# Algebraic Attacks Using IP-Solvers

Ehsan Ullah

The 15th International Workshop on
Computer Algebra in Scientific Computing
September 9 - 13, 2013
Berlin, Germany

# Outline

# Finding $\mathbb{F}_2$-rational Solutions

Consider the field $\mathbb{F}_2$ with two elements. Let $f_1, f_2 \in \mathbb{F}_2[x_1, x_2]$, where $f_1 = x_1x_2 + x_2$, and $f_2 = x_1x_2 + x_1 + 1$. Find a solution of the system

$$f_1 = 0, \ \ f_2 = 0$$

in $\mathbb{F}_2^2$. The four possible solution candidates are:

$$(0,0), \ (0,1), \ (1,0), \ (1,1).$$

The only candidate that qualifies for a solution is $(1,0)$.

# Finding $\mathbb{F}_2$-rational Solutions

Consider the field $\mathbb{F}_2$ with two elements. Let $f_1, f_2 \in \mathbb{F}_2[x_1, x_2]$, where $f_1 = x_1x_2 + x_2$, and $f_2 = x_1x_2 + x_1 + 1$. Find a solution of the system

$$f_1 = 0, \;\; f_2 = 0$$

in $\mathbb{F}_2^2$. The four possible solution candidates are:

$$(0, 0), \;\; (0, 1), \;\; (1, 0), \;\; (1, 1).$$

The only candidate that qualifies for a solution is $(1, 0)$.

### Gröbner Bases Approach

Compute a Gröbner basis of the ideal

$$\langle f_1, f_2, x_1^2 + x_1, x_2^2 + x_2 \rangle$$

which is

$$\{x_1 + x_2 + 1, \;\; x_2\}$$

# Finding $\mathbb{F}_q$-rational Solutions

Let $p$ be a prime and $q = p^e$ with $e > 0$. Let $K = \mathbb{F}_q$ be the finite field and let $F = \{f_1, \ldots, f_\ell\} \subseteq P = K[x_1, \ldots, x_n]$ be a set of polynomials. Find the $K$-rational solutions of the following system of equations.

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_\ell(x_1, \ldots, x_n) &= 0 \end{aligned}$$

# Finding $\mathbb{F}_q$-rational Solutions

Let $p$ be a prime and $q = p^e$ with $e > 0$. Let $K = \mathbb{F}_q$ be the finite field and let $F = \{f_1, \ldots, f_\ell\} \subseteq P = K[x_1, \ldots, x_n]$ be a set of polynomials. Find the $K$-rational solutions of the following system of equations.

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_\ell(x_1, \ldots, x_n) &= 0 \end{aligned}$$

Special Properties of the System:

- The so-called field polynomials $x_1^q - x_1, \ldots, x_n^q - x_n$ play an essential role. For instance, the ideal
$$\langle f_1, \ldots, f_\ell, x_1^q - x_1, \ldots, x_n^q - x_n \rangle$$
is a 0-dimensional radical ideal.

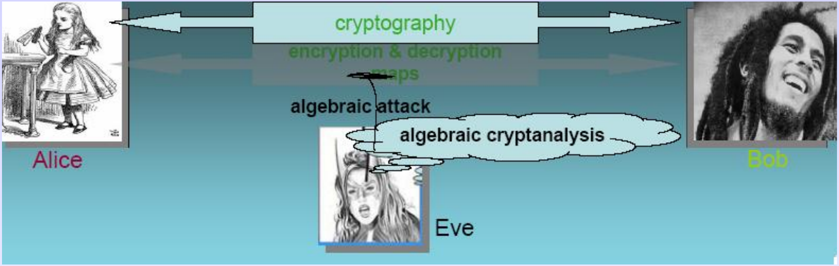
# Finding $\mathbb{F}_q$-rational Solutions

Let $p$ be a prime and $q = p^e$ with $e > 0$. Let $K = \mathbb{F}_q$ be the finite field and let $F = \{f_1, \ldots, f_\ell\} \subseteq P = K[x_1, \ldots, x_n]$ be a set of polynomials. Find the $K$-rational solutions of the following system of equations.

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_\ell(x_1, \ldots, x_n) &= 0 \end{aligned}$$

Special Properties of the System:

- The so-called field polynomials $x_1^q - x_1, \ldots, x_n^q - x_n$ play an essential role. For instance, the ideal
  $$\langle f_1, \ldots, f_\ell, x_1^q - x_1, \ldots, x_n^q - x_n \rangle$$
  is a 0-dimensional radical ideal.
- The system has a unique (or a few) $K$-rational solution(s). The polynomials $f_1, \ldots, f_\ell$ are quadratic and $p = 2$.




## Cryptosystem

A cryptosystem consists of the following components:

- a set $\mathcal{P}$ called plaintext space,
- a set $\mathcal{C}$ called ciphertext space,
- a set $\mathcal{K}$ called key space,
- for every $k \in \mathcal{K}$ an encryption map, $\varepsilon_k : \mathcal{P} \longrightarrow \mathcal{C}$ and a decryption map, $\delta_k : \mathcal{C} \longrightarrow \mathcal{P}$ such that $\delta_k \circ \varepsilon_k = \mathrm{id}_{\mathcal{P}}$.

# Algebraic Attacks

## Idea

Reduce the task of breaking a cryptosystem to the task of solving a polynomial system!

How: Let the plaintext space and the ciphertext space be of the form $\mathcal{P} = K^n$ and $\mathcal{C} = K^m$ with a finite field $K$ (usually $K = \mathbb{F}_2$). Then every map $\varphi : K^n \longrightarrow K^m$ is given by polynomials, i.e. there exist polynomials $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ such that

$$\varphi(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

for all $(x_1, \ldots, x_n) \in K^n$.

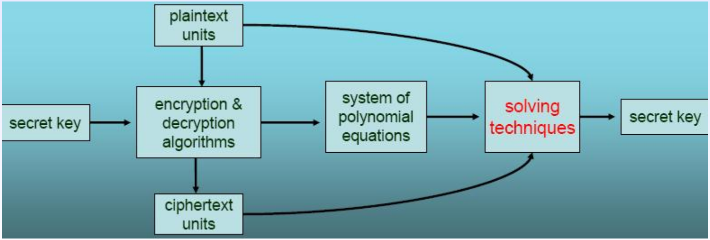
# Algebraic Attacks

## Idea

Reduce the task of breaking a cryptosystem to the task of solving a polynomial system!
How: Let the plaintext space and the ciphertext space be of the form $\mathcal{P} = K^n$ and $\mathcal{C} = K^m$ with a finite field $K$ (usually $K = \mathbb{F}_2$). Then every map $\varphi : K^n \longrightarrow K^m$ is given by polynomials, i.e. there exist polynomials $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ such that

$$\varphi(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

for all $(x_1, \ldots, x_n) \in K^n$.



# Standard Cryptographic Polynomial Systems

Courtois Toy Cipher (CTC)

| CTC(S-Boxes,Rounds) | CTC(3,3) | CTC(4,4) | CTC(5,5) | CTC(6,6) | CTC(7,7) | CTC(8,8) |
|---|---|---|---|---|---|---|
| equations | 216 | 380 | 605 | 864 | 1169 | 1496 |
| variables | 117 | 204 | 330 | 468 | 630 | 795 |
| non-linear terms | 162 | 288 | 450 | 648 | 882 | 1152 |

Small Scale Advanced Encryption Standard (AES)

| AES(n,r,c,w) | AES(9,1,1,4) | AES(10,1,1,4) | AES(4,2,1,4) | AES(2,2,2,4) | AES(3,2,2,4) | AES(1,1,1,8) |
|---|---|---|---|---|---|---|
| equations | 1184 | 1312 | 1088 | 1024 | 1472 | 640 |
| variables | 592 | 656 | 544 | 512 | 736 | 320 |
| non-lin. terms | 1584 | 1760 | 1408 | 1056 | 1584 | 2416 |

Systems used are available at `http://apcocoa.org/polynomialsystems/`

## Our Approach for Solving over Finite Fields

system of equations over $\mathbb{F}_q$

system of equations over $\mathbb{F}_q$

Traditional techniques using Gröbner basis:

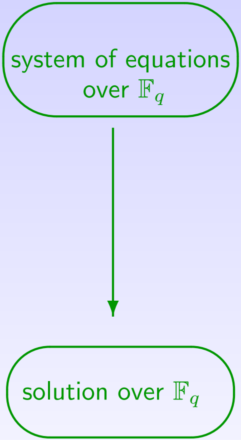
Improvements: Buchberg's algorithm using strategies such as normal selection, sugar cube, etc.

Variants: $\mathrm{F}_4$ and $\mathrm{F}_5$ algorithms, XL-algorithm and its mutant variants.

Border basis algorithm and its improvements.

SAT-Solvers and characteristic set methods.

## Our Approach for Solving over Finite Fields




### Traditional techniques using Gröbner basis:

Improvements: Buchberg's algorithm using strategies such as normal selection, sugar cube, etc.

Variants: $\mathrm{F}_4$ and $\mathrm{F}_5$ algorithms, XL-algorithm and its mutant variants.

### Border basis algorithm and its improvements.

### SAT-Solvers and characteristic set methods.

system of equations over $\mathbb{F}_q$

system of equations over $\mathbb{R}$ (resp. $\mathbb{Z}$)

$\downarrow$

solution over $\mathbb{F}_q$

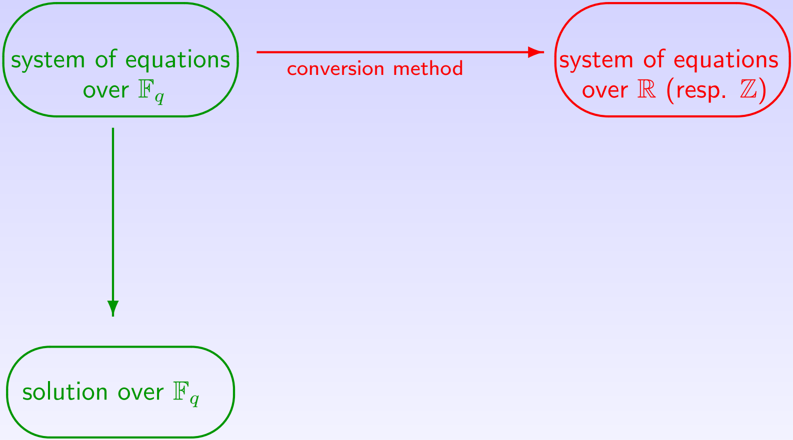
Traditional techniques using Gröbner basis:

Improvements: Buchberg's algorithm using strategies such as normal selection, sugar cube, etc.

Variants: $F_4$ and $F_5$ algorithms, XL-algorithm and its mutant variants.

Border basis algorithm and its improvements.

SAT-Solvers and characteristic set methods.




Traditional techniques using Gröbner basis:

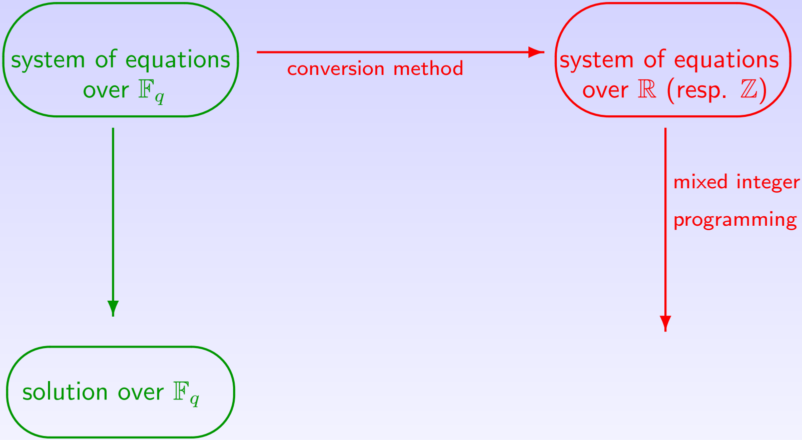
Improvements: Buchberg's algorithm using strategies such as normal selection, sugar cube, etc.

Variants: $F_4$ and $F_5$ algorithms, XL-algorithm and its mutant variants.

Border basis algorithm and its improvements.

SAT-Solvers and characteristic set methods.

## Our Approach for Solving over Finite Fields



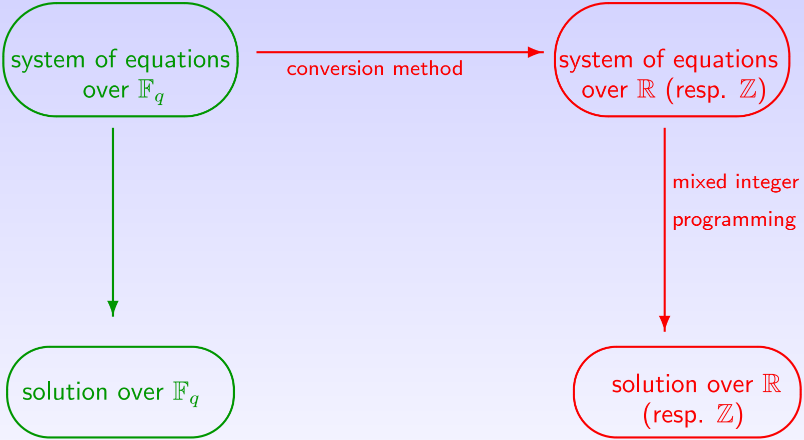

Traditional techniques using Gröbner basis:

Improvements: Buchberg's algorithm using strategies such as normal selection, sugar cube, etc.

Variants: $F_4$ and $F_5$ algorithms, XL-algorithm and its mutant variants.

Border basis algorithm and its improvements.

SAT-Solvers and characteristic set methods.




Traditional techniques using Gröbner basis:

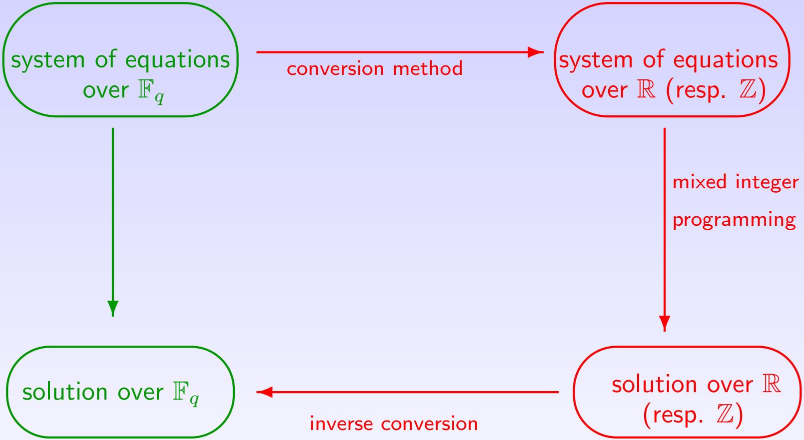
Improvements: Buchberg's algorithm using strategies such as normal selection, sugar cube, etc.

Variants: $F_4$ and $F_5$ algorithms, XL-algorithm and its mutant variants.

Border basis algorithm and its improvements.

SAT-Solvers and characteristic set methods.

## Our Approach for Solving over Finite Fields




Traditional techniques using Gröbner basis:

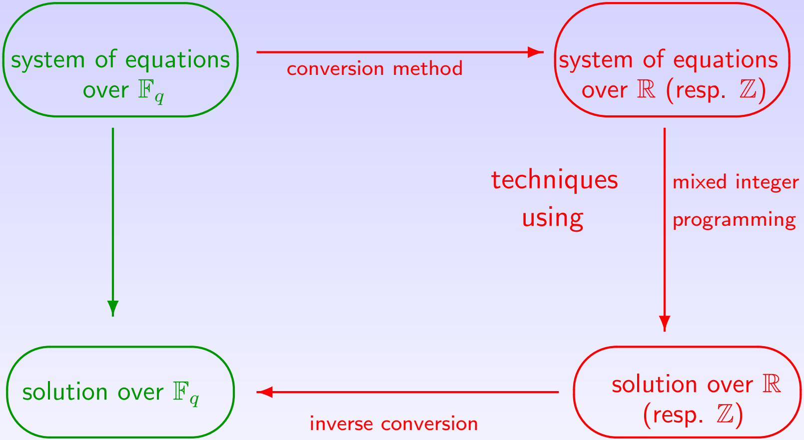
Improvements: Buchberg's algorithm using strategies such as normal selection, sugar cube, etc.

Variants: $F_4$ and $F_5$ algorithms, XL-algorithm and its mutant variants.

Border basis algorithm and its improvements.

SAT-Solvers and characteristic set methods.

## Our Approach for Solving over Finite Fields




Traditional techniques using Gröbner basis:

Improvements: Buchberg's algorithm using strategies such as normal selection, sugar cube, etc.

Variants: $F_4$ and $F_5$ algorithms, XL-algorithm and its mutant variants.

Border basis algorithm and its improvements.

SAT-Solvers and characteristic set methods.

# Objectives

- Look for new techniques and strategies
- Study the impact of various newly developed strategies
- Get advantage of parallel computing, state-of-the-art solvers
- Provide tools for algebraic cryptanalysis through ApCoCoA

system of equations over $\mathbb{F}_2$

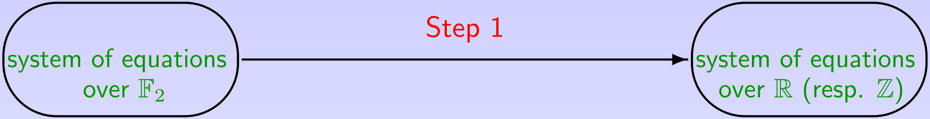
$$\text{system of equations over } \mathbb{F}_2 \xrightarrow{\text{Step 1}} \text{system of equations over } \mathbb{R} \text{ (resp. } \mathbb{Z}\text{)}$$

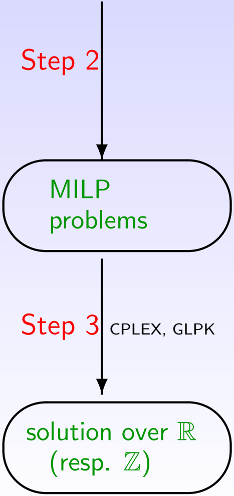
Step 1: transformation to $\mathbb{R}$ or $\mathbb{Z}$

system of equations over $\mathbb{F}_2$ $\xrightarrow{\text{Step 1}}$ system of equations over $\mathbb{R}$ (resp. $\mathbb{Z}$) $\xrightarrow{\text{Step 2}}$ MILP problems

Step 1: transformation to $\mathbb{R}$ or $\mathbb{Z}$

Step 2: modeling MILP problem,
linearization (using strategies) $+$ modeling




Step 1: transformation to $\mathbb{R}$ or $\mathbb{Z}$

Step 2: modeling MILP problem,
linearization (using strategies) + modeling

Step 3: using an IP solver

system of equations over $\mathbb{F}_2$ $\xrightarrow{\text{Step 1}}$ system of equations over $\mathbb{R}$ (resp. $\mathbb{Z}$)

Step 2

MILP problems

Step 3 CPLEX, GLPK

solution over $\mathbb{R}$ (resp. $\mathbb{Z}$)

Step 4

solution over $\mathbb{F}_2$

Step 1: transformation to $\mathbb{R}$ or $\mathbb{Z}$

Step 2: modeling MILP problem, linearization (using strategies) + modeling

Step 3: using an IP solver

Step 4: inverse transformation

Find a $\mathbb{F}_2$-rational solution of

$$f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0,$$

where $f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$.

An overview given by R. Beigel (1993).

Find a $\mathbb{F}_2$-rational solution of

$$f_1(x_1, \dots, x_n) = 0, \dots, f_m(x_1, \dots, x_n) = 0,$$

where $f_1, \dots, f_m \in \mathbb{F}_2[x_1, \dots, x_n]$.
We are looking for a tuple $(a_1, \dots, a_n) \in \{0, 1\}^n$ such that

$$\begin{aligned} F_1(a_1, \dots, a_n) &\equiv 0 \pmod 2 \\ &\vdots \\ F_m(a_1, \dots, a_n) &\equiv 0 \pmod 2 \end{aligned}$$

where $F_i \in \mathbb{Z}[X_1, \dots, X_n]$ ($\mathbb{R}[X_1, \dots, X_n]$) are liftings of the polynomials $f_i$.

An overview given by R. Beigel (1993).

Find a $\mathbb{F}_2$-rational solution of

$$f_1(x_1,\dots,x_n)=0,\dots,f_m(x_1,\dots,x_n)=0,$$

where $f_1,\dots,f_m\in\mathbb{F}_2[x_1,\dots,x_n]$.
We are looking for a tuple $(a_1,\dots,a_n)\in\{0,1\}^n$ such that

$$\begin{aligned}F_1(a_1,\dots,a_n)&\equiv 0 \pmod 2\\&\vdots\\F_m(a_1,\dots,a_n)&\equiv 0 \pmod 2\end{aligned}$$

where $F_i\in\mathbb{Z}[X_1,\dots,X_n]$ ($\mathbb{R}[X_1,\dots,X_n]$) are liftings of the polynomials $f_i$.

- standard representation:

$$\begin{array}{ccc}\overline{0} & \rightarrow & 0\\ \overline{1} & \rightarrow & 1\end{array}$$

iteratively replace each sum $X_1+X_2$ by $X_1+X_2-2X_1X_2$

An overview given by R. Beigel (1993).

Let $f = x_1x_2 + x_3x_4 + x_5 + x_6 + 1 \in \mathbb{F}_2[x_1, \ldots, x_6]$.

Let $f = x_1x_2 + x_3x_4 + x_5 + x_6 + 1 \in \mathbb{F}_2[x_1, \ldots, x_6]$.

## Example

*The standard representation of $f$ is*

$$\begin{aligned} F = {} & 8X_1X_2X_3X_4X_5X_6 - 4X_1X_2X_3X_4X_5 - 4X_1X_2X_3X_4X_6 \\ & +2X_1X_2X_3X_4 - 4X_1X_2X_5X_6 - 4X_3X_4X_5X_6 + 2X_1X_2X_5 \\ & +2X_3X_4X_5 + 2X_1X_2X_6 + 2X_3X_4X_6 - X_1X_2 - X_3X_4 \\ & +2X_5X_6 - X_5 - X_6 + 1 \in \mathbb{R}[X_1, \ldots, X_6] \end{aligned}$$

*The polynomial $F$ has 16 terms in its support and degree 6.*

Let $f = x_1x_2 + x_3x_4 + x_5 + x_6 + 1 \in \mathbb{F}_2[x_1, \ldots, x_6]$.

## Example

*The standard representation of* $f$ *is*

$$\begin{aligned} F = {} & 8X_1X_2X_3X_4X_5X_6 - 4X_1X_2X_3X_4X_5 - 4X_1X_2X_3X_4X_6 \\ & +2X_1X_2X_3X_4 - 4X_1X_2X_5X_6 - 4X_3X_4X_5X_6 + 2X_1X_2X_5 \\ & +2X_3X_4X_5 + 2X_1X_2X_6 + 2X_3X_4X_6 - X_1X_2 - X_3X_4 \\ & +2X_5X_6 - X_5 - X_6 + 1 \in \mathbb{R}[X_1, \ldots, X_6] \end{aligned}$$

*The polynomial* $F$ *has 16 terms in its support and degree 6.*

## Splitting

- $y_1 + x_1x_2 = x_3x_4 + x_5$, $y_1 = x_6 + 1$.
- $y_1 + y_2 = y_3 + x_5$, $y_1 = x_6 + 1$, $y_2 = x_1x_2$, $y_3 = x_3x_4$.
- $Y_1 + Y_2 - 2Y_1Y_2 = Y_3 + X_5 - 2Y_3X_5$, $Y_1 = 1 - X_6$, $Y_2 - X_1X_2 = 0$, $Y_2 - X_3X_4 = 0$.

We require the solution of a polynomial system of equations

$$f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0.$$

with polynomials $f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$.

We require the solution of a polynomial system of equations

$$f_1(x_1,\dots,x_n)=0,\dots,f_m(x_1,\dots,x_n)=0.$$

with polynomials $f_1,\dots,f_m \in \mathbb{F}_2[x_1,\dots,x_n]$.

In other words, find a tuple $(a_1,\dots,a_n)\in\{0,1\}^n$ such that

$$F_1(a_1,\dots,a_n)\equiv 0 \pmod 2,\dots,F_m(a_1,\dots,a_n)\equiv 0 \pmod 2)$$

where $F_i \in \mathbb{Z}[X_1,\dots,X_n]$ are liftings of the polynomials $f_i$.

We require the solution of a polynomial system of equations

$$f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0.$$

with polynomials $f_1, \ldots, f_m \in \mathbb{F}_2[x_1, \ldots, x_n]$.

In other words, find a tuple $(a_1, \ldots, a_n) \in \{0, 1\}^n$ such that

$$F_1(a_1, \ldots, a_n) \equiv 0 \pmod 2, \ldots, F_m(a_1, \ldots, a_n) \equiv 0 \pmod 2$$

where $F_i \in \mathbb{Z}[X_1, \ldots, X_n]$ are liftings of the polynomials $f_i$.

Idea: Formulate these congruences as a system of linear equalities or inequalities over $\mathbb{Z}$ and solve it using an IP-solver.

# Integer Polynomial Conversion (IPC)

Assume we are given a congruence

$$F(a_1, \dots, a_n) \equiv 0 \pmod 2$$

with $F \in \mathbb{Z}[X_1, \dots, X_n]$ and we are looking for solutions with $0 \leq a_i \leq 1$. For simplicity, assume $\deg(F) = 2$ and $F$ is squarefree.

This technique is known due to M. Kreuzer, Algebraic Attacks (2009).

# Integer Polynomial Conversion (IPC)

Assume we are given a congruence

$$F(a_1, \dots, a_n) \equiv 0 \pmod 2$$

with $F \in \mathbb{Z}[X_1, \dots, X_n]$ and we are looking for solutions with $0 \le a_i \le 1$. For simplicity, assume $\deg(F) = 2$ and $F$ is squarefree.

1. Using a new indeterminate $K$, form the inequality

$$K \le \lfloor \#\mathrm{Supp}(F)/2 \rfloor.$$

This technique is known due to M. Kreuzer, Algebraic Attacks (2009).

# Integer Polynomial Conversion (IPC)

Assume we are given a congruence

$$F(a_1, \ldots, a_n) \equiv 0 \pmod 2$$

with $F \in \mathbb{Z}[X_1, \ldots, X_n]$ and we are looking for solutions with $0 \leq a_i \leq 1$. For simplicity, assume $\deg(F) = 2$ and $F$ is squarefree.

1. Using a new indeterminate $K$, form the inequality

$$K \leq \lfloor \#\mathrm{Supp}(F)/2 \rfloor.$$

2. For each term $X_i X_j$ in the support of $F$ introduce a new indeterminate $Y_{ij}$. Let $L$ be the linear part of $F$. Form the equation

$$\sum_{i,j} Y_{ij} + L - 2K = 0.$$

This technique is known due to M. Kreuzer, Algebraic Attacks (2009).

# Integer Polynomial Conversion (IPC)

Assume we are given a congruence

$$F(a_1, \ldots, a_n) \equiv 0 \pmod 2$$

with $F \in \mathbb{Z}[X_1, \ldots, X_n]$ and we are looking for solutions with $0 \leq a_i \leq 1$. For simplicity, assume $\deg(F) = 2$ and $F$ is squarefree.

1. Using a new indeterminate $K$, form the inequality
$$K \leq \lfloor \#\mathrm{Supp}(F)/2 \rfloor.$$
2. For each term $X_i X_j$ in the support of $F$ introduce a new indeterminate $Y_{ij}$. Let $L$ be the linear part of $F$. Form the equation
$$\sum_{i,j} Y_{ij} + L - 2K = 0.$$
3. Form the inequalities
$$X_i \leq 1, Y_{ij} \leq X_i, Y_{ij} \leq X_j \text{ and } Y_{ij} \geq X_i + X_j - 1.$$

This technique is known due to M. Kreuzer, Algebraic Attacks (2009).

# Real Polynomial Conversion (RPC)

Consider the polynomial equation $x_1 + x_2 = x_3 + x_4x_5$ over $\mathbb{F}_2$.

1. $x_1 + x_2 = x_3 + x_6$, where $x_6 = x_4x_5$

This method is known due to J. Borghoff et al., Bivium as MILP Problem (2009).

# Real Polynomial Conversion (RPC)

Consider the polynomial equation $x_1 + x_2 = x_3 + x_4 x_5$ over $\mathbb{F}_2$.

1. $x_1 + x_2 = x_3 + x_6$, where $x_6 = x_4 x_5$
2. Lift over $\mathbb{R}$ using standard representation:

$$X_1 + X_2 - 2X_1X_2 - X_3 - X_6 + 2X_3X_6 = 0, X_6 - X_4X_5 = 0$$

This method is known due to J. Borghoff et al., Bivium as MILP Problem (2009).

# Real Polynomial Conversion (RPC)

Consider the polynomial equation $x_1 + x_2 = x_3 + x_4 x_5$ over $\mathbb{F}_2$.

1. $x_1 + x_2 = x_3 + x_6$, where $x_6 = x_4 x_5$
2. Lift over $\mathbb{R}$ using standard representation:

$$X_1 + X_2 - 2X_1X_2 - X_3 - X_6 + 2X_3X_6 = 0, X_6 - X_4X_5 = 0$$

3. Linearize: $X_1 + X_2 - 2Z_1 - X_3 - X_6 + 2Z_2 = 0,\ X_6 - Z_3 = 0$, where $X_iX_j$ is replaced by $Z_k$

This method is known due to J. Borghoff et al., Bivium as MILP Problem (2009).

# Real Polynomial Conversion (RPC)

Consider the polynomial equation $x_1 + x_2 = x_3 + x_4 x_5$ over $\mathbb{F}_2$.

1. $x_1 + x_2 = x_3 + x_6$, where $x_6 = x_4 x_5$
2. Lift over $\mathbb{R}$ using standard representation:

$$X_1 + X_2 - 2X_1X_2 - X_3 - X_6 + 2X_3X_6 = 0, X_6 - X_4X_5 = 0$$

3. Linearize: $X_1 + X_2 - 2Z_1 - X_3 - X_6 + 2Z_2 = 0,\ X_6 - Z_3 = 0$, where $X_iX_j$ is replaced by $Z_k$
4. $X_i \leq 1,\ Z_k - X_i \leq 0,\ Z_k - X_j \leq 0,\ -Z_k + X_i + X_j - 1 \leq 0$

This method is known due to J. Borghoff et al., Bivium as MILP Problem (2009).

# Converting Boolean Polynomials to CNF Clauses

Let $f \in \mathbb{F}_2[x_1, \dots, x_n]$ be a (squarefree) polynomial. Let $X = \{X_1, \dots, X_n\}$ be a set of boolean variables (atomic formulas), and let $\widehat{X}$ be the set of all (propositional) logical formulas that can be constructed (using $\neg$, $\wedge$, and $\vee$ operations) from them.

## Definition

*A logical representation of $f$ is a logical formula $F \in \widehat{X}$ such that $\varphi_a(F) = f(a_1, \dots, a_n) + 1$ for every $a = (a_1, \dots, a_n) \in \mathbb{F}_2^n$, where $\varphi_a$ denotes the boolean value of $F$ at the tuple of boolean values $a$ with $1 =$ `true` and $0 =$ `false`.*

G. Bard (2007), B. Chen (2008), P. Jovanovic and M. Kreuzer (2010).

# Converting Boolean Polynomials to CNF Clauses

Let $f \in \mathbb{F}_2[x_1, \dots, x_n]$ be a (squarefree) polynomial. Let $X = \{X_1, \dots, X_n\}$ be a set of boolean variables (atomic formulas), and let $\widehat{X}$ be the set of all (propositional) logical formulas that can be constructed (using $\neg$, $\wedge$, and $\vee$ operations) from them.

## Definition

*A logical representation of $f$ is a logical formula $F \in \widehat{X}$ such that $\varphi_a(F) = f(a_1, \dots, a_n) + 1$ for every $a = (a_1, \dots, a_n) \in \mathbb{F}_2^n$, where $\varphi_a$ denotes the boolean value of $F$ at the tuple of boolean values $a$ with $1 = \texttt{true}$ and $0 = \texttt{false}$.*

## Conversion Procedure

- Linearize: introduce a new indeterminate for each nonlinear term
- Cutting: cut the resulting linear polynomial after certain no. of terms
- Logical Equivalent: find logical equivalents using a XOR-CNF conversion

G. Bard (2007), B. Chen (2008), P. Jovanovic and M. Kreuzer (2010).

- Standard Strategy (SS): substitute a new variable $y$ for $t$ in $f$ and form the clauses corresponding to $t + y$.
- Linear Partner Strategy (LPS): replace $x_i x_j + x_i$ in $f$ by $y$ and form the clauses corresponding to $x_i(x_j + 1) + y$.
- Double Partner Strategy (DPS): replace $x_i x_j + x_i + x_j + 1$ in $f$ by $y$ and form the clauses corresponding to $(x_i + 1)(x_j + 1) + y$.
- Quadratic Partner Substitution: replaces combinations of the form $x_i x_j + x_i x_k$.
- Cubic Partner Substitution: replaces combinations of the form $x_i x_j x_k + x_i x_j x_l$.

---

Added by P. Jovanovic and M. Kreuzer (2010).

# The Logic of 0-1 Inequalities

1. Linear inequalities containing 0-1 variables can be viewed as logical propositions.
2. A clause is a special case of 0-1 inequality, namely a clausal inequality.

# The Logic of 0-1 Inequalities

1. Linear inequalities containing 0-1 variables can be viewed as logical propositions.
2. A clause is a special case of 0-1 inequality, namely a clausal inequality.

Any clause in propositional logic

$$X_1 \vee \cdots \vee X_r \vee \neg Y_1 \vee \cdots \vee \neg Y_s$$

can be translated into a clausal inequality

$$X_1 + \cdots + X_r + (1 - Y_1) + \cdots + (1 - Y_s) \geq 1$$

$$X_1 + \cdots + X_r - Y_1 + \cdots + -Y_s \geq 1 - s$$

A clause set is satisfiable if and only if the corresponding system of clausal inequalities together with the bounds $0 \leq X_i, Y_j \leq 1$ has an integer solution.

The LPC (using the LP strategy) of the polynomial $f = x_1 + x_2 + x_3 + x_3x_4$ is:

1. Let $x_1 + x_2 + y_1 = 0$ and form the clauses

$$\neg Y_1 \vee X_3, \neg Y_1 \vee \neg X_4, Y_1 \vee \neg X_3 \vee X_4$$

corresponding to $y_1 = x_3 + x_3x_4$.

The LPC (using the LP strategy) of the polynomial $f = x_1 + x_2 + x_3 + x_3x_4$ is:

1. Let $x_1 + x_2 + y_1 = 0$ and form the clauses

$$\neg Y_1 \vee X_3, \neg Y_1 \vee \neg X_4, Y_1 \vee \neg X_3 \vee X_4$$

   corresponding to $y_1 = x_3 + x_3x_4$.

2. Form the clauses

$$\neg X_1 \vee X_2 \vee Y_1, X_1 \vee \neg X_2 \vee Y_1, X_1 \vee X_2 \vee \neg Y_1, \neg X_1 \vee \neg X_2 \vee \neg Y_1$$

   corresponding to $x_1 + x_2 + y_1 = 0$.

The LPC (using the LP strategy) of the polynomial $f = x_1 + x_2 + x_3 + x_3x_4$ is:

1. Let $x_1 + x_2 + y_1 = 0$ and form the clauses
$$\neg Y_1 \vee X_3, \neg Y_1 \vee \neg X_4, Y_1 \vee \neg X_3 \vee X_4$$
corresponding to $y_1 = x_3 + x_3x_4$.
2. Form the clauses
$$\neg X_1 \vee X_2 \vee Y_1, X_1 \vee \neg X_2 \vee Y_1, X_1 \vee X_2 \vee \neg Y_1, \neg X_1 \vee \neg X_2 \vee \neg Y_1$$
corresponding to $x_1 + x_2 + y_1 = 0$.
3. The clausal inequalities are
$$-X_3 + Y_1 \leq 0, X_4 + Y_1 - 1 \leq 0, X_3 - X_4 - Y_1 \leq 0,$$
$$X_1 - X_2 - Y_1 \leq 0, -X_1 + X_2 - Y_1 \leq 0,$$
$$-X_1 - X_2 + Y_1 \leq 0, X_1 + X_2 + Y_1 - 2 \leq 0.$$

# Hybrid Techniques for Polynomial Conversion

The newly developed strategies (LP, DLP, QP, CP) due to the LPC can be used in combination with the IPC and RPC for further optimizations.

1. Hybrid IPC
2. Hybrid RPC

# Hybrid Techniques for Polynomial Conversion

The newly developed strategies (LP, DLP, QP, CP) due to the LPC can be used in combination with the IPC and RPC for further optimizations.

1. Hybrid IPC
2. Hybrid RPC

## Example

The Hybrid IPC (using the LP strategy) of the equation $x_1 + x_2 + x_3 + x_4 + x_4x_5 = 0$ is:

# Hybrid Techniques for Polynomial Conversion

The newly developed strategies (LP, DLP, QP, CP) due to the LPC can be used in combination with the IPC and RPC for further optimizations.

1. Hybrid IPC
2. Hybrid RPC

## Example

The Hybrid IPC (using the LP strategy) of the equation $x_1 + x_2 + x_3 + x_4 + x_4x_5 = 0$ is:

1. $X_1 + X_2 + X_3 + (X_4 + X_4X_5) - 2K = 0.$

# Hybrid Techniques for Polynomial Conversion

The newly developed strategies (LP, DLP, QP, CP) due to the LPC can be used in combination with the IPC and RPC for further optimizations.

1. Hybrid IPC
2. Hybrid RPC

## Example

The Hybrid IPC (using the LP strategy) of the equation $x_1 + x_2 + x_3 + x_4 + x_4x_5 = 0$ is:

1. $X_1 + X_2 + X_3 + (X_4 + X_4X_5) - 2K = 0.$
2. $K \leq \lfloor \#\mathrm{Supp}(f)/2 \rfloor = 2.$

# Hybrid Techniques for Polynomial Conversion

The newly developed strategies (LP, DLP, QP, CP) due to the LPC can be used in combination with the IPC and RPC for further optimizations.

1. Hybrid IPC
2. Hybrid RPC

## Example

The Hybrid IPC (using the LP strategy) of the equation $x_1 + x_2 + x_3 + x_4 + x_4x_5 = 0$ is:

1. $X_1 + X_2 + X_3 + (X_4 + X_4X_5) - 2K = 0.$
2. $K \leq \lfloor \#\mathrm{Supp}(f)/2 \rfloor = 2$.
3. $X_1 + X_2 + X_3 + Y - 2K = 0$, where $X_4 + X_4X_5$ is replaced by $Y$.

# Hybrid Techniques for Polynomial Conversion

The newly developed strategies (LP, DLP, QP, CP) due to the LPC can be used in combination with the IPC and RPC for further optimizations.

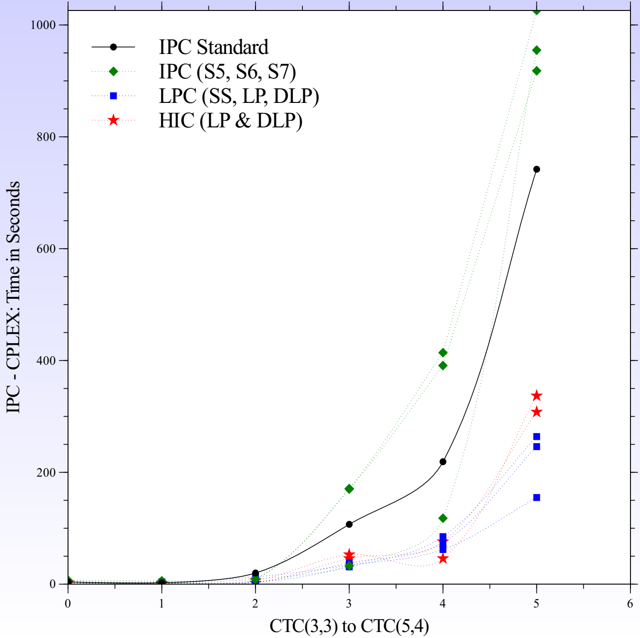
1. Hybrid IPC
2. Hybrid RPC

## Example

The Hybrid IPC (using the LP strategy) of the equation $x_1 + x_2 + x_3 + x_4 + x_4x_5 = 0$ is:

1. $X_1 + X_2 + X_3 + (X_4 + X_4X_5) - 2K = 0$.
2. $K \leq \lfloor \#\mathrm{Supp}(f)/2 \rfloor = 2$.
3. $X_1 + X_2 + X_3 + Y - 2K = 0$, where $X_4 + X_4X_5$ is replaced by $Y$.
4. $X_i \leq 1$, $-X_4 + Y \leq 0$, $X_5 + Y - 1 \leq 0$, $-X_5 - Y + X_4 \leq 0$.

## The Hybrid IPC and RPC Conversions



# Comparison With IPC and RPC

| system | m | n | LPC(QPS) | HRPC(SS) | HRPC(QPS) | HIPC(QPS) | RPC | IPC |
|---|---|---|---|---|---|---|---|---|
| AES(8,1,1,4) | 1056 | 528 | 3908 | 21921 | 298 | **226** | 8351 | 1986 |
| AES(9,1,1,4) | 1184 | 592 | 26406 | 2493 | 814 | **236** | 2493 | 417 |
| AES(10,1,1,4) | 1312 | 656 | 6994 | 9521 | 13211 | **1982** | 9521 | 2655 |
| AES(4,2,1,4) | 1088 | 544 | 1377 | 6391 | 62338 | 3147 | 6391 | **789** |
| AES(2,2,2,4) | 1024 | 512 | 19970 | 19243 | 74982 | 81014 | 19243 | **7830** |
| AES(3,2,2,4) | 1472 | 736 | 523240 | 339069 | 279126 | **61020** | 532100 | 525226 |
| AES(1,1,1,8) | 640 | 220 | 42354 | **2043** | 207180 | 9323 | 10370 | 4684 |

| system | m | n | LPC(LP) | LPC(DLP) | HIPC(LP) | HIPC(DLP) | HRPC(SS) | RPC | IPC |
|---|---|---|---|---|---|---|---|---|---|
| CTC(5,5) | 605 | 330 | 691 | 679 | 1798 | 552 | **480** | 1356 | 2708 |
| CTC(5,6) | 705 | 375 | **270** | 1875 | 9332 | 2421 | 1041 | 1227 | 3088 |
| CTC(6,5) | 708 | 378 | 15540 | 16707 | 14661 | 11621 | 10723 | **7743** | 15656 |
| CTC(6,6) | 864 | 458 | 16941 | 12264 | **10716** | 16757 | 11572 | 25978 | 45272 |
| CTC(6,7) | 984 | 522 | 30868 | 18660 | **2285** | 11031 | 7716 | 9224 | 26209 |
| CTC(7,6) | 987 | 525 | 91358 | 97985 | 68146 | **9436** | 73090 | 11904 | 22198 |

---

CPLEX running on a laptop with a 2.13 GHz Intel Pentium P6200 Dual Core processor and 4GB RAM.

# Summary of Contributions

- We study the IPC and RPC conversions
- A new conversion technique called LPC
- Several new strategies to use with IPC and RPC

# Summary of Contributions

- We study the IPC and RPC conversions
- A new conversion technique called LPC
- Several new strategies to use with IPC and RPC

Invitation:

- Solve your favorite systems with our techniques

# Summary of Contributions

- We study the IPC and RPC conversions
- A new conversion technique called LPC
- Several new strategies to use with IPC and RPC

Invitation:

- Solve your favorite systems with our techniques
- Implementations are available in the CAS ApCoCoA
  http://apcocoa.org/

# Summary of Contributions

- We study the IPC and RPC conversions
- A new conversion technique called LPC
- Several new strategies to use with IPC and RPC

Invitation:

- Solve your favorite systems with our techniques
- Implementations are available in the CAS ApCoCoA
  http://apcocoa.org/
- Polynomial systems available at:
  `http://apcocoa.org/polynomialsystems/`


*for your attention.*

*Questions ?*

*Remarks ?*