cryptography

Article

Algebraic Cryptanalysis with MRHS Equations

Pavol Zajac

Department of Computer Science and Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava, Ilkovičova 3, 812 19 Bratislava, Slovakia; pavol.zajac@stuba.sk

Abstract: In this work, we survey the existing research in the area of algebraic cryptanalysis based on Multiple Right-Hand Sides (MRHS) equations (MRHS cryptanalysis). MRHS equation is a formal inclusion that contains linear combinations of variables on the left-hand side, and a potential set of values for these combinations on the right-hand side. We describe MRHS equation systems in detail, including the evolution of this representation. Then we provide an overview of the methods that can be used to solve MRHS equation systems. Finally, we explore the use of MRHS equation systems in algebraic cryptanalysis and survey existing experimental results.

Keywords: MRHS equation; algebraic cryptanalysis; MRHS solver

Citation: Zajac, P. Algebraic Cryptanalysis with MRHS Equations. *Cryptography* **2023**, *7*, 19. https://doi.org/10.3390/cryptography7020019

Academic Editor: Josef Pieprzyk

Received: 1 March 2023
Revised: 27 March 2023
Accepted: 28 March 2023
Published: 4 April 2023

1. Introduction

The basic concept of algebraic cryptanalysis was already introduced in the seminal work of Shannon [1]. Shannon introduces a method of confusion as a way to prevent statistical cryptanalysis of ciphers. He notes that a set of statistics observed from a secret communication is connected to some coordinates of the key space through some algebraic equations. The ultimate goal of algebraic cryptanalysis is to solve this set of equations. On the other hand, good ciphers are designed in such a way, that this task should be very difficult. A summary of algebraic cryptanalysis can be found in [2]. Methods to solve algebraic equations in cryptanalysis are also summarized in [3].

The basic principle of algebraic cryptanalysis is to represent a cryptanalytic problem in an abstract setting, and then to solve this representation with generic tools. In general, each problem can be represented as a set of non-linear equations over finite fields. Theoretically, non-linear equation systems over finite fields can be solved by using general Gröbner bases techniques and related solvers, such as [4]. However, no algorithm is known that can solve most non-linear systems in practice. Specific techniques, such as XL [5], and XSL [6] were developed for solving problems related to algebraic cryptanalysis [7–10].

Another approach to algebraic cryptanalysis is to encode a cryptographic problem as a hard instance of the satisfiability problem [11], and then to use existing SAT solvers to solve this problem instance [9,12–15]. In our experience, SAT solvers can be employed in large-scale distributed algebraic attacks [16] targeting specific weak keys in large sets of data encoded as an SAT problem.

Algebraic cryptanalysis can support and complement other types of cryptanalytic techniques, such as using algebraic techniques in differential cryptanalysis [17–20]. Algebraic side-channel attacks [21,22] use algebraic techniques to complement information leaked from the cipher through side-channels, or through errors [23].

In this paper, we focus on a different representation of algebraic problems that is suitable for algebraic cryptanalysis. This representation is based on the so-called Multiple Right-Hand Sides (MRHS) equation systems [24]. The MRHS representation can separate the representation of non-linear (confusion-based) and linear (diffusion-based) components of the cipher, and thus represent problems of algebraic cryptanalysis in a way similar to how the ciphers are designed. MRHS representation focuses on the main potential weakness of the symmetric cipher design: unlike random functions (that we try to emulate), practical ciphers must be efficiently implemented in hardware (and software) with a limited number of components. Thus the MRHS representation of a practical cipher is relatively small and compact in comparison to a representation of a random function. In general, the problem of whether a random (polynomially sized) MRHS equation system has a solution is NP-complete [25]. In practice, experiments [26] show that equations derived from (round reduced) ciphers can be in some instances solved faster than with an exhaustive search through the key space.

We describe the MRHS equation system and survey their evolution in Section 2. Section 3 is then devoted to surveying methods that can be used to solve MRHS equation systems. The aim of Section 4 is to introduce the techniques used in MRHS cryptanalysis, connecting the cryptanalytic problems and MRHS representation. In Section 5, we specifically survey the existing results of MRHS cryptanalysis.

2. What is a MRHS Equation System?

MRHS equation systems are related to the ideas of Zakrevskij [27]. Systems of Boolean equations can be sparse in the following sense: each Boolean equation in the system depends on only a small subset of the variables. Such systems can be solved by assigning values for particular variables and removing some potential solutions by observing local dependencies (individual possible values of the active variables in individual sparse Boolean equations).

A new representation of sparse Boolean equations related to the algebraic cryptanalysis was presented by Raddum and Semaev in [28]. The equations were represented by ”symbols” containing lists of active variables and their possible values. The solution of the system was done by manipulating such symbols (Agreeing and Gluing). The representation of sparse equation systems can be generalized from Boolean equations to equations over any finite field [29].

Further generalization comes from replacing individual active variables with linear combinations of variables, coining the term *Multiple Right-Hand Sides* (linear) equation systems [24,30]. The original definition preserves the symbol notation, with a list of possible assignments of values for (active) linear combinations of variables.

In this article, we use a newer definition of MRHS equation systems introduced in [31] (equivalent to the original one). We will use the following symbolic notation:

- Symbol $\mathbb{F}$ denotes a finite field, $\mathbb{Z}$ denotes a ring of integers, $\mathbb{N}$ denotes natural numbers.
- We are using row vectors, denoted by bold lowercase letters: $\mathbf{v} \in \mathbb{F}^n$.
- Matrices are denoted by bold uppercase letters: $\mathbf{M} \in \mathbb{F}^{n\times k}$.
- Standard sets are denoted by uppercase slanted letters: $S \subset \mathbb{F}^n$. The size of the set S is denoted by $|S|$. When S is a set of vectors, $\mathbf{S}$ denotes a matrix with $|S|$ rows, where each row is in S. By $S \cdot \mathbf{A}$ we denote a set of vectors $S' = \{\mathbf{v} \cdot \mathbf{A}; \mathbf{v} \in S\}$.
- Special sets are denoted by calligraphic font: $\mathcal{M}$.

Definition 1. *Let $\mathbb{F}$ be a finite field, $n, l \in \mathbb{N}$. Let $\mathbf{M} \in \mathbb{F}^{n\times l}$ be an $n \times l$ matrix. Let S be a set of vectors of dimension l, $S \subset \mathbb{F}^l$. A Multiple Right-Hand Sides (MRHS) equation is a formal inclusion $\mathcal{M}$ in the form*

$$\mathbf{x} \cdot \mathbf{M} \in S.$$

Vector $\mathbf{x} \in \mathbb{F}^n$ is a solution of the MRHS equation $\mathcal{M}$, if the formal inclusion holds for this $\mathbf{x}$.

The set of solutions of $\mathcal{M}$ is a union of solutions of $\mathbf{x} \cdot \mathbf{M} = \mathbf{v}$, for each $\mathbf{v} \in S$. We can see that if $|S| = 1$, an MRHS equation corresponds to a standard system of linear equations.

Definition 2. *Let $\mathbb{F}$ be a finite field, $n, m \in \mathbb{N}$. For each $i \in \{1, 2, \ldots, m\}$ let $l_i \in \mathbb{N}$, $\mathbf{M}_i \in \mathbb{F}^{n\times l_i}$, and $S_i \subset \mathbb{F}^{l_i}$. MRHS (equation) system is a set of MRHS equations $\mathcal{M}_i$:*

$$\{\mathbf{x} \cdot \mathbf{M}_i \in S_i\}.$$

Vector $\mathbf{x} \in \mathbb{F}^n$ is a solution of the MRHS equation system, if and only if it is a solution of each $\mathcal{M}_i$, in the MRHS equation system.

We can write an MRHS system in a joint form

$$\mathbf{x} \cdot (\mathbf{M}_1|\mathbf{M}_2|\cdots|\mathbf{M}_m) \in S_1 \times S_2 \times \cdots \times S_m.$$

We can see that the joint form of an MRHS system is an MRHS equation, given by left-hand side matrix $\mathbf{M} = (\mathbf{M}_1|\mathbf{M}_2|\cdots|\mathbf{M}_m)$, and the right-hand side set $S = S_1 \times S_2 \times \cdots \times S_m$. The dimension of $\mathbf{M}$ is $n \times \sum_{i=1}^{m} l_i$. The size of set S grows quickly with m, $|S| = \prod_{i=1}^{m} |S_i|$. To store the joint form efficiently, we typically do not evaluate the Cartesian product and store only the individual sets S_i.

Definition 3. *Let $poly(n)$ denote any polynomial function in n. We say that a family of MRHS systems parametrized by n has a polynomial representation if for each n: $m < poly(n)$ and for each $i \in \{1, 2, \ldots, m\}$ we have $l_i < poly(n)$, and $|S_i| < poly(n)$.*

Example 1. *Let us construct a family of MRHS systems with $n \geq 1$ variables, and $m = 1$ MRHS equation ($m < n + 1$ for any n). Let $S_1 = \{0, c\}$, with c some randomly selected constant ($|S_1| < n + 2$). This family has a polynomial representation if we restrict the dimension l_1 by some polynomial function of n. A counterexample is selecting all linear combinations of n input variables as columns of $\mathbf{M}_1$, which requires $l_1 = 2^n > poly(n)$ for any polynomial function $poly(n)$ (and sufficiently large n).*

We can verify whether $\mathbf{x}$ is a solution of an MRHS system from a family with polynomial representation in polynomial time. Firstly, we compute $\mathbf{u} = \mathbf{x} \cdot \mathbf{M}$. Then we verify the right-hand sides with m tests $\mathbf{u}_i \in S_i$, where $\mathbf{u}_i$ represents a projection of $\mathbf{u}$ to coordinates corresponding to S_i. The MRHS problem is a decision problem: Given the MRHS system, is there any solution $\mathbf{x}$ of this MRHS system? In [25] we prove that this problem is NP-complete for a family of MRHS systems with polynomial representation.

Further evolution of MRHS equation systems are Compressed Right-Hand Sides (CRHS) Equations [32]. In this form, the right-hand side set S is represented by a binary decision diagram (BDD). This form can represent large sets of right-hand side vectors efficiently but requires new methods to solve such systems such as [33]. Each MRHS equation system can be rewritten as a CRHS equation. The opposite direction is also possible, but given a general CRHS equation, the number of right-hand sides in the MRHS representation can grow too quickly to be efficiently represented. In the rest of the article, we focus mostly on MRHS equations, but we will try to survey also cryptanalytic results obtained with CRHS representation.

3. Algorithms for Solving MRHS Equations

MRHS problem in a decision setting is a question, of whether there exists some $\mathbf{x} \in \mathbb{F}^n$ that is a solution of the MRHS equation system $\mathbf{xM} \in S_1 \times S_2 \times \cdots \times S_m$. In practical algebraic cryptanalysis, we typically know that some solution of the MRHS system exists. Instead, we focus on computing any solution of the system (or all of the existing solutions).

Multiple algorithms can solve MRHS systems. The basic algorithm is the exhaustive search: iterate through each element of $\mathbb{F}^n$, and verify, whether it is a solution of the system. This gives us the upper bound on the complexity of the MRHS problem: $|\mathbb{F}^n|$ iterations, and in each iteration we do one vector-matrix multiplication (on the left-hand-side) plus verification of the set membership (on the right-hand side). The iteration can be improved by classic techniques such as using Grey code for element enumeration.

A specific issue arises in algebraic cryptanalysis. Suppose that some MRHS system with n unknowns over $\mathbb{F}_2$ is derived from a cryptanalytic problem with $k < n$ unknown key bits. Then in the cryptanalytic setting, the complexity of the search should be bounded by 2^k key verification operations, instead of 2^n, the complexity of the exhaustive MRHS solver. Thus, a generic MRHS solver based on an exhaustive search seems unsuitable for algebraic cryptanalysis.

3.1. Solving MRHS Systems with Linear Algebra

Similarly to standard systems of linear equations, we can perform some operations on the MRHS system that do not change the (size of the) set of solutions of the MRHS system:

- **Column operations.** Let $\mathbf{B}$ be an invertible diagonal matrix

$$\mathbf{B} = \begin{pmatrix} \mathbf{B}_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{B}_2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{B}_m \end{pmatrix}$$

with $\mathbf{B}_i \in \mathbb{F}^{l_i \times l_i}$. Vector $\mathbf{x}$ is a solution of $\mathcal{M}$ if and only if it is a solution of the equivalent MRHS system

$$\mathbf{x} \cdot \mathbf{M} \cdot \mathbf{B} \in S_1 \cdot \mathbf{B}_1 \times \cdots \times S_m \cdot \mathbf{B}_m$$

Note that it would be possible to define a similar operation with a general invertible matrix $\mathbf{B}$. However, in such a case we would have to evaluate Cartesian products of S_i's, and thus in general the equivalent system would lose the polynomial representation.

- **Row operations.** Let $\mathbf{A}$ be an invertible $n \times n$ matrix. Vector $\mathbf{x}$ is a solution of $\mathcal{M}$ if and only if vector $\mathbf{y}$ is a solution of

$$\mathbf{y} \cdot (\mathbf{A} \cdot \mathbf{M}) \in S_1 \times \cdots \times S_m$$

and $\mathbf{x} = \mathbf{y} \cdot \mathbf{A}$.

- **RHS joining.** Vector $\mathbf{x}$ is a solution of $\mathcal{M}$ if and only if it is a solution of the equivalent MRHS system

$$\mathbf{x} \cdot \mathbf{M} \in S_1 \times \cdots \times S_{m-2} \times S'_{m-1}$$

where $S'_{m-1} = S_{m-1} \times S_m$. The main difference between the MRHS systems is that S'_{m-1} requires more space to explicitly list all its vectors, in comparison to the original MRHS system. In general, we can join any pair of RHS sets (computing $S_i \times S_j$).

- **RHS compression.** Let $\mathrm{rank}(\mathbf{M}_i) < l_i$ for some i. We can use **column operations** with matrix $\mathbf{B}_i$ to change the first column of $\mathbf{M}_i$ to all zeroes. The vector $\mathbf{x}$ is a solution of $\mathcal{M}$ if and only if it is a solution of

$$\mathbf{x} \cdot \mathbf{M} \in S_1 \cdot \times \cdots S'_i \cdot \times \cdots S_m$$

where $S'_i = \{\mathbf{v} \in S_i;\ \mathrm{proj}_1(\mathbf{v} \cdot \mathbf{B}_i) = 0\}$. This means we can remove all vectors from S_i that have non-zero first coordinates after the column operation.

We can transform the joint form of the MRHS equation to a single compact MRHS equation by a series of RHS joining and compression operations. This is the basis of the original Gluing algorithm [28,30] proposed to solve MRHS equation systems. Note that during the sequence of operations during the Gluing algorithm we can lose the polynomial representation property.

Another solving algorithm that uses linear algebra was proposed in [34]. This algorithm uses the reduced row echelon form of the joint matrix to efficiently expand and test partial solutions of the system.

3.2. Solving MRHS Systems with Local Reduction

It was already observed in the seminal works [28,30] that (sparse) MRHS equation systems can be solved more efficiently than with exhaustive search. They proposed a method of Agreeing and Gluing to solve the MRHS system. The main idea of the Agreeing is to use ”local information” obtained from individual MRHS equations in the system to reduce the size of individual right-hand side sets. Let us suppose that we have two MRHS equations $\mathbf{x} \cdot \mathbf{M}_i \in S_i$, and $\mathbf{x} \cdot \mathbf{M}_j \in S_j$ within the target MRHS system, with linearly dependent columns in $(\mathbf{M}_i|\mathbf{M}_j)$. There exists matrix $\mathbf{U}$, such that $(\mathbf{M}_i|\mathbf{M}_j) \cdot \mathbf{U} = \mathbf{0}$. Thus on the right-hand side, we can remove each $\mathbf{v} \in S_i \times S_j$ for which $\mathbf{v} \cdot \mathbf{U} \neq \mathbf{0}$. Agreeing method verifies parts of $\mathbf{v} = (\mathbf{v}_i, \mathbf{v}_j)$ separately. Vector $\mathbf{v}_i$ is removed from S_i, if there is no $\mathbf{v}_j$ such that $(\mathbf{v}_i, \mathbf{v}_j) \cdot \mathbf{U} = \mathbf{0}$ (and similarly for $\mathbf{v}_j$ and S_j).

In [35], it was observed that Agreeing algorithm can be translated into the language of electric wires and switches, and can be efficiently implemented in specialized hardware. In [36], a special-purpose architecture to implement an algebraic attack in hardware (called PET SNAKE) was proposed. The proposed use of ASICs seems to enable significant performance gains over a software implementation of MRHS solver based on Agreeing.

The Agreeing method can be generalized to different polynomial time ”local reduction” methods [26], such as the Method of Syllogisms, or the Relinearisation method. However, MRHS systems in general cannot be solved by just these local reduction methods. When considering random sparse Boolean equations there is an observable phase transition between systems that can be solved by local reduction (easy problems) and systems that cannot be solved directly (hard problems) [37]. The main strategy in utilizing the local reduction is to combine it with Guessing. This means that we explicitly try to substitute some value (either of some variable or some combination of variables), and try to verify (with Agreeing) whether the reduced system still has a solution. This leads to a class of algorithms based on recursive search similar to DPLL algorithm [38] used in SAT solvers. Similarly to DPLL, additional information from guess and verify can be learned and used to improve further guessing [39].

Alternatively, local reduction methods can be combined with the Gluing method, which means explicitly joining individual MRHS equations to find all solutions of the MRHS system. Local reduction is used to keep the size of the intermediate systems as low as possible. An analysis of the improved Agreeing-Gluing algorithm can be found in [40]. The Gluing algorithm complexity depends on the order of MRHS equations used by individual Gluing operations. This gives rise to a new combinatorial MaxMinMax problem [41–43]. The solution to this problem can provide an optimal Gluing strategy. It is an open problem whether the MaxMinMax also applies to MRHS solver based on linear algebra [34], which has a complexity that also depends on the order of the MRHS equations within the joint form of the MRHS system.

3.3. Solving MRHS Systems in Dual Code

A new method to solve MRHS equation systems and their connection to group factorization was studied in [44]. The method is essentially a generalization of Agreeing to the whole joint matrix of the MRHS system for MRHS systems over a binary field $\mathbf{F}_2$. We can observe that on the left-hand side, possible vectors $\mathbf{xM}$ form a binary linear code $\mathcal{C}$ with parity check matrix $\mathbf{H}$. Thus, valid solutions $\mathbf{x}$ correspond exactly to those right-hand side vectors $\mathbf{v} \in S$, which are also codewords of $\mathcal{C}$, and $\mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}$. The problem of solving an MRHS system can be reduced to solving a group factorization problem in the form $\bigoplus S_i \cdot \mathbf{H}^T = \mathbf{0}$, where $S_i \cdot \mathbf{H}^T = \{\mathbf{v} \cdot \mathbf{H}^T; \mathbf{v} \in S_i\}$.

In [31], we have followed this reduction to change the MRHS problem into a specific instance of a decoding problem. We also explore how the complexity of solving Multivariate Quadratic (MQ) and MRHS systems is connected to the complexity of the decoding problem. In [45] we show how the transformation to the decoding problem can be used to estimate the upper bounds on the complexity of algebraic attacks on ciphers with low multiplicative complexity (low number of AND gates).

3.4. Solving MRHS Systems with Heuristic Search

In [46] we have introduced a new method for solving sparse random MRHS systems based on bit-flipping. This method starts with random $\mathbf{x}$. In sufficiently sparse systems, each bit of unknown $\mathbf{x}$ only influences a limited number of individual MRHS equations. The bit-flipping method is based on marking those bits of $\mathbf{x}$ that can change unsatisfied MRHS equations ($\mathbf{x} \cdot \mathbf{M}_i \notin S_i$) to a satisfied state. We then change (some of) the marked bits, gradually improving the number of satisfied MRHS equations (until the system is solved, or we end in a cycle and need to restart the method). Experiments show that this method can solve MRHS systems more efficiently than exhaustive search, but its complexity is significantly influenced by the density of the left-hand side joint matrix $\mathbf{M}$.

An alternative formulation of the bit-flipping approach is based on the hill-climbing algorithm [46,47]. In this case we again start from random $\mathbf{x}$, and choose some neighboring $\mathbf{x} \oplus \mathbf{e}^i$, where $w_H(\mathbf{e}^i) = 1$. With the greedy approach, we try to maximize the new number of satisfied MRHS equations (or restart, if this is not possible). Experiments show that the hill-climbing-based method has a better success chance than bit-flipping, but the individual steps of the algorithm are slower (as we need to explore all neighbors of $\mathbf{x}$).

A natural extension of the hill-climbing method is the application of evolutionary computing and stochastic optimization algorithms. Successful solving of (specific random) MRHS equations with genetic algorithms was reported in [48]. This research area is however still very fresh, with many open questions and potential for research: Which methods are suitable for generic systems/specific systems related to algebraic cryptanalysis? How to select the parameters of the heuristic methods? Which scoring functions should be used? Can the methods be combined with other MRHS-solving methods?

4. Using MRHS Systems in Algebraic Cryptanalysis

Algebraic cryptanalysis typically involves three basic steps. Firstly, we transform the cryptanalytic problem into an algebraic representation. Then we solve the algebraic problem with a solver. Finally, we use the algebraic solution to determine the result of the cryptanalysis (e.g., extracting the key bits). We will call algebraic cryptanalysis that involves MRHS representation an MRHS cryptanalysis.

MRHS representation is especially suited for the cryptanalysis of block ciphers composed of small non-linear elements (S-boxes) and linear diffusion layers. Let us consider an example based on the Substitution-Permutation Network (SPN). SPN has r rounds composed of key addition, bricklayer substitution with s parallel S-boxes given by non-linear Boolean function $F : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$, and a diffusion layer that can be described as a linear transformation by an invertible diffusion matrix $\mathbf{L} \in \mathbb{Z}_2^{sm} \times \mathbb{Z}_2^{sm}$.

Let us denote the input plaintext by $\mathbf{x}$, the output ciphertext by $\mathbf{y}$, and the unknown key bits by $\mathbf{k}$. For the sake of simplicity, let us suppose that round keys are computed from key bits $\mathbf{k}$ by linear transformation given by matrices $\mathbf{K}_i$ (for round i, the round key is $\mathbf{k}_i = \mathbf{k} \cdot \mathbf{K}_i$). Note that a non-linear key schedule can be included in the MRHS system similar to individual rounds.

Let us denote S-box inputs in round i by $\mathbf{u}_i$, and S-box outputs by $\mathbf{v}_i$. The first S-box layer input is computed as $\mathbf{u}_1 = \mathbf{x} + \mathbf{k}_1$ (here $\mathbf{x}$ is just the plaintext). The diffusion layer gives us linear equations $\mathbf{u}_{i+1} = \mathbf{v}_i \cdot \mathbf{L} \oplus \mathbf{k}_{i+1}$, and in the final round we get $\mathbf{y} = \mathbf{v}_r \cdot \mathbf{L} \oplus \mathbf{k}_{r+1}$.

The initial MRHS system has a set of "unknowns" given by concatenation of $\mathbf{z} = (\mathbf{k}, \mathbf{x}, \mathbf{y}, \mathbf{u}_1, \ldots, \mathbf{u}_r, \mathbf{v}_1, \ldots, \mathbf{v}_r)$. Individual MRHS equations in the system are based on S-boxes. Each S-box corresponds to a single MRHS equation in the form of

$$\mathbf{z} \cdot \begin{pmatrix} \mathbf{0} & \mathbf{0} \\ \vdots & \vdots \\ \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{J} \\ \vdots & \vdots \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \in S,$$

where $\mathbf{I}$ and $\mathbf{J}$ are identity matrices selecting corresponding input and output bits of the S-box. Set S consists of all possible pairs of S-box inputs and outputs: $S = \{(\mathbf{a}, \mathbf{b}) \in \mathbb{Z}_2^m \times \mathbb{Z}_2^m;\ \mathbf{b} = F(\mathbf{a})\}$.

The final MRHS system is obtained by substituting known values of plaintext and ciphertext, and partially solving the system of linear equations given by diffusion layers and key schedule. The resulting linear expressions are substituted into the MRHS system. The detailed algorithm is presented in [49].

Example 2. *Let us have a toy SPN-like cipher with 4-bit input and 4-bit key repeated in each round. The cipher uses 2-bit S-box given by permutation* $(3, 2, 0, 1)$*, and linear layer that swaps "middle" bits of the state. The encryption can be described by MRHS system:*

$$
\begin{pmatrix} \mathbf{x}, \\ \mathbf{k}, \\ \mathbf{y}, \\ \mathbf{u}_1, \\ \mathbf{u}_2, \\ \mathbf{v}_1, \\ \mathbf{v}_2 \end{pmatrix}^T \cdot
\left(\begin{array}{ccccccc}
1000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0100 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0010 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0001 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
\hline
1000 & 0000 & 0000 & 1000 & 0000 & 0000 & 1000 \\
0100 & 0000 & 0000 & 0010 & 0000 & 0000 & 0100 \\
0010 & 0000 & 0000 & 0100 & 0000 & 0000 & 0010 \\
0001 & 0000 & 0000 & 0001 & 0000 & 0000 & 0001 \\
\hline
0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 1000 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0100 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0010 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0001 \\
\hline
1000 & 1000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0100 & 0100 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0010 & 0000 & 1000 & 0000 & 0000 & 0000 & 0000 \\
0001 & 0000 & 0100 & 0000 & 0000 & 0000 & 0000 \\
\hline
0000 & 0000 & 0000 & 1000 & 1000 & 0000 & 0000 \\
0000 & 0000 & 0000 & 0100 & 0100 & 0000 & 0000 \\
0000 & 0000 & 0000 & 0010 & 0000 & 1000 & 0000 \\
0000 & 0000 & 0000 & 0001 & 0000 & 0100 & 0000 \\
\hline
0000 & 0010 & 0000 & 1000 & 0000 & 0000 & 0000 \\
0000 & 0001 & 0000 & 0010 & 0000 & 0000 & 0000 \\
0000 & 0000 & 0010 & 0100 & 0000 & 0000 & 0000 \\
0000 & 0000 & 0001 & 0001 & 0000 & 0000 & 0000 \\
\hline
0000 & 0000 & 0000 & 0000 & 0010 & 0000 & 1000 \\
0000 & 0000 & 0000 & 0000 & 0001 & 0000 & 0100 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0010 & 0010 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0001 & 0001
\end{array}\right)
\in \{0000\} \times S \times S \times \{0000\} \times S \times S \times \{0000\},
$$

where $S = \{0011, 0110, 1000, 1101\}$.

Let us suppose that $\mathbf{x} = 0000$*, and* $\mathbf{y} = 1111$*. We can compress the MRHS system by partially solving the linear parts (*$\mathbf{u}_1 = \mathbf{k}$*,* $\mathbf{v}_2 = \mathbf{k} \oplus 1111$*,* $\mathbf{u}_2 = \mathbf{P} \cdot (\mathbf{k} \oplus \mathbf{v}_1)$*), and get the new system:*

$$
\begin{aligned}
\begin{pmatrix} \mathbf{k}, \\ \mathbf{v}_1 \end{pmatrix}^T \cdot &\left(\begin{array}{cccc}
1000 & 0000 & 1010 & 0000 \\
0100 & 0000 & 0001 & 1000 \\
0000 & 1000 & 0100 & 0010 \\
0000 & 0100 & 0000 & 0101 \\
\hline
0010 & 0000 & 1000 & 0000 \\
0001 & 0000 & 0000 & 1000 \\
0000 & 0010 & 0100 & 0000 \\
0000 & 0001 & 0000 & 0100
\end{array}\right) \\
&\oplus \begin{pmatrix} 0000 & 0000 & 0011 & 0011 \end{pmatrix} \\
&\in S \times S \times S \times S.
\end{aligned}
$$

We can move constant $(0000, 0000, 0011, 0011)$ *to the right hand side, by replacing the last two sets* S *by* $S \oplus (0011) = \{0000, 0101, 1011, 1110\}$*.*

It is possible to represent the same system on different levels, e.g., by replacing S-boxes with their AND-XOR decomposition [47]. In general, any family of Boolean functions that can be implemented with a polynomial number of AND gates in an AND-XOR logic leads to a family of MRHS systems with polynomial representation.

Note that every MRHS system can be rewritten as an XOR-SAT problem [25], and then converted to a CNF-SAT instance used by SAT solvers. The main advantage of MRHS representation in comparison with CNF-SAT representation is that the MRHS system can handle XOR clauses from complex diffusion layers more naturally. There is also a simple correspondence between MRHS representation and MQ (multivariate quadratic) representation of the system [31].

Various representations of the same cryptanalytic problem can exploit different types of ”sparsity”. As there is a polynomial-time algorithm to transform between the representations, the expected theoretical complexity of the problem should remain the same (decision versions of these problems are NP-complete). It is an open research question, which of these representations is more suitable for particular cryptanalytic tasks?

5. Experimental MRHS Cryptanalysis

From the research perspective, the aim of cryptanalysis is not to ”break ciphers”, but to give insights into cipher security. Experimental algebraic cryptanalysis focuses on performing practical attacks on a smaller version of the cipher (with a reduced number of rounds, state size, key bits, ...). It might be problematic to compare results across different types of algebraic cryptanalysis, as different types of attacks use different methodologies and metrics. Some optimizations in algebraic solvers can be advantageous for small systems but do not scale well with the increasing system size (parameters).

In [26] we have proposed a methodology of experimental MRHS cryptanalysis that splits the algebraic attack into a polynomial part (local reduction), and an exponential part (guessing), respectively. The evaluator uses instances with known solutions to estimate the complexity of the attacks, and the response to changing parameters of the problem. The methodology can be used to reject weak ciphers, or as a tool for qualitative comparison of cipher designs. The methodology is exemplified by the example of algebraic cryptanalysis of former encryption standard DES [50].

Experimental algebraic cryptanalysis was applied to multiple well-known ciphers. In [51], local reduction techniques were used to evaluate the security of the block cipher GOST [52]. A comparison of local reduction techniques and SAT-solver-based algebraic attacks used in cryptanalysis of SHA-3 candidates JH [53] and Keccak [54] were presented in [55]. In [56], a particular local reduction method (the method of syllogisms) was used to solve reduced versions of stream cipher Trivium [57]. In [58], the local reduction method was independently applied to algebraic cryptanalysis of lightweight cipher Present [59]. Block Cipher DESL [60] was analyzed in [61].

The stream cipher Trivium was also analyzed in [32]. However, in this case, a representation based on compressed right-hand side (CRHS) equations were used. This approach was later explored in more detail in [62], in the context of the DES and the MiniAES ciphers. Algebraic attacks based on CRHS equations on small-scale variants of AES [63] was explored in more detail in [64]. In [65], the CRHS representation was adapted for the factorization problem. In [66], a new tool called CryptaPath for assisted algebraic cryptanalysis of symmetric primitives that can be described with SPN structure was proposed. This tool also uses CRHS representation.

In [34], a new solver that can solve MRHS equations was proposed alongside a methodology for using the solver in algebraic cryptanalysis. The methodology was tested on instances of scaled-down DES, AES, Present, and LowMC [67] ciphers. The experimental MRHS cryptanalytis of LowMC based on the custom implementation of the algorithm proposed in [45] was conducted in [68]. However, the results of the attack were worse than the brute-force approach. The use of the hill-climbing method for MRHS cryptanalysis was explored in [47] in the context of cryptanalysis of the block cipher Ascon [69].

The use of MRHS representation is not limited to algebraic cryptanalysis. In [70], a new approach to linear cryptanalysis of the block cipher DES was proposed. MRHS equation system is collected from linear approximations obtained by linear cryptanalysis. This approach was later extended to multidimensional linear cryptanalysis in [71].

6. Conclusions

Multiple Right-Hand Sides equation systems can be used in algebraic cryptanalysis instead of standard representations such as CNF for SAT solvers and ANF for Gröbner bases and related solvers. The main advantage of MRHS equations is the separation of linear and non-linear components of analyzed ciphers and cryptographic primitives. As the main disadvantage, we perceive a lack of freely available universal and specialized MRHS solvers, as well as a relative lack of research on using MRHS equation systems other than cryptographic applications.

While MRHS equation systems were primarily used for experimental algebraic cryptanalysis, they have also been used in theoretical studies. In [45] we use MRHS systems and their transformation to a decoding problem to provide upper bounds on the complexity of algebraic cryptanalysis of ciphers with low multiplicative complexity. In [31], we use the MRHS equation system as a middle step in connecting the complexity of MQ-and code-based cryptosystems used in post-quantum cryptography. We have even proposed a new type of post-quantum signature scheme that can be derived from an MRHS representation of a symmetric cipher such as AES or LowMC [49].

We conclude that the use of MRHS equation systems in not only algebraic cryptanalysis has still significant research potential, both theoretical and experimental. We believe that there is also a potential for applications of MRHS systems and solvers in other problem areas dominated by SAT solvers, such as circuit optimization.

Funding: This work was supported by the Slovak Research and Development Agency under the Contract no. APVV-19-0220.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AES	Advanced Encryption Standard
CRHS	Compressed Right-Hand Sides
MQ	Multivariate Quadratic
MRHS	Multiple Right-Hand Sides
RHS	Right-Hand Side
SPN	Substitution-Permutation Network

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Bard, G. *Algebraic Cryptanalysis*; Springer: Berlin/Heidelberg, Germany, 2009.
3. Semaev, I.; Mikuš, M. Methods to solve algebraic equations in cryptanalysis. *Tatra Mt. Math. Publ.* **2010**, *45*, 107–136. [CrossRef]
4. Faugere, J.C.; Joux, A. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *Proceedings of the Advances in Cryptology-CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2003*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 44–60.
5. Courtois, N.; Klimov, A.; Patarin, J.; Shamir, A. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *Proceedings of the Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, 14–18 May 2000*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 392–407.
6. Courtois, N.T.; Pieprzyk, J. Cryptanalysis of block ciphers with overdefined systems of equations. In *Proceedings of the Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 1–5 December 2002*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 267–287.
7. Courtois, N.T. Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt. In *Proceedings of the Information Security and Cryptology—ICISC 2002: 5th International Conference, Seoul, South Korea, 28–29 November 2002*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 182–199.
8. Cho, J.Y.; Pieprzyk, J. Algebraic Attacks on SOBER-t32 and SOBER-t16 without Stuttering. In *Proceedings of the Fast Software Encryption, New Delhi, India, 5–7 February 2004*; Roy, B., Meier, W., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 49–64.
9. Courtois, N.T.; Bard, G.V. Algebraic cryptanalysis of the data encryption standard. In *Proceedings of the Cryptography and Coding: 11th IMA International Conference, Cirencester, UK, 18–20 December 2007*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 152–169.
10. Courtois, N.T. Algebraic complexity reduction and cryptanalysis of GOST. Cryptology ePrint Archive, Paper 2011/626. 2011. Available online: https://eprint.iacr.org/2011/626 (accessed on 1 March 2023).
11. Cook, S.A.; Mitchell, D.G. Finding hard instances of the satisfiability problem: A survey. *Satisf. Probl. Theory Appl.* **1997**, *35*, 1–17.
12. Massacci, F. Using Walk-SAT and Rel-SAT for cryptographic key search. In Proceedings of the IJCAI, Stockholm, Sweden, 31 July–6 August 1999; Volume 99, pp. 290–295.
13. McDonald, C.; Charnes, C.; Pieprzyk, J. An algebraic analysis of trivium ciphers based on the boolean satisfiability problem. In *Proceedings of the 4th International Workshop on Boolean Functions: Cryptography and Applications, Paris, France, 3 June 2008*; Laboratoire d'Informatique Algorithmique: Fondements et Applications: Paris, France, 2008; pp. 173–184.
14. Dwivedi, A.D.; Klouček, M.; Morawiecki, P.; Nikolic, I.; Pieprzyk, J.; Wöjtowicz, S. SAT-based Cryptanalysis of Authenticated Ciphers from the CAESAR Competition. Cryptology ePrint Archive, Paper 2016/1053. 2016. Available online: https://eprint.iacr.org/2016/1053 (accessed on 1 March 2023).
15. Andrzejczak, M.; Dudzic, W. SAT Attacks on ARX Ciphers with Automated Equations Generation. *Infocommunications* **2019**, *9*, 2–7. [CrossRef]
16. Hromada, V.; Öllős, L.; Zajac, P. Using SAT solvers in large scale distributed algebraic attacks against low entropy keys. *Tatra Mt. Math. Publ.* **2015**, *64*, 187–203. [CrossRef]
17. Albrecht, M.; Cid, C. Algebraic techniques in differential cryptanalysis. In Proceedings of the International Workshop on Fast Software Encryption, Leuven, Belgium, 22–25 February 2009; Springer: Berlin/Heidelberg, Germany, 2009; pp. 193–208.
18. Faugère, J.C.; Perret, L.; Spaenlehauer, P.J. Algebraic-differential cryptanalysis of DES. In Proceedings of the Western European Workshop on Research in Cryptology-WEWoRC, Graz, Austria, 7–9 July 2009; pp. 1–5.
19. Wang, M.; Sun, Y.; Mouha, N.; Preneel, B. Algebraic techniques in differential cryptanalysis revisited. In *Proceedings of the Australasian Conference on Information Security and Privacy, Melbourne, VI, Australia, 11–13 July 2011*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 120–141.
20. Bednáriková, A.; Zajac, P. A new representation of S-boxes for algebraic differential cryptanalysis. *Rad Hrvat. Akad. Znan. Umjet. Mat. Znan.* **2021**, *25*, 33–49. [CrossRef]
21. Renauld, M.; Standaert, F.X. Algebraic side-channel attacks. In *Proceedings of the Information Security and Cryptology: 5th International Conference, Inscrypt 2009, Beijing, China, 12–15 December 2009*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 393–410.
22. Carlet, C.; Faugere, J.C.; Goyet, C.; Renault, G. Analysis of the algebraic side channel attack. *J. Cryptogr. Eng.* **2012**, *2*, 45–62. [CrossRef]

23. Oren, Y.; Kirschbaum, M.; Popp, T.; Wool, A. Algebraic side-channel analysis in the presence of errors. In *Proceedings of the Cryptographic Hardware and Embedded Systems, CHES 2010: 12th International Workshop, Santa Barbara, CA, USA, 17–20 August 2010*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 428–442.
24. Raddum, H. MRHS equation systems. In *Proceedings of the Selected Areas in Cryptography: 14th International Workshop, SAC 2007, Ottawa, ON, Canada, 16–17 August 2007*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 232–245.
25. Zajac, P. MRHS equation systems that can be solved in polynomial time. *Tatra Mt. Math. Publ.* **2016**, *67*, 205–219. [CrossRef]
26. Zajac, P. Using Local Reduction for the Experimental Evaluation of the Cipher Security. *Comput. Inform.* **2018**, *37*, 349–366. [CrossRef]
27. Zakrevskij, A.; Vasilkova, I. Reducing large systems of Boolean equations. In Proceedings of the 4th Internationl Workshop on Boolean Problems, San Jose, CA, USA, 20–22 March 2000.
28. Raddum, H.; Semaev, I. New Technique for Solving Sparse Equation Systems. Cryptology ePrint Archive, Paper 2006/475. 2006. Available online: https://eprint.iacr.org/2006/475 (accessed on 1 March 2023).
29. Semaev, I. Sparse algebraic equations over finite fields. *SIAM J. Comput.* **2009**, *39*, 388–409. [CrossRef]
30. Raddum, H.; Semaev, I. Solving multiple right hand sides linear equations. *Des. Codes Cryptogr.* **2008**, *49*, 147–160. [CrossRef]
31. Zajac, P. Connecting the Complexity of MQ-and Code-Based Cryptosystems. *Tatra Mt. Math. Publ.* **2017**, *70*, 163–177. [CrossRef]
32. Schilling, T.E.; Raddum, H. Analysis of trivium using compressed right hand side equations. In *Proceedings of the Information Security and Cryptology-ICISC 2011: 14th International Conference, Seoul, South Korea, 30 November–2 December 2011*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 18–32.
33. Schilling, T.E.; Raddum, H. Solving compressed right hand side equation systems with linear absorption. In *Proceedings of the International Conference on Sequences and Their Applications, Waterloo, ON, Canada, 4–8 June 2012*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 291–302.
34. Raddum, H.; Zajac, P. MRHS solver based on linear algebra and exhaustive search. *J. Math. Cryptol.* **2018**, *12*, 143–157. [CrossRef]
35. Semaev, I. Sparse Boolean equations and circuit lattices. *Des. Codes Cryptogr.* **2011**, *59*, 349–364. [CrossRef]
36. Geiselmann, W.; Matheis, K.; Steinwandt, R. PET SNAKE: A Special Purpose Architecture to Implement an Algebraic Attack in Hardware. In *Transactions on Computational Science X*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 298–328.
37. Schilling, T.; Zajac, P. Phase transition in a system of random sparse Boolean equations. *Tatra Mt. Math. Publ.* **2010**, *45*, 93–105. [CrossRef]
38. Davis, M.; Putnam, H. A computing procedure for quantification theory. *J. ACM (JACM)* **1960**, *7*, 201–215. [CrossRef]
39. Schilling, T.E.; Raddum, H. Solving equation systems by agreeing and learning. In *Proceedings of the International Workshop on the Arithmetic of Finite Fields, Istanbul, Turkey, 27–30 June 2010*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 151–165.
40. Semaev, I. Improved agreeing-gluing algorithm. *Math. Comput. Sci.* **2013**, *7*, 321–339. [CrossRef]
41. Horak, P.; Semaev, I.; Tuza, Z. An application of Combinatorics in Cryptography. *Electron. Notes Discret. Math.* **2015**, *49*, 31–35. [CrossRef]
42. Semaev, I. MaxMinMax problem and sparse equations over finite fields. *Des. Codes Cryptogr.* **2016**, *79*, 383–404. [CrossRef]
43. Horak, P.; Semaev, I.; Tuza, Z. A combinatorial problem related to sparse systems of equations. *Des. Codes Cryptogr.* **2017**, *85*, 129–144. [CrossRef]
44. Zajac, P. A new method to solve MRHS equation systems and its connection to group factorization. *J. Math. Cryptol.* **2013**, *7*, 367–381. [CrossRef]
45. Zajac, P. Upper bounds on the complexity of algebraic cryptanalysis of ciphers with a low multiplicative complexity. *Des. Codes Cryptogr.* **2017**, *82*, 43–56. [CrossRef]
46. Zajac, P. On solving sparse MRHS equations with bit-flipping. *Publ. Math. Debrecen* **2022**, *100* (Suppl. S8), 683–700. [CrossRef]
47. Smičík, M.; Zajac, P. MRHS cryptanalysis of Ascon. In *Proceedings of Central European Conference on Cryptology—CECC'22, Smolenice, Slovakia, 26–29 June 2022*; Mathematical Institute, Slovak Academy of Sciences: Bratislava, Slovakia, 2022; pp. 87–89.
48. Tito-Corrioso, O.; Borges-Quintana, M.; Borges-Trenard, M.A. Improving search of solutions of MRHS systems using the Genetic Algorithm. *Rev. Cuba. Cienc. Inform.* **2023**, *17*, 38–52.
49. Zajac, P.; Spacek, P. A New Type of Signature Scheme Derived from a MRHS Representation of a Symmetric Cipher. *Infocommunications J.* **2019**, *11*, 23–30. [CrossRef]
50. Biryukov, A.; De Cannière, C. Data encryption standard (DES). In *Encyclopedia of Cryptography and Security*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 295–301.
51. Zajac, P.; Čagala, R. Local reduction and the algebraic cryptanalysis of the block cipher GOST. *Period. Math. Hung.* **2012**, *65*, 239–255. [CrossRef]
52. Courtois, N.T. Security evaluation of GOST 28147-89 in view of international standardisation. *Cryptologia* **2012**, *36*, 2–13. [CrossRef]
53. Wu, H. The hash function JH. Submission to NIST (Round 3). 2011. Available online: https://www3.ntu.edu.sg/home/wuhj/research/jh/jh_round3.pdf (accessed on 1 March 2023).
54. Bertoni, G.; Daemen, J.; Peeters, M.; Van Assche, G. Keccak. In *Proceedings of the Advances in Cryptology—EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, 26–30 May 2013*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 313–314.

55. Adamček, P.; Loderer, M.; Zajac, P. A comparison of local reduction and SAT-solver based algebraic cryptanalysis of JH and Keccak. *Tatra Mt. Math. Publ.* **2012**, *53*, 1–20. [CrossRef]
56. Zajac, P. Solving Trivium-based Boolean Equations Using the Method of Syllogisms. *Fundam. Informaticae* **2012**, *114*, 359–373. [CrossRef]
57. De Canniere, C.; Preneel, B. Trivium. *New Stream Cipher Designs: The eSTREAM Finalists*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 244–266.
58. Lacko-Bartošová, L. Algebraic cryptanalysis of Present based on the method of syllogisms. *Tatra Mt. Math. Publ.* **2012**, *53*, 201–212. [CrossRef]
59. Bogdanov, A.; Knudsen, L.R.; Leander, G.; Paar, C.; Poschmann, A.; Robshaw, M.J.; Seurin, Y.; Vikkelsoe, C. PRESENT: An ultra-lightweight block cipher. In *Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, 10–13 September 2007*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 450–466.
60. Poschmann, A.; Leander, G.; Schramm, K.; Paar, C. A family of light-weight block ciphers based on DES suited for RFID applications. In Proceedings of the Workshop on RFID Security–RFIDSec, Graz, Austria, 12–14 July 2006; Volume 6.
61. Matheis, K.; Steinwandt, R.; Suárez Corona, A. Algebraic Properties of the Block Cipher DESL. *Symmetry* **2019**, *11*, 1411. [CrossRef]
62. Raddum, H.; Kazymyrov, O. Algebraic attacks using binary decision diagrams. In *Proceedings of the International Conference on Cryptography and Information Security in the Balkans, Istanbul, Turkey, 16–17 October 2014*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 40–54.
63. Daemen, J.; Rijmen, V. *The Design of Rijndael*; Springer: Berlin/Heidelberg, Germany, 2002.
64. Indrøy, J.P. Algebraic Attack on Small Scale Variants of AES using Compressed Right Hand Sides. Master's Thesis, The University of Bergen, Bergen, Norway, 2018.
65. Raddum, H.; Varadharajan, S. Factorization using binary decision diagrams. *Cryptogr. Commun.* **2019**, *11*, 443–460. [CrossRef]
66. Indrøy, J.P.; Costes, N.; Raddum, H. Boolean Polynomials, BDDs and CRHS Equations-Connecting the Dots with CryptaPath. In *Proceedings of the International Conference on Selected Areas in Cryptography, Kingston, ON, Canada, 11–12 August 2020*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 229–251.
67. Albrecht, M.R.; Rechberger, C.; Schneider, T.; Tiessen, T.; Zohner, M. Ciphers for MPC and FHE. In *Proceedings of the Advances in Cryptology–EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 26–30 April 2015*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 430–454.
68. Grassi, L.; Kales, D.; Rechberger, C.; Schofnegger, M. Survey of Key-Recovery Attacks on LowMC in a Single Plaintext/Ciphertext Scenario. 2020. Available online: https://raw.githubusercontent.com/lowmcchallenge/lowmcchallenge-material/master/docs/survey.pdf (accessed on 1 March 2023).
69. Dobraunig, C.; Eichlseder, M.; Mendel, F.; Schläffer, M. Ascon v1. 2. *Submiss. CAESAR Compet.* **2016**, *5*, 7.
70. Semaev, I. New results in the linear cryptanalysis of DES. Cryptology ePrint Archive, Paper 2014/361. 2006. Available online: https://eprint.iacr.org/2014/361 (accessed on 1 March 2023).
71. Fauskanger, S.; Semaev, I. Separable statistics and multidimensional linear cryptanalysis. *IACR Trans. Symmetric Cryptol.* **2018**, *2*, 79–110. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.