STREAM CIPHER USING FINITE-FIELD WAVELETS

Farshid Delgosha and Faramarz Fekri

School of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, GA 30332-0250
E-mail: {farshid,fekri}@ece.gatech.edu

ABSTRACT

We propose a novel framework to design a stream cipher based on wavelets over finite fields. Encryption and decryption are performed by inverse wavelets and their corresponding wavelet transforms. The system is iterative with each round consisting of two wavelet systems and a nonlinear feedback in the encryption and a nonlinear feed-forward in the decryption. The input to the proposed wavelet stream cipher (WSC) is a sequence in the Galois field $\mathrm{GF}(2^8)$. The key consists of 16 symbols of $\mathrm{GF}(2^8)$ that specify the wavelet systems. The security of the system relies on the difficulty of solving nonlinear equations over finite fields which is known to be NP-complete. We have studied the vulnerability of our system to several attacks. Our studies show that although one round might be vulnerable, two rounds resists against all known attacks.

1. INTRODUCTION

Stream ciphers are cryptographic tools used to encrypt a stream of digital data. They are more appropriate for applications where buffering is limited or when data must be individually processed as they are received. Since they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable. The stream cipher RC4 is widely used since it is very fast in software implementation [1]. Although no feasible attack has been found on RC4, it is believed to be insecure [2, 3].

In [4], we show that finite-field wavelets can be used to design efficient block ciphers. In this paper, we extend those ideas and propose a new approach in designing stream cipher based on finite-field wavelets. At the core of our proposed scheme is a wavelet transform that operates over the Galois field $\mathrm{GF}(2^8)$. Since this transform is linear, we also employ nonlinear mappings in the system. The proposed WSC is an iterative cryptosystem. One round of the encryption system consists of two wavelet transforms and a nonlinear mapping in the main path connecting the input to the output and also a nonlinear feedback. The key consists of 16 symbols from $\mathrm{GF}(2^8)$ that are exchanged between users by the Diffie-Hellman key exchange protocol. The key symbols are used to set up the wavelet transform.

In Section 2, we briefly review the filter bank realization of wavelets. We provide a linear time-variant model for wavelets in Section 3 that is used to investigate the security of WSC. The basic round of the WSC is proposed in Section 4. In Section 5, we study the vulnerability of the WSC to some attacks. Finally, Section 6 gives the concluding remarks.

Notation: The Galois field $\mathrm{GF}(2^q)$ is denoted by $\mathbb{F}_{2^q}$ or $\mathbb{F}$ when the value of q is not important. The symbol $\mathbb{N}_n^0$ is defined as $\mathbb{N}_n^0 \triangleq \{0, 1, \ldots, n\}$. The variable n is used for time-domain signals and the variable z for signals in the z domain. A matrix $\mathbf{A}$ is called unitary if $\mathbf{A}^T\mathbf{A} = \mathbf{I}$. A matrix $\mathbf{E}(z)$ over the ring $\mathbb{F}[z^{-1}]$ is called paraunitary (PU) if $\mathbf{E}^T(z^{-1})\ \mathbf{E}(z) \equiv \mathbf{I}$.

2. REVIEW OF THE WAVELET TRANSFORM

The filter bank realization of the wavelet is shown in Figure 1. The analysis bank realizes the wavelet transform that consists of the FIR filters $\tilde{g}_0(n)$ and $\tilde{g}_1(n)$ of odd length L. (It is proved in [5] that L is always odd.) The inverse wavelet transform is realized by the synthesis bank consisting of the FIR filters $\tilde{h}_0(n)$ and $\tilde{h}_1(n)$ of the same length. If $\mathbf{E}(z) = [E_{ij}(z)]$ and $\mathbf{R}(z) = [R_{ij}(z)]$ are the polyphase matrices of the analysis and synthesis banks, then [6]

$$\tilde{G}_i(z) = E_{i0}(z^2) + z^{-1}E_{i1}(z^2) \tag{1a}$$

$$\tilde{H}_i(z) = z^{-1}R_{0i}(z^2) + R_{1i}(z^2). \tag{1b}$$

When the polyphase matrix is PU, the two filters in the analysis bank are polynomial inverses of each other [6], i.e.,

$$\tilde{G}_1(z) = z^{-L}\tilde{G}_0(z^{-1}) \tag{2}$$

where L is the order of the filters. The same is true for the filters in the synthesis bank.

We design the polyphase matrix of the filter bank as a PU matrix since, by the following theorem, there are building blocks to generate all 2×2 PU matrices over fields of characteristic two [5].

Theorem 1. *A 2×2 matrix $\mathbf{E}(z)$ over $\mathbb{F}[z^{-1}]$ is PU if and only if it can be factorized as*

$$\mathbf{E}(z) = \prod_{i=1}^{N} \mathbf{A}_i\, \mathbf{D}(z;\ \mathbf{v}_i)\, \mathbf{S}_{2\tau_i}(z;\ \zeta_i) \tag{3}$$

where $\mathbf{A}_i$ is either the identity or a unitary matrix and the building blocks $\mathbf{D}$ and $\mathbf{S}$ respectively are:

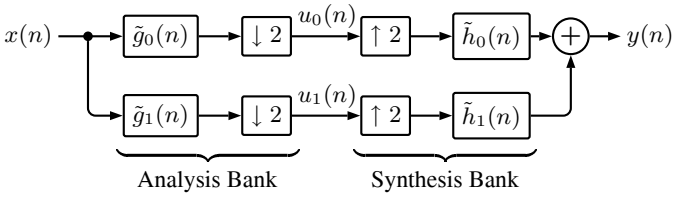

Fig. 1. Two-band filter bank.

1. *The degree-one building block*

$$\mathbf{D}(z;\ \mathbf{v}) \triangleq \mathbf{I} + \mathbf{v}\mathbf{v}^T + \mathbf{v}\mathbf{v}^T z^{-1} \tag{4}$$

where $\mathbf{v} \in \mathbb{F}^2$ *is either zero or* $\mathbf{v} = \begin{bmatrix} a, 1+a \end{bmatrix}^T$ *for some* $a \in \mathbb{F}$.

2. *The degree-*2τ *building block*

$$\mathbf{S}_{2\tau}(z;\ \zeta) \triangleq \zeta \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \mathbf{I} z^{-\tau} + \zeta \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} z^{-2\tau} \tag{5}$$

where $\zeta \in \mathbb{F}$ *and* τ *is a nonnegative integer.*

If the numbers of the $\mathbf{D}$ *and* $\mathbf{S}$ *building blocks in (3) are* d *and* s*, respectively, then the degree of the PU matrix* $\mathbf{E}(z)$ *is* $d + 2\sum_{i=1}^{s} \tau_i$.

By this theorem, if we ignore the unitary matrices in (3), in order to design a 2×2 PU matrix, we must know

1. The number of $\mathbf{D}$ and $\mathbf{S}$ building blocks denoted by d and s, respectively.
2. Degrees $2\tau_1, \ldots, 2\tau_s$ of the $\mathbf{S}$ building blocks.
3. The vector $\mathbf{v}_i$ and the constant ζ_i in the $\mathbf{D}$ and $\mathbf{S}$ building blocks, respectively.
4. The order in which building blocks are multiplied together. (Since the $\mathbf{S}$ building blocks commute, we avoid the arrangements in which these building blocks are adjacent in order to prevent decreasing the number of effective keys.)

All this information is assumed to be public except the vectors $\mathbf{v}_i$ and the constant ζ_i that are determined using the secret key. The secret key consists of $K = d + s$ randomly chosen elements from $\mathbb{F}$ that are exchanged using the Diffie-Hellman key exchange protocol or any public-key scheme.

By Theorem 1, the degrees of the PU matrix $\mathbf{E}(z)$ is $d + 2\sum_{i=1}^{s} \tau_i$. Hence, from (1a), the degree of $\tilde{G}_i(z)$ as a polynomial is $L = 2\left(d + 2\sum_{i=1}^{s} \tau_i\right) + 1$. If $\tau_i = \tau$ for all i, then

$$L = 2K + 2(2\tau - 1)s + 1. \tag{6}$$

For the typical values $K = 16$, $s = 1$, and $\tau = 1$, we get $L = 35$.

3. LINEAR TIME-INVARIANT MODEL OF THE WAVELET

In this section, we modify the structure of the filter-bank realization of the wavelet transform to suit in designing a stream cipher. We also give linear time-invariant models of the given structures.

The systems in Figures 2 and 3 can be considered as a wavelet transform and its inverse. We use these structures in our stream cipher design since each of them has a single input and a single output in contrary to the analysis and synthesis banks of the filter bank in Figure 1.

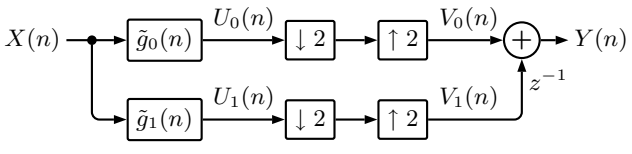

Fig. 2. Modified wavelet transform.

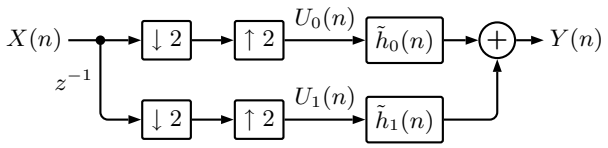

Fig. 3. Modified inverse wavelet transform.

It can be easily verified that the input and output of the system in Figure 2 are related as

$$Y(n) = \sum_{k=-\infty}^{\infty} g(n,k)\, X(k) \tag{7}$$

where

$$g(n,k) = \begin{cases} \tilde{g}_0(n-k), & n \text{ even} \\ \tilde{g}_1(n-k-1), & n \text{ odd.} \end{cases} \tag{8}$$

The filter $g(n,k)$ can be considered as the kernel of a linear time-variant (LTV) system with the following properties:

Causality: The filters $\tilde{g}_0(n)$ and $\tilde{g}_1(n)$ are designed to be causal. Therefore, $g(n,k) = 0$ for $n < k$.

Odd Indices: By definition, $g(n,n) = \tilde{g}_1(-1)$ when n is odd. Since $\tilde{g}_1(n)$ is causal, we have $g(n,n) = 0$ for odd n.

Periodicity: By (8), $g(n+2, k+2) = g(n,k)$. Hence, $g(n,k)$ is completely known if we learn about $g(n,k)$ when the second argument k is restricted to $\mathbb{N}_1^0$.

It can be easily shown that the LTV model of the system in Figure 3 is as follows

$$Y(n) = \sum_{k=-\infty}^{\infty} h(n,k)\, X(k) \tag{9}$$

where

$$h(n,k) = \begin{cases} \tilde{h}_0(n-k), & k \text{ even} \\ \tilde{h}_1(n-k-1), & k \text{ odd.} \end{cases} \tag{10}$$

4. THE BASIC ROUND OF THE WSC

The wavelet transform introduced in the previous section, is used to scramble the plaintext. Equation (7) reveals that the output of the filter $g(n,k)$ is a linear combination of the coefficients of $g(n,k)$ that are unknown to the adversary. Since convolution is a linear operator, we add some nonlinearity and suggest the structure of Figure 4 as the basic round of the wavelet encryption system. In this figure, h_1 and h_2, given by (10), are the LTV systems of the two inverse wavelet transforms and f is a nonlinear function. Since the mapping f is located at the feedback, we also include a unit delay. The information about the function f is stored in a public directory. The mapping $(\cdot)^d$ is another nonlinearity where

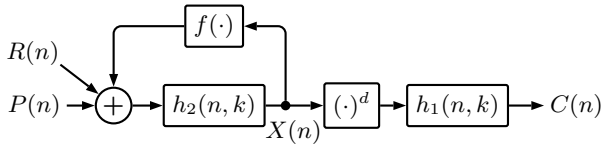

Fig. 4. One round of the WSC.

$d > 1$ is a positive integer that will be determined later in this section. All sequences are assumed over $\mathbb{F}_{2^8}$.

The filters $h_1(n,k)$ and $h_2(n,k)$ are designed by constructing two PU matrices as explained in Section 2. The key symbols and a bit-permutation of their concatenation are used as the parameters of these PU matrices. In other words, if $\mathcal{K}$ is the bit string obtained by concatenating the K key symbols from $\mathbb{F}$, then the two PU matrices are designed using $\mathcal{K}$ and $\sigma(\mathcal{K})$ where σ, a permutation on $K|\mathbb{F}|$ elements, is public. For more than one round of the WSC, all PU matrices are designed using public bit-permutations of $\mathcal{K}$.

The random *time-limited* sequence $R(n)$ is added to $P(n)$ at the input of the system to mask the plaintext. (If there is more than one round of the system, $R(n)$ is added only to the input of the first round.) This sequence is changed for every new plaintext stream. Because of the feedback, $R(n)$ affects all the ciphertext symbols. This makes the encryption system very hard to attack. The output of the decryption system is $P(n) + R(n)$. Since $R(n) = 0$ for $n \geq n_R$, where n_R is a fixed positive integer, then only the first n_R symbols of the decrypted sequence are affected by $R(n)$ and must be ignored since the decryption system does not know $R(n)$. The protection we gain by using $R(n)$ worths ignoring a few symbols.

The equations relating the plaintext and ciphertext are

$$X(n) = \sum_{k=0}^{n} h_2(n,k)\Big[P(k) + R(k) + f(X(k-1))\Big] \quad (11a)$$

$$C(n) = \sum_{k=0}^{n} h_1(n,k)\, X^d(k). \quad (11b)$$

The basic round of the decryption system is depicted in Figure 5. Here, as in (8), $g_1(n,k)$ and $g_2(n,k)$ are the LTV systems of the two wavelet transforms. They undo the effects of $h_1(n,k)$ and $h_2(n,k)$ respectively. The mapping $(\cdot)^m$ undoes the effect of $(\cdot)^d$.

Inspired by the design of the S-box in AES [7], we suggest using the inversion function for the mapping f, i.e.,

$$f(x) = \begin{cases} x^{-1} & x \neq 0 \\ 0 & x = 0. \end{cases} \quad (12)$$

Equations describing the decryption system are

$$X(n) = \sum_{k=0}^{n} g_1(n,k)C(k) \quad (13a)$$

$$P(n) = \sum_{k=0}^{n} g_2(n,k)X^m(k) + f(X^m(n-1)). \quad (13b)$$

Integers d and m are chosen such that $x^{dm} = x$ for all $x \in \mathbb{F}$, i.e., $m \equiv d^{-1} \pmod{|\mathbb{F}| - 1}$. Since the characteristic of the field is two, d and m should not be powers of two. Moreover, they should have high hamming weights (the number of ones in their binary expansions). This is because if $c = \sum_{i=0}^{B} c_i 2^i$, where $c_i \in \mathbb{N}_1^0$, is the binary expansion of the positive integer c, then for $x \in \mathbb{F}$, we have $x^c = \prod_{\substack{i=0 \\ c_i=1}}^{B} x^{2^i}$ where each term x^{2^i} is $\mathbb{F}$-linear. We suggest $d = 248$ and $m = 182$ to satisfy these criterion.

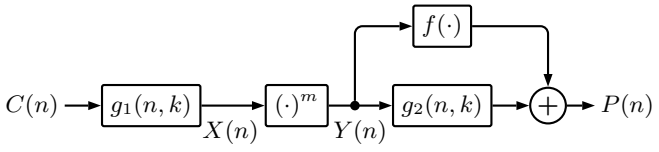

Fig. 5. One round of the decryption system.

5. CRYPTANALYSIS OF THE WSC

Because of the feedback in the encryption, the ciphertext symbol $C(n)$ at time instance n is related to all symbols of the plaintext $P(k)$ at time instances $k \in \mathbb{N}_n^0$. Moreover, the presence of the random sequence in the encryption makes the cryptanalysis of the encryption very hard. Therefore, all the attacks we study in this section are focused on the decryption. The realistic scenario is the chosen-ciphertext attack: the adversary has limited access to the decryption algorithm, so he can choose a few arbitrary ciphertexts, decrypt them, and analyze the resultant plaintext-ciphertext pairs. However, the adversary's goal is having the ability to decrypt all ciphertext messages that he receives.

Exhaustive search is infeasible since if the secret key consists of K symbols from $\mathbb{F}_{2^8}$, then the size of the key space is $|\mathbb{F}_{2^8}|^K = 2^{8K}$. For $K \geq 16$, we have $2^{8K} \geq 2^{128}$. In this section, we explore the resistance of one and two rounds of the WSC against some known attacks: Gröbner basis and interpolation attack. We also propose a new attack called delta attack. Our studies show that one round is vulnerable to this attack. However, two rounds are resistant.

5.1. Gröbner Bases

Gröbner bases is a tool for solving systems of polynomial equations [8]. From (13), in one round, there is an algebraic equation relating the ciphertext C to the plaintext P with the coefficients of $g_1(n,k)$ and $g_2(n,k)$ as $2(L+1)$ unknowns. Combining the two equations (13), we get a multivariate polynomial consisting of two homogenous parts of degrees m and $2m+1$. Algorithms for computing the Gröbner basis are exponential time [8]. However, for small values of m and L, solving this equation might be feasible using the fast algorithm of [9]. For the typical values of m and L in our system, computing the Gröbner basis for one round seems to be infeasible. For two rounds, equations are more complicated and involve more variables. Hence, the complexity of attacking more than one round by computing Gröbner basis is even higher.

5.2. Interpolation Attack

In this attack, the adversary establishes an algebraic relation between the plaintext and the ciphertext with unknown coefficients [10]. Using a set of plaintext-ciphertext pairs, the adversary is able to construct a system of linear equations in the unknown coefficients. Solving this linear system, the adversary can decrypt any ciphertext without knowing the key.

To apply this attack to one round of the WSC, we observe that $X(n)$ in (13a) is a polynomial over $\mathbb{F}_{2^8}$ in ciphertext symbols $C(n-L-1)), \ldots, C(n)$. Similarly, $P(n)$ in (13b) is a polynomial in $X(n-L-1), \ldots, X(n)$. Hence, $P(n)$ is a polynomial in ciphertext symbols. The number of monomials of this polynomial, given by the following lemma, determines the size of the final system of linear equations.

Lemma 1. *Given f as (12), $P(n)$ in (13) is an $(2L+3)$-variate polynomial with at most $(L+2)^{\ell^+ + 1} + (L+2)^{\ell^-}$ monomials*

where ℓ^+ and ℓ^- are the hamming weights of m and $255-m$, respectively.

Proof. For a fixed large value of n, the term $g_2(n,k)X^m(k)$ in (13b) is a polynomial in $C(k-(L+1)),\ldots,C(k)$. The summation term of $P(n)$ in (13b) is a polynomial in $C(n-2(L+1)),\ldots,C(n)$. The term $X^m(n-1)$ inside the function f is also a polynomial in $C(n-(L+2)),\ldots,C(n-1)$. Therefore, $P(n)$ is a $(2L+3)$-variate polynomial. $X^m(k)$ in (13b) has $(L+2)^{\ell^+}$ monomials. The summation in this equation has at most $L+2$ nonzero terms that leads to the total of $(L+2)^{\ell^++1}$ monomials. The term $f(X^m(n-1))$ in $P(n)$ has $(L+2)^{\ell^-}$ monomials. □

For $m=182$, we have $\ell^+=5$ and $\ell^-=3$. For the typical value of $L=35$, the number of monomials is approximately 2^{31}. Finding 2^{31} unknowns from a system of linear equation has complexity $O(2^{93})$ even using fast algorithms such as LUP decomposition [11]. Hence, the interpolation attack is infeasible on one round and henceforth on two rounds of the WSC.

5.3. Delta Attack

This is a chosen-ciphertext attack. A number of ciphertext streams are chosen and applied to the decryption system. Using the output plaintext streams, it is possible to recover the coefficients of the filters $g_1(n,k)$ and $g_2(n,k)$ in one round of the WSC.

In this attack, the adversary feeds the system with two ciphertext streams $C_{n_0 i}(n)=\alpha_i\delta(n-n_0)$ where $n_0\in\mathbb{N}_1^0$, $\alpha_i\in\mathbb{F}\setminus\{0\}$, and $i=1,2$. We require $\alpha_1\neq\alpha_2$. By (13), we can write

$$P_{n_0 i}(n)=\alpha_i^m\underbrace{\sum_{k=0}^{n}g_2(n,k)g_1^m(k,n_0)}_{G(n,n_0)}+f(\alpha_i^m g_1^m(n-1,n_0)). \tag{14}$$

Using two ciphertext-plaintext pairs $(C_{n_0 1},P_{n_0 1})$ and $(C_{n_0 2},P_{n_0 2})$, we obtain a system of two equations that can be solved for $g_1(n-1,n_0)$ as follows

$$g_1(n-1,n_0)=\left[\frac{(\alpha_2/\alpha_1)^m+(\alpha_1/\alpha_2)^m}{\alpha_2^m P_{n_0 1}(n)+\alpha_1^m P_{n_0 2}(n)}\right]^d. \tag{15}$$

Hence, the adversary is able to recover the coefficients of $g_0(n,k)$ and those of $g_1(n,k)$ by (2).

For two rounds of the system, the corresponding equation is

$$\begin{aligned}P_{n_0 i}(n)=&\sum_{k=0}^{n}g_4(n,k)\Bigg[\alpha_i^m G(k,n_0)\\&+\sum_{j=0}^{k}g_3(k,j)f(\alpha_i^m g_1^m(j-1,n_0))\Bigg]^m+f\Bigg(\Bigg[\alpha_i^m G(n-1,n_0)\\&+\sum_{k=0}^{n-1}g_3(n-1,k)f(\alpha_i^m g_1^m(k-1,n_0))\Bigg]^m\Bigg)\end{aligned} \tag{16}$$

where $G(n,k)$ consists only of a combination of the coefficients of the filters $g_i(n,k)$ for $1\le i\le 4$. Considering the number of unknowns, there does not seem to exist a polynomial-time algorithm to solve this equation for the unknowns except computing the Gröbner basis. Hence, the delta attack is infeasible on two rounds of the system.

6. CONCLUSION

A new iterative stream cipher, called WSC, based on wavelets over finite fields is introduced in this paper. One round of the WSC consists of two wavelet transforms that are implemented by filter banks. Since wavelet transform is a linear operator by itself, a nonlinear feedback is employed in the encryption and a nonlinear feed-forward in the decryption. The input to the system is a sequence of symbols from $\mathrm{GF}(2^8)$. The key consists of 16 symbols from $\mathrm{GF}(2^8)$ that are exchanged using the Diffie-Hellman key exchange protocol. They are used as the parameters of the PU building blocks that generate the wavelet system. One important feature of the proposed system is to have a short-time random sequence that is added to the plaintext sequence before encryption. This sequence enhances the security of the encryption system with subtle extra computations. The study of the vulnerability of the system has shown that one round of the WSC is vulnerable to the delta attack. However, two rounds of the WSC is resistant against this attack and the other explored attacks. Because the major operation of the wavelet transform is convolution, the proposed system can be implemented efficiently in hardware.

7. REFERENCES

[1] I. Mantin, "Analysis of the stream cipher RC4," M.S. thesis, The Weizmann Ins. of Sience, Israel, Nov. 2001.

[2] Scott Fluhrer, Itsik Mantin, and Adi Shamir, "Weaknesses in the key scheduling algorithm of RC4," *Lecture Notes in Computer Science*, vol. 2259, pp. 1–24, 2001.

[3] I. Mironov, "(Not so) random shuffles of RC4," in *Advances in Cryptology - CRYPTO'02*, M. Yung, Ed., Berlin, 2002, vol. 2442 of *Lecture Notes in Computer Science*, pp. 304–319, Springer-Verlag.

[4] K. S. Chan and F. Fekri, "A block cipher cryptosystem using wavelet transforms over finite fields," *accepted in IEEE Trans. Signal Processing Supplement on Secure Media*, 2003.

[5] F. Fekri, R. M. Mersereau, and R. W. Schafer, "Theory of paraunitary filter banks over fields of characteristic two," *IEEE Trans. Inform. Theory*, vol. IT-48, no. 11, pp. 2964–2979, Nov. 2002.

[6] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*, Prentice-Hall, NJ, 1993.

[7] Joan Daemen and Vincent Rijmen, *The Design of Rijndael: AES-The Advanced Encryption Standard*, Springer-Verlag, Berlin, 2002.

[8] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, vol. 150 of *Graduate Texts in Mathematics*, Springer-Verlag, NY, 1995.

[9] Jean-Charles Faugére, "A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5)," in *Proc. Int. Symp. Symbolic and Algebraic Computation - ISSAC'02*, T. Mora, Ed., NY, 2002, pp. 75–83, ACM.

[10] T. Jakobsen, "Attacks on block ciphers of low algebraic degree," *J. Cryptology*, vol. 14, no. 3, pp. 197–210, 2001.

[11] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein, *Introduction to Algorithms*, The MIT Press, MA, 2nd edition, 2001.