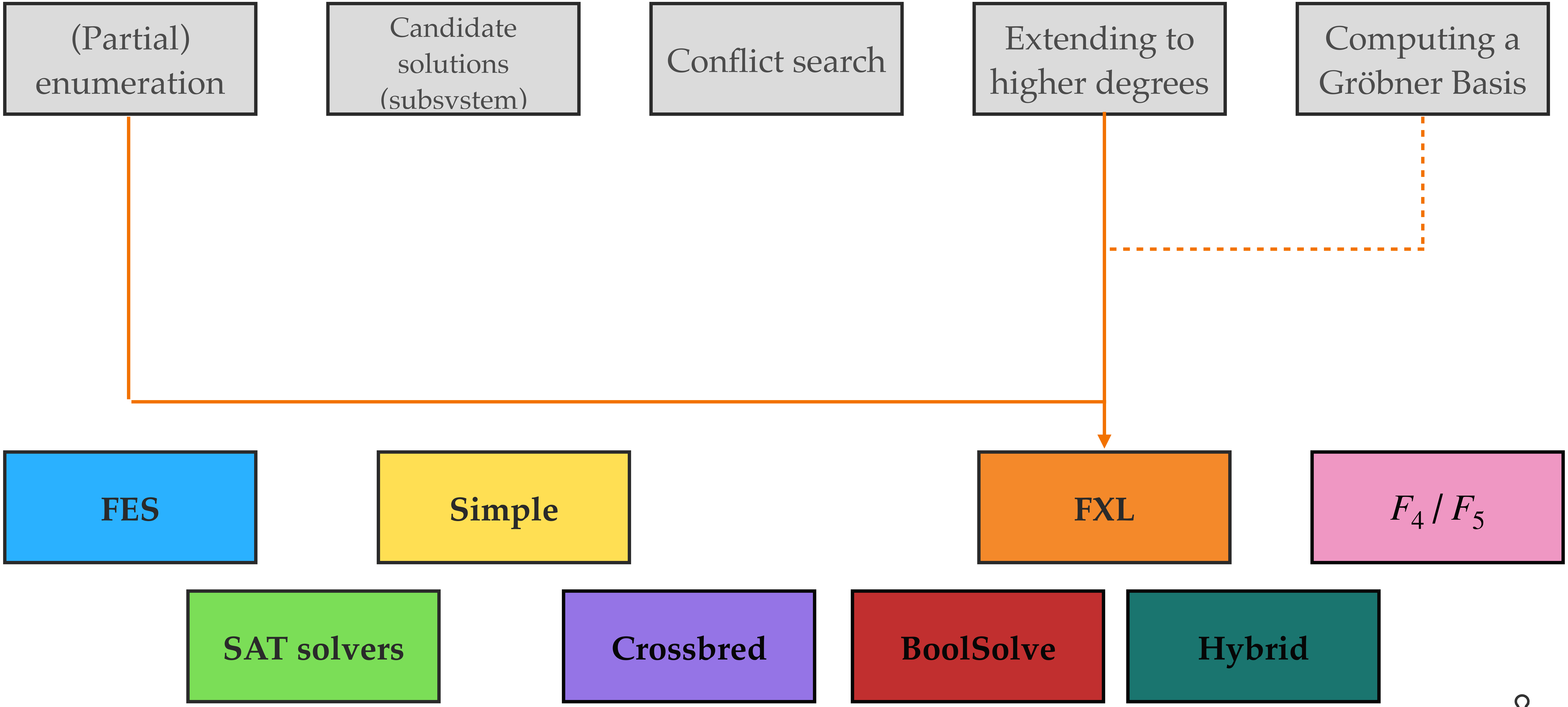
```
m=8
n=7
R.<t> = PowerSeriesRing(ZZ)
hs = ((1-t^2)^(m)) / (1-t)^(n)
print(hs)
```

[3] ✓ 0.0s

```
1 + 7*t + 20*t^2 + 28*t^3 + 14*t^4 - 14*t^5 - 28*t^6 - 20*t^7 - 7*t^8 - t^9 + O(t^20)
```

The number of monomials (columns) minus linearly independent equations (rows) at degree $D = 4$ is 14.

Summary


(Partial) enumeration
Candidate solutions (subsystem)
Conflict search
Extending to higher degrees
Computing a Gröbner Basis
FES
Simple
FXL
F_4 / F_5
SAT solvers
Crossbred
BoolSolve
Hybrid