Deterministic Algorithms for Solving Boolean Polynomial Equations Based on Channel Coding Theory

WU, Guangfu; LV, Yijie; HE, Daojing; HE, Jiguang; ZHOU, Huan; CHAN, Sammy

Published in:
IEEE Access

Published: 01/01/2020

Document Version:
Final Published version, also known as Publisher's PDF, Publisher's Final version or Version of Record

License:
CC BY

Publication record in CityU Scholars:
Go to record

Published version (DOI):
10.1109/ACCESS.2020.2971393

Publication details:
WU, G., LV, Y., HE, D., HE, J., ZHOU, H., & CHAN, S. (2020). Deterministic Algorithms for Solving Boolean Polynomial Equations Based on Channel Coding Theory. IEEE Access, 8, 26764-26772. Article 8979348. https://doi.org/10.1109/ACCESS.2020.2971393

Citing this paper
Please note that where the full-text provided on CityU Scholars is the Post-print version (also known as Accepted Author Manuscript, Peer-reviewed or Author Final version), it may differ from the Final Published version. When citing, ensure that you check and use the publisher's definitive version for pagination and other details.

General rights
Copyright for the publications made accessible via the CityU Scholars portal is retained by the author(s) and/or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights. Users may not further distribute the material or use it for any profit-making activity or commercial gain.

Publisher permission
Permission for previously published items are in accordance with publisher's copyright policies sourced from the SHERPA RoMEO database. Links to full text versions (either Published or Post-print) are only available if corresponding publishers allow open access.

Take down policy
Contact lbscholars@cityu.edu.hk if you believe that this document breaches copyright and provide us with details. We will remove access to the work immediately and investigate your claim.
Deterministic Algorithms for Solving Boolean Polynomial Equations Based on Channel Coding Theory

GUANGFU WU1, YIJIE LV1, DAOJING HE1,2, (Member, IEEE), JIGUANG HE3, (Member, IEEE), HUAN ZHOU1, AND SAMMY CHAN4, (Member, IEEE)
1Department of Information Engineering, Jiangxi University of Science and Technology, Ganzhou 330006, China
2Department of Software Engineering, East China Normal University, Shanghai 200241, China
3Centre for Wireless Communications, University of Oulu, 90014 Oulu, Finland
4Department of Electronic Engineering, City University of Hong Kong, Hong Kong 999077

Corresponding authors: Guangfu Wu (wuguangfu@126.com) and Yijie Lv (lvsejianke@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 11461031, in part by the Natural Science Foundation of Jiangxi Province under Grant 20181BBE58018, in part by the Science and Technology Project of Jiangxi Education Department under Grant GJJ180442, and in part by the Science and Technology Key Project of the Education Department of Jiangxi Province under Grant GJJ170492.

ABSTRACT Solving the satisfiability problems of Boolean polynomial equations is still an open challenge in the fields of mathematics and computer science. In this paper, our goal is to propose a non-algebraic method for solving maximal Boolean polynomial equations (Max-PoSSo problem). By leveraging channel coding theory and dynamic programming, we propose three deterministic and robust algorithms for solving the satisfiability problems of Boolean polynomial equations. Comparisons are made among the three proposed algorithms and Genetic and Gröbner algorithms. Simulation results show that the proposed algorithms exhibit better performance in terms of the largest number of Boolean polynomials equal to 0 compared to the benchmark schemes in the literature.

INDEX TERMS Boolean polynomial equations, non-algebraic, channel coding theory, deterministic, robust.

I. INTRODUCTION
Solving Boolean polynomial equations is one of the major elements for algebraic side-channel attacks, also known as side channel cryptanalysis, which was proposed by Kocher [1] in the late 1990s. It is an attack method based on information gained from the implementation of a computer system. The algebraic attack is to set the cryptographic information as a variable, then establish a set of polynomial equations by considering the relationship between the known information and the cryptographic information, and finally recover the cryptographic information through solving the set of polynomial equations. Algebraic side-channel attacks combine algebraic attacks with side-channel attacks [2]. Algebraic side-channel attacks reduce the attack complexity via introducing side channel information, thereby improve the attack efficiency. The challenge in algebraic side-channel attacks is that polynomial equations are difficult to solve.

Boolean polynomials were proposed by George Boer in his book The Mathematical Analysis of Logic, and further detailed in An Investigation of the Laws of Thought [3] in the nineteenth century. Solving (general) Boolean polynomial equations [4] is still one of the most difficult problems in the fields of mathematics and computer science [5], [6]. Namely, a set of Boolean polynomials is selected to find variable assignments so that the values of these polynomials are all 0. The satisfiability problem of solving maximal Boolean polynomial equations (Max-PoSSo problem) is an extended problem of solving general Boolean polynomial equations [7]. It falls into the category of NP-hard problems [8] and is widely used in cryptographic probabilistic algebraic attacks and side-channel algebraic attacks. In the process of establishing a polynomial equation set, noise...
makes certain mistakes in some terms of the set of polynomial equations (generally constant terms), resulting in partial non-zero polynomials [9]. In order to restore the secret information, the attacker needs to find the largest number of Boolean polynomials equal to 0.

There are two main approaches for dealing with the Max-PoSSo problem in the literature. One is to traverse the variable and reduce the search branch as to find the optimal variable assignment. It mainly uses some algebraic transformations to transform the Max-PoSSo problem into new problems with already-existing solutions [10]. Therefore, how to transform the Max-PoSSo problem into other equivalent problems to make the solution readily obtained is the key of the method. The other approach is fixing the value of each polynomial to solve the corresponding general Boolean polynomial equations. If one can find the polynomial that corresponds to the solution of the general polynomial equations and has the largest number of 0, the solution of the general polynomial equations is taken as the solution of the Max-PoSSo problem [11]. To solve the general polynomial equations, effective algorithms include the method based on Gröbner basis [12], [13], the SAT method [8], random Multi-Bit flipping method [14], and the feature column method [15]. However, how to effectively combine the algebraic solution algorithm with the search strategy to reduce the search branch and improve the efficiency of the single branch needs to be further studied.

In this paper, we propose new deterministic algorithms to solve the Max-PoSSo problem. The algorithms are different from the previous ones in the literature, which are non-algebraic. By leveraging channel coding theory and dynamic programming, three deterministic and robust algorithms are proposed to solve the satisfiability problems of Boolean polynomial equations. By exploiting channel coding theory, the proposed algorithms are capable of making the initial solutions uniformly distributed over the entire space [16]. Then, a better solution can be found by searching within a fixed radius.

II. PROBLEM DESCRIPTION
The satisfiability problem of maximal Boolean polynomial equations is an extended problem of general Boolean polynomial equation. The satisfiability problem of maximal Boolean polynomial equations is expressed in the sequel. Given the following $m$ Boolean polynomial equations with $n$ variables:

\[
\begin{align*}
& f_1(x_0, x_1, \ldots, x_{n-1}), \\
& f_2(x_0, x_1, \ldots, x_{n-1}), \\
& \vdots \\
& f_m(x_0, x_1, \ldots, x_{n-1}),
\end{align*}
\]

the Max-PoSSo problem is to find a set of $x_0, x_1, \ldots, x_{n-1}$ in GF(2) to make Boolean polynomial equations $f_1, f_2, \ldots, f_m$ have the largest number of value 0 [17], where GF(2) is the Galois field of two elements, 0 or 1.

III. THE ALGORITHM BASED ON CHANNEL CODING THEORY IS DETERMINISTIC AND ROBUST
Forward error correction (FEC) coding is an important technique in communication. In 1948, Shannon demonstrated in the seminal paper that [18], errors induced by a noisy channel or the storage medium can be reduced to be arbitrarily small without sacrificing the information transmission rate or storage rate [19].

The fundamental principle of error-correcting codes [20] is that the sender encodes a message by adding redundant information. The redundancy allows the receiver to detect or correct a limited number of errors that may occur anywhere in the message, thus messages with errors can be recovered without requiring any retransmission. The message that is allowed to be sent is called a codeword, and the set of codewords forms an error correction code. If the received signal is not a legitimate codeword, it is certain that error(s) occurs in the transmission. It is still possible to recover the information from the error-prone message if the number of errors are within certain limit, which is determined by the minimum Hamming distance of the code [21].

**Definition 1:** A $(n, k)$ linear block code has $2^k$ codewords forming a $k$-dimensional subspace of the vector space of all the $n$-tuples in GF(2).

The modulo-2 addition of any two codewords will be another codeword. Three algorithms based on error correction coding will be presented in the sequel for solving the Max-PoSSo problem. These algorithms are deterministic and robust. The core idea of these three algorithms is that the construction of the linear block code is progressively enhanced in terms of the largest number of Boolean polynomials equal to 0.

Algorithm 1 is described as follows:

1) Construct a $k \times n$ generator matrix (i.e., $G$) of a linear block code.

2) Obtain all the codewords $C = \{c_1, \ldots, c_{2^k}\}$ according to the generator matrix, $|C| = 2^k$. In order to solve Boolean polynomial equations, a generator matrix needs to be constructed in a pre-specified manner.

3) Take one codeword obtained in Step 2 as an initial solution and compute the number of Boolean polynomials equal to 0.

4) Start from the initial solution and set the number of erroneous bits as $r$ (i.e., search radius). Candidate solutions obtained from the initial solution has a Hamming distance less than or equal to $r$. Go through all the candidate solutions $D = \{d_1, d_2, \ldots\}$ with $|D| = \binom{n}{r} + \cdots + \binom{n}{0}$ and compute their corresponding numbers of Boolean polynomials equal to 0. Find the candidate solution with the largest number of Boolean polynomials equal to 0 and set it as a suboptimal solution associated with the codeword in Step 3. In one round of search, until going through all variables within radius $r$ the algorithm will stop.

5) Obtain the largest number of Boolean polynomial equations equal to 0.
Algorithm 1 Based on Coding Theory

Require:
- $k$: Number of rows of the generated matrix;
- $G$: Generator matrix;
- $r$: Search radius;
- $f_1, f_2, \ldots, f_m$: Boolean polynomial equations;
- $gen(c)$: Generate all the candidates which have Hamming distance less than or equal to $r$ with $c$;
- $count()$: Count the number of $f_1, f_2, \ldots, f_m$ being 0;

Ensure:
- Max: Maximum number of $f_1, f_2, \ldots, f_m$ being 0;

1: for $j = 1 : 2^k$ do
2: $D_j = gen(c_j)$;
3: for $m = 1 : \binom{k}{0} + \cdots + \binom{k}{r}$ do
4: $C(j, 1) = count(c_j)$; \triangleright $C$ is a matrix, collecting the number of polynomials being 0
5: $C(j, m + 1) = count(d_{jm})$; \triangleright $d_{jm}$ denotes the $m$-th element in the set $D_j$ at $i$-th iteration
6: end for
7: end for
8: $m = max(C)$; \triangleright $m$ is a column vector containing the maximum value of each row
9: $Max = max(m)$;
10: return $Max$

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The concept of FEC coding is used to solve the Max-PoSSo problem in this experiment.

As an introductory example, the number of Boolean polynomial equations is set to be 8 and the number of variables is set to be 4. The Boolean polynomial equations are provided in (2).


generate matrix $A$ is a binary representation of natural numbers from 0 to 7 while each row of matrix $B$ is a binary representation of odd numbers from 0 to 7. Multiplying $A$ with $B$ offers an initial solution (in total 8 solutions). Then, based on each initial solution, we increase the search radius $r$ until finding the candidate solution with the largest number of Boolean polynomials equal to 0. The experimental results are shown in Table 1, Table 2 and Table 3. Most search results with a radius of 1 in Table 1 cannot satisfy the condition that six polynomials in (2) are equal 0. When the search radius is increased to 2, the number of satisfying polynomials saturates.

Table 1. The results of searching radius 1 in Algorithm 1.

| Initial solution | Largest value | Initial solution | Largest value |
|------------------|---------------|-----------------|---------------|
| 1                | 6             | 5               | 5             |
| 2                | 5             | 6               | 5             |
| 3                | 4             | 7               | 6             |
| 4                | 6             | 8               | 5             |

Table 2. The results of searching radius 2 in Algorithm 1.

| Initial solution | Largest value | Initial solution | Largest value |
|------------------|---------------|-----------------|---------------|
| 1                | 6             | 5               | 6             |
| 2                | 6             | 6               | 6             |
| 3                | 6             | 7               | 6             |
| 4                | 6             | 8               | 6             |

Table 3. The results of searching radius 3 in Algorithm 1.

| Initial solution | Largest value | Initial solution | Largest value |
|------------------|---------------|-----------------|---------------|
| 1                | 5             | 6               | 6             |
| 2                | 6             | 6               | 6             |
| 3                | 6             | 7               | 6             |
| 4                | 6             | 8               | 6             |

Next, we extend Algorithm 1 to more complicated cases, where the number of Boolean polynomials $m$ is set to 256 and the number of variables $n$ in all the equations is set to 128. Table 4, and Table 5 show the results of this experiment. As shown in tables, each of the 256 initial solutions satisfies the largest number of Boolean polynomials equal to 0. In the tables, 1:181 means the largest number of Boolean polynomials equal to 0 is 181 for the first initial solution. Table 4 shows the search results of Algorithm 1 with radius 2, and the number of Boolean polynomials that being 0 is between 173 and 200. Table 5 shows the search results of Algorithm 1 with radius 4, and the number of Boolean polynomials being 0 is between 189 and 223. Table 6 presents the statistics of the experimental results. Fig. 1 shows the
TABLE 4. The results of searching radius 2 in Algorithm 1.

| Search radius | Largest value | Expected value | Standard Deviation |
|---------------|---------------|----------------|-------------------|
| 1             | 186           | 170.758        | 4.9066            |
| 2             | 200           | 186.0625       | 5.0321            |
| 3             | 208           | 195.3110       | 4.9072            |
| 4             | 223           | 207.2891       | 6.7251            |

320 initial are randomly generated and the largest numbers of Boolean polynomials are calculated accordingly. Comparing to the results in Table 6, the randomly constructed initial solution results in almost the same largest value as long as the search radii are the same. In other words, Algorithm 1 converges regardless of the initial generator matrix in the first step. Therefore, Algorithm 1 is deterministic and robust to find the maximum value of Boolean polynomial equations.

In order to verify the stability of the algorithm 1, we choose 8 out of 256 suboptimal solutions which have the largest number of Boolean polynomials equal to 0. Then, we construct a new generator matrix with the 8 suboptimal solutions as its rows and continue Step 2 until the largest number of Boolean polynomials equal to 0 is not increasing or the maximum number of iterations is 10.

Algorithm 2 is described as follows:

1) Construct a \( k \times n \) generator matrix (i.e., \( G \)) of a linear block code.

VOLUME 8, 2020

26767
2) Obtain all the codewords \( C = \{ c_1, \cdots, c_k \} \) according to the generator matrix, \( |C| = 2^k \).

3) Take one codeword obtained in Step 2 as an initial solution and compute the number of Boolean polynomials equal to 0.

4) Start from the initial solution and set the number of erroneous bits as \( r \) (i.e., search radius). Candidate solutions obtained from the initial solution has a Hamming distance less than or equal to \( r \). Go through all the candidate solutions \( D = \{ d_1, d_2, \cdots \} \) with \( |D| = \binom{n_1}{r} + \cdots + \binom{n_r}{r} \)

\[ |D| = \binom{n_1}{r} + \cdots + \binom{n_r}{r} \]
Algorithm 2 Iterative Algorithm Based on Coding Theory

Require:
- \( k \): Number of rows of the generated matrix;
- \( G^{(1)} \): Generator matrix;
- \( r \): Search radius;
- \( f_1, f_2, \ldots, f_m \): Superscript \((1)\) is the iteration index

Iterate: Maximum number of iterations;
- \( \Delta \): Number of polynomials equal to 0;
- \( \Delta_{\text{max}} \): Increase of the largest number of \( f_1, f_2, \ldots, f_m \) being 0, which is initialized as 0.

Ensure:
- \( \Delta \): Generate all the candidates which have Hamming distance less than or equal to \( r \) with \( c \);
- \( \Delta_{\text{max}} \): Count the number of polynomials being 0.

Ensure:
- \( \Delta \): Maximum number of \( f_1, f_2, \ldots, f_m \) being 0;

1: while \( i < \text{Iter}_{\text{max}} \) and \( \Delta_{\text{max}} > 1 \) do
2: \( T_0 = \text{gen}(c_{(i)}) \); \( i \) is the iteration index
3: \( T_0 = \text{gen}(c_{(i)}) \); \( i \) is the iteration index
4: \( m = 1 : ( \frac{r}{2} ) + \ldots + ( \frac{r}{2} ) \) do
5: \( C(j, 1) = \text{count}(c_{(i)}) \); \( C \) is a matrix, collecting the number of polynomials being 0
6: \( C(j, m + 1) = \text{count}(d_{(i)}) \); \( d_{(i)} \) denotes the \( m \)-th element in the set \( T_0 \) at \( i \)-th iteration
7: end for
8: end for
9: \( m_{(i)} = \text{max}(C) \); \( m_{(i)} \) is a column vector containing the maximum value of each row
10: \( m_{(i)} = \text{max}(C) \); \( m_{(i)} \) is a column vector containing the maximum value of each row
11: Choose \( k \) \( n \)-tuples corresponding to the \( k \) largest values in \( m_{(i)} \) as rows of new generator matrix \( G^{(i+1)} \);
12: \( \Delta_{\text{max}} = \text{max}(m_{(i)}) \); \( \Delta_{\text{max}} \) is the maximum value in \( m_{(i)} \)
13: \( \Delta = \Delta_{\text{max}} \); \( \Delta \)
14: end while
15: return \( \Delta \)

The results of the first, fifth and tenth iterations show that the number of polynomials equal to 0 is stable.

and compute their corresponding numbers of Boolean polynomials equal to 0. Find the candidate solution with the largest number of Boolean polynomials equal to 0 and set it as a suboptimal solution associated with the codeword in Step 3.

5) Repeat Steps 3 and 4 until all the codewords are covered. Choose \( k \) out of \( 2^k \) suboptimal solutions which have the largest number of Boolean polynomials equal to 0. Construct a new generator matrix with the \( k \) suboptimal solutions as its rows and continue Step 2 until the largest number of Boolean polynomials equal to 0 is not increasing or the maximum number of iterations is reached.

6) Obtain the largest number of Boolean polynomials equal to 0 and set its corresponding \( n \)-tuples as the final solution.

The experimental results are shown in the Tables 10, 11, 12. The results of the first, fifth and tenth iterations show that the number of polynomials equal to 0 is stable.

V. COMPARISON WITH OTHER ALGORITHMS

In [22], solving the maximum Boolean polynomial equations is consistent with the problem studied in this paper.

Genetic algorithm is a computational method that simulates natural selection and biological evolution. The optimal solution is searched by simulating the natural evolutionary process. The initial individual is selected based on a fitness function while the optimal individual is obtained in the last generation after crossover and mutation operations [22]. Because of the "premature phenomenon" of the Genetic algorithm, the local convergence rate is slow in the absence of effective heuristic information, and the final solution is...
TABLE 11. The results of searching radius 3 in Algorithm 2 and the number of iterations is 5.

| Algorithm | Genetic | Proposed |
|-----------|---------|----------|
| 1.2 | 32.210 | 65.210 | 97.210 | 129.210 | 161.210 | 193.210 | 225.210 |
| 2.3 | 34.210 | 66.210 | 98.210 | 130.210 | 162.210 | 194.210 | 226.210 |
| 3.4 | 35.210 | 67.210 | 99.210 | 131.210 | 163.210 | 195.210 | 227.210 |
| 4.5 | 36.210 | 68.210 | 100.210 | 132.210 | 164.210 | 196.210 | 228.210 |
| 5.6 | 37.210 | 69.210 | 101.210 | 133.210 | 165.210 | 197.210 | 229.210 |
| 6.7 | 38.210 | 70.210 | 102.210 | 134.210 | 166.210 | 198.210 | 230.210 |

TABLE 12. The results of searching radius 3 in Algorithm 2 and the number of iterations is 10.

| Algorithm | Genetic | Proposed |
|-----------|---------|----------|
| 1.2 | 32.210 | 65.210 | 97.210 | 129.210 | 161.210 | 193.210 | 225.210 |
| 2.3 | 34.210 | 66.210 | 98.210 | 130.210 | 162.210 | 194.210 | 226.210 |
| 3.4 | 35.210 | 67.210 | 99.210 | 131.210 | 163.210 | 195.210 | 227.210 |
| 4.5 | 36.210 | 68.210 | 100.210 | 132.210 | 164.210 | 196.210 | 228.210 |
| 5.6 | 37.210 | 69.210 | 101.210 | 133.210 | 165.210 | 197.210 | 229.210 |
| 6.7 | 38.210 | 70.210 | 102.210 | 134.210 | 166.210 | 198.210 | 230.210 |

TABLE 13. Comparison with other algorithms.

| Algorithm | Genetic | Proposed |
|-----------|---------|----------|
| Largest value | 182 | 223 |

usually the local optimal rather than the global optimal. In order to overcome this problem, [22] made several fine tunings of parameters in their experiment, and the optimal solution has 182 Boolean polynomials equal to 0. The comparison between the proposed algorithms and genetic algorithm is shown in Table 13. Our proposed Algorithm 1 achieves better results of 223 Boolean polynomials equal to 0. Our proposed algorithm is able to find 200 Boolean equations equal to 0 when the search radius is 2, and the convergence speed is much faster than that of the genetic algorithm. In addition to the premature phenomenon of genetic algorithm, the randomness of genetic algorithm is also an important factor to affect the performance of the algorithm. When solving a large number of variables, it is difficult to find a good solution.

The complexity of the proposed Algorithm 1 is closely related to the search radius $r$, and $k$ is only used to construct the generating matrix. In terms of a small search radius, our proposed Algorithm 1 is much more efficient than the algorithm in [22]. Compared with the randomness of genetic algorithm, our proposed Algorithm 1 is more deterministic.

Comparison is also made with the Gröbner basis algorithm, taking the polynomial in equation (2) as an example. We enumerate all combinations of polynomials and then compute them using the Gröbner basis method. Gröbner basis is capable of obtaining up to five Boolean polynomials equal to 0. Our proposed algorithm can find six Boolean polynomials equal to 0. Regarding the complexity, our algorithm has complexity $O(n^r)$, while Gröbner basis algorithm has complexity $O(2^n)$. It is clear that the complexity of the Gröbner basis algorithm is much higher than that of our proposed algorithm. The Gröbner algorithm can solve general Boolean polynomial equations. However, due to the high complexity of the algorithm, it is necessary to consider the computation efficiency when solving a large number of variable equations. Therefore, Gröbner algorithm is not suitable for solving maximal Boolean polynomial equations.

VI. EXTENSION ALGORITHM

In step 4) of Algorithm 2, some candidate solutions may be repetitively chosen. Therefore, a modified algorithm, denoted as Algorithm 3, will be introduced to address the aforementioned drawback.

We explain the potential for further improving the efficiency of solving the Max-PoSSo problem in the sequel. Let the Hamming distance between $c_1$ and $c_2$ be denoted by $d$. The location set of different bits between $c_1$ and $c_2$ is denoted by $M$, then $|M| = d$. The location set of the same bits between $c_1$ and $c_2$ is denoted by $N$, $|N| = n - d$. Fig. 4 shows the relationship between $c_1$ and $c_2$ with...
Algorithm 3 Enhanced Version of Algorithm 2

Require:

- $k$: Number of rows of the generated matrix;
- $G^{(1)}$: Generator matrix;
- $r$: Search radius;
- $f_1, f_2, \cdots, f_m$: Superscript (1) is the iteration index $\text{Iter}_{\text{max}}$: Maximum number of iterations;
- $\Delta_{\text{max}}$: Increase of the largest number of Boolean polynomials being 0, which is initialized as 0.

$\text{gen}(c_j|c_{j-1})$: Generate all the candidates which have Hamming distance less than or equal to $r$ with $c_j$ conditioned on $c_{j-1}$;

$\text{count}(\cdot)$: Count the number of $f_1, f_2, \cdots, f_m$ being 0.

Ensure:

Max: Maximum number of $f_1, f_2, \cdots, f_m$ being 0;

1: while $i < \text{Iter}_{\text{max}}$ and $\Delta_{\text{max}} > 1$ do
   2: for $j = 1 : 2^k$ do
      3: $D_j^{(i)} = \text{gen}(c_j|c_{j-1})$;
      4: for $m = 1 : |D_j^{(i)}|$ do
         5: $C(j, 1) = \text{count}(c_j^{(i)})$;
         6: $C(j, m + 1) = \text{count}(c_{j,m}^{(i)})$;
      7: end for
   8: end for
   9: $m^{(i)} = \max(C)$;
   10: $\max^{(i)} = \max(m^{(i)})$;
   11: Choose the $k$ $n$-tuples corresponding to the $k$ largest values in $m^{(i)}$ as rows of new generator matrix $G^{(i+1)}$;
   12: $i++$;
   13: $\Delta_{\text{max}} = \max^{(i)} - \text{Max}$;
   14: Max = $\max^{(i)}$;
15: end while
16: return Max

In this case, the candidate solutions for $c_1$ and $c_2$ are overlapping with each other (overlapped area is filled with lines). In Algorithm 2, the candidate solutions for $c_1$ will be in the ball centered at $c_j$ with radius $r$. Similarly, the candidate solutions for $c_2$ will be in the ball centered at $c_j$ with radius $r$. Overlapped area is considered twice. Therefore, in Algorithm 3, only the candidate solutions in the gray area are considered for $c_2$. The first three steps of Algorithm 3 are the same as Algorithm 2.

The remaining steps of Algorithm 3 are described as follows:

4) Start from the initial solution denoted $c_1$, and set the number of erroneous bits as $r$ (i.e., search radius). Candidate solutions obtained from the initial solution have a Hamming distance less than or equal to $r$. Compute the number of Boolean polynomials equal to 0 for all the candidate solutions. The candidate solution with largest number of Boolean equation equal to 0 is taken as a suboptimal solution associated with the corresponding codeword $c_1$.

5) In order to avoid repeated search for $c_2$, choose $u$ bits in the location set $\mathcal{M}$ and $s$ bits in the location set $\mathcal{N}$. Note that $u$ and $s$ must satisfy the condition $r + u - d < s \leq r - u$ and $0 < u \leq d/2$. The candidate solution with largest number of Boolean equation equal to 0 is taken as a suboptimal solution associated with the corresponding codeword $c_2$.

6) Repeat steps 3), 4) and 5) until all the codewords are covered. Choose $k$ out of $2^K$ suboptimal solutions which have the largest number of Boolean polynomials equal to 0. Construct a new generator matrix with the $k$ suboptimal solutions as its rows and continue step 2) until the largest number of Boolean polynomials equal to 0 is not increasing or the largest number of iterations is reached.

7) Obtain the largest number of Boolean polynomials equal to 0 and set its corresponding $n$-tuples as the final solution.

The experiment in Section IV is repeated by using Algorithm 3. In order to evaluate the performance improvement of the algorithm, we consider the actual running time as a performance metric for comparison. It turns out that Algorithm 3 has the same performance as Algorithm 1 and Algorithm 2, while the running time of Algorithm 3 is 20% less than that of Algorithm 1 and Algorithm 2.

VII. CONCLUSION

In this paper, a non-algebraic method has been proposed to solve the maximal Boolean polynomial. Three deterministic and robust algorithms have been proposed to solve the problem of the satisfiability of Boolean polynomial equations based on coding theory. As the search radius $r$ increases, the number of the Boolean polynomials equal to 0 increases. Algorithm 3 has the same performance as Algorithm 1 and Algorithm 2, while Algorithm 3 runs about 20% faster than Algorithm 1 and Algorithm 2. The number of Boolean polynomials equal to 0 obtained by the proposed algorithms has been significantly increased compared to the benchmark scheme in [21]. Compared to the randomness of genetic algorithm, our proposed algorithms are more deterministic and robust. The complexity of the proposed algorithms is much less than Gröbner algorithm. In addition, the proposed algorithms are capable of solving non-deterministic hard problem in a more effective way.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 1999, pp. 388–397.

[2] M. Renaud and F.-X. Standaert, “Algebraic side-channel attacks,” in Proc. Int. Conf. Sel. Areas Cryptogr. Berlin, Germany: Springer, 2009, pp. 393–410.

[3] I. Grattan-Guinness, “George Boole, An investigation of the laws of thought on which are founded the mathematical theory of logic and probabilities (1854),” in Landmark Writings in Western Mathematics. Amsterdam, The Netherlands: Elsevier, 2005, pp. 470–479.

[4] Z. Huang and D. Lin, “A new method for solving polynomial systems with noise over $\mathbb{F}_2$ and its applications in cold boot key recovery,” in Proc. Int. Conf. Sel. Areas Cryptogr. Berlin, Germany: Springer, 2012, pp. 16–33.

[5] P. Rizomiliotis, “On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation,” IEEE Trans. Inf. Theory, vol. 56, no. 8, pp. 4014–4024, Aug. 2010.
[6] K.-Y. Chao and J.-C. Lin, “Secret image sharing: A Boolean-operations-based approach combining benefits of polynomial-based and fast approaches,” Int. J. Pattern Recognit. Artif. Intell., vol. 23, no. 2, pp. 263–285, 2009.

[7] D. S. Kim, T. Kim, and J. J. Seo, “A note on q-analogue of boole polynomials,” Appl. Math. Inf. Sci., vol. 9, no. 6, pp. 3153–3158, 2014.

[8] G. V. Bard, N. T. Coutoís, and C. Jefferson, “Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over GF(2) via SAT-solvers,” Cryptology ePrint Arch., Tech. Rep. 2007/024, 2007. [Online]. Available: https://eprint.iacr.org/2007/024

[9] M. Albrecht and C. Cid, “Cold boot key recovery by solving polynomial systems with noise,” in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur. Berlin, Germany: Springer, 2011, pp. 57–72.

[10] Q. Wang, J. Peng, H. Kan, and X. Xue, “Constructions of cryptographically significant Boolean functions using primitive polynomials,” IEEE Trans. Inf. Theory, vol. 56, no. 6, pp. 3048–3053, Jun. 2010.

[11] S. Mesnager, “Bent and hyper-bent functions in polynomial form and their link with some exponential sums and dickson polynomials,” IEEE Trans. Inf. Theory, vol. 57, no. 9, pp. 5966–6009, Sep. 2011.

[12] Z. Huang and D. Lin, “Solving polynomial systems with noise over $F_2$: Revisited,” Theor. Comput. Sci., vol. 676, pp. 52–68, May 2017.

[13] M. Brickenstein and A. Dreyer, “PolyBoRi: A framework for Gröbner-basis computations with Boolean polynomials,” J. Symbolic Comput., vol. 44, no. 9, pp. 1326–1345, 2009.

[14] Y. Lv, F. Liu, and Z. Ting, “Random muti-bit flipping algorithm solves the satisfiability problems of Boolean polynomial equations,” J. Jiangxi Univ. Sci. Technol., vol. 39, no. 1, pp. 60–65, 2018.

[15] X.-S. Gao and Z. Huang, “Characteristic set algorithms for equation solving in finite fields,” J. Symbolic Comput., vol. 47, no. 6, pp. 655–679, Jun. 2012.

[16] G. Wu, Y. Lv, and J. He, “Design of high-rate LDPC codes based on matroid theory,” IEEE Commun. Lett., vol. 23, no. 12, pp. 2146–2149, Dec. 2019.

[17] W. Ryan and S. Lin, Channel Codes: Classical and Modern. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[18] C. E. Shannon, “A mathematical theory of communication,” Bell Syst. Tech. J., vol. 27, no. 3, pp. 379–423, Jul./Oct. 1948.

[19] C. Shannon, “Communication in the presence of noise,” Proc. IEEE, vol. 72, no. 9, pp. 1192–1201, Jan. 1984.

[20] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, vol. 16. Amsterdam, The Netherlands: Elsevier, 1977.

[21] S. Zhang, P. Lin, G. Wu, and L. Jiang, “Construct the systematic binary quasi-cyclic codes with rate 1/p based on variable matroid search algorithm,” J. Electron. Inf. Technol., vol. 38, no. 11, pp. 2916–2921, 2016.

[22] S. Y. Yang, “The solution for satisfaction of maximal boolean polynomial equations based on genetic algorithm,” in Proc. Int. Conf. Comput., Automat. Power Electron., 2017, vol. 1, no. 5, pp. 71–77.

**GUANGFU WU** was born in Yushan, Jiangxi, China, in 1977. He received the B.S. degree in mathematics education from Wuyi University, Guangdong, in 2000, the M.S. degree from the School of Mathematical Sciences, Xiamen University, Xiamen, in 2008, and the Ph.D. degree from the School of Information Science and Engineering, Xiamen University, in 2012. Since 2016, he has been an Assistant Professor with the School of Information Engineering, Jiangxi University of Science and Technology. He is the author of more than ten articles, and more than ten inventions. His research interests include coding theory and cryptography, blockchain, and artificial intelligence. Dr. Wu became a member (M) of the Chinese Association for Cryptologic Research (CACR), in 2014. YUIE LV was born in Yantai, Shandong, China, in 1991. He received the B.Eng. degree from the Jiangxi University of Science and Technology, Ganzhou, China, in 2015, where he is currently pursuing the master’s degree in computer technology. From 2015 to 2017, he was with China Telecom. His research interests include coding theory and cryptography.

**DAOJING HE** (Member, IEEE) received the B.Eng. and M.Eng. degrees in computer science from the Harbin Institute of Technology, China, in 2007 and 2009, respectively, and the Ph.D. degree in computer science from Zhejiang University, China, in 2012. He is currently a Professor with the Department of Software Engineering, East China Normal University, and also a Guest Professor with the Department of Information Engineering, Jiangxi University of Science and Technology. His research interest includes network and systems security. He is an Associate Editor or on the Editorial Board of some international journals, such as IEEE Communications Magazine and the IEEE/KICS JOURNAL OF COMMUNICATIONS AND NETWORKS.

**JIGUANG HE** (Member, IEEE) received the B.Eng. degree from the Harbin Institute of Technology, Harbin, China, in 2010, the M.Sc. degree from Xiamen University, Xiamen, China, in 2013, and the D.Sc. degree from the University of Oulu, Oulu, Finland, in 2018, all in communications engineering. From September 2013 to March 2015, he was with the Key Laboratory of Millimeter Waves, City University of Hong Kong, and conducting research on channel tracking over millimeter wave MIMO systems. Since June 2015, he has been with the Centre for Wireless Communications (CWC), University of Oulu. His research interests span cooperative communications, network information theory, joint source and channel coding, and distributed compressive sensing.

**HUAN ZHOU** was born in Ganzhou, Jiangxi, China, in 1995. He received the B.Eng. degree from the Jiangxi University of Science and Technology, in 2017, where he is currently pursuing the master’s degree in computer technology. His main research interests are artificial intelligence and neural networks.

**SAMMY CHAN** (Member, IEEE) received the B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and the Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. From 1989 to 1994, he was with the Telecom Australia Research Laboratories, first as a Research Engineer, and from 1992 to 1994 as a Senior Research Engineer and a Project Leader. Since December 1994, he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an Associate Professor.