

Multivariate Cryptography

2WC12 Cryptography I – Fall 2013

Ruben Niederhagen

TU / **e**

Technische Universiteit
Eindhoven
University of Technology

December 5th, 2013

1. Introduction

Cryptography

NP-hard, NP-complete

Post-Quantum Crypto

Multivariate Cryptography

NP-Completeness of \mathcal{MQ}

2. Cryptosystems

Hashing

Asymmetric Schemes

Signatures

Symmetric Schemes

3. System Solving

Gröbner Bases

Extended Linearization

Brute Force

Basic idea:

Use computations that are easy (**polynomial time**) for the legitimate user but hard (**exponential time**) for an attacker.

⇒ Use secret knowledge (**key**) that makes computations easy.

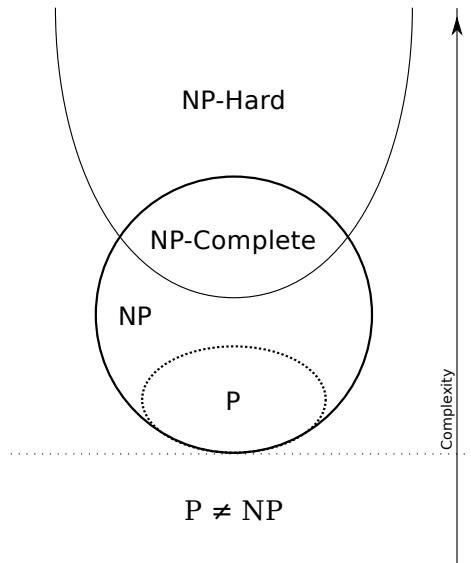
Basic idea:

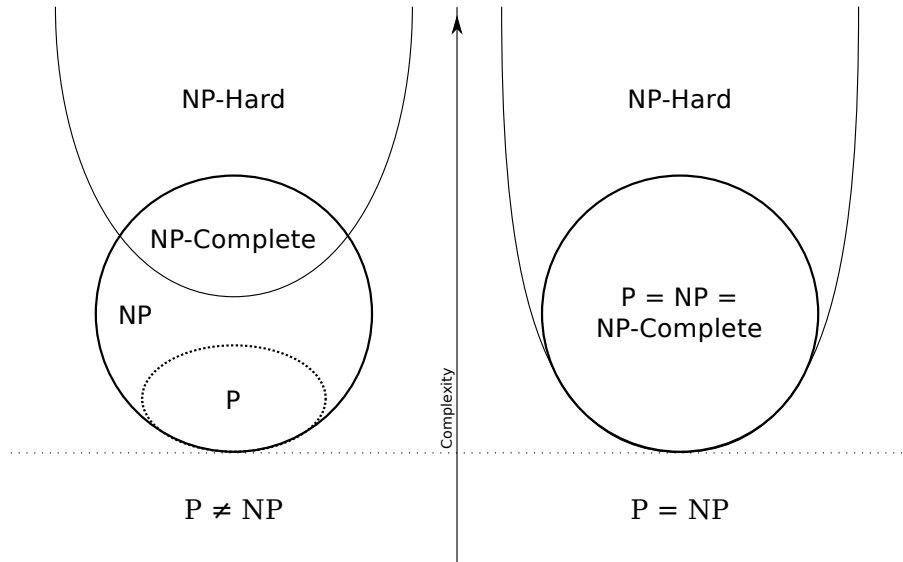
Use computations that are easy (**polynomial time**) for the legitimate user but hard (**exponential time**) for an attacker.

⇒ Use secret knowledge (**key**) that makes computations easy.

Commonly used hard problems:

- ▶ discrete logarithm (DLP),
- ▶ factorization,
- ▶ codes,
- ▶ lattices,
- ▶ multivariate polynomial systems,
- ▶ ...





Threat of quantum computers:

Shor's algorithm makes polynomial time:

- ▶ integer factorization
- ▶ DLP in finite fields
- ▶ DLP on elliptic curves
- ▶ DLP in general class groups

Threat of quantum computers:

Shor's algorithm makes polynomial time:

- ▶ integer factorization
- ▶ DLP in finite fields
- ▶ DLP on elliptic curves
- ▶ DLP in general class groups

Grover's algorithm brings faster simultaneous search in data

- ▶ some security loss in symmetric crypto
(block and stream ciphers)
- ▶ some security loss in hash functions

Compensate for Grover by doubling key size.

The “survivors”:

Public-key encryption:

- ▶ Lattice-based cryptography (e.g. NTRU, (Ring)-LWE)
- ▶ Code-based cryptography (e.g. McEliece, Niederreiter)

Public-key signatures:

- ▶ Multivariate-quadratic-equations cryptography (e.g. UOV)
- ▶ Hash based cryptography (e.g. Merkle's hash-trees signatures)

For these systems no efficient usage of Shor's algorithm is known.
Grover's algorithm has to be taken into account when choosing key sizes.

The “survivors”:

Public-key encryption:

- ▶ Lattice-based cryptography (e.g. NTRU, (Ring)-LWE)
- ▶ Code-based cryptography (e.g. McEliece, Niederreiter)

Public-key signatures:

- ▶ **Multivariate-quadratic-equations cryptography** (e.g. UOV)
- ▶ Hash based cryptography (e.g. Merkle's hash-trees signatures)

For these systems no efficient usage of Shor's algorithm is known.
Grover's algorithm has to be taken into account when choosing key sizes.

Underlying problem:

Solving a system of m multivariate polynomial equations in n variables over \mathbb{F}_q is called the **MP problem**.

Underlying problem:

Solving a system of m multivariate polynomial equations in n variables over \mathbb{F}_q is called the **MP problem**.

Example:

$$5x_1^3x_2x_3^2 + 17x_2^4x_3 + 23x_1^2x_2^4 + 13x_1 + 12x_2 + 5 = 0$$

$$12x_1^2x_2^3x_3 + 15x_1x_3^3 + 25x_2x_3^3 + 5x_1 + 6x_3 + 12 = 0$$

$$28x_1x_2x_3^4 + 14x_2^3x_3^2 + 16x_1x_3 + 32x_2 + 7x_3 + 10 = 0$$

Underlying problem:

Solving a system of m multivariate polynomial equations in n variables over \mathbb{F}_q is called the **MP problem**.

Example:

$$5x_1^3x_2x_3^2 + 17x_2^4x_3 + 23x_1^2x_2^4 + 13x_1 + 12x_2 + 5 = 0$$

$$12x_1^2x_2^3x_3 + 15x_1x_3^3 + 25x_2x_3^3 + 5x_1 + 6x_3 + 12 = 0$$

$$28x_1x_2x_3^4 + 14x_2^3x_3^2 + 16x_1x_3 + 32x_2 + 7x_3 + 10 = 0$$

Hardness:

The MP problem is an **NP-complete** problem even for multivariate *quadratic* systems and $q = 2$.

Underlying problem:

Solving a system of m multivariate polynomial equations in n variables over \mathbb{F}_q is called the **MP problem**.

Example:

$$x_3x_2 + x_2x_1 + x_2 + x_1 + 1 = 0$$

$$x_3x_1 + x_3x_2 + x_3 + x_1 = 0$$

$$x_3x_2 + x_3x_1 + x_3 + x_2 = 0$$

Hardness:

The MP problem is an **NP-complete** problem even for multivariate *quadratic* systems and $q = 2$.

Notation:

For a set $f = (f_1, \dots, f_m)$ of m quadratic polynomials in n variables over \mathbb{F}_2 , let $f(x) = (f_1(x), \dots, f_m(x)) \in \mathbb{F}_2^m$ be the solution vector of the evaluation of f for a vector $x \in \mathbb{F}_2^n$.

Notation:

For a set $f = (f_1, \dots, f_m)$ of m quadratic polynomials in n variables over \mathbb{F}_2 , let $f(x) = (f_1(x), \dots, f_m(x)) \in \mathbb{F}_2^m$ be the solution vector of the evaluation of f for a vector $x \in \mathbb{F}_2^n$.

Definition (\mathcal{MQ} over \mathbb{F}_2):

Let $\mathcal{MQ}(\mathbb{F}_2^n, \mathbb{F}_2^m)$ be the set of all systems of quadratic equations in n variables and m equations over \mathbb{F}_2 .

We call one element $P \in \mathcal{MQ}(\mathbb{F}_2^n, \mathbb{F}_2^m)$ an instance of \mathcal{MQ} over \mathbb{F}_2 .

Solvable in NP-time:

The following non-deterministic polynomial-time algorithm solves $MQ-\mathbb{F}_2$ for a given system of equations:

1. Guess an assignment A for $(x_0, \dots, x_{n-1}) \in \{0, 1\}^n$.
2. Check if all m equations are satisfied by A .
3. Output A or go to an infinity loop, respectively.

NP-hardness:

Reduce 3-SAT to $MQ-\mathbb{F}_2$.

$$(b_1 \vee \neg b_2 \vee b_3) \wedge (b_1 \vee b_2) \wedge (\neg b_4)$$

NP-hardness:

Reduce 3-SAT to $\mathcal{MQ}\text{-}\mathbb{F}_2$.

$$(b_1 \vee \neg b_2 \vee b_3) \wedge (b_1 \vee b_2) \wedge (\neg b_4)$$

Replace all $(l_i \vee l_j)$ by $(l_i + l_j + l_i l_j)$,
replace all $(l_i \vee l_j \vee l_k)$ by $(l_i + l_j + l_k + l_i l_j + l_i l_k + l_j l_k + l_i l_j l_k)$:

$$(b_1 + \neg b_2 + b_3 + b_1 \neg b_2 + b_1 b_3 + \neg b_2 b_3 + b_1 \neg b_2 b_3) \wedge (b_1 + b_2 + b_1 b_2) \wedge (\neg b_4)$$

NP-hardness:

Reduce 3-SAT to $MQ_{\mathbb{F}_2}$.

$$(b_1 \vee \neg b_2 \vee b_3) \wedge (b_1 \vee b_2) \wedge (\neg b_4)$$

Replace all b_i by x_i and all $\neg b_i$ by $(1 - x_i)$:

$$\left(x_1 + (1 - x_2) + x_3 + x_1(1 - x_2) + x_1x_3 + (1 - x_2)x_3 + x_1(1 - x_2)x_3 \right) \wedge \\ (x_1 + x_2 + x_1x_2) \wedge (1 - x_4)$$

NP-hardness:

Reduce 3-SAT to $\mathcal{MQ}\text{-}\mathbb{F}_2$.

$$(b_1 \vee \neg b_2 \vee b_3) \wedge (b_1 \vee b_2) \wedge (\neg b_4)$$

Construct an equation $e_i : c_i = 1$ for each clause c_i :

$$x_1 + (1 - x_2) + x_3 + x_1(1 - x_2) + x_1x_3 + (1 - x_2)x_3 + x_1(1 - x_2)x_3 = 1$$

$$x_1 + x_2 + x_1x_2 = 1$$

$$1 - x_4 = 1$$

NP-hardness:

Reduce 3-SAT to $MQ-\mathbb{F}_2$.

$$(b_1 \vee \neg b_2 \vee b_3) \wedge (b_1 \vee b_2) \wedge (\neg b_4)$$

Expand all terms:

$$x_1x_2 + x_1x_2x_3 + x_2x_3 + x_2 = 0$$

$$x_1x_2 + x_1 + x_2 + 1 = 0$$

$$x_4 = 0$$

NP-hardness:

Reduce 3-SAT to $MQ-\mathbb{F}_2$.

$$(b_1 \vee \neg b_2 \vee b_3) \wedge (b_1 \vee b_2) \wedge (\neg b_4)$$

Iteratively add a new equation for each remaining cubic term:

$$x_1x_2 + x_5x_3 + x_2x_3 + x_2 = 0$$

$$x_1x_2 + x_1 + x_2 + 1 = 0$$

$$x_4 = 0$$

$$x_5 = x_1x_2$$

NP-hardness:

Reduce 3-SAT to $MQ_{\mathbb{F}_2}$.

$$(b_1 \vee \neg b_2 \vee b_3) \wedge (b_1 \vee b_2) \wedge (\neg b_4)$$

Final equation system:

$$x_3x_5 + x_2x_3 + x_2 + x_5 = 0$$

$$x_1 + x_2 + x_5 + 1 = 0$$

$$x_4 = 0$$

$$x_1x_2 + x_5 = 0$$

NP-hardness:

Reduce 3-SAT to $MQ-\mathbb{F}_2$.

$$(b_1 \vee \neg b_2 \vee b_3) \wedge (b_1 \vee b_2) \wedge (\neg b_4)$$

Final equation system:

$$x_3x_5 + x_2x_3 + x_2 + x_5 = 0$$

$$x_1 + x_2 + x_5 + 1 = 0$$

$$x_4 = 0$$

$$x_1x_2 + x_5 = 0$$

$$3\text{-SAT} \leq_{\text{poly}} MQ-\mathbb{F}_2$$

Theorem:

$\mathcal{MQ}\text{-}\mathbb{F}_2$ is NP-complete.

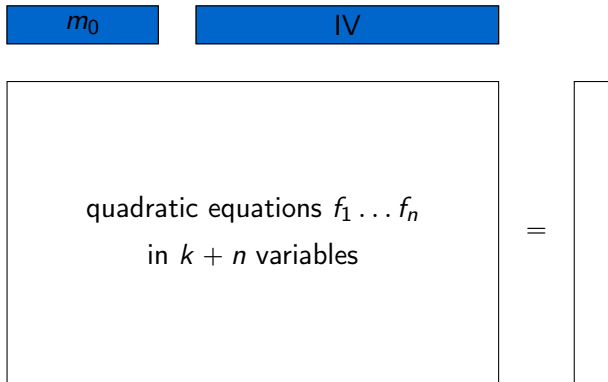
Proof.

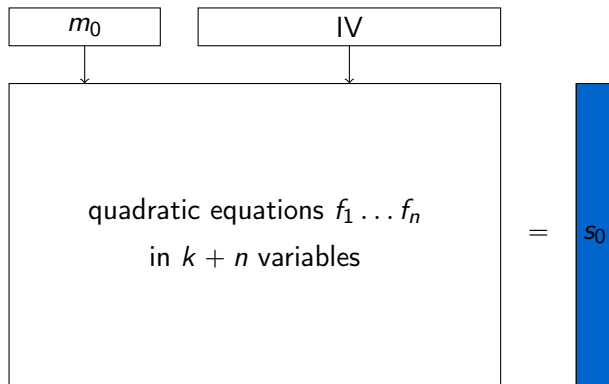
We showed that $\mathcal{MQ}\text{-}\mathbb{F}_2 \in \text{NP}$ and $3\text{-SAT} \leq_{\text{poly}} \mathcal{MQ}\text{-}\mathbb{F}_2$.

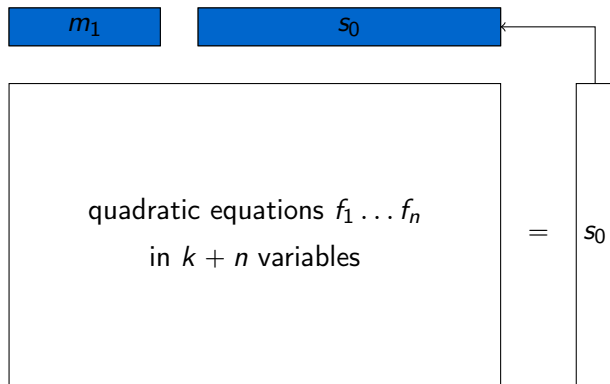
Thus, $\mathcal{MQ}\text{-}\mathbb{F}_2$ is NP-complete. □

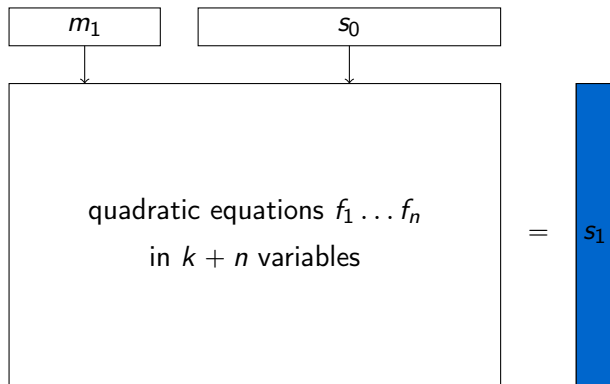
Cryptographic hash function:

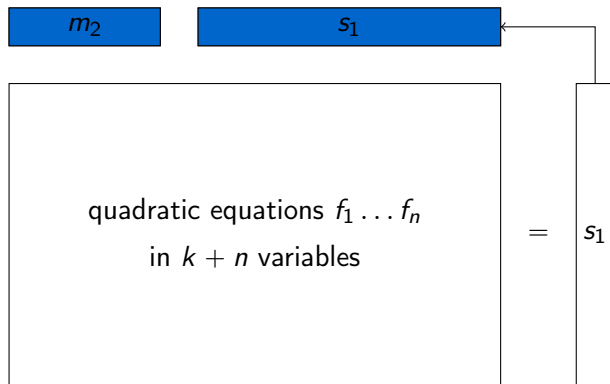
- ▶ Pre-image resistance:
Given a hash h it should be difficult to find any message m such that $h = H(m)$.
- ▶ Second pre-image resistance:
Given an input m_0 it should be difficult to find another input m_1 such that $m_0 \neq m_1$ and $H(m_0) = H(m_1)$.
- ▶ Collision resistance:
It should be difficult to find two different messages m_0 and m_1 such that that $m_0 \neq m_1$ and $H(m_0) = H(m_1)$.

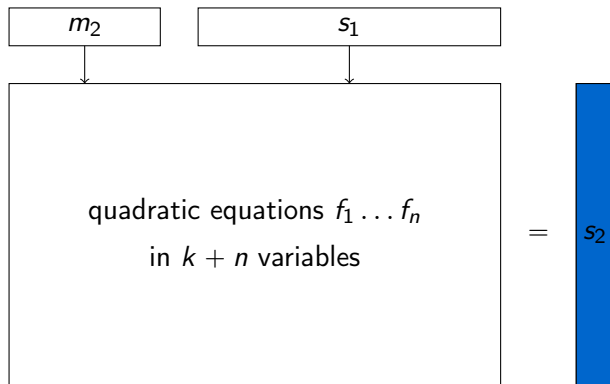


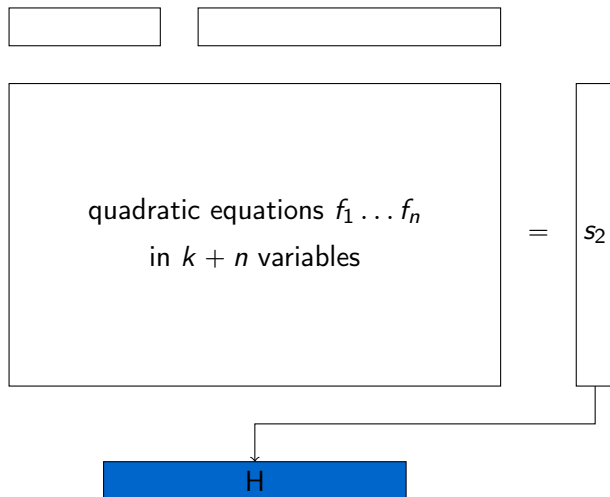












Problem: Easy to find collisions!

$$f(m, IV) = f(m', IV')$$

$$f(m, IV) = f(m + a, IV + b)$$

$$f(m, IV) - f(m + a, IV + b) = 0$$

Problem: Easy to find collisions!

$$f(m, IV) = f(m', IV')$$

$$f(m, IV) = f(m + a, IV + b)$$

$$f(m, IV) - f(m + a, IV + b) = 0$$

$$f_0(x) = c_{2,1}x_2x_1 + c_{2,0}x_2x_0 + c_{1,0}x_1x_0 + c_2x_2 + c_1x_1 + c_0x_0 + c$$

Problem: Easy to find collisions!

$$f(m, IV) = f(m', IV')$$

$$f(m, IV) = f(m + a, IV + b)$$

$$f(m, IV) - f(m + a, IV + b) = 0$$

$$f_0(x) = c_{2,1}x_2x_1 + c_{2,0}x_2x_0 + c_{1,0}x_1x_0 + c_2x_2 + c_1x_1 + c_0x_0 + c$$

$$f_0(x) - f_0(x + a) = c_{2,1}x_2x_1 + c_{2,0}x_2x_0 + c_{1,0}x_1x_0 + c_2x_2 + c_1x_1 + c_0x_0 + c \\ - (c_{2,1}(x_2 + a_2)(x_1 + a_1) + \dots c_2(x_2 + a_2) + \dots + c)$$

Problem: Easy to find collisions!

$$f(m, IV) = f(m', IV')$$

$$f(m, IV) = f(m + a, IV + b)$$

$$f(m, IV) - f(m + a, IV + b) = 0$$

$$f_0(x) = c_{2,1}x_2x_1 + c_{2,0}x_2x_0 + c_{1,0}x_1x_0 + c_2x_2 + c_1x_1 + c_0x_0 + c$$

$$f_0(x) - f_0(x + a) = c_{2,1}x_2x_1 + c_{2,0}x_2x_0 + c_{1,0}x_1x_0 + c_2x_2 + c_1x_1 + c_0x_0 + c \\ - (c_{2,1}(x_2 + a_2)(x_1 + a_1) + \dots c_2(x_2 + a_2) + \dots + c)$$

$$f_0(x) - f_0(x + a) = c_{2,1}x_2x_1 + c_{2,0}x_2x_0 + c_{1,0}x_1x_0 + c_2x_2 + c_1x_1 + c_0x_0 + c \\ - (c_{2,1}(x_2x_1 + a_1x_2 + a_2x_1 + a_1a_2) + \dots c_2x_2 + c_2a_2 + \dots + c)$$

Problem: Easy to find collisions!

$$f(m, IV) = f(m', IV')$$

$$f(m, IV) = f(m + a, IV + b)$$

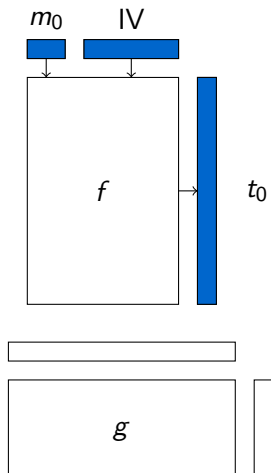
$$f(m, IV) - f(m + a, IV + b) = 0$$

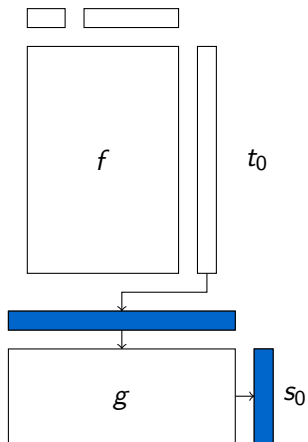
$$f_0(x) = c_{2,1}x_2x_1 + c_{2,0}x_2x_0 + c_{1,0}x_1x_0 + c_2x_2 + c_1x_1 + c_0x_0 + c$$

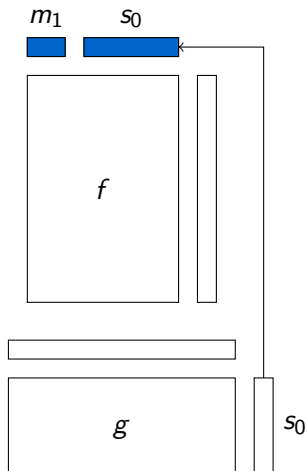
$$f_0(x) - f_0(x + a) = c_{2,1}x_2x_1 + c_{2,0}x_2x_0 + c_{1,0}x_1x_0 + c_2x_2 + c_1x_1 + c_0x_0 + c - (c_{2,1}(x_2 + a_2)(x_1 + a_1) + \dots c_2(x_2 + a_2) + \dots + c)$$

$$f_0(x) - f_0(x + a) = c_{2,1}x_2x_1 + c_{2,0}x_2x_0 + c_{1,0}x_1x_0 + c_2x_2 + c_1x_1 + c_0x_0 + c - (c_{2,1}(x_2x_1 + a_1x_2 + a_2x_1 + a_1a_2) + \dots c_2x_2 + c_2a_2 + \dots + c)$$

⇒ Underdefined linear system of $k + n$ variables and n equations!







Example (MQ-HASH):

$$f : \mathbb{F}_2^{n+k} \rightarrow \mathbb{F}_2^r$$

$$g : \mathbb{F}_2^r \rightarrow \mathbb{F}_2^n$$

$$H : (g \circ f)(s_1, \dots, s_n, m_1, \dots, m_k)$$

MQ-HASH: $k = 32$, $n = 160$ and $r = 464$.

Composition of functions with known inverse:

Secretly choose f, g, h with known inverse functions f^{-1}, g^{-1}, h^{-1} .

Release $F = f \circ g \circ h$ as public key and h^{-1}, g^{-1}, f^{-1} as private key.

Composition of functions with known inverse:

Secretly choose f, g, h with known inverse functions f^{-1}, g^{-1}, h^{-1} .

Release $F = f \circ g \circ h$ as public key and h^{-1}, g^{-1}, f^{-1} as private key.

Example:

Choose $f = (f_1, \dots, f_n), h = (h_1, \dots, h_n)$ as sets of independent linear equations and

$$g(g_1, \dots, g_n) = \begin{pmatrix} g_1 : & x_1, \\ g_2 : & x_2 + p_2(x_1), \\ g_3 : & x_3 + p_3(x_1, x_2), \\ & \dots \\ g_4 : & x_n + p_4(x_1, \dots, x_{n-1}) \end{pmatrix},$$

with p_i quadratic in x_1, \dots, x_i .

Example:

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

Example:

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$F = f \circ g \circ h = \begin{pmatrix} x_3 x_2 + x_3 x_1 + x_2 x_1 + x_4 + x_3 + x_2 + x_1 \\ x_4 x_3 + x_4 x_1 + x_3 x_2 + x_2 x_1 + x_4 + 1 \\ x_4 x_3 + x_4 x_1 + x_3 x_1 + x_2 + 1 \\ x_3 x_2 + x_3 x_1 + x_2 x_1 + x_4 + x_1 \end{pmatrix}$$

Example (Encryption):

$$F = \begin{pmatrix} x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 \\ x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 + 1 \\ x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 \\ x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 \end{pmatrix}$$

$$F(1,0,0,1) = \begin{pmatrix} 0 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 + 1 + 0 + 0 + 1 \\ 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 + 0 \cdot 1 + 1 + 1 \\ 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 + 0 + 1 \\ 0 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 + 1 + 1 \end{pmatrix} = (0, 1, 0, 0)$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$f^{-1} = \begin{pmatrix} y_4 + y_3 + y_2 \\ y_3 + y_2 + y_1 + 1 \\ y_4 + y_3 + y_2 + y_1 + 1 \\ y_3 + y_1 + 1 \end{pmatrix}$$

$$f^{-1}(0, 1, 0, 0) = (1, 0, 0, 1)$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 + (1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 + (0 \cdot 1 + 0) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 + (0 \cdot 1 + 0 \cdot 0 + 1) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 + 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$g^{-1}(1, 0, 0, 1) = (1, 0, 0, 0)$$

Example (Decryption):

$$f = \begin{pmatrix} x_3 + x_1 + 1 \\ x_4 + x_2 \\ x_4 + x_3 + x_1 \\ x_3 + x_2 \end{pmatrix}, g = \begin{pmatrix} x_1 \\ x_2 + (x_1 + 1) \\ x_3 + (x_2 x_1 + x_2) \\ x_4 + (x_3 x_1 + x_3 x_2 + x_1) \end{pmatrix}, h = \begin{pmatrix} x_2 + x_1 \\ x_3 + x_2 \\ x_4 + x_2 + 1 \\ x_4 + x_2 + x_1 \end{pmatrix}.$$

$$h^{-1} = \begin{pmatrix} y_4 + y_3 + 1 \\ y_4 + y_3 + y_1 + 1 \\ y_4 + y_2 + y_3 + y_1 + 1 \\ y_4 + y_1 \end{pmatrix}$$

$$h^{-1}(1, 0, 0, 0) = (1, 0, 0, 1)$$

Attention!

$$g(g_1, \dots, g_n) = \begin{pmatrix} g_1 : & x_1, \\ g_2 : & x_2 + p_2(x_1), \\ g_3 : & x_3 + p_3(x_1, x_2), \\ & \dots \\ g_4 : & x_n + p_4(x_1, \dots, x_{n-1}) \end{pmatrix}$$

Attention!

$$g(g_1, \dots, g_n) = \begin{pmatrix} g_1 : & x_1, \\ g_2 : & x_2 + p_2(x_1), \\ g_3 : & x_3 + p_3(x_1, x_2), \\ & \dots \\ g_4 : & x_n + p_4(x_1, \dots, x_{n-1}) \end{pmatrix}$$

$f \circ g \circ h$ is **not** a hard instance of $\mathcal{MQ}\text{-}\mathbb{F}_2$
due to the linearity of g_1 and g_2 !

Attention!

$$g(g_1, \dots, g_n) = \begin{pmatrix} g_1 : & x_1, \\ g_2 : & x_2 + p_2(x_1), \\ g_3 : & x_3 + p_3(x_1, x_2), \\ & \dots \\ g_4 : & x_n + p_4(x_1, \dots, x_{n-1}) \end{pmatrix}$$

$f \circ g \circ h$ is **not** a hard instance of $\mathcal{MQ}\text{-}\mathbb{F}_2$
due to the linearity of g_1 and g_2 !

Solution:

Make composition more complicated; this is ongoing research.

Attention!

$$g(g_1, \dots, g_n) = \begin{pmatrix} g_1 : & x_1, \\ g_2 : & x_2 + p_2(x_1), \\ g_3 : & x_3 + p_3(x_1, x_2), \\ & \dots \\ g_4 : & x_n + p_4(x_1, \dots, x_{n-1}) \end{pmatrix}$$

$f \circ g \circ h$ is **not** a hard instance of $\mathcal{MQ}\text{-}\mathbb{F}_2$
due to the linearity of g_1 and g_2 !

Solution:

Make composition more complicated; this is ongoing research.

All asymmetric $\mathcal{MQ}\text{-}\mathbb{F}_2$ schemes that have been proposed so far
have been broken!

Basic scheme:

- ▶ Signing: Encrypt message hash with private key.
- ▶ Verification: Decrypt signature with public key and compare to message hash.

Basic scheme:

- ▶ Signing: Encrypt message hash with private key.
- ▶ Verification: Decrypt signature with public key and compare to message hash.

No secure multivariate public key system \rightarrow no secure signature scheme...

Basic scheme:

- ▶ Signing: Encrypt message hash with private key.
- ▶ Verification: Decrypt signature with public key and compare to message hash.

No secure multivariate public key system \rightarrow no secure signature scheme...

Wrong!

There actually are secure multivariate signature schemes that are not based on public key encryption.

Example (Oil and Vinegar):

Private key:

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, g = \begin{pmatrix} x_6x_1 + x_5x_2 + x_4x_2 + x_2x_1 + x_4 + x_3 \\ x_4x_1 + x_3x_2 + x_4 + x_1 + 1 \\ x_6x_3 + x_5x_3 + x_3x_2 + x_6 + x_5 + x_1 + 1 \end{pmatrix}$$

Example (Oil and Vinegar):

Private key:

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, g = \begin{pmatrix} x_6x_1 + x_5x_2 + x_4x_2 + x_2x_1 + x_4 + x_3 \\ x_4x_1 + x_3x_2 + x_4 + x_1 + 1 \\ x_6x_3 + x_5x_3 + x_3x_2 + x_6 + x_5 + x_1 + 1 \end{pmatrix}$$

Public key: $g \circ f =$

$$\begin{pmatrix} x_6x_5 + x_6x_4 + x_6x_3 + x_5x_3 + x_4x_3 + x_4x_1 + x_3x_1 + x_4 + x_2 \\ x_6x_5 + x_6x_4 + x_6x_3 + x_6x_2 + x_5x_3 + x_5x_1 + x_4x_3 + x_3x_2 + x_3x_1 + x_6 + x_1 \\ x_6x_5 + x_6x_3 + x_5x_3 + x_5x_2 + x_3x_2 + x_3 + x_1 \end{pmatrix}$$

Example (Oil and Vinegar):

Private key:

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, g = \begin{pmatrix} x_6x_1 + x_5x_2 + x_4x_2 + x_2x_1 + x_4 + x_3 \\ x_4x_1 + x_3x_2 + x_4 + x_1 + 1 \\ x_6x_3 + x_5x_3 + x_3x_2 + x_6 + x_5 + x_1 + 1 \end{pmatrix}$$

Public key: $g \circ f =$

$$\begin{pmatrix} x_6x_5 + x_6x_4 + x_6x_3 + x_5x_3 + x_4x_3 + x_4x_1 + x_3x_1 + x_4 + x_2 \\ x_6x_5 + x_6x_4 + x_6x_3 + x_6x_2 + x_5x_3 + x_5x_1 + x_4x_3 + x_3x_2 + x_3x_1 + x_6 + x_1 \\ x_6x_5 + x_6x_3 + x_5x_3 + x_5x_2 + x_3x_2 + x_3 + x_1 \end{pmatrix}$$

- ▶ Sign hash h : $s = f^{-1} \circ g^{-1}(h)$.
- ▶ Verify s : $h' = g \circ f(s)$; $h' = h$?

Example (Signing):

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, g = \begin{pmatrix} x_6x_1 + x_5x_2 + x_4x_2 + x_2x_1 + x_4 + x_3 \\ x_4x_1 + x_3x_2 + x_4 + x_1 + 1 \\ x_6x_3 + x_5x_3 + x_3x_2 + x_6 + x_5 + x_1 + 1 \end{pmatrix}$$

Example (Signing):

Oil variables: x_6, x_5, x_4 ; Vinegar variables: x_3, x_2, x_1 .

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, g = \begin{pmatrix} x_6 x_1 + x_5 x_2 + x_4 x_2 + x_2 x_1 + x_4 + x_3 \\ x_4 x_1 + x_3 x_2 + x_4 + x_1 + 1 \\ x_6 x_3 + x_5 x_3 + x_3 x_2 + x_6 + x_5 + x_1 + 1 \end{pmatrix}$$

Example (Signing):

Oil variables: x_6, x_5, x_4 ; Vinegar variables: x_3, x_2, x_1 .

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, g = \begin{pmatrix} x_6x_1 + x_5x_2 + x_4x_2 + x_2x_1 + x_4 + x_3 \\ x_4x_1 + x_3x_2 + x_4 + x_1 + 1 \\ x_6x_3 + x_5x_3 + x_3x_2 + x_6 + x_5 + x_1 + 1 \end{pmatrix}$$

Randomly choose x_3, x_2, x_1 , e.g., $x_3 = 0, x_2 = 1, x_1 = 0$:

$$g' = \begin{pmatrix} 0x_6 + 1x_5 + 1x_4 + 1 \cdot 0 + x_4 + 0 \\ 0x_4 + 0 \cdot 1 + x_4 + 0 + 1 \\ 0x_6 + 0x_5 + 0 \cdot 1 + x_6 + x_5 + 0 + 1 \end{pmatrix}$$

Example (Signing):

Oil variables: x_6, x_5, x_4 ; Vinegar variables: x_3, x_2, x_1 .

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, g = \begin{pmatrix} x_6x_1 + x_5x_2 + x_4x_2 + x_2x_1 + x_4 + x_3 \\ x_4x_1 + x_3x_2 + x_4 + x_1 + 1 \\ x_6x_3 + x_5x_3 + x_3x_2 + x_6 + x_5 + x_1 + 1 \end{pmatrix}$$

Randomly choose x_3, x_2, x_1 , e.g., $x_3 = 0, x_2 = 1, x_1 = 0$:

$$g' = \begin{pmatrix} 0x_6 + 1x_5 + 1x_4 + 1 \cdot 0 + x_4 + 0 \\ 0x_4 + 0 \cdot 1 + x_4 + 0 + 1 \\ 0x_6 + 0x_5 + 0 \cdot 1 + x_6 + x_5 + 0 + 1 \end{pmatrix} = \begin{pmatrix} x_5 \\ x_4 + 1 \\ x_6 + x_5 + 1 \end{pmatrix}$$

Example (Signing):

Oil variables: x_6, x_5, x_4 ; Vinegar variables: x_3, x_2, x_1 .

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, g = \begin{pmatrix} x_6x_1 + x_5x_2 + x_4x_2 + x_2x_1 + x_4 + x_3 \\ x_4x_1 + x_3x_2 + x_4 + x_1 + 1 \\ x_6x_3 + x_5x_3 + x_3x_2 + x_6 + x_5 + x_1 + 1 \end{pmatrix}$$

Sign $h = (1, 1, 0)$:

$$x_5 = 1$$

$$x_4 + 1 = 1$$

$$x_6 + x_5 + 1 = 0$$

Example (Signing):

Oil variables: x_6, x_5, x_4 ; Vinegar variables: x_3, x_2, x_1 .

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, g = \begin{pmatrix} x_6 x_1 + x_5 x_2 + x_4 x_2 + x_2 x_1 + x_4 + x_3 \\ x_4 x_1 + x_3 x_2 + x_4 + x_1 + 1 \\ x_6 x_3 + x_5 x_3 + x_3 x_2 + x_6 + x_5 + x_1 + 1 \end{pmatrix}$$

Sign $h = (1, 1, 0)$:

$$x_5 = 1$$

$$x_4 = 0$$

$$x_6 = 0$$

Example (Signing):

Oil variables: x_6, x_5, x_4 ; Vinegar variables: x_3, x_2, x_1 .

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, g = \begin{pmatrix} x_6 x_1 + x_5 x_2 + x_4 x_2 + x_2 x_1 + x_4 + x_3 \\ x_4 x_1 + x_3 x_2 + x_4 + x_1 + 1 \\ x_6 x_3 + x_5 x_3 + x_3 x_2 + x_6 + x_5 + x_1 + 1 \end{pmatrix}$$

Sign $h = (1, 1, 0)$:

$$x_5 = 1$$

$$x_4 = 0$$

$$x_6 = 0$$

$$g^{-1}(1, 1, 0) = (0, 1, 0, 0, 1, 0)$$

Example (Signing):

$$g^{-1}(1, 1, 0) = (0, 1, 0, 0, 1, 0)$$

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix},$$

Example (Signing):

$$g^{-1}(1, 1, 0) = (0, 1, 0, 0, 1, 0)$$

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, f^{-1} = \begin{pmatrix} x_2 + x_1 + 1 \\ x_6 + x_5 + x_3 + x_2 + x_1 + 1 \\ x_6 + x_3 + x_2 + x_1 \\ x_6 + x_5 + x_4 + x_3 + x_2 + x_1 \\ x_6 + x_2 + x_1 + 1 \\ x_6 + x_3 + x_2 + 1 \end{pmatrix}$$

Example (Signing):

$$g^{-1}(1, 1, 0) = (0, 1, 0, 0, 1, 0)$$

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, f^{-1} = \begin{pmatrix} x_2 + x_1 + 1 \\ x_6 + x_5 + x_3 + x_2 + x_1 + 1 \\ x_6 + x_3 + x_2 + x_1 \\ x_6 + x_5 + x_4 + x_3 + x_2 + x_1 \\ x_6 + x_2 + x_1 + 1 \\ x_6 + x_3 + x_2 + 1 \end{pmatrix}$$

$$f^{-1}(0, 1, 0, 0, 1, 0) = (0, 0, 0, 1, 1, 0)$$

Example (Signing):

$$g^{-1}(1, 1, 0) = (0, 1, 0, 0, 1, 0)$$

$$f = \begin{pmatrix} x_6 + x_3 + 1 \\ x_6 + x_3 + x_1 \\ x_5 + x_3 + 1 \\ x_4 + x_2 + 1 \\ x_3 + x_2 + 1 \\ x_5 + x_1 \end{pmatrix}, f^{-1} = \begin{pmatrix} x_2 + x_1 + 1 \\ x_6 + x_5 + x_3 + x_2 + x_1 + 1 \\ x_6 + x_3 + x_2 + x_1 \\ x_6 + x_5 + x_4 + x_3 + x_2 + x_1 \\ x_6 + x_2 + x_1 + 1 \\ x_6 + x_3 + x_2 + 1 \end{pmatrix}$$

$$f^{-1}(0, 1, 0, 0, 1, 0) = (0, 0, 0, 1, 1, 0)$$

$$s = f^{-1}g^{-1}(1, 1, 0) = (0, 0, 0, 1, 1, 0)$$

Example (Verification):

$$h = (1, 1, 0), s = (0, 0, 0, 1, 1, 0)$$

Example (Verification):

$$h = (1, 1, 0), s = (0, 0, 0, 1, 1, 0)$$

$$g \circ f =$$

$$\begin{pmatrix} x_6 x_5 + x_6 x_4 + x_6 x_3 + x_5 x_3 + x_4 x_3 + x_4 x_1 + x_3 x_1 + x_4 + x_2 \\ x_6 x_5 + x_6 x_4 + x_6 x_3 + x_6 x_2 + x_5 x_3 + x_5 x_1 + x_4 x_3 + x_3 x_2 + x_3 x_1 + x_6 + x_1 \\ x_6 x_5 + x_6 x_3 + x_5 x_3 + x_5 x_2 + x_3 x_2 + x_3 + x_1 \end{pmatrix}$$

Example (Verification):

$$h = (1, 1, 0), s = (0, 0, 0, 1, 1, 0)$$

$$g \circ f =$$

$$\begin{pmatrix} x_6x_5 + x_6x_4 + x_6x_3 + x_5x_3 + x_4x_3 + x_4x_1 + x_3x_1 + x_4 + x_2 \\ x_6x_5 + x_6x_4 + x_6x_3 + x_6x_2 + x_5x_3 + x_5x_1 + x_4x_3 + x_3x_2 + x_3x_1 + x_6 + x_1 \\ x_6x_5 + x_6x_3 + x_5x_3 + x_5x_2 + x_3x_2 + x_3 + x_1 \end{pmatrix}$$

$$h' = g \circ f(0, 0, 0, 1, 1, 0) = (1, 1, 0)$$

Public key encryption scheme?

Oil and Vinegar can not be used as public key encryption scheme due to the randomness of the vinegar variables.

Public key encryption scheme?

Oil and Vinegar can not be used as public key encryption scheme due to the randomness of the vinegar variables.

Oil and Vinegar is broken!

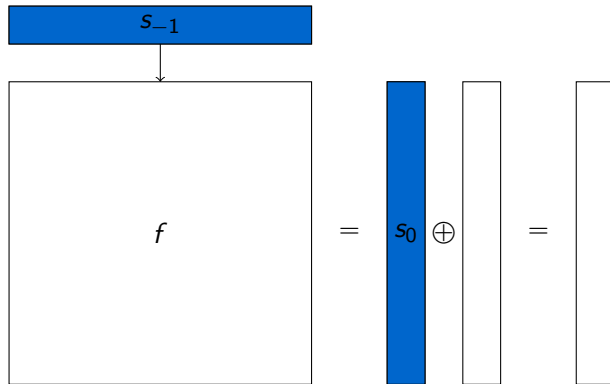
Public key encryption scheme?

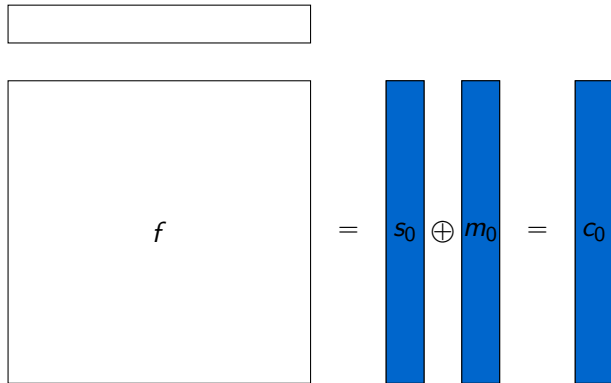
Oil and Vinegar can not be used as public key encryption scheme due to the randomness of the vinegar variables.

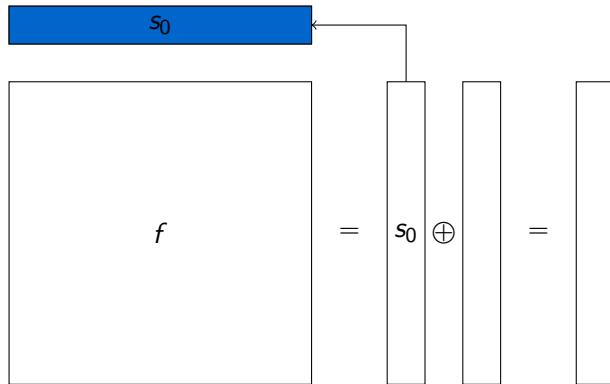
Oil and Vinegar is broken!

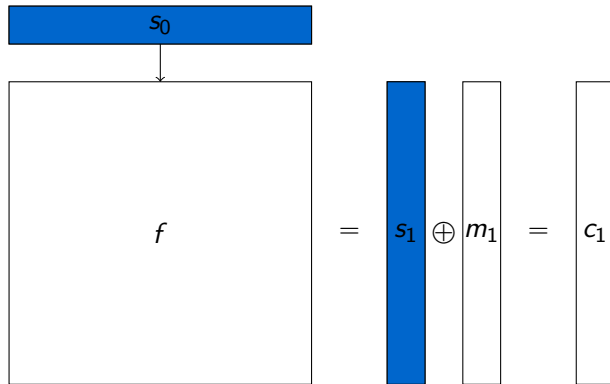
There are variations of Oil and Vinegar, e.g., Unbalanced Oil and Vinegar (UOB), that are (not yet) broken.

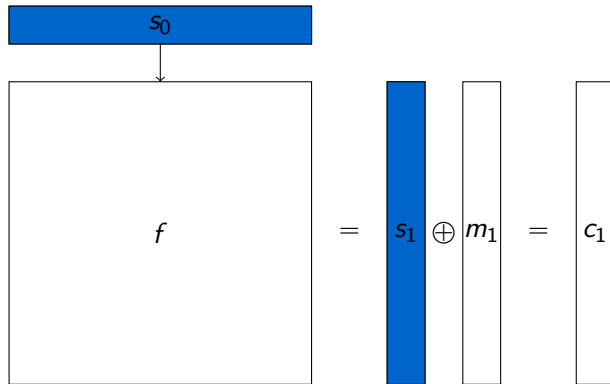
Pre-process symmetric key and IV to obtain initial state s_{-1} .





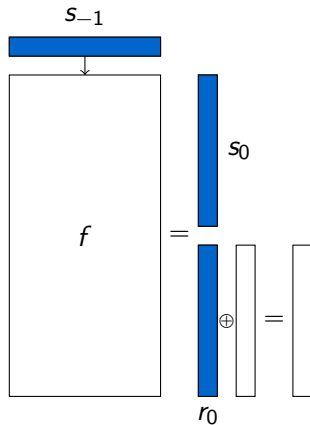


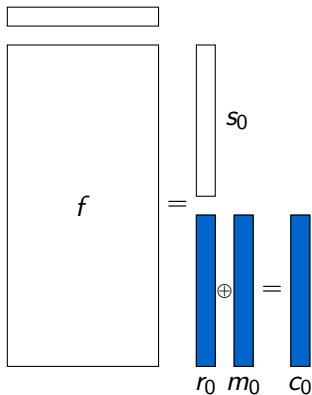


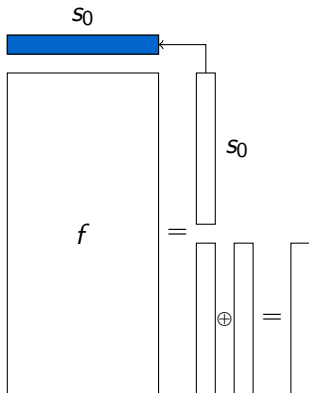


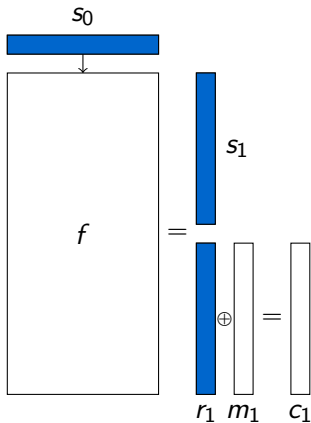
Easy to obtain key stream with a single known plain text block!

Pre-process symmetric key and IV to obtain initial state s_{-1} .









QUAD stream cipher

Provable secure!

QUAD stream cipher

“Provable secure!”

Suggested parameters QUAD(256,20,20) have been broken!

QUAD stream cipher

“Provable secure!”

Suggested parameters QUAD(256,20,20) have been broken!

Parameters that are still considered secure:

QUAD(2,160,160), QUAD(2,256,256), QUAD(2,350,350), ...

Algebraic Cryptanalysis:

Obtain a system of multivariate polynomial equations with the secret among the variables.

- ▶ Naturally breaks multivariate crypto schemes,
- ▶ does not break AES as first advertised,
- ▶ but does break, e.g., KeeLoq.

Example:

$$F = \begin{pmatrix} x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 \\ x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 + 1 \\ x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 \\ x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 \end{pmatrix}$$

Find x for $F(x) = (0, 1, 0, 0)$.

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 + 1 = 1 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 + 1 = 1 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_2 + 1 = 0 \quad (2) + (3) = \quad (5)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_2 + 1 = 0 \quad (2) + (3) = \quad (5)$$

$$x_2 + x_1 + 1 = 0 \quad (4) + (5) = \quad (6)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_2 + 1 = 0 \quad (2) + (3) = \quad (5)$$

$$x_2 + x_1 + 1 = 0 \quad (4) + (5) = \quad (6)$$

$$x_3 + x_2 = 0 \quad (1) + (4) = \quad (7)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_2 + 1 = 0 \quad (2) + (3) = \quad (5)$$

$$x_2 + x_1 + 1 = 0 \quad (4) + (5) = \quad (6)$$

$$x_3 + x_2 = 0 \quad (1) + (4) = \quad (7)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 + x_3 = 0 \quad x_3(1) + (2) = \quad (8)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_2 + 1 = 0 \quad (2) + (3) = \quad (5)$$

$$x_2 + x_1 + 1 = 0 \quad (4) + (5) = \quad (6)$$

$$x_3 + x_2 = 0 \quad (1) + (4) = \quad (7)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 + x_3 = 0 \quad x_3(1) + (2) = \quad (8)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_3x_1 + x_2 + 1 = 0 \quad x_3(4) + (3) = \quad (9)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_2 + 1 = 0 \quad (2) + (3) = \quad (5)$$

$$x_2 + x_1 + 1 = 0 \quad (4) + (5) = \quad (6)$$

$$x_3 + x_2 = 0 \quad (1) + (4) = \quad (7)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 + x_3 = 0 \quad x_3(1) + (2) = \quad (8)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_3x_1 + x_2 + 1 = 0 \quad x_3(4) + (3) = \quad (9)$$

$$x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + 1 = 0 \quad (8) + (9) = \quad (10)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_2 + 1 = 0 \quad (2) + (3) = \quad (5)$$

$$x_2 + x_1 + 1 = 0 \quad (4) + (5) = \quad (6)$$

$$x_3 + x_2 = 0 \quad (1) + (4) = \quad (7)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 + x_3 = 0 \quad x_3(1) + (2) = \quad (8)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_3x_1 + x_2 + 1 = 0 \quad x_3(4) + (3) = \quad (9)$$

$$x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + 1 = 0 \quad (8) + (9) = \quad (10)$$

$$x_4 + x_3 + x_2 + 1 = 0 \quad x_1(7) + (10) = \quad (11)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_2 + 1 = 0 \quad (2) + (3) = \quad (5)$$

$$x_2 + x_1 + 1 = 0 \quad (4) + (5) = \quad (6)$$

$$x_3 + x_2 = 0 \quad (1) + (4) = \quad (7)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 + x_3 = 0 \quad x_3(1) + (2) = \quad (8)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_3x_1 + x_2 + 1 = 0 \quad x_3(4) + (3) = \quad (9)$$

$$x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + 1 = 0 \quad (8) + (9) = \quad (10)$$

$$x_4 + x_3 + x_2 + 1 = 0 \quad x_1(7) + (10) = \quad (11)$$

$$x_4 + 1 = 0 \quad (7) + (11) = \quad (12)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_2 + 1 = 0 \quad (2) + (3) = \quad (5)$$

$$x_2 + x_1 + 1 = 0 \quad (4) + (5) = \quad (6)$$

$$x_3 + x_2 = 0 \quad (1) + (4) = \quad (7)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 + x_3 = 0 \quad x_3(1) + (2) = \quad (8)$$

$$x_3x_2x_1 + x_4x_1 + x_3x_2 + x_3x_1 + x_2 + 1 = 0 \quad x_3(4) + (3) = \quad (9)$$

$$x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + 1 = 0 \quad (8) + (9) = \quad (10)$$

$$x_4 + x_3 + x_2 + 1 = 0 \quad x_1(7) + (10) = \quad (11)$$

$$x_4 = 1 \quad (7) + (11) = \quad (12)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_2 + x_1 + 1 = 0 \quad (6)$$

$$x_3 + x_2 = 0 \quad (7)$$

$$x_4 = 1 \quad (12)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_2 + x_1 + 1 = 0 \quad (6)$$

$$x_3 + x_2 = 0 \quad (7)$$

$$x_4 = 1 \quad (12)$$

$$x_4x_3x_1 + x_4x_3 + x_2x_1 + x_4 + x_3 + x_1 = 0 \quad x_3(3) + (4) = \quad (13)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_2 + x_1 + 1 = 0 \quad (6)$$

$$x_3 + x_2 = 0 \quad (7)$$

$$x_4 = 1 \quad (12)$$

$$x_4x_3x_1 + x_4x_3 + x_2x_1 + x_4 + x_3 + x_1 = 0 \quad x_3(3) + (4) = (13)$$

$$x_4x_3x_1 + x_3x_2x_1 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1) + x_3(2) = (14)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_2 + x_1 + 1 = 0 \quad (6)$$

$$x_3 + x_2 = 0 \quad (7)$$

$$x_4 = 1 \quad (12)$$

$$x_4x_3x_1 + x_4x_3 + x_2x_1 + x_4 + x_3 + x_1 = 0 \quad x_3(3) + (4) = \quad (13)$$

$$x_4x_3x_1 + x_3x_2x_1 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1) + x_3(2) = \quad (14)$$

$$x_2 = 0 \quad (14) + (13) + (9) + x_4(7) + x_4(6) + x_2(7) + (12) = \quad (15)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_2 + x_1 + 1 = 0 \quad (6)$$

$$x_3 + x_2 = 0 \quad (7)$$

$$x_4 = 1 \quad (12)$$

$$x_4x_3x_1 + x_4x_3 + x_2x_1 + x_4 + x_3 + x_1 = 0 \quad x_3(3) + (4) = \quad (13)$$

$$x_4x_3x_1 + x_3x_2x_1 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1) + x_3(2) = \quad (14)$$

$$x_2 = 0 \quad (14) + (13) + (9) + x_4(7) + x_4(6) + x_2(7) + (12) = \quad (15)$$

$$x_3 = 0 \quad (7) + (15) = \quad (16)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_2 + x_1 + 1 = 0 \quad (6)$$

$$x_3 + x_2 = 0 \quad (7)$$

$$x_4 = 1 \quad (12)$$

$$x_4x_3x_1 + x_4x_3 + x_2x_1 + x_4 + x_3 + x_1 = 0 \quad x_3(3) + (4) = \quad (13)$$

$$x_4x_3x_1 + x_3x_2x_1 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1) + x_3(2) = \quad (14)$$

$$x_2 = 0 \quad (14) + (13) + (9) + x_4(7) + x_4(6) + x_2(7) + (12) = \quad (15)$$

$$x_3 = 0 \quad (7) + (15) = \quad (16)$$

$$x_1 = 1 \quad (6) + (15) = \quad (17)$$

Example:

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1)$$

$$x_4x_3 + x_4x_1 + x_3x_2 + x_2x_1 + x_4 = 0 \quad (2)$$

$$x_4x_3 + x_4x_1 + x_3x_1 + x_2 + 1 = 0 \quad (3)$$

$$x_3x_2 + x_3x_1 + x_2x_1 + x_4 + x_1 = 0 \quad (4)$$

$$x_2 + x_1 + 1 = 0 \quad (6)$$

$$x_3 + x_2 = 0 \quad (7)$$

$$x_4 = 1 \quad (12)$$

$$x_4x_3x_1 + x_4x_3 + x_2x_1 + x_4 + x_3 + x_1 = 0 \quad x_3(3) + (4) = \quad (13)$$

$$x_4x_3x_1 + x_3x_2x_1 + x_3x_1 + x_2x_1 + x_4 + x_3 + x_2 + x_1 = 0 \quad (1) + x_3(2) = \quad (14)$$

$$x_2 = 0 \quad (14) + (13) + (9) + x_4(7) + x_4(6) + x_2(7) + (12) = \quad (15)$$

$$x_3 = 0 \quad (7) + (15) = \quad (16)$$

$$x_1 = 1 \quad (6) + (15) = \quad (17)$$

Algorithm due to Buchberger:

- ▶ Transform set of equations to a Gröbner basis; obtain solution of the system from the final representation.
- ▶ During computation, the maximum degree increases to $D > 2$.
- ▶ There are several improvements of Buchbergers algorithm, e.g., Faugère's F_4 and F_5 (implemented, e.g., in Magma).

The XL algorithm

- ▶ *XL* is an acronym for *extended linearization*:
 - ▶ *extend* a quadratic system by multiplying with appropriate monomials,
 - ▶ *linearize* by treating each monomial as an independent variable,
 - ▶ solve the linearized system.
- ▶ Special case of Gröbner basis algorithms.
- ▶ First suggested by Lazard (1983).
- ▶ Reinvented by Courtois, Klimov, Patarin, and Shamir (2000).
- ▶ More “easy” to parallelize compared to Gröbner basis solvers.

Basic idea:

For $b \in \mathbb{N}^n$ denote by x^b the monomial $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n}$ and by $|b| = b_1 + b_2 + \dots + b_n$ the total degree of x^b .

given: finite field $K = \mathbb{F}_q$

system \mathcal{A} of m multivariate quadratic equations:

$$l_1 = l_2 = \dots = l_m = 0, \quad l_i \in K[x_1, x_2, \dots, x_n]$$

choose: operational degree $D \in \mathbb{N}$

extend: system \mathcal{A} to the system

$$\mathcal{R}^{(D)} = \{x^b l_i = 0 : |b| \leq D - 2, l_i \in \mathcal{A}\}$$

linearize: consider x^d , $d \leq D$ a new variable, obtain linear system \mathcal{M}

solve: linear system \mathcal{M}

Basic idea:

For $b \in \mathbb{N}^n$ denote by x^b the monomial $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n}$ and by $|b| = b_1 + b_2 + \dots + b_n$ the total degree of x^b .

given: finite field $K = \mathbb{F}_q$

system \mathcal{A} of m multivariate quadratic equations:

$$l_1 = l_2 = \dots = l_m = 0, \quad l_i \in K[x_1, x_2, \dots, x_n]$$

choose: operational degree $D \in \mathbb{N}$ **How?**

extend: system \mathcal{A} to the system

$$\mathcal{R}^{(D)} = \{x^b l_i = 0 : |b| \leq D - 2, l_i \in \mathcal{A}\}$$

linearize: consider x^d , $d \leq D$ a new variable, obtain linear system \mathcal{M}

solve: linear system \mathcal{M}

Basic idea:

For $b \in \mathbb{N}^n$ denote by x^b the monomial $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n}$ and by $|b| = b_1 + b_2 + \dots + b_n$ the total degree of x^b .

given: finite field $K = \mathbb{F}_q$

system \mathcal{A} of m multivariate quadratic equations:

$$l_1 = l_2 = \dots = l_m = 0, \quad l_i \in K[x_1, x_2, \dots, x_n]$$

choose: operational degree $D \in \mathbb{N}$ **How?**

extend: system \mathcal{A} to the system

$$\mathcal{R}^{(D)} = \{x^b l_i = 0 : |b| \leq D - 2, l_i \in \mathcal{A}\}$$

linearize: consider x^d , $d \leq D$ a new variable, obtain linear system \mathcal{M}

solve: linear system \mathcal{M}

minimum degree D_0 for reliable termination (Yang and Chen):

$$D_0 := \min\{D : ((1 - \lambda)^{m-n-1} (1 + \lambda)^m)[D] \leq 0\}$$

Basic idea:

For $b \in \mathbb{N}^n$ denote by x^b the monomial $x_1^{b_1} x_2^{b_2} \dots x_n^{b_n}$ and by $|b| = b_1 + b_2 + \dots + b_n$ the total degree of x^b .

given: finite field $K = \mathbb{F}_q$

system \mathcal{A} of m multivariate quadratic equations:

$$l_1 = l_2 = \dots = l_m = 0, \quad l_i \in K[x_1, x_2, \dots, x_n]$$

choose: operational degree $D \in \mathbb{N}$ **How?**

extend: system \mathcal{A} to the system

$$\mathcal{R}^{(D)} = \{x^b l_i = 0 : |b| \leq D - 2, l_i \in \mathcal{A}\}$$

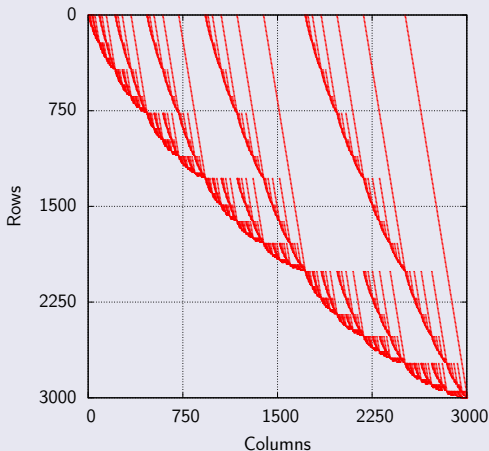
linearize: consider x^d , $d \leq D$ a new variable, obtain linear system \mathcal{M}

solve: linear system \mathcal{M} **How?**

minimum degree D_0 for reliable termination (Yang and Chen):

$$D_0 := \min\{D : ((1 - \lambda)^{m-n-1} (1 + \lambda)^m)[D] \leq 0\}$$

Solve the sparse linear system \mathcal{M} :



Use, e.g., the (block) Lanczos or the (block) Wiedemann algorithm.

Efficiency:

Gröbner basis solvers and XL are efficient for solving multivariate polynomial systems over *large* finite fields.

Efficiency:

Gröbner basis solvers and XL are efficient for solving multivariate polynomial systems over *large* finite fields.

Most Efficient Algorithm for \mathbb{F}_2 :

Brute-force search, testing all 2^n possible inputs.

Full-Evaluation Approach

- ▶ Evaluate the whole equation for each possible input.
- ▶ Time Complexity: $O(2^n n^2)$
- ▶ Memory Complexity: $O(n)$

Full-Evaluation Approach

- ▶ Evaluate the whole equation for each possible input.
- ▶ Time Complexity: $O(2^n n^2)$
- ▶ Memory Complexity: $O(n)$

Gray-Code Approach

- ▶ Only re-compute those parts of the equation that have changed.
- ▶ Enumerate input vector in Gray-code order.
- ▶ Update solution using the derivatives of the involved variables.
- ▶ Time Complexity: $O(2^n m)$
- ▶ Memory Complexity: $O(n^2 m)$

Trade computation for memory.

$$k = 01010_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 0$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01010_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 0$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01011_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 1$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01010_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 0$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01011_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 1$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01100_b; x_4 = 0, x_3 = 1, x_2 = 1, x_1 = 0, x_0 = 0$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01010_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 0$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01011_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 1$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01001_b \text{ in Gray-code order}$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01010_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 0$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01011_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 1$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01001_b \text{ in Gray-code order}$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$f = f(01011_b) - 0 \cdot 1 - 1 + 0 \cdot 0 + 0$$

$$k = 01010_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 0$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01011_b; x_4 = 0, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 1$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$k = 01001_b \text{ in Gray-code order}$$

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

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

$$f = f(01011_b) - 0 \cdot 1 - 1 + 0 \cdot 0 + 0$$

$$f = f(01011_b) + \frac{\partial f}{\partial x_1}(01001_b)$$

Full-Evaluation Approach

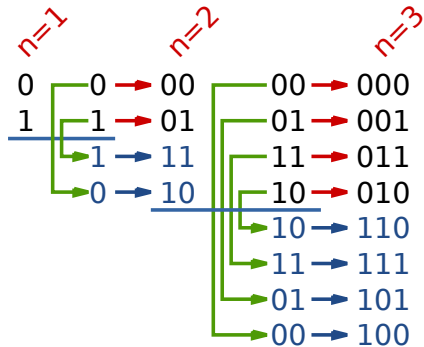
- ▶ Evaluate the whole equation for each possible input.
- ▶ Time Complexity: $O(2^n n^2)$
- ▶ Memory Complexity: $O(n)$

Gray-Code Approach

- ▶ Only re-compute those parts of the equation that have changed.
- ▶ Enumerate input vector in Gray-code order.
- ▶ Update solution using the derivatives of the involved variables.
- ▶ Time Complexity: $O(2^n m)$
- ▶ Memory Complexity: $O(n^2 m)$

Trade computation for memory.

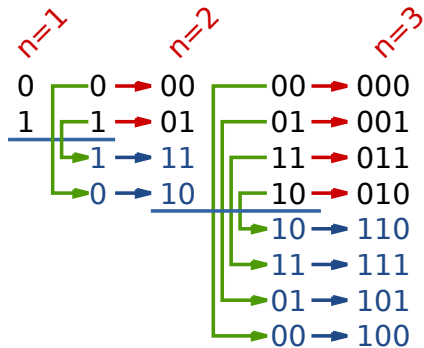
Gray Code



Binary to Gray:
 $(ctr \gg 1) \wedge ctr$

ctr	bin	gray
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

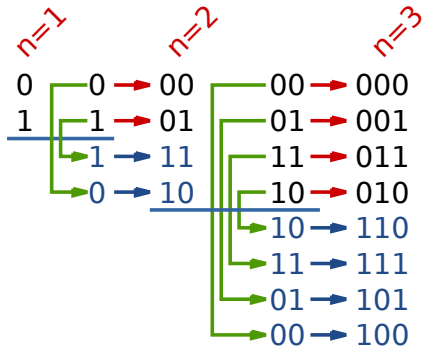
Gray Code



Binary to Gray:
 $(ctr \gg 1) \wedge ctr$

ctr	bin	gray
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

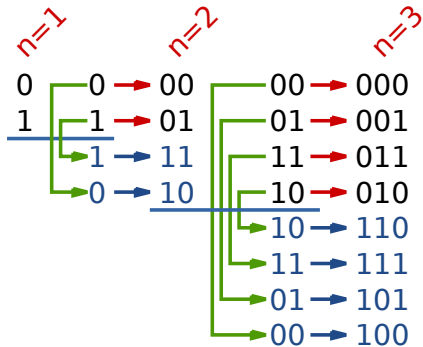
Gray Code



Binary to Gray:
 $(ctr \gg 1) \wedge ctr$

ctr	bin	gray
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

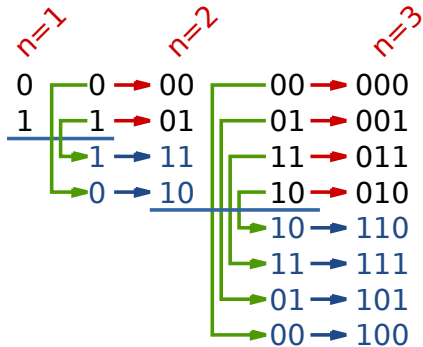
Gray Code



Binary to Gray:
 $(ctr \gg 1) \wedge ctr$

ctr	bin	gray
0	0000	0000
1	0001	0001
2	0010	0011
3	001 1	001 0
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

Gray Code

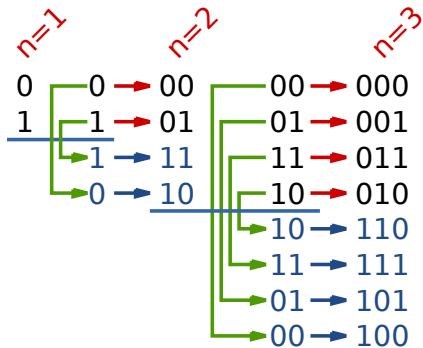


Binary to Gray:

$$(\text{ctr} \gg 1) \wedge \text{ctr}$$

ctr	bin	gray
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

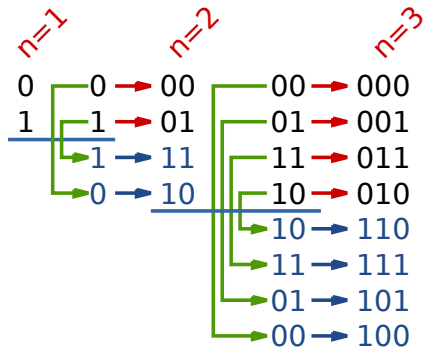
Gray Code



Binary to Gray:
 $(ctr \gg 1) \wedge ctr$

ctr	bin	gray
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

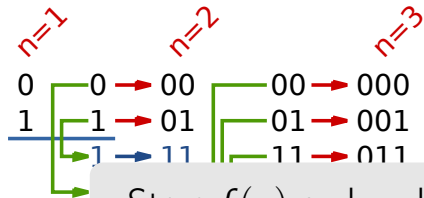
Gray Code



Binary to Gray:
 $(ctr \gg 1) \wedge ctr$

ctr	bin	gray
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

Gray Code



ctr	bin	gray
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111

Store $f(x)$ and update using $\frac{\partial f}{\partial x_i}(x)$;
 store $\frac{\partial f}{\partial x_i}(x)$ and update using $\frac{\partial^2 f}{\partial x_i \partial x_j}(x)$.

00 → 100

10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

Binary to Gray:

$(ctr \gg 1) \wedge ctr$

```
24: function EVAL( $s$ )
25:   while  $s.i < 2^n$  do
26:      $s.i \leftarrow s.i + 1$ ;
27:      $k_1 \leftarrow \text{BIT}_1(s.i)$ ;
28:      $k_2 \leftarrow \text{BIT}_2(s.i)$ ;
29:     if  $k_2$  valid then
30:        $s.d'[k_1] \leftarrow s.d'[k_1] \oplus s.d''[k_1, k_2]$ ;
31:     end if
32:      $s.y \leftarrow s.y \oplus s.d'[k_1]$ ;
33:     if  $s.y = 0$  then
34:       return  $\text{shr}(s.i, 1) \oplus s.i$ ;
35:     end if
36:   end while
37: end function
```

Fix i Variables for 2^i Parallel Instances:

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

e.g. $i = 2$:

$$f_{00_b} = 0 \cdot x_2 + 0 \cdot x_0 + x_2x_1 + 0 + x_1 + x_0 + 1$$

$$f_{01_b} = 0 \cdot x_2 + 1 \cdot x_0 + x_2x_1 + 1 + x_1 + x_0 + 1$$

$$f_{10_b} = 1 \cdot x_2 + 0 \cdot x_0 + x_2x_1 + 0 + x_1 + x_0 + 1$$

$$f_{11_b} = 1 \cdot x_2 + 1 \cdot x_0 + x_2x_1 + 1 + x_1 + x_0 + 1$$

2^i independent equations (systems)

Fix i Variables for 2^i Parallel Instances:

$$f = x_4x_2 + x_3x_0 + x_2x_1 + x_3 + x_1 + x_0 + 1$$

e.g. $i = 2$:

$$f_{00_b} = 0 \cdot x_2 + 0 \cdot x_0 + x_2x_1 + 0 + x_1 + x_0 + 1$$

$$f_{01_b} = 0 \cdot x_2 + 1 \cdot x_0 + x_2x_1 + 1 + x_1 + x_0 + 1$$

$$f_{10_b} = 1 \cdot x_2 + 0 \cdot x_0 + x_2x_1 + 0 + x_1 + x_0 + 1$$

$$f_{11_b} = 1 \cdot x_2 + 1 \cdot x_0 + x_2x_1 + 1 + x_1 + x_0 + 1$$

2^i independent equations (systems)
sharing the *same* quadratic terms!

80-bit Security:

Solving a system of 80 variables requires 1042 days on 65,536 Spartan-6 FPGAs at a total cost of about US\$40 million.

