Attacks on the Firekite cipher

Thomas Johansson[1], Willi Meier[2] and Vu Nguyen[1]

[1] Lund university, Lund, Sweden
thomas.johansson@eit.lth.se, vu.nguyen@eit.lth.se
[2] FHNW, Windisch, Switzerland
willi.meier@fhnw.ch

Abstract. Firekite is a synchronous stream cipher using a pseudo-random number generator (PRNG) whose security is conjectured to rely on the hardness of the *Learning Parity with Noise* (LPN) problem. It is one of a few LPN-based symmetric encryption schemes, and it can be very efficiently implemented on a low-end SoC FPGA. The designers, Bogos, Korolija, Locher and Vaudenay, demonstrated appealing properties of Firekite, such as requiring only one source of cryptographically strong bits, small key size, high attainable throughput, and an estimate for the bit level security depending on the selected practical parameters.
We propose distinguishing and key-recovery attacks on Firekite by exploiting the structural properties of its PRNG. We adopt several *birthday-paradox* techniques to show that a particular sum of Firekite's output has a low Hamming weight with higher probability than the random case. We achieve the best distinguishing attacks with complexities $2^{66.75}$ and $2^{106.75}$ for Firekite's parameters corresponding to 80-bit and 128-bit security, respectively. By applying the distinguishing attacks and an additional algorithm we describe, one can also recover the secret matrix used in the Firekite PRNG, which is built from the secret key bits. This key recovery attack works on most large instances of Firekite parameters and has slightly larger complexity, for instance, $2^{69.87}$ on the 80-bit security parameters $n = 16,384, m = 216, k = 216$.

Keywords: PRNG · Firekite PRNG · Birthday paradox · k-list algorithm · LPN · LPN-based symmetric encryption

1 Introduction

Since Shor [Sho99] in his seminal work introduced quantum algorithms that efficiently break the *discrete-log* and *factoring* problems, researchers have set their sights to cryptographic alternatives that promise to be quantum-resistant such as *lattice-based* or *code-based* cryptography. In particular, cryptographic primitives whose security relies on *learning problems*, such as *Learning Parity with Noise* (LPN), *Learning with Errors* (LWE), and the closely related Ring-LPN, are receiving great attentions as they are built on supposedly hard problems.[1] Moreover, Impagliazzo and Levin showed that cryptography is only possible if efficient learning is not [IL90]. Besides the absence of an efficient LPN-solving quantum algorithm, LPN-based constructions are desired as they can be efficiently implemented using mainly XOR ('exclusive or') operations, thus achieving popularity in lightweight cryptography on constrained, low-powered devices. However, most LPN constructions are inclined towards asymmetric cryptography and they have their own disadvantages. These include the requirement to produce and extract randomness (cryptographically secure bits) from an entropy-limited source, causing a significant overhead cost [HDWH12, Sho99], and that they also often require large public keys.

[1] LPN with adversarial errors is $\mathcal{NP}$-hard.

Bogos, Korolija, Locher and Vaudenay [BKLV21] proposed *Firekite*, a synchronous symmetric cipher, using an LPN-based PRNG which requires only one cryptographically strong bit vector to construct the secret matrix key. A small key size is attained by moving from an LPN problem to a Ring-LPN problem [HKL+07]. Their study conjectures that the corresponding Ring-LPN instance remains hard to solve when using said matrix instead of a fully random matrix. They demonstrated that using the Firekite noise distribution for an LPN instance is still secure and there is a 'partial' transformation to an LPN instance. Using the best BKW-style algorithm proposed by Levieil and Fouque [LF06], Firekite's designers estimated the complexity to break the transformed LPN instances, thus derived concrete complexity results for attacking their cipher. The cipher's efficiency was tested in terms of the throughput, which is the number of bytes encrypted or decrypted per second using both desktop computers and FPGAs. They also showcased that, given dedicated hardware, the Firekite PRNG can be parallelized, hence throughput improved substantially for larger parameters.

One can draw many parallels between Firekite and the closely related LPN-C [GRS08b]; in particular, both involve computing a noisy product using a secret random matrix $\mathbf{M}$ and a random error vector $\mathbf{e}$. However, LPN-C further requires an error correcting code $\mathcal{C}$ and the error vectors are drawn from a Bernoulli distribution, as opposed to being bounded as in the Firekite PRNG. This could make the decrypting process fail once the error weight exceeds the code's error correcting capacity. This drawback could be amended by truncating the binomial distribution to make sure not too many bits are set in the error vectors. However, it is speculated that doing so may have a negative impact to the security of LPN-C [BKLV21]. Furthermore, LPN-C inherently requires a large random secret matrix and samples two uniformly random vectors for every invocation of the encryption algorithm. Hence, it becomes infeasible to implement it efficiently when implemented in a constrained environment. Firekite, besides avoiding such undesirable features, surpasses LPN-C by not requiring fresh random bits for each output block.

Even more important than constructing schemes that are potentially quantum secure, it is crucial to try to attack them with the most suitable approaches to better understand their security.

1.1 Contributions

In this work, we propose both distinguishing and key-recovery attacks for Firekite. We observe that the secret matrix is fixed throughout every round of encryption. Hence, if the vector components in the internal states collide to the zero codeword, the outputs of Firekite, when combined together appropriately, result in unusually low weight sums and can be detected. In other words, finding such occurrences amounts to solving a birthday paradox problem with a specific target weight.

We then consider the secret matrix as the generator for a code and by carefully determining which positions in the above combinations are free of errors, we describe a key-recovery attack with a slightly higher complexity than that of the distinguishing attack.

As an example, we apply the distinguishing attacks on the Firekite cipher with specific parameters that target 80-bit and 128-bit to understand better Firekite's security. In particular, we launch both a distinguishing attack and a key recovery attack on parameters $n = 16384, m = 216, k = 216$ with complexity $2^{68.87}$ and $2^{69.97}$, respectively. As there are many choices of parameter sets for each security level, the complexity numbers vary a bit depending on selected parameter sets.

1.2 Related work

Due to their difficulty, either proved or conjectured, LPN and Ring-LPN have made their way into many cryptographic constructions such as human identification protocols which were firstly introduced by Hopper and Blum [HB01], later modified and improved to HB^+ and $HB^\#$ [JW05, KS06, GRS08a]. Recent LPN-based encryption schemes that can be found are Helen by Duc and Vaudenay [DV13], or LPN-C by Gilbert et al. [GRS08b]. Using the Ring-LPN variant, Heyse et al. [HKL+12] proposed an efficient two-round identification protocol in constrained environments, called Lapin. One can also find LPN useful in other applications, e.g., message authentication codes (MACs) [KPV+17, DKPW12], pseudo-random generators [ACPS09, BFKL93], or CCA-secure public-key encryption schemes [YZ16].

Since its introduction, LPN has drawn a plethora of LPN-solving studies with different approaches. It is natural to see LPN as a decoding problem; hence a generic decoding technique applies. Attacks on LPN can be categorized as *Information-set decoding* (ISD) or BKW-type algorithms and they prove advantageous in different scenarios, namely, low noise-rate and constant noise. Information-set decoding was first introduced by Prange [Pra62], and further improved by Leon [Leo88], Lee and Brickell [LB88] and Stern [Ste93]. Recently, several methods have been proposed to achieve better attacks, to name a few, *Ball-collision technique* by Bernstein et al. [BLP11], *representation technique* by Becker, Joux, May, Meurer [BJMM12], or the state-of-the-art algorithm [BV15]. On the other hand, BKW began with the foundation laid by Blum, Kalai, and Wasserman [BKW03]. Besides the improvement by Levieil and Fouque who used Walsh-Hadamard transform to recover several bits of the secret vector, using a limited number of queries, notable advancements can be found such as the use of covering codes by Guo et al. [GJL14], or on the use of the *Generalized birthday attack* (GBA) [Wag02] as in [Kir11].

Generalized birthday attack is one of the most pertinent generic attacks in cryptology, in particular, analyzing the security of an LPN-based cryptographic scheme. There have been many notable works related to the generalized birthday problem. Our study is inspired by the seminal works of Wagner [Wag02] and May et al.'s approximate k-list algorithm [BM17].

1.3 Organization

The paper is organized as follows. Section 2 presents preliminary and background knowledge regarding the LPN problem and its variants such as Ring-LPN. A brief review of the LPN-based Firekite PRNG, and how it gave rise to the Firekite synchronous stream cipher follows. We then describe our idea, and formally analyze our attack for Firekite in Section 3. In Section 4, we attack different parameters proposed for Firekite and verify our approach by a simulation with smaller parameters. We describe our key-recovery attack in Section 5 and discussions on how to improve Firekite finally concludes our work.

2 Background

Whereas the LPN problem usually finds its cryptographic applications in the public-key domain, we will be interested in its application in symmetric cryptography. In particular, we have seen constructions of a few synchronous stream ciphers [GRS08b, BKLV21] based on LPN.

A synchronous stream cipher is a symmetric cipher, in which a stream of pseudorandom bits is generated independently of the plaintext and ciphertext messages, and then bitwise XOR-ed to the plaintext, to encrypt, or to the ciphertext, in order to decrypt. Cryptanalytic attacks either aim to distinguish the output of the pseudorandom bit generator from random source, recover the state of the pseudorandom generator, or recover the key. As known

plaintext for a segment of ciphertext implies knowledge of the keystream for the same segment, a known plaintext attack of a synchronous stream cipher assumes that a large part of the keystream is available to an attacker which is only limited by the maximum number of keystream bits allowed to be output for a same key. Distinguishing attacks [HJB09] on the (known) keystream are relevant to the security of stream ciphers as well: depending on the nonranomness detected, some information on the plaintext may be leaked. For some stream ciphers, a distinguishing feature can even be elaborated to a key recovery attack, as is the case for the distinguishing property we shall derive for Firekite.

2.1 The LPN problem

LPN is an important problem in cryptography. It appears as one of main problems on which we base post-quantum cryptography. Due to the existence of fast algorithms for quantum computers that can solve the factorization and the discrete logarithm problems [Sho99], the LPN problem (and the related LWE problem) including its different versions are of great interest. No fast quantum algorithm that solves the LPN problem is known. Although current omnipresent symmetric encryption schemes such as AES will likely not be rendered obsolete in the near future, studies in post-quantum cryptography, namely aforementioned works, are of absolute necessity. We need post-quantum cryptographic primitives to have *efficiency, confidence,* and *usability* [Ber09].

Cryptographic constructions based on LPN are also appealing, since only simple operations such as bit-wise addition (XOR) and scalar products are used. This can give rise to efficient algorithms or protocols.

The LPN problem can informally be described as the problem of solving a noisy binary system of equations. We formally define it below.

Let Ber_η be the Bernoulli distribution with parameter $\eta \in (0, \frac{1}{2})$ and a bit $e \leftarrow \mathsf{Ber}_\eta$ be such that $\mathbf{Pr}[e = 1] = \eta$, $\mathbf{Pr}[e = 0] = 1 - \eta$. Denote by $\mathbf{x} \xleftarrow{U} \{0,1\}^m$ the event that a vector $\mathbf{x}$ is drawn uniformly from $\{0,1\}^m$.

Definition 1. (LPN oracle). Let $\mathbf{x} \xleftarrow{U} \{0,1\}^m$ and $\eta \in (0, \frac{1}{2})$. An LPN *oracle* Π_{LPN} for $\mathbf{x}$ and η returns pairs of the form

$$\left(\mathbf{g} \xleftarrow{U} \{0,1\}^m, \langle \mathbf{x}, \mathbf{g} \rangle \oplus e\right),$$

where $e \leftarrow \mathsf{Ber}_\eta$, and $\langle \mathbf{x}, \mathbf{g} \rangle$ denotes the scalar product of vectors $\mathbf{x}$ and $\mathbf{g}$.

Definition 2. (LPN problem). Given an LPN oracle Π_{LPN} with parameters m and η. The (m, η)-LPN problem is finding the secret vector $\mathbf{x}$ and is said to be (T, N, δ)-solvable if there exists an algorithm $\mathfrak{A}$ asking for at most N oracle queries, using time at most T and

$$\mathbf{Pr}\left[\mathfrak{A}(\Pi_{\text{LPN}}) = \mathbf{x} : \mathbf{x} \xleftarrow{U} \{0,1\}^m\right] \geq \delta.$$

The definition above is known as the search version of the LPN problem. In the decisional version of the LPN problem, the objective is to distinguish pairs from Π_{LPN} from uniformly random samples. The search and decisional versions are proved to be computationally equivalent [KS06].

We briefly look at a subclass of LPN problems called Ring-LPN which proves to be useful in general and specifically used in the Firekite PRNG. Let f be a polynomial over $\mathbb{Z}_2$ and $R = \mathbb{Z}_2[x]/(f)$ denote the quotient ring. Hence R consists of all polynomials over $\mathbb{Z}_2$ of degree less than that of f. We say $r \leftarrow \mathsf{Ber}_\eta^R$ if the coefficients of the ring element $r \in R$ are assigned independently following the distribution Ber_η. If r is drawn uniformly from R, we write $r \xleftarrow{U} R$. The Ring-LPN problem can be defined similarly to the standard LPN problem.

Definition 3. (Ring-LPN oracle). Let $s \xleftarrow{U} R$ and $\eta \in (0, \frac{1}{2})$. A Ring-LPN oracle $\Pi_{\text{Ring-LPN}}$ for s and η returns pairs of the form

$$(r \xleftarrow{U} R, r \cdot s + e),$$

where $e \leftarrow \mathsf{Ber}_\eta^R$.

Definition 4. (Ring-LPN problem). Given a Ring-LPN oracle $\Pi_{\text{Ring-LPN}}$ with parameters η and a polynomial ring R. The Ring-LPN problem is finding the secret polynomial $s \in R$ and is said to be (T, N, δ)-solvable if there exists an algorithm $\mathfrak{A}$ asking for at most N oracle queries, using time at most T and

$$\mathbf{Pr}\left[\mathfrak{A}(\Pi_{\text{Ring-LPN}}) = s\right] \geq \delta.$$

It is worth pointing out the essential difference between LPN and Ring-LPN. If we query the LPN oracle N times, then we can collect an $m \times N$ matrix $\mathbf{G} = \left(\mathbf{g}_1^{\mathrm{T}} \cdots \mathbf{g}_N^{\mathrm{T}}\right)$ and each column is generated independently. In the case of Ring-LPN, only one polynomial r is generated uniformly random in R. If we consider a polynomial as its coefficient vector, only the first column $\mathbf{r}$ is drawn uniformly random. The other columns are obtained via shifting $\mathbf{r}$. While the LPN problem has been shown to be $\mathcal{NP}$-hard in the worst case [BMvT78], the hardness of Ring-LPN is not known. However, there is a reduction from Ring-LPN to LPN and the assumption is that Ring-LPN is also hard.

2.2 Firekite's PRNG and Firekite construction

We recall that the decisional version of the LPN assumption can be interpreted as one can not efficiently distinguish an LPN oracle from a source providing random bit vectors of length $m + 1$. Naturally, it can be extended into stating that distinguishing a noisy product of an $m \times n$ matrix M and a secret vector $\mathbf{v}$, i.e., $\mathbf{vM} + \mathbf{e}$ from a random n-bit vector in $\mathbb{Z}_2$, where $\mathbf{e}$ is a n-bit noise vector is hard. As an example, LPN-C further used a $[k, n]$ error correcting code $\mathcal{C}$ with a generator matrix $\mathbf{G}$ to encode a plaintext $\mathbf{x}$ to a ciphertext $\mathbf{c}$ through

$$\mathbf{c} = \mathbf{xG} + \mathbf{vM} + \mathbf{e}.$$

However, this construction inherently asks the source to produce random $\mathbf{v}$ and $\mathbf{e}$ for encrypting a single plaintext. The Firekite PRNG circumvents this problem by extracting both $\mathbf{v}$ and $\mathbf{e}$ from the noisy product and feeding them iteratively into the next encryption invocations. Out of n bits, one can spare $m + k \cdot \log n$ bits to initialize the next round of Firekite.[2] Let $||$ denote the usual concatenation of vectors. We write

$$\mathbf{vM} + \mathbf{e} = (\mathbf{g}||\mathbf{v}'||\mathbf{c}_e). \tag{1}$$

Assuming $n \gg m$, one can split the noisy product into three components as in (1), then m bits are used for producing the next vector $\mathbf{v}'$. Since $\mathbf{e}$ is only required to be a sparse n-bit vector, we can have a compact representation of the next noise vector, called $\mathbf{c}_e$. Then, the remaining bits, forming $\mathbf{g}$, are the PRNG's output. We are now in the position to describe the Firekite PRNG formally.

Let m, n, and k be some integer parameters, where $n \gg m$ and n is a power of 2. A secret key $\mathbf{M}$ is a binary matrix of size $m \times n$, and $\mathbf{w}$ is a vector of length $m + k \log n < n$. Together they form a pair $(\mathbf{M}, \mathbf{w})$, the *state* of the PRNG. We define $\mathbf{w} = \mathbf{v}||\mathbf{c}_e$, where $\mathbf{v}$ and $\mathbf{c}_e$ are of length m and $k \log n$, respectively. As stated above, $\mathbf{M}$ is fixed and $\mathbf{w}$ is updated for every iteration. It is straightforward to assign $\mathbf{v} = \mathbf{v}'$. To get the next error vector $\mathbf{e}$, we further parse $\mathbf{c}_e = \mathbf{c}_1||\mathbf{c}_2||...||\mathbf{c}_k$ where $\mathbf{c}_i$ is of length $\log n$. Hence, each $\mathbf{c}_i$

[2] Throughout the paper, log(.) denotes logarithm to base 2.

can be seen as the binary presentation of a non-negative integer less than n. Therefore, $\mathbf{c}_e$ encodes an n-bit error vector of weight at most k. In particular, let $\mathbf{b}_{\mathbf{c}_j}$ be the unit vector of length n, where the bit at the position represented by $\mathbf{c}_j$ is 1. Then the error vector $\mathbf{e}$ is defined as $\mathbf{e} = \bigvee_{j=1}^{k} \mathbf{b}_{\mathbf{c}_j}$. Note that this construction implies $\mathbf{e}$ is not a Bernoulli distributed error. The execution of the Firekite PRNG is described by Algorithm 1.

Algorithm 1: Firekite PRNG

Input: An $m \times n$ secret matrix M and a nonce $\mathbf{w}$, $r > 0$: randomization rounds.

while $r \neq 0$ **do**
  Parse: $\mathbf{w} = \mathbf{v}||\mathbf{c}_1||\mathbf{c}_2||...||\mathbf{c}_k$;
  $\mathbf{e} \leftarrow \bigvee_{j=1}^{k} \mathbf{b}_{\mathbf{c}_j}$;
  $\mathbf{g}||\mathbf{w}' := \mathbf{vM} + \mathbf{e}$; `// Randomization`
  $\mathbf{w} \leftarrow \mathbf{w}'$;
  $r \leftarrow r - 1$;
while *true* **do**
  Parse: $\mathbf{w} = \mathbf{v}||\mathbf{c}_1||\mathbf{c}_2||...||\mathbf{c}_k$;
  $\mathbf{e} \leftarrow \bigvee_{j=1}^{k} \mathbf{b}_{\mathbf{c}_j}$;
  $\mathbf{g}||\mathbf{w}' := \mathbf{vM} + \mathbf{e}$; `// Generating keystream`
  $\mathbf{w} \leftarrow \mathbf{w}'$;
  Return: $\mathbf{g}$

At each iteration, the PRNG's input is its state $(\mathbf{M}, \mathbf{w})$, where the first m bits and the remaining $k \log n$ bits of $\mathbf{w}$ are set to be $\mathbf{v}$ and $\mathbf{c}_e$ respectively. Then the error vector $\mathbf{e}$ is derived from its concise representation $\mathbf{c}_e$ and the noisy n-bit product is computed as $\mathbf{vM} + \mathbf{e}$. This vector is again parsed into $\mathbf{g}$ and $\mathbf{w}'$ of length $d = n - m - k \log n$ and $m + k \log n$, respectively. The internal state is then updated to $(\mathbf{M}, \mathbf{w}')$ and $\mathbf{g}$ is the output of the PRNG. The number r of randomization rounds is needed to guarantee that $\mathbf{v}$ is free from significant biases when Firekite begins to output its keystream [BKLV21].

Firekite is a synchronous stream cipher that makes use of this PRNG to produce the d-bit keystream $\mathbf{g}$ directly. Therefore, for each invocation, d-bit data of a plaintext is encrypted, and the next output of Firekite depends on the updated internal state. The designers pointed out that, for practicality, the parameters m, n, and k need to be large which in turn makes the secret key $\mathbf{M}$ big. In order to solve this problem, they proposed the following technique, which turns the LPN instance into a Ring-LPN instance. Consider $R = \mathbb{Z}_2[X]/(X^b - 1)$, i.e, the polynomial ring with binary coefficients reduced modulo $X^b - 1$ such that $(X^b - 1)/(X - 1)$ is irreducible. It is well known that every polynomial in R can be represented by its coefficient vectors in $\mathbb{Z}_2^b$. Pick $\mathbf{q}_1 \xleftarrow{U} \mathbb{Z}_2^b$ and define $\mathbf{q}_i := X^{i-1}\mathbf{q}_1, i = 1, ...b$, meaning that we shift the entries in the coefficient vectors $\mathbf{q}_1$ by $i - 1$ times. Hence, we can construct a $b \times b$ matrix $\mathbf{Q}$ by shifting the first row to the left consecutively $b - 1$ times. The secret matrix $\mathbf{M}$ is obtained by generating the first m rows, then dropping the last $b - n$ columns of $\mathbf{Q}$. Therefore, the secret key of Firekite PRNG is, in fact, the random b-bit vector $\mathbf{q}_1$ rather than an $m \times n$ matrix $\mathbf{M}$. The designers conjectured that using such $\mathbf{M}$ does not substantially reduce the security compared to a fully random matrix $\mathbf{M}$.

Table 1 shows a few sets of suggested parameters for Firekite that correspond to 80 and 128 security bit levels. Other proposed parameter sets can be found in [BKLV21].

To derive an estimation of the concrete security of Firekite, one faces two problems: first, the noise vectors from Firekite has weight at most k and the noise distribution is not

Table 1: Firekite's parameters for 80 and 128-bit security with the properties in terms of key size b, and number of randomization rounds r.

Parameters			Properties		
m	n	k	Key size (b)	r	Security level
216	1024	16	1061	18	82.76
216	2048	32	2053	18	82.76
216	16,384	216	16,421	21	80.68
352	2048	32	4099	18	129.07
352	8192	120	8219	18	128.99
352	16,384	228	16,421	18	128.93

binomial, as opposed to a standard LPN instance. Second, an adversary only sees a part of the noisy product. Therefore, it is necessary to prove that using Firekite noise distribution for an LPN variant is still hard, and the underlying problem of solving Firekite is as hard as LPN.

The first problem is solved as follows. Let $\Delta(\mathbf{e})$ denote the Hamming weight of an n-bit vector and e_j the j-th bit of $\mathbf{e}$. If $\mathbf{e}$ comes from Firekite and assume each $\mathbf{c}_e$ is uniformly distributed, then $\mathbf{Pr}[e_j = 0] = \left(\frac{n-1}{n}\right)^k$. Therefore, the expected Hamming weight of the Firekite noise (denoted by $\Delta^{\text{Firekite}}(\mathbf{e})$) is

$$\mathbb{E}[\Delta^{\text{Firekite}}(\mathbf{e})] = n\left(1 - \left(\frac{n-1}{n}\right)^k\right),$$

and one can show that

$$\frac{2}{3}k < \mathbb{E}[\Delta^{\text{Firekite}}(\mathbf{e})] < k.$$

In a standard LPN problem with parameters η and m, $\mathbb{E}[\Delta^{\text{LPN}}(\mathbf{e})] = \eta m$ and $\mathbf{Pr}[\Delta^{\text{LPN}}(\mathbf{e}) = \lfloor \mathbb{E}[\Delta^{\text{LPN}}(\mathbf{e})] \rfloor] \in \Omega(1/n)$. Therefore, given such an LPN instance, we set k such that $\eta m \leq k$, e.g., $k := \frac{3}{2}\eta m$. Then the noise of this LPN instance could come from the Firekite noise distribution with probability at least $\Omega(1/n)$. In other words, if the LPN instance with the Firekite noise distribution can be broken efficiently, any standard LPN instance can also be broken with $O(n)$ more work.

As for the underlying problem of solving Firekite, Firekite's designers were able to show that it is *at most* as hard as the LPN problem, and they also conjectured that the reverse is also true [BKLV21]. Using this transformation to attack Firekite with the most efficient LPN-solving algorithm, namely the one by Levieil and Fouque [LF06], they were able to derive the concrete proposed parameters for the different security levels.

2.3 The problem of observing noisy codewords from an unknown code

The task of recovering *partially* the secret matrix $\mathbf{M}$ (by observing vectors $\mathbf{g}_i$) can be seen as identifying an unknown code by observing noisy codewords. The problem often arises in different contexts [MGB12], especially in analyzing cryptosystems where encryption involves error-correcting codes and the transmission is carried over a noisy channel (e.g., a binary symmetric channel). General approaches consist of three steps: first, arranging noisy codewords as rows of a matrix, then running the Gaussian elimination, and finally from the non-echelon part finding sums of vectors that are candidates to construct dual codewords (i.e, parity-check equations). Instead of looking at only columns that sum to 0, Sicot, Houcke and Barbier argued that sparse sums of columns can also be candidates for being

dual codewords [BSH06, SHB09]. Therefore, the last step can be reduced to an instance of the well known *close neighbors search problem*. Beside the *projection method* proposed by Cluzeau and Finiasz [CF09], which aimed to find sparse sums of p columns (with complexity of order $\Omega(n^{p/2})$ when p is even) that are equal in some positions using birthday paradox and hashtables, there have been many improvements and extensive studies to the close neighbors search problem recently. In particular, one being the *Dubiner method* which later was applied by Carrier and Tillich in their generalized approach [CT19]. Their algorithm only performed a *partial* Gaussian elimination for the second steps. The argument is that the Gaussian elimination increases the noise by combining noisy codewords, hence it is more likely to obtain sparse sums in the early stage of the Gaussian elimination and minimizing the dual codewords that might have been undetected by Sicot-Houcke-Barbier algorithm [CT19]. Moreover it also allowed them to find dual codewords of much larger weight (compared to the full Gaussian elimination) with reasonable complexities.

In practice, the recovery of an unknown code by observing noisy codewords concerns useful families of codes, such as cyclic codes, convolutional codes, turbo codes, or the ubiquitous LDPC, which is important as finding low-weight dual codewords is essential in determining communication components such as unknown interleaver [BSH06, Tix15] or reconstructing other families of codes.

In the next section we introduce a new method, namely finding a small number of noisy codewords summing to the zero codeword through a generalized birthday type of algorithm.

3 The proposed distinguishing algorithm

In this section, we aim to give a brief description of the idea used in our distinguishing attacks on Firekite. We firstly observe that the secret key matrix $\mathbf{M}$ is fixed throughout the rounds of Firekite; hence, the keystream output by Firekite PRNG is subjected to accumulating non-randomness. Let us look at the Firekite PRNG, fulfilling

$$\mathbf{vM} + \mathbf{e} = (\mathbf{g}||\mathbf{v}'||\mathbf{c}_e),$$

where $\mathbf{v}'$ and $\mathbf{c}_e$ are used in the next iteration by assigning $\mathbf{v}' = \mathbf{v}$ and $\mathbf{e} = \bigvee_{j=1}^{k} \mathbf{b}_{\mathbf{c}_j}$, and $\mathbf{g}$ is the PRNG's output. In the initial part of the attack, we concentrate on assuming the knowledge of

$$\mathbf{g} = \mathbf{vM}' + \mathbf{e}',$$

where $\mathbf{g}$ is a known d-bit vector, $\mathbf{M}'$ is now considered as an $m \times d$ secret binary matrix (obtained from the first d columns of the original $\mathbf{M}$ matrix) and $\mathbf{e}'$ is a secret d-bit noise vector, being the first d positions of $\mathbf{e}$. It is known that $\Delta(\mathbf{e}) \leq k$ (which is small); hence, the weight of $\mathbf{e}'$ is also small. The expected weight of $\mathbf{e}'$ denoted by $\hat{k}$, where $\hat{k} = \frac{k \cdot d}{n}$ since it is assumed that the ones in $\mathbf{e}$ are uniformly distributed among all d positions.

In a synchronous stream cipher attack, we assume that an adversary has access to a long output stream, which means access to a large number of d-bit vectors $\mathbf{g}$. The set of these vectors is written as $\{\mathbf{g}_i, i = 1, \ldots, S\}$, where now $\mathbf{g}_i = \mathbf{v}_i\mathbf{M}' + \mathbf{e}'_i$ and for some S to be addressed in the following subsections. We first sketch the ideas behind our distinguishing attack, i.e., given an aforementioned set of vectors, decide whether they originate from Firekite or if they are random vectors.

Our goal is to find a subset of $\mathbf{g}_{i_j}$ vectors, $j = 1, ..., l$, such that the corresponding $\sum_{j=1}^{l} \mathbf{v}_{i_j} = \mathbf{0}$, i.e., we find a set of noisy codewords such that the underlying information vectors sum to zero. If l vectors $\mathbf{v}_{i_j}$, $j = 1, \ldots, l$, sum to zero, then the sum of the corresponding $\mathbf{g}_{i_j}$ is expected to be of weight $c_\omega = \lceil l \cdot \hat{k} \rceil$ with nonzero contributions

coming only from the errors $\mathbf{e}'_{i_j}$. Indeed, we then have

$$\sum_{j=1}^{l} \mathbf{g}_{i_j} = \sum_{j=1}^{l} \mathbf{v}_{i_j}\mathbf{M}' + \sum_{j=1}^{l} \mathbf{e}'_{i_j} = \sum_{j=1}^{l} \mathbf{e}'_{i_j}.$$

Therefore, when l is not too large, e.g. $l = 4$ or $l = 8$, the expected weight in $\sum_{j=1}^{l} \mathbf{g}_{i_j}$ will be low if $\sum_{j=1}^{l} \mathbf{v}_{i_j} = 0$. Since d is much larger than c_ω (with proposed parameters for Firekite), such a weight is very unlikely if the vectors $\mathbf{g}_{i_j}$ are random vectors. In the Firekite PRNG, such a collision of vectors of length m (i.e, with probability proportional to 2^{-m}) guarantees a low weight vector of length d. It is only intuitive to deduce that we can detect such occurrences more frequently than what is expected in the random case.

3.1 A basic algorithm for finding noisy codewords summing to the zero codeword

Recall that we want to find l different $\mathbf{g}_{i_j}$ vectors, $j = 1, \cdots, l$, such that the associated unknown vectors $\mathbf{v}_{i_j}$ sum to zero. Our approach is built from ideas from the generalized birthday attack [Wag02] and the BKW algorithm [BKW03]. A different but related approach is also May et al.'s *Match-and-Filter* algorithm [BM17].

In a simplified description following [Wag02], we set up l ($l = 2^t$ is a power of 2) lists of size 2^c filled by $\mathbf{g}_i$ vectors. We then combine the lists pairwise, resulting in a new list containing vectors created as a sum of two vectors, one from each initial list, such that some c predetermined positions are all zero. The expected number of vectors in the new list is 2^c. After the first step we have $l/2$ lists. We then perform the same procedure again, reducing another c positions to zero until one single list remains, i.e, after t steps. In the remaining list, we will finally examine whether there are vectors $\sum_{j=1}^{l} \mathbf{g}_{i_j}$ that are candidates to satisfy $\sum_{j=1}^{l} \mathbf{v}_{i_j} = 0$. In fact, they are quite easily detected, since if this is the case then $\sum_{j=1}^{l} \mathbf{g}_{i_j} = \sum_{j=1}^{l} \mathbf{e}'_{i_j}$, which has very low weight.

As in the BKW algorithm framework, one may use the same list for $\mathbf{g}_i$ vectors and we increase the list size to roughly $3 \cdot 2^c$. Starting with a list $L^{(0)}$, we can write up a sequence of updated lists $L^{(0)} \to L^{(1)} \to L^{(2)} \cdots \to L^{(t)}$, where in each step we reduce another c positions. This means that $L^{(i)}$ have vectors where the first $i \cdot c$ positions are all zero. On average, there are three vectors that collide in given c positions. Therefore, we can have three combinations for such vectors and the size of $L^{(i)}$ can be kept (hence, the motivation for the factor 3). We formally describe this approach in Algorithm 2.

Algorithm 2: t-step Distinguisher

Input: A list $L^{(0)}$, with $\mathbf{g}_i \in \mathbb{Z}_2^n$, $i = 1, ..., 3 \cdot 2^c$ ($|L^{(0)}| = 3 \cdot 2^c$), parameters $k, d, l, t = \log l$, $c_\omega = \lceil \frac{l \cdot k \cdot d}{n} \rceil$.

for $i = 1, ..., t$ **do**
  $L^{(i)} = \text{COMBINE}(L^{(i-1)})$; `// Combine list, cancelling c bits.`
minweight $= k \cdot l$;
for $\mathbf{g}'$ **in** $\mathbf{L^{(t)}}$ **do**
  if $\mathsf{HammingWt}(\mathbf{g}') \leq$ minweight **then**
    minweight $= \mathsf{HammingWt}(\mathbf{g}')$; `// Filtering low weight sums.`
if minweight $\leq c_\omega$ **then**
  Return: 'Firekite'
else
  Return: 'Random'

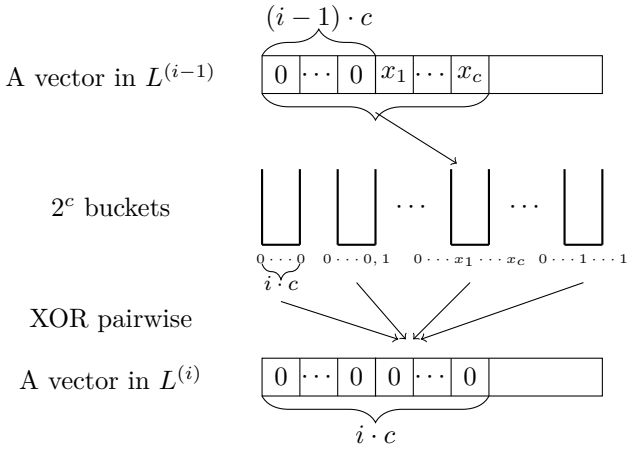


Figure 1: COMBINE for $L^{(i-1)}$.

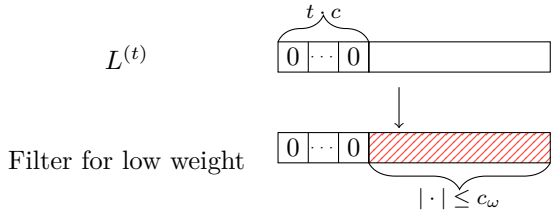


Figure 2: Filter $L^{(t)}$ with c_ω.

Figure 1 and Figure 2 are visualizations of the COMBINE step for the $(i-1)$-th list $L^{(i-1)}$ and the filtering for the last list, respectively.[3].

We need to consider complexity and memory of the algorithm. Let this computational complexity measured in simple operations be denoted C and the used memory in bits be denoted Mem. Its main parts are the $L^{(i)} = \text{COMBINE}(L^{(i-1)})$ steps in the loop. We assume that the vectors in the list $L^{(i-1)}$ are organized in a hash table. We have that the first $(i-1)\cdot c$ positions are all zero in all vectors in $L^{(i-1)}$, and they are again sorted in different buckets in the hash table according to the value of the next c positions, i.e., position $(i-1)\cdot c$ to $i\cdot c-1$, for $i = 1, ..., t$. The COMBINE step now creates new vectors for the new list $L^{(i)}$ by adding together all possible pairs that are stored in the same bucket. This will cancel out another c positions so that vectors in $L^{(i)}$ start with $i\cdot c$ zeros. New vectors are created until the list $L^{(i)}$ has cardinality $3\cdot 2^c$ and the sorting procedure is repeated for the next iteration.[4] The complexity of one COMBINE step is then $3\cdot 2^c$ bit-wise additions of vectors of length at most d and storing the result in memory. We adopt Firekite's designers' notation by letting p be the word-length of a bit-wise addition operation, i.e, the number of bits for which an XOR operation can be computed.[5]. We write the cost of one d-bit XOR operation as $(1 + \lfloor d/p \rfloor)$ This procedure is repeated t times in Algorithm 2. The final check for low weight vectors actually does not need to

[3]Inspired by Erik Mårtensson's poster "Coded-BKW with Sieving"[Må18].

[4]The input could be not uniformly distributed and we might have more combinations than $3\cdot 2^c$. If we obtain significantly fewer vectors after COMBINE (unlikely) due to input non-uniformity, the list size gradually decreases and Algorithm 2 might fail.

[5]For example, the *Advance Vector Extension* AVX-512 allows XOR to have 512 bits computed per cycle.

go through all buckets, but only those with a low weight (for instance, one can sort the vectors in $L^{(t)}$ by their next c positions). This cost is then much smaller than the previous steps and can be disregarded. The complexity can thus be estimated as

$$C = t \cdot (3 \cdot 2^c) \cdot (1 + \lfloor d/p \rfloor). \tag{2}$$

The required memory Mem is the storage of two lists, altogether at most $\text{Mem} = 2 \cdot 3 \cdot 2^c \cdot d$ in bits. In the next subsection, we investigate the success probability of the distinguisher.

3.2 Parameter choices and the success probability of the proposed algorithm

3.2.1 Algorithmic steps

Since the added noise in the $\sum_{j=1}^{l} \mathbf{g}_{i_j} = \sum_{j=1}^{l} \mathbf{v}_{i_j}\mathbf{M}' + \sum_{j=1}^{l} \mathbf{e}'_{i_j} = \sum_{j=1}^{l} \mathbf{e}'_{i_j}$ expression becomes significant as l grows large, a low-weight sum from Firekite will become hard to distinguish as l grows (from the random case). We hence fix the number of algorithmic steps t to 2 or 3, corresponding to $l = 4$ and $l = 8$ in the proposed algorithm, respectively.

3.2.2 The required Firekite output observations

A vector formed as $\sum_{j=1}^{l} \mathbf{g}_{i_j} = \sum_{j=1}^{l} \mathbf{v}_{i_j}\mathbf{M}' + \sum_{j=1}^{l} \mathbf{e}'_{i_j} = \sum_{j=1}^{l} \mathbf{e}'_{i_j}$ will be called a *zero sum vector*. Furthermore, considering a sum of error vectors, e.g., $\sum_{j=1}^{l} \mathbf{e}'_{i_j}$, we say that a position is *error free* mod 2 if $\sum_{j=1}^{l} \mathbf{e}'_{i_j}$ is zero in that position; we say that a position is simply *error free* if all $\mathbf{e}'_{i_j}$ are zero in the position. It can happen that a *double error* event occurs, i.e., two ones in the same position and $1 + 1 = 0$. The required Firekite output observations (i.e., $|L^{(0)}| = 3 \cdot 2^c$) has to be chosen such that zero sum vectors can be found after Algorithm 2. Moreover, they must be noise-free in the first $t \cdot c$ positions. This probability is denoted P_{nf} (noise-free), and we investigate this probability for both case $l = 4$ and $l = 8$.

The case $l = 4$ Starting with $l = 4$, we are interested in knowing if a zero sum vector can be found in the final list. The expected number of zero sum vectors in the final list is denoted by N. We have

$$N = \binom{3 \cdot 2^c}{4} \cdot 2^{-m} \cdot 3 \cdot 2^{-c} \cdot P_{\text{nf}} \tag{3}$$

such zero sum vectors, which can be roughly explained as follows: there are $\binom{3 \cdot 2^c}{4}$ possible combinations from the initial list. Among all such 4-sums, only a fraction 2^{-m} will correspond to a zero sum in $\mathbf{v}_{i_j}, j = 1, \cdots, 4$. Then, there are 3 ways to choose 2 pairs as in Algorithm 2. We consider two particular pairs $\{\mathbf{g}_{i_1}, \mathbf{g}_{i_2}\}$ and $\{\mathbf{g}_{i_3}, \mathbf{g}_{i_4}\}$ summing to a zero sum, we further condition $\mathbf{g}_{i_1}$ and $\mathbf{g}_{i_2}$ to cancel in the first c bits with probability 2^{-c} (the other pair automatically follows). Finally, we assume that $\mathbf{e}'_{i_1} + \mathbf{e}'_{i_2} + \mathbf{e}'_{i_3} + \mathbf{e}'_{i_4}$ is zero in the first $2c$ positions, i.e, error free mod 2.

P_{nf} can be bounded by the probability that the first $2c$ positions are error free. For each $\mathbf{e}'_{i_1}$, there are at most k bits set, uniformly distributed among n positions,[6] so the probability of one error vector, being error free in the first $2c$ position, is roughly $((n - 2c)/n)^k$. Therefore, we have

$$P_{\text{nf}} \geq ((n - 2c)/n)^{4k}.$$

[6] The expected weight of $\mathbf{e}'$ from Firekite is smaller than k, but we can compute probabilities from error assignment in $\mathbf{e}$.

Lemma 1. *When $l = 4$, we expect to have*

$$N > \binom{3 \cdot 2^c}{4} \cdot 2^{-m-c} \cdot 3 \cdot \left(\frac{n-2c}{n}\right)^{4k} \tag{4}$$

zero sum vectors in the final list in Algorithm 2.

The case $l = 8$ Next, we investigate $l = 8$. Similar to the case $l = 4$, we have:

$$N = \binom{3 \cdot 2^c}{8} \cdot 2^{-m} \cdot 105 \cdot 2^{-4c} \cdot P_{\text{nf}}. \tag{5}$$

The explanation is again as follows: the number of different sums of 8 vectors that can be constructed is $\binom{3\cdot 2^c}{8}$. Among them, we expect a fraction of 2^{-m} summing to the zero case. There are $7 \cdot 5 \cdot 3 = 105$ ways to form 4 pairs of 8 vectors. Consider the particular pairing $\{\mathbf{g}_{i_1}, \mathbf{g}_{i_2}\}$, $\{\mathbf{g}_{i_3}, \mathbf{g}_{i_4}\}$, $\{\mathbf{g}_{i_5}, \mathbf{g}_{i_6}\}$, and $\{\mathbf{g}_{i_7}, \mathbf{g}_{i_8}\}$. A sum constructed from this pairing will be in the final list of Algorithm 2 if $\mathbf{g}_{i_1} + \mathbf{g}_{i_2}$, $\mathbf{g}_{i_3} + \mathbf{g}_{i_4}$ and $\mathbf{g}_{i_5} + \mathbf{g}_{i_6}$ are all zero in the first c positions. Then $\mathbf{g}_{i_7} + \mathbf{g}_{i_8}$ has to be zero in the first c positions. The probability of this event for each choice of fixed indices is 2^{-3c}. Similarly to the 4-sum, now $(\mathbf{g}_{i_1} + \mathbf{g}_{i_2}) + (\mathbf{g}_{i_3} + \mathbf{g}_{i_4})$ must sum to zero in the next c positions, with probability 2^{-c}. Finally, we also need the sum of error vectors to be error free mod 2 in $3c$ positions.

As before, P_{nf} can be bounded by the probability that no errors occur in the first $3c$ positions. The probability of such a distribution for a single error vector is then roughly $((n-3c)/n)^k$ and for all eight of them we have

$$P_{\text{nf}} \geq ((n-3c)/n)^{8k}.$$

Lemma 2. *When $l = 8$, we expect to have*

$$N > \binom{3 \cdot 2^c}{8} \cdot 2^{-m-4c} \cdot 105 \cdot \left(\frac{n-3c}{n}\right)^{8k} \tag{6}$$

zero sum vectors in the final list in Algorithm 2.

For $l = 8$ there are more errors in general, meaning that P_{nf} is much smaller compared to $l = 4$. This gives a stronger motivation for examining other error patterns such as the double errors canceling out. In particular, the sums from our algorithm can have $1 + 1 = 0$ in the first $3c$ bits. More specifically, if two error vectors have a one in the same position, their combination still survives the COMBINE step in Algorithm 2. For some parameters proposed by Firekite's designers, certain double error events are even more likely than having no error at all in the first $3c$ positions and thus should not be neglected. Since the error vectors are sparse (e.g., $k = 16 \ll n = 1024$), if a double error occurs at a position, it most likely happens only **once**, i.e, coming from one pair of $\mathbf{g}_{i_j}$ (or equivalently, $\mathbf{e}'_{i_j}$). Having four ones in the same position is exceedingly rare for interested parameters (see Appendix, Example 1). Therefore, we can have a lower bound of P_{nf} by considering only non-repeating double errors. Let us look at the simple case where errors from Firekite have exactly k bits set.[7]

Assume we have $\epsilon \leq k$ double errors, and the probability is denoted by P_ϵ. Then P_ϵ is equal the sum of all possible error patterns/combinations of $\mathbf{g}_i$ vectors, provided they result in ϵ collisions. One writes

$$\epsilon = \sum_{i,j>i} \epsilon_{ij},$$

[7] The expected weight of errors from Firekite can be smaller than k. Hence using binomial expressions, while not entirely correct, gives a good approximation.

where ϵ_{ij} denotes the number of double errors between $\mathbf{g}_i$ and $\mathbf{g}_j$. The total number of errors in $3 \cdot c$ positions of $\mathbf{g}_i$ is $\epsilon_i = \sum_j \epsilon_{ij}$. Hence

$$P_\epsilon = \sum_{\{(\epsilon_{ij})\}} P_{\epsilon,\{(\epsilon_{ij})\}},$$

where $\{(\epsilon_{ij})\}$ is an eligible error colliding pattern of $\mathbf{g}_i$ vectors with the corresponding probability $P_{\epsilon,\{(\epsilon_{ij})\}}$.

Lemma 3. *Let $\mathbf{g}_i, i = 1, \ldots, 8$ be binary vectors. Then, the noise-free probability of $\sum_{i=1}^{8} \mathbf{g}_i$ in the first $3 \cdot c$ bits is*

$$P_{\text{nf}} = \sum_{\epsilon=0,\ldots,k} P_\epsilon = \sum_{\substack{\epsilon=0,\ldots,k \\ \{(\epsilon_{ij})\}}} P_{\epsilon,\{(\epsilon_{ij})\}}, \tag{7}$$

where

$$P_{\epsilon,\{(\epsilon_{ij})\}} \approx \prod_{i=1}^{8} \binom{k}{\epsilon_i} \left(\frac{3c}{n}\right)^{\epsilon_i} \left(\frac{n-3c}{n}\right)^{k-\epsilon_i} \frac{\binom{\epsilon_1}{\epsilon_{1i}}\binom{\epsilon_2-\epsilon_{12}}{\epsilon_{2i}} \cdots \binom{3c-\epsilon_{1i}-\ldots-\epsilon_{i-1i}}{\epsilon_i-\epsilon_{1i}-\ldots-\epsilon_{i-1i}}\binom{\epsilon_{i-1}-\epsilon_{1i-1}-\ldots\epsilon_{i-2i-1}}{\epsilon_{i-1i}}}{\binom{3c}{\epsilon_i}}.$$

Proof. Assume ϵ double errors and a fixed error colliding pattern $\{(\epsilon_{ij})\}$. Without loss of generality, we further assume that $\epsilon_i \geq \epsilon_j$ for $i < j$, i.e., $\mathbf{g}_1$ has the most errors in the first $3c$ bits. The probability of $\mathbf{g}_i$ having ϵ_i errors in the first $3c$ bits is

$$\binom{k}{\epsilon_i} \left(\frac{3c}{n}\right)^{\epsilon_i} \left(\frac{n-3c}{n}\right)^{k-\epsilon_i}.$$

We also requires $\mathbf{g}_2$ to have ϵ_{12} colliding positions out of ϵ_2. This probability is

$$\frac{\binom{\epsilon_1}{\epsilon_{12}}\binom{3c-\epsilon_{12}}{\epsilon_2-\epsilon_{12}}}{\binom{3c}{\epsilon_2}}.$$

Similarly, for vector $\mathbf{g}_3$, the colliding probability is

$$\frac{\binom{\epsilon_1}{\epsilon_{13}}\binom{\epsilon_2-\epsilon_{12}}{\epsilon_{23}}\binom{3c-\epsilon_{13}-\epsilon_{23}}{\epsilon_3-\epsilon_{13}-\epsilon_{23}}}{\binom{3c}{\epsilon_3}}.$$

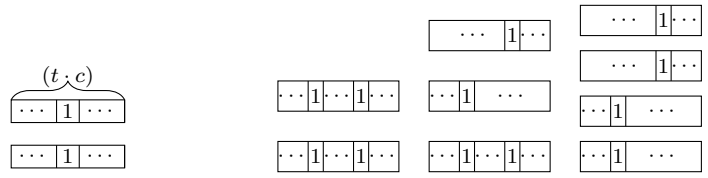
Generalizing for $\mathbf{g}_i$ and the lemma follows. □

However, it is not practical to take into account all possible double error events. For instance, if the expected numbers of 1's in the first $t \cdot c$ positions for each error vector is small, e.g., fewer than 2, multiple double error events occur with decreasingly small probability (from a certain point). Moreover, they do not contribute substantially to our estimate (Appendix, Example 2). Moreover, an improvement in estimating P_{nf} only suggests that we need less input for Algorithm 2, i.e., the bigger P_{nf} is, the smaller c to satisfy (5). A reasonable approximation suffices for us to deduce the necessary initial list size $|L^{(0)}|$ so that the expected number of zero sums is $N > 1$.

To illustrate this argument, we consider the case where we have the relative Hamming weight of the error vectors $\mathbf{e}_i$'s in the first $3 \cdot c$ positions to be slightly larger than 2 ($l = 8$). Hence, we focus only on the scenarios of up to 2 double errors in Figure 3.

One can find the inspiration from Wagner l-tree algorithm [Wag02] in Algorithm 2, namely, by consecutively canceling out c bits. Wagner argued that one needs lists of size $O(2^{\frac{m}{1+\log l}})$ to have a solution in the exact *l-list birthday problem*. In our algorithm, we need slightly more,[8] i.e, $O(2^{\frac{m}{1+\log l}+a})$ where a depends on P_{nf}. Note that P_{nf} remains relatively the same if $c \approx \frac{m}{1+\log l}$. Therefore, we initially set $c = \lfloor \frac{m}{1+\log l} \rfloor$, then raising until we get $N > 1$. Finally, we verify $N > 1$ again with P_{nf} estimated by said c.

[8] Wagner showed that one can find $\alpha^{1+\log l}$ more solutions at the expense of α times more work, provided $\alpha \leq 2^{m/(\log l \cdot (1+\log l))}$ [Wag02].



(a) 1 double error **(b)** 2 double errors

Figure 3: Illustration for the colliding patterns

3.2.3 The success probability

Previously, we have seen that if we choose parameters suitably, we can detect zero sum vectors in the final list. We now need to check whether low weight sums can stem from random vectors. In other words, the zero sums must be easily distinguished from those coming from the random case.

Assume Algorithm 2 outputs 'Firekite' for the random case. This means that it has found a vector in the final list of weight at most c_ω. It is thus of interest to derive the likelihood of such a vector in the random case. Recall $\Delta(\mathbf{g})$ as the Hamming weight of a binary vector $\mathbf{g}$, and let $\mathbf{g}_{[i]}$ be the i-bit truncated $\mathbf{g}$ (first i positions). A vector in the final list will have the first $t \cdot c$ positions all zero, but the remaining positions $d - t \cdot c$ positions are just formed by XOR-ing l random bit values; thus, they are independent and uniformly distributed on $\{0, 1\}$. The probability of such a vector having Hamming weight at most c_ω is

$$\mathbf{Pr}\left[\Delta(\mathbf{g}) \leq c_\omega : \mathbf{g} \in \mathbb{Z}_2^d, \mathbf{g}_{[t\cdot c]} = 0\right] = \frac{\sum_{i=0}^{c_\omega} \binom{d-t\cdot c}{i}}{2^{d-t\cdot c}},$$

and the expected number of vectors of weight at most c_ω, denoted by N_{random}, in the final list is

$$N_{\text{random}} = 3 \cdot 2^c \cdot \frac{\sum_{i=0}^{c_\omega} \binom{d-t\cdot c}{i}}{2^{d-t\cdot c}}. \tag{8}$$

Information theoretically, we have an approximation[9] as

$$N_{\text{random}} = 3 \cdot 2^c \cdot \frac{\sum_{i=0}^{c_\omega} \binom{d-t\cdot c}{i}}{2^{d-t\cdot c}} \approx \sum_{i=0}^{c_\omega} 2^{-\left(1-H\left(\frac{i}{d-t\cdot c}\right)\right)(d-t\cdot c)+c} \approx 2^{-\left(1-H\left(\frac{c_\omega}{d-t\cdot c}\right)\right)(d-t\cdot c)+c},$$

where H is the binary entropy function and $H(p) = -p\log(p) - (1-p)\log(1-p)$ with $p \in (0, 1)$. Therefore, if there exists a low weight sum in the final list $L^{(t)}$ and N_{random} is 'vanishingly small' (i.e., $N_{\text{random}} \ll 1$), we have shown that the Firekite's output vectors are indeed not random. Different values of N_{random} for various parameters can be found in Table 2.

4 Results for the distinguisher

In this section we give the results for our distinguishing attack as described in Section 3 when it is applied on the suggested parameter sets for Firekite.

4.1 Theoretical complexity estimation for the proposed parameters of Firekite

We investigate the results for Firekite's proposed parameters. As an example, we explain our distinguishing attack for the case $n = 1024, m = 216, d = 648, k = 16$, where the

[9] We use $2^n\binom{n}{i} \approx 2^{(1-H(i/n))n}$. The final approximation is due to overwhelming contribution of $2^{-(1-H(c_\omega/(d-t\cdot c)))(d-t\cdot c)+c}$.

claimed security level is 82.

1. For $l = 4$ we derive the following: we pick $c = 76$, $c_w = \lceil 4 \cdot \hat{k} \rceil = 41$, where $\hat{k} = \frac{k \cdot d}{n}$. Let P_0 denote the probability of the first $2 \cdot c$ position being error free. By simply setting $P_{\text{nf}} \approx P_0 = \left(\frac{n - 2 \cdot c}{n}\right)^{4k} \approx 2^{-14.83}$, we get $N > 1.42$ and

$$N_{\text{random}} \approx 2^{-215.76}.$$

2. For $l = 8$ we derive the following: picking $c = 62$ and similarly, $c_\omega = \lceil l \cdot k \cdot \frac{d}{n} \rceil = 81$, we have N_{random} very close to zero.

   As an example, we approximate P_{nf} by the sum of probabilities of no double errors P_0, one double errors P_1, and two double errors P_2 ($\epsilon = 0, 1, 2$). As discussed, many double errors are improbable and we focus on the most likely cases.

   - If there is no double error, $P_0 = \left(\frac{n - 3c}{n}\right)^{8k} \approx 2^{-37.02}$.
   - Assume there is one double error occurring. For the colliding pair of vectors, the probability of having exactly one 1 in the same position $\frac{k^2}{3c}\left(\frac{3c}{n}\right)^2\left(\frac{n-3c}{n}\right)^{2(k-1)}$, and there are $\binom{8}{2}$ ways to select a pair/colliding pattern $\{(\epsilon_{ij})\}$, hence

$$P_1 \approx \binom{8}{2}\frac{k^2}{3c}\left(\frac{3c}{n}\right)^2\left(\frac{n - 3c}{n}\right)^{2(k-1)}\left(\frac{n - 3c}{n}\right)^{6k} \approx 2^{-36.09}.$$

   - If there are two double errors, then there are two cases: the double errors happen in one pair or two pairs (note that a vector in the first pair can appear in the second pair). Let P_{21} and P_{22} denoted such events, respectively, then

$$P_2 \approx P_{21} + P_{22}.$$

   where

$$P_{21} \approx \binom{8}{2}\frac{\binom{k}{2}^2}{\binom{3c}{2}}\left(\frac{3c}{n}\right)^4\left(\frac{n - 3c}{n}\right)^{2(k-2)}\left(\frac{n - 3c}{n}\right)^{6k}.$$

   and

$$P_{22} \approx \binom{8}{3}\binom{k}{2}\left(\frac{3c}{n}\right)^2\left(\frac{n - 3c}{n}\right)^{k-2} \cdot 2 \cdot \left[\frac{k}{3c}\left(\frac{3c}{n}\right)\left(\frac{n - 3c}{n}\right)^{(k-1)}\right]^2\left(\frac{n - 3c}{n}\right)^{5k}$$
$$+ \binom{8}{2}\binom{6}{2}\left(\frac{k^2}{3c}\right)^2\left(\frac{3c}{n}\right)^4\left(\frac{n - 3c}{n}\right)^{4(k-1)}\left(\frac{n - 3c}{n}\right)^{4k}.$$

   Therefore, $P_2 \approx 2^{-35.86}$, and $P_{\text{nf}} > P_0 + P_1 + P_2 \approx 2^{-34.65} \approx 4P_0$ which gives $N > 2.7$. The failure probability for this attack when $c_\omega = 81$ can be indicated by

$$N_{\text{random}} \approx 2^{-90.23}.$$

Table 2 shows our attack's complexity and the corresponding N_{random} for a few sets of parameters suggested by the Firekite's designers. The number of required Firekite output observations is indicated by the parameter c. Recall that the theoretical complexity is

$$C = t \cdot (3 \cdot 2^c) \cdot (1 + \lfloor d/p \rfloor).$$

Table 2: Our distinguishing attack complexity corresponding to a few selected sets of parameters for 80-bit and 128-bit security of Firekite's stream cipher.

Parameters				c		Attacks(log)		N_{random}(log)	
m	n	k	Security	4-sum	8-sum	4-sum	8-sum	4-sum	8-sum
216	1024	16	82.76	76	62	80.17	66.75	-215.76	-90.23
216	2048	32	82.76	76	62	81.17	67.75	-765.79	-465.74
216	16,384	216	80.68	75	60	83.28	68.87	-9011.62	-6541.71
352	2048	32	129.07	125	101	130.16	106.75	-541.40	-275.94
352	4096	58	128.95	124	99	130.17	105.75	-1739.41	-1150.69
352	16,384	228	128.93	123	99	131.26	107.84	-8510.19	-6023.39

In their implementation, beside several optimization flags, they also use a compilation flag `-mavx2` that allows XOR operations to apply on 256 bits per cycle. Therefore, in our complexity estimates, we set $p = 256$.

With 4-sum attacks and for small parameters of 80-bit secured Firekite, we can only refine Firekite's designer estimates marginally. However, our 8-sum distinguisher manages to break Firekite for all parameters, except for the smallest 128-bit secure instance, which is $n = 1024, m = 352,$ and $k = 16$. In particular, we can find a zero sum with the cost $2^{107.75}$ but $\log(N_{\text{random}}) \approx 83$. Therefore, we were unable to claim that the Firekite's output is not randomly distributed as the low weight sums found could easily come from random vectors. The explanation is that $d = n - m - k \log n$ is not so large compared to $8 \cdot \hat{k}$ in this case; hence, it is impossible to distinguish from the case of random vectors $\mathbf{g}_i$. In general, 8-sum attack performs slightly better when the parameters n and k grows (with the same factor, as suggested by Firekite's designers). This is owing to the fact that d grows bigger while m remains relatively unchanged; hence we have even smaller failure probability and bigger error free probability P_{nf}. In fact, we need a smaller initial list ($3 \cdot 2^{60}$ compared to $3 \cdot 2^{62}$) when attacking Firekite instance with $n = 16384, m = 216, k = 216$.

These theoretical results above can be improved; larger Firekite parameters make the double error events more probable. For instance, attacking the parameters $n = 16384, m = 352, k = 228$ with 8-sum distinguisher, we find that two double errors (P_2) are twice as likely as no error (P_0). Therefore, P_{nf} should be better approximated by taking, e.g., P_3 and P_4 into consideration.

4.2 Simulation results for smaller parameters

We verify our approach and formulas by performing simulations.[10] As a toy example, we set up a mini version of Firekite with small parameters (where the ratios $\frac{n}{k}$ are kept constant as in Table 1 and m is also reduced by a similar factor) and run Algorithm 2. Our parameters are $m = 52, n = 256, k = 4, b = 269$ and $r = 15$. Recall that b is the secret key's length used to generate the first row of Firekite's secret matrix $\mathbf{M}$ such that $(X^b - 1)/(X - 1)$ is irreducible in $\mathbb{Z}_2[x]$ and r is the number of randomization rounds before Firekite generates its actual output.

- For the 4-sum distinguisher, the filter weight is $c_\omega = 11$. The parameter c is chosen so that
$$N = \binom{3 \cdot 2^c}{4} \cdot 2^{-m} \cdot 3 \cdot 2^{-c} \cdot P_{\text{nf}} > 1.$$
One has $P_0 = \left(\frac{n - 2c}{n}\right)^{4k} \approx 2^{-3.5}$. If we choose $c = 18$, i.e $|L^{(0)}| = 3 \cdot 2^{18}$, there

[10] Our simple implementation can be found at https://anonymous.4open.science/r/FirekiteDistinguisher-553B/README.md

are, on average, less than 1 bit set of the error vectors in the first $2c$ bits. One can safely assume $P_{\text{nf}} \approx P_0$, and it gives $N \approx 3.6$. The simulation returns, on average, 1.65 low weight vectors after 10^2 tests. The discrepancy can be explained as follows: the assumption that we can keep the list's size $|L^{(i)}| = 3 \cdot 2^c$ is often violated as there are **more** vectors after every COMBINE step owing to vectors being not evenly distributed among buckets. Therefore, 'good' combinations that are present in zero sums might be discarded by chance. Keeping all combinations from COMBINE, we obtain more low weight sums after filtering with c_ω (at the cost of higher complexity) and the simulation is more consistent with the theoretical estimate. We now look at the probability of 4 random vectors summing to such sums:

$$\mathbf{Pr}\left[\Delta(\mathbf{g}) \leq c_\omega = 11 : \mathbf{g} \in L^{(2)}, \mathbf{g}_{[2\cdot 18]} = 0\right] = \frac{\sum_{i=0}^{c_\omega} \binom{d-2\cdot c}{i}}{2^{d-2\cdot c}} \approx 2^{-83.76},$$

therefore,

$$N_{\text{random}} \approx 2^{-64.18}.$$

- For the 8-sum distinguisher, the filter weight is chosen to be $c_\omega = 21$. Again, c must fulfill

$$N = \binom{3 \cdot 2^c}{8} \cdot 2^{-m-4c} \cdot 105 \cdot P_{\text{nf}} > 1,$$

where $P_{\text{nf}} \approx P_0 + P_1 + P_2 \approx 2^{-7.67}$. Setting $c = 14$, meaning $|L^{(0)}| = 3 \cdot 2^{14}$, suffices and gives $N > 1.35$. It needs to be clarified that in the 8-sum attack's implementation, the effect of keeping $|L^{(i)}| = 3 \cdot 2^{14}$ is more visible. In particular, we might discard all 'good combinations' when N is very close to 1. We adapt by allowing $|L^{(1)}|$ and $|L^{(2)}|$ to be at most $2 \cdot |L^{(0)}|$, then directly filter combinations from $|L^{(2)}|$ with c_ω. Therefore, the complexity is slightly higher than the theoretical estimate provided in the previous section. We suppose said negative impact can be mitigated when c is large as the vectors in $|L^{(i)}|$ might be more evenly distributed among buckets. The simulation returns 1.52 low weight vector on average after 10^2 tests.

  In the random case, the probability of having a vector having Hamming weight up to c_ω is:

$$\mathbf{Pr}\left[\Delta(\mathbf{g}) \leq c_\omega = 21 : \mathbf{g} \in L^{(3)}, \mathbf{g}_{[3\cdot 14]} = 0\right] = \frac{\sum_{i=0}^{c_\omega} \binom{d-3\cdot c}{i}}{2^{d-3\cdot c}} \approx 2^{-50.16},$$

which yields

$$N_{\text{random}} \approx 2^{-34.58}.$$

5 A key-recovery attack on Firekite

In this section we show a possible way to turn the distinguishing attack into a key-recovery attack with slightly higher complexity. We focus on the recovery of the secret $m \times d$ matrix $\mathbf{M}'$. First, we recall that the secret matrix $\mathbf{M}$ in Firekite is constructed by choosing a part of the bigger a $b \times b$ matrix $\mathbf{Q}$ as described in Section 2. We pick $\mathbf{q}_1 \xleftarrow{U} \mathbb{Z}_2^b$ and defined rows in the matrix $\mathbf{Q}$ as $\mathbf{q}_i = X^{i-1}\mathbf{q}_1, i = 1, ...b$, i.e., by shifting the first row to the left consecutively $b-1$ times. The secret matrix $\mathbf{M}$ is obtained by dropping the last $b-n$ columns of $\mathbf{Q}$ and keeping only the first m rows. The secret key is only the random b-bit vector $\mathbf{q}_1$ rather than a $m \times n$ matrix $\mathbf{M}$. Let the unknown bits in $\mathbf{q}_1$ be written as $\mathbf{q}_1 = (k_1, k_2, \ldots, k_b)$.

More specifically, we can now see that if $\mathbf{M} = [m_{ij}]_{m\times n}$ then every entry in the matrix $\mathbf{M}$ corresponds to an unknown key bit. As $\mathbf{M}'$ is the first part of $\mathbf{M}$, the same holds for $\mathbf{M}'$.

We can view $\mathbf{M}'$ as a generator matrix spans a code $\mathcal{C}$. But there are many generator matrices spanning the same code. One particular case is when $\mathbf{M}'$ is transformed to the systematic form, that is $\mathbf{M}'' = [\mathbf{I}\ \mathbf{J}]$, where $\mathbf{I}$ is the $m \times m$ identity matrix and $\mathbf{M}'' = \mathbf{S}\mathbf{M}'$ for some $m \times m$ unknown matrix $\mathbf{S}$. We assume $\mathcal{C} = \{\mathbf{v}\mathbf{M}', \mathbf{v} \in \mathbb{Z}_2^m\} = \{\mathbf{v}[\mathbf{I}\ \mathbf{J}], \mathbf{v} \in \mathbb{Z}_2^m\}$. In this case, entries in $\mathbf{J}$ are linear combinations of the secret key bits. Therefore, we consider all entries in $\mathbf{J}$ as unknown. There is an assumption here that the fist m columns of $\mathbf{M}'$ are linearly independent, which is adopted.

The key-recovery attack consists of running the aforementioned distinguisher, finding several zero sum vectors, and then deducing $\mathbf{M}'$. We first show how to derive the secret key from such zero sum vectors if we assume that the first m positions are all error free (no double error). Again, a zero sum vector fulfills

$$\sum_{j=1}^{l} \mathbf{g}_{i_j} = \sum_{j=1}^{l} \mathbf{v}_{i_j}\mathbf{M}' + \sum_{j=1}^{l} \mathbf{e}_{i_j} = \sum_{j=1}^{l} \mathbf{e}_{i_j}.$$

Therefore, finding a zero sum amounts to knowing the corresponding $\sum_{j=1}^{l} \mathbf{e}_{i_j}$. We now consider a single $\mathbf{g}_{i_j}$ vector. Its positions can be split in two parts, namely those for which we know that they are (most likely) error free mod 2 (since the error vector is zero in this position) and those for which we do not have knowledge of, since one of the l involved vectors has an error. Note that the first $t \cdot c$ positions are error free, but there are, on average, c_ω positions where at least one of the eight vectors will have an error.

If the first m positions are all of the error free type, one can write

$$\mathbf{g}_{i_j} = \mathbf{v}_{i_j}[\mathbf{I}\ \mathbf{J}] + \mathbf{e}_{i_j}. \tag{9}$$

We further have roughly $d - t \cdot c - c_\omega$ additional positions to be error free. For each such position, we can form a linear equation. Denote by $\mathbf{J}_q$ the q-th column of $\mathbf{J}$. Assume a position $q > m$ is error free. Then

$$\mathbf{g}_{i_j}(q) = \sum_{i'=1}^{m} \mathbf{v}_{i_j}(i')\mathbf{J}_q(i'). \tag{10}$$

Here $\mathbf{g}_{i_j}(q)$ denotes position q in vector $\mathbf{g}_{i_j}$, etc. Since $\mathbf{g}_{i_j}(q)$ and $\mathbf{v}_{i_j}$ are known, it gives a linear equation in the unknowns of vector $\mathbf{J}_q$. Collecting many such equations will enable us to derive $\mathbf{J}_q$ and eventually, the full $\mathbf{J}$ matrix. However, such approach is not adequate as we have seen in Section 4 that, for interested parameters, double error probability can not be disregarded. Hence, we need to consider a more complicated approach where we try to detect columns with double errors.

Assume we have found N zero sum vectors with the 8-sum distinguisher. Let the first seven vectors in the first zero sum vector $\sum_{j=1}^{l} \mathbf{g}_{i_j}$ be denoted $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_7$, the first seven vectors in the next zero sum vector be denoted $\mathbf{g}_8, \mathbf{g}_9, \ldots, \mathbf{g}_{14}$, and so forth. We construct a matrix

$$\mathbf{G} = (\mathbf{g}_i)_{i=1,\ldots,7N}$$

where $\mathbf{g}_i$ are row vectors.

Now we will examine the columns and the related known error vector for the corresponding zero sum vector. Recall that the first $t \cdot c$ columns are error free mod 2, by virtue of Algorithm 2. For the remaining columns, if $\sum_{j=1}^{l} \mathbf{g}_{i_j}$ is zero in the q-th position for **all** detected zero sum vectors, the corresponding column $\mathbf{G}_q$ is free of 'direct errors' and is kept. If it is not true, then we discard the column. After this process, we have a new matrix $\mathbf{G}'$ of length $t \cdot c + U$, where U is the number of columns kept in the previous step. If $t \cdot c + U > 7N > m$ there will be low-weight codewords in the code spanned by $\mathbf{G}'$. Namely, if $7N > m$ then there are linear combinations of rows that correspond to

a zero codeword plus error terms. As we have removed all 'direct errors', the only error contribution in the code must come from double errors.

Each double error will give either a 0 or a 1 as contribution in that position. Assume there are D double errors in the columns in $\mathbf{G}'$, then we expect to find codewords in the code spanned by $\mathbf{G}'$ that have weight around $D/2$. More, because we can form 2^{P-m} different combinations of rows that sum to zero in the underlying code, we have 2^{P-m} low weight codewords of weight around $D/2$. Finally, every column in $\mathbf{G}'$ can be found to contain a double error or not as follows. If this position is zero in all (or almost all) low-weight codewords, there is no double error. Otherwise, we detected a double error in that position. From this information, it is possible to do a full recovery through additional steps. A description of this key recovery attack is given in Appendix, Algorithm 3.

There arises a problem of finding enough columns free of direct errors. When the length n is small, there will be very few columns free of direct errors and the length of $\mathbf{G}'$ is not enough to have low-weight codewords. Therefore, in the following example, we choose a large n instance of Firekite to illustrate our attack.

5.1 Example of the key recovery attack on Firekite with $n = 16384$

Consider the Firekite parameters choice $m = 216$, $n = 16384$ and $k = 216$. The attack works as follows. First we run the 8-sum distinguisher to obtain zero sum vectors. In this case, we need to have slight more than $m/7$, e.g., 32 zero sum vectors. Applying (5), we choose $c = 60$ generating $N \approx 3.5$ zero sum vectors using the 8-sum distinguisher. Instead of repeating the distinguishing attacks 32 times or, equivalently 2^5 more work, we can instead increase the initial list size to $3 \cdot 2^{61}$ to obtain sufficient low-weight sum ($N \approx 41$), with an affordable complexity of $2^{69.87}$. We denote this cost by $C_{\text{distinguishing}}$.

We now consider a matrix $\mathbf{G}$ of dimension $32{\cdot}7$ consisting of the $\mathbf{g}_i$ vectors as its rows and we then remove columns with direct associated errors. In a zero sum vector, there are $216 \cdot 8$ errors inserted, so a positon is error free with probability $(1-1/(16384-61\cdot 3))^{216\cdot 8} \approx 0.899$. In our case, we want the position to be error free in all 32 zero sum vectors, which brings the probability to about 0.033. Since $d = 13144$, we can have about 432 columns error free. We then form the matrix $\mathbf{G}'$ which is of dimension $P = 224$ and length $189 + 432 = 621$. There will be $2^{224-216} = 2^8$ codewords in the code spanned by $\mathbf{G}'$ with support corresponding to the double errors.

By computing the likelihood of double errors, we find that a column in $\mathbf{G}'$ is error free with probability at most $0.995^{32} = 0.85$. For instance, consider a simple case where there is no non-repeating double error at position j-th of a zero sum. Then the probability is

$$1 - \binom{8}{2} \cdot \left(1 - \left(\frac{16383}{16384}\right)^{216}\right)^2 \cdot \left(\frac{16383}{16384}\right)^{216\cdot 6} \approx 0.995$$

One can expect $621 \cdot 0.15 = 93$ columns to have double errors. In conclusion, the code spanned by $\mathbf{G}'$ will contain 2^8 codewords where the weight is distributed around 47. Finding low-weight codewords in a random binary linear code is a well-known problem that has been studied extensively. One can use ISD algorithms to complete the task. For our example, an improved Stern's ISD algorithm[11] yields the bit-complexity estimate, denoted C_{ISD}, to be $2^{44.6}$, which is small compared to the distinguishing step.

A random linear code with dimension 224 and length 621 will have an expected minimum distance of about 100 according to the Varshamov-Gilbert bound, so the low weight codewords would come from the observation above. Finally, generating say 16 such low weight codewords, we look for the positions where all the 16 of these codewords are

[11] The estimate is obtained in a recent work by Andre Esser and Emanuele Bellini [EB21], where they unify ISD-algorithm variants (Prange,Stern,MMT,BJMM) in a *Nearest-Neighbor* framework. They also provided a complexity estimator for independent parameters.

zero. This would be the case for more than 500 positions and in this way we have identified 500 columns that are completely error free. Using a selection of them as the information set of the code we can recover remaining parts of the code $\mathbf{M}'$. The total complexity is therefore

$$C = C_{\text{distinguishing}} + C_{\text{ISD}} \approx 2^{69.87} + 16 \cdot 2^{44.6} \approx 2^{69.87}.$$

6 Discussion and Conclusions

Having seen how Firekite is vulnerable to our distinguisher, especially the 8-sum distinguishing attack, it is natural to ask how we can make Firekite and other similar ciphers resilient to a generic birthday problem solving algorithm. From the result and performance of our attacks, there are certain approaches one can consider. First, we observed that N_{random}, or in other words, the failure probability inflates when the filtering weight c_ω grows. That is to say, unless c_ω is very small compared to d, it is difficult to distinguish Firekite's zero sum vectors from those that could stem from random vectors $\mathbf{g}_i$. Therefore, instantiating Firekite with larger k can be beneficial. Second, we have discussed that the attack complexity depends on the parameter c which is solely determined by m (if we fix l), the number of rows in $\mathbf{M}$. Therefore, if the security level is close to $m/(1 + \log l)$, our attack becomes infeasible. As a contribution to Firekite's design criteria, we propose a few modifications as follows.

For small Firekite's parameters, one can increase k slightly, which yields an LPN instance with a higher noise rate; therefore more difficult to solve in general. In our estimate, larger k suggests a drastic decrease in P_{nf} and an increase in N_{random}. It is now exceedingly unlikely to have no error in the first $t \cdot c$ bits and d becomes smaller, which makes it more difficult to distinguish the zero sum found by Algorithm 2 from those stemming from the random case. As an example, by setting $k = 24$ for the instance $n = 1024, m = 216$, our attack was rendered useless as N_{random} is always larger than 1. This comes at the cost of decreasing the number of bits encrypted per invocation; hence more instructions need to be executed *per bit*. However, larger parameter instances of Firekite are less affected by this 'fix' as d becomes large relatively to k. For instance, our 8-sum attack still succeeds with $n = 16384, m = 216$ despite raising k from its original $k = 216$ to $k = 400$. We only need to slightly increase $|L^{(0)}| = 3 \cdot 2^{67}$ and we still obtain a good failure probability as $N_{\text{random}} \approx 2^{-2835}$. An extreme adjustment such as $k = 600$ gives Firekite resistance to our attack. We apply this idea to our simulation with toy parameters to verify the countermeasure (see Appendix, Example 3).

Finally, we may discuss possible future improvements to the proposed attack. We believe that there can be a possibility to gain some small amount in terms of decreased complexity by smaller changes in the distinguishing algorithm. One idea could be to not only allow sums of vectors that sum to zero in c positions, but also those that have weight 1 in these c positions. Still, it would not change the complexity significantly and with modified parameters as suggested above the Firekite should meet the intended security level. Moreover, since our approach relies heavily on GBA, it would be amenable in principle to quantum search approach, e.g., using result in [NPS20].

References

[ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA,*

August 16-20, 2009. Proceedings, volume 5677 of *Lecture Notes in Computer Science*, pages 595–618. Springer, 2009.

[Ber09] Daniel J Bernstein. Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer, 2009.

[BFKL93] Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. In Douglas R. Stinson, editor, *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, volume 773 of *Lecture Notes in Computer Science*, pages 278–291. Springer, 1993.

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in 2 n/20: How 1 + 1 = 0 improves information set decoding. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 520–536. Springer, 2012.

[BKLV21] Sonia Bogos, Dario Korolija, Thomas Locher, and Serge Vaudenay. Towards efficient lpn-based symmetric encryption. In Kazue Sako and Nils Ole Tippenhauer, editors, *Applied Cryptography and Network Security - 19th International Conference, ACNS 2021, Kamakura, Japan, June 21-24, 2021, Proceedings, Part II*, volume 12727 of *Lecture Notes in Computer Science*, pages 208–230. Springer, 2021.

[BKW03] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. *J. ACM*, 50(4):506–519, 2003.

[BLP11] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Smaller decoding exponents: Ball-collision decoding. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 743–760. Springer, 2011.

[BM17] Leif Both and Alexander May. The approximate k-list problem. *IACR Trans. Symmetric Cryptol.*, 2017(1):380–397, 2017.

[BMvT78] Elwyn R. Berlekamp, Robert J. McEliece, and Henk C. A. van Tilborg. On the inherent intractability of certain coding problems (corresp.). *IEEE Trans. Inf. Theory*, 24(3):384–386, 1978.

[BSH06] Johann Barbier, Guillaume Sicot, and Sébastien Houcke. Algebraic approach for the reconstruction of linear and convolutional error correcting codes. *International Journal of Applied Mathematics and Computer Science*, 2(3):113–118, 2006.

[BV15] Sonia Bogos and Serge Vaudenay. How to sequentialize independent parallel attacks? - biased distributions have a phase transition. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 704–731. Springer, 2015.

[CF09] Mathieu Cluzeau and Matthieu Finiasz. Recovering a code's length and synchronization from a noisy intercepted bitstream. In *IEEE International Symposium on Information Theory, ISIT 2009, June 28 - July 3, 2009, Seoul, Korea, Proceedings*, pages 2737–2741. IEEE, 2009.

[CT19] Kevin Carrier and Jean-Pierre Tillich. Identifying an unknown code by partial gaussian elimination. *Des. Codes Cryptogr.*, 87(2-3):685–713, 2019.

[DKPW12] Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, and Daniel Wichs. Message authentication, revisited. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 355–374. Springer, 2012.

[DV13] Alexandre Duc and Serge Vaudenay. HELEN: A public-key cryptosystem based on the LPN and the decisional minimal distance problems. In Amr M. Youssef, Abderrahmane Nitaj, and Aboul Ella Hassanien, editors, *Progress in Cryptology - AFRICACRYPT 2013, 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22-24, 2013. Proceedings*, volume 7918 of *Lecture Notes in Computer Science*, pages 107–126. Springer, 2013.

[EB21] Andre Esser and Emanuele Bellini. Syndrome decoding estimator. *IACR Cryptol. ePrint Arch.*, page 1243, 2021.

[GJL14] Qian Guo, Thomas Johansson, and Carl Löndahl. Solving LPN using covering codes. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2014.

[GRS08a] Henri Gilbert, Matthew J. B. Robshaw, and Yannick Seurin. $\mathrm{Hb}^{\#}$: Increasing the security and efficiency of hb^{+}. In Nigel P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 361–378. Springer, 2008.

[GRS08b] Henri Gilbert, Matthew J. B. Robshaw, and Yannick Seurin. How to encrypt with the LPN problem. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II - Track B: Logic, Semantics, and Theory of Programming & Track C: Security and Cryptography Foundations*, volume 5126 of *Lecture Notes in Computer Science*, pages 679–690. Springer, 2008.

[HB01] Nicholas J. Hopper and Manuel Blum. Secure human identification protocols. In Colin Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 52–66. Springer, 2001.

[HDWH12] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J Alex Halderman. Mining your ps and qs: Detection of widespread weak keys in network devices. In *21st {USENIX} Security Symposium ({USENIX} Security 12)*, pages 205–220, 2012.

[HJB09] Martin Hell, Thomas Johansson, and Lennart Brynielsson. An overview of distinguishing attacks on stream ciphers. *Cryptogr. Commun.*, 1(1):71–94, 2009.

[HKL+07] Stefan Heyse, Eike Kiltz, Vadim Lyubashesvky, Christof Paar, and Krzysztof Pietrzak. An efficient authentication protocol based on ring-lpn. In *ECRYPT Workshop on Lightweight Cryptography*, volume 2011. Citeseer, 2007.

[HKL+12] Stefan Heyse, Eike Kiltz, Vadim Lyubashevsky, Christof Paar, and Krzysztof Pietrzak. Lapin: An efficient authentication protocol based on ring-lpn. In Anne Canteaut, editor, *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*, pages 346–365. Springer, 2012.

[IL90] Russell Impagliazzo and Leonid A. Levin. No better ways to generate hard NP instances than picking uniformly at random. In *31st Annual Symposium on Foundations of Computer Science, St. Louis, Missouri, USA, October 22-24, 1990, Volume II*, pages 812–821. IEEE Computer Society, 1990.

[JW05] Ari Juels and Stephen A. Weis. Authenticating pervasive devices with human protocols. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 293–308. Springer, 2005.

[Kir11] Paul Kirchner. Improved generalized birthday attack. *IACR Cryptol. ePrint Arch.*, page 377, 2011.

[KPV+17] Eike Kiltz, Krzysztof Pietrzak, Daniele Venturi, David Cash, and Abhishek Jain. Efficient authentication from hard learning problems. *J. Cryptol.*, 30(4):1238–1275, 2017.

[KS06] Jonathan Katz and Ji Sun Shin. Parallel and concurrent security of the HB and hb+ protocols. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 73–87. Springer, 2006.

[LB88] Pil Joong Lee and Ernest F. Brickell. An observation on the security of mceliece's public-key cryptosystem. In Christoph G. Günther, editor, *Advances in Cryptology - EUROCRYPT '88, Workshop on the Theory and Application of of Cryptographic Techniques, Davos, Switzerland, May 25-27, 1988, Proceedings*, volume 330 of *Lecture Notes in Computer Science*, pages 275–280. Springer, 1988.

[Leo88] Jeffrey S. Leon. A probabilistic algorithm for computing minimum weights of large error-correcting codes. *IEEE Trans. Inf. Theory*, 34(5):1354–1359, 1988.

[LF06] Éric Levieil and Pierre-Alain Fouque. An improved LPN algorithm. In Roberto De Prisco and Moti Yung, editors, *Security and Cryptography for Networks, 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006, Proceedings*, volume 4116 of *Lecture Notes in Computer Science*, pages 348–359. Springer, 2006.

[MGB12] Mélanie Marazin, Roland Gautier, and Gilles Burel. Algebraic method for blind recovery of punctured convolutional encoders from an erroneous bitstream. *IET Signal Process.*, 6(2):122–131, 2012.

[Må18] Erik Mårtensson. Poster: Coded-bkw with sieving. In *Training School on Cryptanalysis of Ubiquitous Computing Systems*, Ponta Delgada, Azores, Portugal, April 2018.

[NPS20] María Naya-Plasencia and André Schrottenloher. Optimal merging in quantum k-xor and k-sum algorithms. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 311–340, Cham, 2020. Springer International Publishing.

[Pra62] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Trans. Inf. Theory*, 8(5):5–9, 1962.

[SHB09] Guillaume Sicot, Sébastien Houcke, and Johann Barbier. Blind detection of interleaver parameters. *Signal Process.*, 89(4):450–462, 2009.

[Sho99] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.*, 41(2):303–332, 1999.

[Ste93] Jacques Stern. A new identification scheme based on syndrome decoding. In Douglas R. Stinson, editor, *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, volume 773 of *Lecture Notes in Computer Science*, pages 13–21. Springer, 1993.

[Tix15] Audrey Tixier. Blind identification of an unknown interleaved convolutional code. In *IEEE International Symposium on Information Theory, ISIT 2015, Hong Kong, China, June 14-19, 2015*, pages 71–75. IEEE, 2015.

[Wag02] David A. Wagner. A generalized birthday problem. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 288–303. Springer, 2002.

[YZ16] Yu Yu and Jiang Zhang. Cryptography with auxiliary input and trapdoor from constant-noise LPN. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 214–243. Springer, 2016.

A

Algorithm 3: Firekite key recovery algorithm

Input: A list $L^{(0)}$, with $\mathbf{g}_i \in \mathbb{Z}_2^n$, parameters k, m, d, $c_\omega = \lceil \frac{8 \cdot k \cdot d}{n} \rceil, D/2, G = \emptyset, E = \emptyset$.

for $i = 1, ..., 3$ **do**
  $L^{(i)} = \text{COMBINE}(L^{(i-1)})$;
for $\mathbf{s}_i = \sum_{j=1}^{8} \mathbf{g}_{i_j}$ **in** $L^{(3)}$ **do**
  if $\mathsf{HammingWt}(\mathbf{s}_i) \leq c_\omega$ **then**
    $G \leftarrow G \cup \{\mathbf{g}_{i_1}, \cdots, \mathbf{g}_{i_7}\}$;
$\mathbf{G} = (\mathbf{g}_j)_{j=1 \cdots |G|}$; `// constructing G`
for $i = 1, ..., d$ **do**
  if $\exists \mathbf{s} \in L^{(3)}, \mathbf{s}_i = 1$ **then**
    $\mathbf{G} \leftarrow \mathbf{G} \setminus \mathbf{G}_i$; `// removing columns with direct error`
Finding all vectors $\mathbf{e}_i$ spanned by $\mathbf{G}$ that are of Hamming weight less than $D/2$;
Keep columns of $\mathbf{G}$ if $\mathbf{e}_i$ are all 0 in that position;
Recover $\mathbf{M}'$ from $\mathbf{G}$;
return $\mathbf{M}'$;

Example 1. (Probability of repeating double error.)

To convince readers that P_{nf} can be reasonably approximated by taking into account only non-repeating double error, we give an example where there is 1 double-error. We consider the probabilities of this event in both cases: the double error comes from only 2 or 4 vectors out of 8. Our parameters are $n = 1024, k = 16, c = 62$ (see Section 4 for the choice of c).

The probability of 4 error vectors having a one in the same position in the first $3 \cdot c$ bits is:

$$P_1 \approx \binom{8}{4} \frac{k^4}{(3c)^3} \left(\frac{3c}{n}\right)^4 \left(\frac{n-3c}{n}\right)^{4(k-1)} \left(\frac{n-3c}{n}\right)^{4k} \approx 2^{-46.19}.$$

The probability of 2 error vectors having a one in the same position in the first $3 \cdot c$ bits is:

$$P_1' \approx \binom{8}{2} \frac{k^2}{3c} \left(\frac{3c}{n}\right)^2 \left(\frac{n-3c}{n}\right)^{2(k-1)} \left(\frac{n-3c}{n}\right)^{6k} \approx 2^{-36.09} \gg P.$$

Table 3: Repeating (P_1) and non-repeating double errors (P_1') probabilities for some parameters of Firekite.

Parameters			Probabilities	
m	n	k	$\log(P_1)$	$\log(P_1')$
216	1024	16	-46.19	-36.09
216	2048	32	-44.95	-34.54
216	16,384	216	-33.37	-27.70

Example 2. (Multiple double errors)

Let us compare the probabilities of multiple double errors in the first $t \cdot c$ bits to justify our assumption that P_{nf} can be 'practically' approximated. We continue with Firekite parameters in Example 1, with $c = 76$ (4-sum distinguisher).

The probability of no double error in the first $2 \cdot 76$ bits is:

$$P_0 = \left(\frac{n - 2 \cdot c}{n}\right)^{4k} \approx 2^{-14.83}.$$

The probability of one double error in the first $2 \cdot 76$ bits is:

$$P_1 \approx \binom{4}{2} \frac{k^2}{(2c)} \left(\frac{2c}{n}\right)^2 \left(\frac{n - 2c}{n}\right)^{2(k-1)} \left(\frac{n - 2c}{n}\right)^{2k} \approx 2^{-17.13}.$$

Therefore, $P_0 + P_1 \approx 2^{-14.57}$, and more importantly, this 'better approximation' of P_{nf} does not affect our algorithm significantly.

Another example being P_{nf} in our simulation (Section 4) where $n = 256, m = 52, k = 4$. For the 8-sum distinguisher, the double error probabilities are:

$$P_0 \approx 2^{-8.27},$$

$$P_1 \approx 2^{-9.55},$$

$$P_2 \approx 2^{-11.58}.$$

Example 3. (Improve Firekite by increasing noise level)

Recall in our simulation, the parameters are $n = 256, m = 52, k = 4$. We increase k to $k = 7$ and apply the 8-sum distinguisher again with $c = 14$. One can verify, with the new parameters, that

$$N_{\text{random}} \approx 3.15.$$

$$N \approx 0.03.$$

As discussed in Section 4, due to non-uniformity of the input, we exhaust all combinations in the last Combine step. On average, there are 2^{18} vectors in $L^{(3)}$ which raises N_{random} (in our simulation) to $\frac{2^{18}}{3 \cdot 2^{14}} \cdot 3.15 \approx 18.9$. After 10^2 tests, we observe on average, 18.8 low weight vectors. Therefore our distinguishing attack does not work.