On the Circuit Complexity of Isomorphic Galois Field Transformations

Charanjit S. Jutla
IBM TJ Watson Research Center

Vijay Kumar
Amazon.com

Atri Rudra
IBM India Research Lab

Abstract

We study the circuit complexity of linear transformations between Galois fields $\mathrm{GF}(2^{mn})$ and their isomorphic composite fields $\mathrm{GF}((2^m)^n)$. For such a transformation, we show a lower bound of $\Omega(mn)$ on the number of gates required in any circuit consisting of constant-fan-in XOR gates, except for a class of transformations between representations of such fields which are nicely characterized. The exceptions show that the polynomials representing the fields must be of a regular form, which may be of independent interest. We characterize a family of transformations which can be implemented as crosswires (permutations), without using any gates, which is very useful in designing hardware implementations – and through bit-slicing, software implementations – of computations based on Galois Field arithmetic. We also show that our lower bound is tight, by demonstrating a class of transformations which only require a linear number of gates.

1 Introduction

Galois Field Arithmetic finds wide use in engineering applications such as error-correcting codes [4, 14], cryptography [26], switching theory [2] and digital signal processing [3, 15]. However the bulk of the applications have been in cryptography and coding theory. Galois fields have been extensively used in public key cryptography. In Diffie-Hellman [7] key exchange protocol, and in ElGamal public key encryption scheme [8], the cyclic multiplicative group of Galois fields is employed. In elliptic curve cryptogrpahy [12][17] the elliptic curves are considered over Galois fields. Galois fields have also been used in symmetric key cryptography, mostly to use different non-compatible groups to introduce non-linearity. The best example of this is perhaps the recently selected AES algorithm Rijndael [28]. There has been a growing interest to develop hardware and software methods for implementing the finite field arithmetic operations particularly for cryptographic application [22, 27, 19, 25]. In search for efficiency, computations are often performed in alternate bases. Two such conversions have been addressed in the recent past [11, 10].

It is well known [13] that a finite field of q^n elements can be represented by polynomials modulo an irreducible polynomial of degree n, the polynomials being defined over $GF(q)$. Thus, a field with 2^{mn} elements can be derived either (1) by an irreducible polynomial f over $\mathrm{GF}(2)$ of degree mn, or (2) by an irreducible polynomial g over $\mathrm{GF}(2^n)$ of degree m. The latter representation is called a composite field representation. Efficient hardware and software implementations have been obtained in composite fields [27, 19, 21, 23]. The best hardware and software performance numbers for Rijndael [28] reported so far are for implementations of Rijndael in composite fields [21, 23]. The use of composite fields for a software Rijndael encryption in [21] reduced the encryption latency by a significant 20%. Satoh et al. [23] achieved a performance increase as high as 6 times the previous hardware circuits.

The performance of a composite field implementation depends both on the cost of performing arithmetic in the composite field as well as the cost of transforming elements from the original field to the composite field and vice-versa. The latter cost is an overhead that varies by the computation performed, and may be significant, particularly in situations involving large fields. Essentially, when transforming the $GF(2^k)$ operations in an algorithm to operations in some composite field, the isomorphism (and its inverse) would need to be applied to certain inputs (and outputs) of the algorithm. Moreover, in some cases we may need to perform the conversion from the original field to a composite field and vice-versa multiple times in the execution of the algorithm. The latter is done in the Rijndael implementation in [23], where the isomorphism matrix (and it's inverse) are placed at the input and output of the S-box (and thus, the conversion is done in every round of Rijndael). In this scenario, the actual cost of the transformation becomes more significant. Though there are some algorithms to compute the transformations[18], no systematic study of the complexity of the operation has been done so far.

In this paper, we show a lower bound (linear in GF(2)) on the circuit complexity of transformation between $\mathrm{GF}(2^{mn})$ and the isomorphic composite field $\mathrm{GF}((2^m)^n)$, except for a few classes of transformations which are nicely characterized. The lower bound is linear in nm. The exceptional classes are important in themselves, as they can offer advantages to designer of cryptographic algorithms. There are many instances where the cryptographer has a wide choice of field representations to pick from. In such a case our study of the lower bound and the exceptional classes can help in both cryptanalysis and efficiency considerations.

When the irreducible polynomial g over $\mathrm{GF}(2^n)$ is a binomial, i.e. of the form $x^m + \omega$, where ω is in $\mathrm{GF}(2^n)$, then there exist a family of representations where the transformation between the two isomorphic fields is just a permutation, and thus the number of gates required in a circuit implementation is zero. We exactly characterize this infinite family when the order of ω is small (less than $2n$). Because of this family, we do not have a lower bound on the general circuit complexity of such transformations when g is a binomial.

In addition, we show that when the order of an irreducible polynomial (i.e., the order of its roots) of degree n is less than $2n$, then the polynomial must be of the form $(x^{p^r} - 1)/(x^{p^{r-1}} - 1)$, where p is a prime. This could be of independent interest, especially to the study of linear feedback shift registers (LFSRs). It is this fact which allows us to characterize the permutations mentioned above.

However, when g is not a binomial, we prove a linear lower bound on the gate complexity of such transformations, where the circuits themselves are linear over GF(2) – that is, they *employ only XOR gates*. Even in the case that g is a binomial, except for a very special class of transformations, we do indeed prove a linear lower bound. We also show a family of transformations which require only a linear number of gates, showing that our bound is tight. Linear circuits over GF(2) are studied in [1], where it is proved that Boolean Hadamard Matrix transformations require $\Omega(n \log n)$ gates.

The rest of the paper is organized as follows. In section 2 we prove two lemmas which could be of independent interest to finite field theory. In section 3 we set forth definitions of isomorphisms, transformations, and circuit complexity. In section 4 we prove the lower bound for the case when the polynomial g is not a binomial. In section 5 we address the binomial case. In the appendix A we generalize the result to tower composite fields. In appendix B, we give a brief introduction to the relevant concepts in Galois Fields.

2 The Regularity and Shifting Lemmas

In this section we present two lemmas which may be of independent interest to the reader, beyond their use in the proofs herein.

Lemma 1 (**Regularity Lemma**) *Let $f(x)$ be a degree n irreducible polynomial over $GF(q)$. Let m be the least number such that $f(x)$ divides $x^m - 1$ (i.e., m is the order of the polynomial). If $m < 2n$, then m is a prime power p^e, and*

$$f(x) = \frac{x^{p^e} - 1}{x^{p^{e-1}} - 1}$$

The following proof of this lemma is due to Coppersmith[5].

Proof: Let α be a root of $f(x)$ in some extension field of $GF(q)$. Then, $f(x)$ is the minimal polynomial of α over $GF(q)$. Moreover, α has order m, and $\gcd(m, q) = 1$ (since q is a prime power, and m divides $q^n - 1$).

Let $m = \prod_i p_i^{e_i}$ be the prime factorization of m. Then $\phi(m) = \prod_i (p_i - 1)p_i^{e_i-1}$. Note that $q^{\phi(m)} = 1 \bmod m$ as $\gcd(m, q) = 1$. Let $\lambda(m) = \mathrm{lcm}\{(p_i - 1)(p_i^{e_i-1})\}$. Then, $q^{\lambda(m)} = 1 \bmod m$, as $q^{\lambda(m)} - 1$ is divisible by each prime power in m.

For any γ in an extension field of $GF(q)$ (with order of γ being s), the minimal polynomial of γ over $GF(q)$ is $\prod_{i=0}^{t-1}(x - \gamma^{q^i})$ where t is the smallest integer such that $q^t = 1(\bmod s)$. Thus, $deg(f(x)) = n$ is the order of q mod m. This implies that $\lambda(m) = nc$, where c is an integer ≥ 1.

If m is not a prime power then $\lambda(m) < m/2$, a contradiction since $n > m/2$. Thus, m is a prime power, say $m = p^e$. Thus, $\lambda(m) = \phi(m) = (p-1)p^{e-1}$. As $\lambda(m) = nc$ and $n > m/2$, $n = \lambda(m)$ and $m - n = p^{e-1}$. We know $x^{p^{e-1}} - 1$ is a divisor of $x^m - 1$, of the right degree, so that is the only choice for $(x^m - 1)/f(x)$. ∎

Let $[s)$ denote the set $\{0, 1, \ldots, s-1\}$.

Let $q < 2n$ and $gcd(r, q) = 1$, where $1 < r < q$. Also let $W = \{0, 1, \cdots, q-1\}$, $W_1 = \{0, 1, \cdots, n-1\}$ and $W_2 = W - W_1$. $\mathcal{R}_r = \{ir \bmod (q) | i \in [n)\}$ and $\mathcal{R}'_r = \{j \in \mathcal{R}_r | j \in W_2\}$.

Lemma 2 (**Shifting Lemma**) *$\forall r, 1 < r < q$, $|\mathcal{R}'_r| = \Omega(q - n)$.*

Proof: We will consider three ranges of values for r:

- Case 1 : $n \leq r < q$ Define $d = q - r$.
  Also let $[n) = \bigcup_{j=0}^{n/\lfloor \frac{q}{d} \rfloor} S_j$, where $S_j = \{j\lfloor \frac{q}{d} \rfloor, j\lfloor \frac{q}{d} \rfloor + 1, \cdots, (j+1)\lfloor \frac{q}{d} \rfloor - 1\}$. Further let $s_{j,i} \in S_j = (j\lfloor \frac{q}{d} \rfloor + i)$ and $r_{j,i} = r.s_{j,i} \bmod (q)$. Then note the following points–
  - $r_{j,(i+1)} \bmod (q) = r_{j,i} \bmod (q) - d$.
  - $\{s_{j,0}, s_{j,1}, \cdots, s_{j,(\lfloor \frac{q-n}{d} \rfloor - 1)}\} \subseteq W_2$.
  - $(q - s_{j,0}) > (q - s_{(j+1),0})$.

  The above implies that $|\mathcal{R}'_r| = \frac{n}{\lfloor \frac{q}{d} \rfloor} \times \lfloor \frac{q-n}{d} \rfloor = \Omega(q - n)$.

- Case 2 : $q - n < r < n$. Note that in this case $ir \bmod (q) \in W_2 \Rightarrow (i+1)r \bmod (q) \in W_1$. To see this note that $\min\{ir \bmod (q) + r\} > n + (q - n) = q$ and $\max\{ir \bmod (q) + r\} < q + n$.We further define $G = \{i \in [q) | ir \bmod (q) \in W_2\}$ and $G + 1 = \{j \in [q) | j - 1 \in G\}$. Note that G has $q - n$ elements.
  Suppose less than $\frac{q-n}{2}$ values from both G and $G + 1$ fall in $[n)$, then
  $|[n)| < q - |G| - |G + 1| + 2.\frac{q-n}{2} < n$, which is contradiction. Hence

– at least $\frac{q-n}{2}$ elements from G are taken which implies $|\mathcal{R}'_r| \geq \frac{q-n}{2}$; or
– at least $\frac{q-n}{2}$ elements from $G+1$ are taken which implies $|\mathcal{R}'_r| \geq \frac{q-n}{2} - 1$.

- Case 3 : $1 < r \leq (q-n)$. Note that $\forall i \in [n)$, $ir \bmod (q) = (q-i)(q-r) \bmod (q) = x(q-r)$, where $x \in \{q-n+1, \cdots, q\}$. A proof similar to Case 1 works as $(q-r) \geq n$.

■

3 Preliminaries

First, we set for some notation and lemmas which will be used in the later sections of the paper.

Lemma 3 [16] *Let r be an odd prime. Suppose that 2 is primitive modulo r and r^2 does not divide $2^{r-1}-1$. Then the polynomial $x^{(r-1)r^l} + x^{(r-2)r^l} + \cdots + x^{r^l} + 1$ is irreducible over $GF(2)$ for each $l \geq 0$.*

Lemma 4 *Let r be a prime. If 2 is primitive modulo r, then the polynomial $x^{r-1}+x^{r-2}+\cdots+x+1$ is irreducible over $GF(2)$.*

Proof: Let α be a primitive rth root of unity in some extension field of $GF(2)$. Since, 2 is primitive modulo r, then the primitive polynomial of α is a degree $r-1 = \phi(r)$ polynomial. Thus, $(x^r - 1)/(x-1)$ must be this primitive polynomial.

■

A $k \times k$ binary matrix $M = [m_{ij}]$ is called a *(k,t)-row matrix* if $\exists r_1, r_2, \cdots, r_t \in \{1, \cdots, k\}$ such that

$$\sum_{j=1}^{k} m_{lj} \begin{cases} \geq 2 & \text{if } l \in \{r_1, r_2, \cdots, r_t\} \\ = 1 & \text{otherwise} \end{cases}$$

M is called a *(k,t)-column matrix* if M^T is a (k,t)-row matrix.

Consider a transformation matrix T that performs the isomorphic mapping from $GF(2^k)$ to some composite field. That is, $\vec{y} = T.\vec{x}$ is the element of the composite field corresponding to $\vec{x} \in GF(2^k)$. Such a matrix T is called a *(k,t)-row (column) iso-transform* if it is a (k,t)-row (column) matrix.

For any matrix T, we denote by $s(T)$ the smallest possible number of fan-in 2, arbitrary fan-out gates in any linear (over $GF(2)$) circuit that computes $T.\vec{x}$. Note that over $GF(2)$ linear circuit means that all gates are just exclusive-or gates.

Note that in circuit complexity literature, the complexity is measured by the number of edges in the directed acyclic graph representing the circuit (with each node being a gate), while we are counting the number of actual gates in the circuit. These measures are equivalent when the number of gates is super-linear. However, in our case, as we shall show, we have permutations as well as transform with linear gates– the edge-count would have the same order in both cases while the gate count is a more accurate measure.

Lemma 5 *For any (k,t)-row iso-transform M, $s(M) = \Omega(t)$.*

Proof: The hamming distance between any two rows in M is at least one. Let $\mathcal{R}$ be the set of rows where the number of 1s is greater than 1. Let $\vec{y} = M \cdot \vec{x}$. For each $r_i \in \mathcal{R}$, the corresponding y_i is the output of some circuit gate. Each such y_i is the output of a distinct gate, since otherwise there will be fewer than 2^k distinct possible $\vec{y}$ values. ■

Note that the previous lemma holds for any circuit, and not just linear circuits. However, for the next lemma we do require that the circuit be a linear circuit.

Lemma 6 [1] *For any boolean matrix B, $s(B) = s(B^T)$.*

Lemma 5 and Lemma 6 together imply

Corollary 1 *For any (k,t)-column iso-transform M, $s(M) = \Omega(t)$.* ■

Let $R(z)$ be the field polynomial of $GF(2^k)$, and β a root of $R(z)$. Let $\mathcal{B}$ denote $\{1, \beta, \beta^2, \cdots, \beta^{k-1}\}$, the standard basis for representing elements of $GF(2^k)$. Let $\mathcal{S}$ denote the set $\{1, \beta, \beta^2, \cdots, \beta^{k/2-1}\}$. Note that if $\gamma \in \mathcal{S}$, then $\gamma^2 \in \mathcal{B}$.

We denote by $\mathcal{O}(f)$ and $\mathcal{D}(f)$, the order and degree respectively of an irreducible polynomial $f(x)$. We have the following observation–

Observation 1 *For any irreducible polynomial f, $\mathcal{O}(f)$ is odd.*

Further, $f(x)$ is a *good* polynomial if $\mathcal{O}(f) \geq 2\mathcal{D}(f)$.

Let the underlying field polynomials of $GF((2^n)^m)$ be $Q(y)$ and $P(x)$, where $Q(y)$ generates $GF(2^n)$. Let α and ω be a root of $P(x)$ and $Q(y)$ respectively. Any $a \in GF((2^n)^m)$ can be written as $a = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + ... + a_1\alpha + a_0$ for some $a_i \in GF(2^n)$.

Consider a $k \times k$ binary matrix T which implements some isomorphism H from $GF(2^k)$ to the composite $GF((2^n)^m)$. Suppose T is a (k,t)-column matrix. Let $\{r_1, ..., r_t\}$ be the columns of T with more than one non-zero entries. Let $\mathcal{T}$ be the set $\{\beta^{r_1}, \beta^{r_2}, \cdots, \beta^{r_t}\}$. Thus,

$$H(\beta^l) = \begin{cases} \Sigma_{i=0}^{m-1}\Sigma_{j=0}^{n-1} c_{ij}^l \alpha^i \omega^j, & \text{where alteast two } c_{ij}^l = 1, \quad \text{if } \beta^l \in \mathcal{T} \\ \alpha^{i_l}\omega^{j_l}, & \text{for some unique tuple } (i,j) \text{ where } i_l < m \text{ and } j_l < n, \quad \text{if } \beta^l \in \mathcal{B} - \mathcal{T}. \end{cases}$$

Let $\sqrt{\mathcal{T}} \subseteq \mathcal{B}$ denote the set $\{\beta^j \mid \beta^{2j} \in \mathcal{T}\}$. Let $\mathcal{Z} = (\sqrt{\mathcal{T}} \cup \mathcal{T}) \cap \mathcal{S}$. Note that $|\mathcal{Z}| \leq 2|\mathcal{T}| = 2t$. Further, for any set A, let $H(A) = \{H(x)| \ x \in A\}$.

Lemma 7 *Let $\{1, \gamma, \gamma^2, ..., \gamma^{k-1}\}$be linearly independent over $GF(2)$, where $\gamma \in GF((2^n)^m)$. H is defined in the following manner - $H(\sum_{i=0}^{k-1} c_i\beta^i) = \sum_{i=0}^{k-1} c_i\gamma^i$, for all possible distinct vectors $(c_0, \cdots, c_{k-1})$, where $c_i \in GF(2)$. If $R(\gamma) = 0$ then H is an isomorphism.*

Proof: By definition, H satisfies additive homomorphism.

Let $\delta \in GF(2^k)$ be a generator. To show that H satisfies multiplicative homomorphism (and hence is an isomorphism), it is sufficient to show that $\forall i \in [0, 2^k - 2] H(\delta^i)H(\delta) = H(\delta^{i+1})$. To this end we first show that $\forall x \in GF(2^k)$, $H(x)H(\beta) = H(x\beta)$. Let $\beta^k = \sum_{i=0}^{k-1} d_i\beta^i$ and $x = \sum_{i=0}^{k-1} c_i^x\beta^i$. Now $x\beta = \sum_{i=1}^{k-1}(c_{i-1}^x + c_{k-1}^x d_i)\beta^i + c_{k-1}^x d_0$. By the definition of H, $H(x) = \sum_{i=0}^{k-1} c_i^x\gamma^i$ and the fact that $R(\gamma) = 0$, $\gamma^k = \sum_{i=0}^{k-1} d_i\gamma^i$. $H(x)H(\beta) = H(x\beta)$ follows by noting that $H(x\beta) = \sum_{i=1}^{k-1}(c_{i-1}^x + c_{k-1}^x d_i)\gamma^i + c_{k-1}^x d_0$.

By definition of H and repeated application of $H(x)H(\beta) = H(x\beta)$, we have $\forall j \in [1, k-1]$, $H(\delta^i)H(\beta^j) = H(\delta^i\beta^j)$. The proof follows from the fact that H satisfies additive homomorphism and that δ is a linear combination of $\{1, \beta, \cdots, \beta^{k-1}\}$. ■

Claim 1 *If $H(\beta) \neq \alpha^u\omega^v$ for any $u \in [0\cdots(\mathcal{O}(P)-1)], v \in [0\cdots(\mathcal{O}(Q)-1)]; u+v \neq 0$, then $s(T) = \Omega(k)$.*

Proof: $H(\beta) \neq \alpha^u\omega^v$ implies that there does not exist an i such that

- $H(\beta^i) = \alpha^{u'}\omega^{v'}$ for some $u' \in [0\cdots(\mathcal{O}(P)-1)], v' \in [0\cdots(\mathcal{O}(Q)-1)]$; and
- $H(\beta^{i+1}) = \alpha^{u''}\omega^{v''}$ for some $u'' \in [0\cdots(\mathcal{O}(P)-1)], v'' \in [0\cdots(\mathcal{O}(Q)-1)]$.

This implies that T is a (k,t')–column transform, where $t' > k/2$. The claim follows from Corollary 1 ■

4 Lower bound proof

Here we present the proof for the linear lower bound when none of the polynomials are binomials. We proceed in the following manner – first we prove that if H is of a particular type, then we trivially have the liner lower bound (Claim 1). The proof does case analysis on whether $P(x)$ and/or $Q(y)$ are *good*. In all the cases we prove the bound by using contradiction and counting arguments.

We consider three cases depending on whether $P(x)$ and $Q(y)$ are *good*.

Case 1 : Both $P(x)$ and $Q(y)$ are *good* polynomials.

Lemma 8 $|H(\mathcal{S}-\mathcal{Z})-\{1\}| \leq k/4-1$.

Proof: Consider $\beta^s \in (\mathcal{S}-\mathcal{Z})$. Since $(\mathcal{S}-\mathcal{Z}) \subset (\mathcal{B}-\mathcal{T})$, $H(\beta^s)$ is of the form $\alpha^{i_s}\omega^{j_s}$. Since H is an isomorphism, $(H(\beta^s))^2 = H(\beta^{2s})$. That is, $\alpha^{2i_s \bmod (\mathcal{O}(P))}\omega^{2j_s \bmod (\mathcal{O}(Q))} = \alpha^{i_{2s}}\omega^{j_{2s}}$ for some i_{2s} and j_{2s}.

Note that $(2i_s) \leq 2(m-1)$, which is less than $\mathcal{O}(P)$ for all $m > 1$. Thus, $2i_s \bmod (\mathcal{O}(P)) = 2i_s$, and similarly $2j_s \bmod (\mathcal{O}(Q)) = 2j_s$.

Next, we argue that $2i_s < m$ and $2j_s < n$. Assume that such is not the case, and that $2i_s \geq m$. Then $\alpha^{2i_s} = \Sigma_{r=0}^{m-1} v_r\alpha^r$ where $v_r \in GF(2^n)$, and there are at least two values of r for which $v_r \neq 0$. Thus, $\alpha^{2i_s}\omega^{2j_s} = \Sigma_{r=0}^{m-1}\alpha^r(v_r\omega^{2j_s})$, where at least two terms in the summation have non-zero coefficients. But that is not possible since $\beta^s \in (\mathcal{S}-\mathcal{Z})$ implies that $\beta^{2s} \in (\mathcal{B}-\mathcal{T})$, which implies that $H(\beta^{2s})$ must be of the form $\alpha^i\omega^j$ for some $i < m,\ j < n$. It follows that $2i_s < m$. A similar argument shows that $2j_s < n$.

Thus, $i_s \in [0..(m/2-1)]$ and $j_s \in [0..(n/2-1)]$, which implies that the number of unique (i_s, j_s) tuples is $n/2 \times m/2 = k/4$. Since that is an upper bound on the total number of elements in $H(\mathcal{S}-\mathcal{Z}))$, the lemma follows. ■

H is a one-to-one mapping, so $|\mathcal{S}-\mathcal{Z}| = |H(\mathcal{S}-\mathcal{Z})|$. Since, as noted above, $|\mathcal{Z}| \leq 2t$, Lemma 8 implies that $t \geq k/8$. In other words, for case 1, the following holds –

Corollary 2 *For any $t < k/8$ there cannot exist a (k,t)-column iso-transform that performs an isomorphic mapping from $GF(2^k)$ to a composite field $GF((2^n)^m)$, provided none of the irreducible polynomials is a binomial.* ■

Case 2: Exactly one of $P(x)$ and $Q(y)$ is a *good* polynomial .

Without loss of generality let us assume that $Q(y)$ is not a *good* polynomial.

Suppose $H(\beta) = \alpha^u\omega^v$. Now consider the set $H(\mathcal{B})$ and the powers of α and ω. We denote by $\mathcal{U}$ and $\mathcal{V}$ the sequences $\{u, 2u \bmod (\mathcal{O}(P)), \cdots, (k-1)u \bmod (\mathcal{O}(P))\}$ and $\{v, 2v \bmod (\mathcal{O}(Q)), \cdots, (k-1)v \bmod (\mathcal{O}(Q))\}$ respectively. Let η be the minimum value such that $\eta u = 0 \bmod (\mathcal{O}(P))$ and let ρ be the minimum number such that $\rho v = 0 \bmod (\mathcal{O}(Q))$.

Also we denote a special case of $\mathcal{V}$ as $\mathcal{V}^* = \{1, 2, \cdots, \mathcal{O}(Q)-1\}$. Further let $\mathcal{A}_\mathcal{V} = \{\omega^v | v \in \mathcal{V}\}$.

Lemma 9 *If $\mathcal{V} = \mathcal{V}^*$ and for each $\omega^j \in \mathcal{A}_{\mathcal{V}^*}$ let $\mathcal{X}_j = \{\omega^j\alpha^{u_0}, \alpha^{u_1}\omega^j, \cdots, \alpha^{u_{x-1}}\omega^j\}$ such that each power of α is different. Then $\bigcup_{\omega^j \in \mathcal{A}_{\mathcal{V}^*}} \mathcal{X}_j$ requires $\Omega(xn)$ gates to be implemented.*

Proof: By Lemma 1 each element of $\{\omega^n, \omega^{n+1}, \cdots, \omega^{\mathcal{O}(Q)-1}\}$ has $\frac{n}{\mathcal{O}(Q)-n}$ entries and each is independent of the other, that is $\forall i, j < (\mathcal{O}(Q)-n); \omega^{n+i} + \omega^{n+j}$ has $\frac{2n}{\mathcal{O}(Q)-n}$ entries. As each power of α is different in $\mathcal{X}_j$, the above observations implies that $\mathcal{X}_j$ requires at least $(\mathcal{O}(Q)-n)\frac{n}{\mathcal{O}(Q)-n} - \mathcal{O}(Q) + n = \Omega(n)$ gates[1]. Also note any $\mathcal{X}_j$ will not be able to reuse the gates of another as ω^js are independent. Hence, the lemma. ∎

Lemma 10 *If the condition of Claim 1 does not hold and $gcd(v, \mathcal{O}(Q)) = 1$ then $s(T) = \Omega(k)$.*

Proof: As $gcd(v, \mathcal{O}(Q)) = 1$, $\mathcal{V} = \mathcal{V}^*$. The proof follows from Lemma 9 and noting that $x = \Omega(\frac{k}{\mathcal{O}(Q)}) = \Omega(m)$. ∎

Lemma 11 *In Case 2, $s(T) = \Omega(k)$.*

Proof: If the condition of Claim 1 holds, then we are done. Thus, $H(\beta) = \alpha^u\omega^v$. There are $\min(k-1, \eta)$ distinct values in $\mathcal{U}$. If $\eta \geq 3m/2$, then we are done (as there are at most m distinct is such that α^i is a singleton and hence, T is a $(k, k/3)$-column iso-transform).

Assume $\gcd(v, \mathcal{O}(Q)) > 1$. $\mathcal{V}$ has at most ρ distinct values.By Observation 1, $\rho \leq \mathcal{O}(Q)/3$. Thus, $|H(\beta)| < \rho\eta \leq (3m/2) \times (\mathcal{O}(Q)/3) \leq k$ which is a contradiction. Lemma 10 completes the proof. ∎

Case 3: Both $P(x)$ and $Q(y)$ are not *good* polynomials .

Here also we have the following lemma –

Lemma 12 *In Case 3, $s(T) = \Omega(k)$.*

Proof: As in the proof of Lemma 11 assume that the condition of Claim 1 does not hold. Also let $\gcd(u, \mathcal{O}(P)) > 1$ and $\gcd(v, \mathcal{O}(Q)) > 1$. Here $\eta \leq \mathcal{O}(P)/3$ and $\rho \leq \mathcal{O}(Q)/3$ and thus $H(\beta) \leq 4k/9$ which is a contradiction. Without loss of generality, $\gcd(u, \mathcal{O}(P)) = 1$. Lemma 10 completes the proof. ∎

5 Binomials

The proof in Section 4 does not work if any of the irreducible polynomials is a binomial. These classes of transformation matrices are also interesting as they have an infinite family of permutations (Section 5.2.1).

[1] Consider any two elements of $\mathcal{X}_j$, say $\omega^j\alpha^{u_{i_1}}$ and $\omega^j\alpha^{u_{i_2}}$. $\alpha^{u_{i_1}}$ differs from $\alpha^{u_{i_2}}$ by at least one α^l, where $l < m$. $\alpha^l\omega^j$ will require $\frac{n}{\mathcal{O}(Q)-n} - 1$ gates.

5.1 Preliminaries

Here we present some lemmas and observations about some of the irreducible polynomials being a binomial. First we give a characterization of irreducible binomials due to Serret.

Lemma 13 [13, 16] *Let $a \in GF^*(2^n)$[2] with order e. The binomial $x^t + a$ is irreducible over $GF(2^n)$ if and only if the integer $t \geq 2$ satisfies the following conditions–*

1. *$gcd(t, (2^n - 1)/e) = 1$.*
2. *each prime factor of t divides e.*
3. *if $4|t$, then $4|(2^n - 1)$.*

Note that there cannot be an irreducible binomial over $GF(2)$ (as 1 would be a root of such a binomial), that is only $P(x)$ can be a binomial. Also the order of an irreducible binomial $P(x) = x^m + a$, where $a \in GF(2^n)$ is greater than $2m$. To see this note that the $\mathcal{O}(P) = m.order(a)$ and for $\forall n > 2, order(a) \geq 3$, that is $P(x)$ is a *good* polynomial. This implies that while extending the proof of Section 4 for binomials we have to consider only Case1 and Case 2 of the proof.

5.2 Family of Transformation Matrices

Here we describe three infinite families of transformation matrices. Matrices in Section 5.2.1 are permutations (that is 0-gate circuits) and those in Section 5.2.2 will prove our linear lower bounds to be a tight one.

Let p be an odd prime such that 2 is primitive modulo p and p^2 does not divide $2^{p-1} - 1$.[3] Consider the following polynomials for $l \geq 1$:

- $R(z) = z^{(p-1)p^l} + z^{(p-2)p^l} + \cdots + z^{p^l} + 1$ – which is irreducible by Lemma 3.
- $Q(y) = y^{p-1} + y^{p-2} + \cdots + y + 1$ – which is irreducible by Lemma 4.
- $P(x) = x^{p^l} + \omega^r$, where $Q(\omega) = 0$ and r will be fixed later. Note that if $r = 1$ or $r = p - 1$, then $P(x)$ is irreducible by Lemma 13.

Note that $k = (p - 1)p^l$, $m = p^l$ and $n = (p - 1)$.

5.2.1 Permutations

When $r = 1$ we get a permutation by letting $H(\beta) = \alpha$. Two points to note here are –

- $H(\beta) = \alpha$ is a valid transform by Lemma 7.
- $s(T) = 0$.

[2] $GF^*(2^n)$ denotes the multiplicative group of $GF(2^n)$.

[3] It is an open question – do infinitely many such primes p exist. A prime r is called a Wieferich prime if $2^{r-1} = 1 \bmod (r^2)$. The *Generalized Riemann Hypothesis* implies that there are infinitely many primes q, such that 2 is primitive modulo q. [24] shows that *abc-conjecture* implies that there are infinitely many primes s, such that s is not a Wieferich prime. Also the only two known Wieferich primes till $< 4.10^{12}$ are 1093 and 3511 [6]. Interestingly 2 is not primitive modulo these primes.

5.2.2 Linear number of gates family

When $r = p - 1$, we again let $H(\beta) = \alpha$. Two points to note here are –

- $H(\beta) = \alpha$ is a valid transform by Lemma 7.
- $s(T) = k - m$.

5.2.3 Other cases

When r is neither 1 nor $p - 1$, and $P(x)$ is still irreducible (by satisfying the condition in lemma 13).

Note that since $Q(\omega) = 0$, ω has order p. Thus the order of ω^r is $p/\gcd(r, p)$. Since $\omega^r \neq 1$, order of ω^r is p. Hence, $\gcd(r, p) = 1$.

Let $u = r^{-1} \bmod (p)$. Then $H(\beta) = \alpha^u$ is an isomorphism by lemma 7. To see this note that $R(\beta) = 0$. Hence the condition in lemma 7 that needs to be checked is that $R(\alpha^u) = 0$. But $R(\alpha^u) = Q(\alpha^{up^l}) = Q(\omega^{ru}) = Q(\omega) = 0$. Also, that the powers of α^u generate a basis of the composite field is easy to see.

A similar isomorphism can be obtained if $(mv + ru) = 1 mod p$, where $m = p^l$, and $H(\beta) = \alpha^u \omega^v$.

In both these cases it is difficult to give a lower bound, as the transformation matrix obtained can indeed be anything from almost a permutation to one requiring more than linear number of gates (see case 2 of next section).

5.3 Lower bound proof

We first prove Lemma 14 and then extend the proof of Section 4.

Lemma 14 *If $P(x) = x^m + z$, where $\forall i, z \neq \omega^i$, then $s(T) = \Omega(k)$.*

Proof: Note that if $z^j = \omega^l$, for some $l < \mathcal{O}(Q)$, then $\forall s, z^{j+1} \neq \omega^s$ (by definition of z), that is, in the sequence $\{z^i\}$, every alternate element is a non-singleton (we will refer to such elements as *NSZ*) – also for any such element z^j, $\forall r \forall s, z^j \omega^r \neq \omega^s$ [by definition of NSZ] . By Claim 1, we have $H(\beta) = \alpha^u \omega^v \Rightarrow H(\beta^t) = \alpha^{ut \bmod (m)} z^{\lfloor \frac{ut}{m} \rfloor} \omega^{vt}$. By our observation that every alternate element of $\{z^i\}$ is NSZ , for any $(2m/u)$ continuous values of t, for at least (m/u) values of t, $z^{\lfloor \frac{ut}{m} \rfloor} \omega^{vt}$ is non-singleton . Hence, $s(T) = \Omega(k)$. ∎

Lemma 14 imples that we need to consider binomials only of the form $P(x) = x^m + \omega^r$.As noted in Section 5.1, we need to extend the proof of Section 4 for the following cases (and $P(x)$ is a *good* polynomial) –

- Case 1 : $Q(y)$ is *good.* We do a case analysis on the value of r.
  - Case A: $n < r < \mathcal{O}(Q) - n(1 + \frac{1}{d})$, where d is a constant .
    We proceed along the lines of Lemma 8. Here we have to find the number of unique (i_s, j_s) tuples such that $\alpha^{2i_s} \omega^{2j_s}$ is a singleton. Note that $i_s \in \{0, \cdots, m-1\}$ and $j_s \in \{0, \cdots, n-1\}$.
    - If $2i_s < m$, then only for $2j_s < n$, $\alpha^{2i_s} \omega^{2j_s}$ is a singleton; else
    - $m \leq 2i_s < 2m - 1$. Here $\alpha^{2i_s} \omega^{2j_s} = \alpha \omega^{r+2j_s}$. Now we have to ensure that ω^{r+2j_s} is a singleton i.e. $i + 2j_s > O(Q)$ i.e. the number of possible values of $2j_s$ here is at most $n(1 - \frac{1}{d}) - 1$.

Thus, the total number of unique (i_s, j_s) tuples such that $\alpha^{2i_s}\omega^{2j_s}$ is a singleton (which is an upper bound on $|H(\mathcal{S}-\mathcal{Z})|$) is $(m/2)(n/2)+(m/4)(n(1-\frac{1}{d})-1) = (k/4)(2-\frac{1}{d})-m/4$. Now $|\mathcal{S}-\mathcal{Z}| = |H(\mathcal{S}-\mathcal{Z})| \Rightarrow k/2-2t \leq (k/4)(2-\frac{1}{d})-m/4 \Rightarrow t \geq (k/(8d))+(m/8) = (k/8)(\frac{1}{d}+\frac{1}{n})$.

  - Case B: $1 < r < n(1-\frac{1}{d})$, where d is a constant and $d > 2$. An analysis similar to Case A, gives a $t \geq (k/8)(1-\frac{2}{d})$.
  - Case C : otherwise This case falls under the analysis done in section 5.2.3.

- Case 2 : $Q(y)$ is a *bad* polynomial.

  Let $q = \mathcal{O}(Q)$. Note that $H(\beta^t) = \alpha^{ut \bmod (m)}\omega^{\lfloor \frac{ut}{m} \rfloor r + vt mod q}$, for $t < k$. Since H is an isomorphism, we can not have two values $t_1, t_2 < k$ such that $H(\beta^{t_1}) = H(\beta^{t_2})$. Note that this is only possible if (1) $ut_1 = ut_2 \bmod (m)$, and (2) $\lfloor \frac{ut_1}{m} \rfloor r + vt_1 = (\lfloor \frac{ut_2}{m} \rfloor r + vt_2) \bmod (q)$. (1) can be satisfied iff $t_2 = t_1 + im/\gcd(m,u)$, for some $i < n\gcd(m,u)$, with $t_1, t_2 < k$. Thus (1) and (2) can be satisfied iff $i(ur+vm) = 0 \bmod (q)$, and $t_2 = t_1 + im/\gcd(m,u)$, for some $i < n\gcd(m,u)$, with $t_1, t_2 < k$. If $\gcd(m,u) > 1$, then since $q < 2n$, $i = q$, $t_1 = 1$ is a solution, contradicting that H is an isomorphism. Thus, $\gcd(m,u) = 1$. Similarly, $(ur+vm)$ and q are relatively prime.

  Now, let t_1 and t_2 be such that $ut_1 = ut_2 \bmod (m)$. Also, let $t_2 = t_1 + im$, $i < n$. For these values of t (i.e. t_1, t_2), the powers of α are the same. The difference in the powers of ω is $i(ur+vm) \bmod (q)$. Thus, for values of t, such that $H(\beta^t)$ has the same α power, the powers of ω are multiples of $(ur+vm) \bmod (q)$ apart.

  For each $a < m$, denote by S^a the sequence of powers of ω, corresponding to the ath power of α. More precisely, for any $a < m$, let $t = au^{-1} \bmod (m)$, and $t < m$ (since $\gcd(u,m) = 1$). Then, S^a_i, the ith element in the sequence S^a, for $i < n$ is defined as $S^a_i = (\lfloor \frac{u(t+im)}{m} \rfloor r + v(t+im)) \bmod (q) = (\lfloor \frac{ut}{m} \rfloor r + vt + (ur+vm)i) \bmod (q)$.

  Thus, by shifting lemma (Lemma 2) and regularity lemma (Lemma 1), if $(ur+vm) \neq 1 \bmod (q)$, then we have a lower bound of $\Omega(k)$.

  If $(ur+vm) = 1 \bmod (q)$, and $v = 0$, we have two cases. If $r = 1$, then $u = 1$, and in this case we indeed have permutations (i.e. zero gate circuits), for instance see the class described in Section 5.2.1. If $r > 1$, we have $u = r^{-1} \bmod (q)$, as $gcd(ur, q) = 1$. If we could show that S^a_0 is nicely distributed among integers mod q, the proof would follow by $ur = 1 \bmod (q)$. But, this seems difficult to prove. Instead we show that for every $j < q$, there are $m/2$ different a such that for each such a, there is an $i < n$ with $j = S^a_i$. In other words, each ω power appears in at least $m/2$ sequences.

  Let $j' = jr^{-1} \bmod (q)$. Let $t = \lfloor \frac{j'm}{u} \rfloor$. Note that $t < k$, as $u > 1$. Now, $\lfloor \frac{ut}{m} \rfloor = \lfloor \frac{j'm - (j'm \bmod (u))}{m} \rfloor = j'$, as $u < m$. Thus, $j = \lfloor \frac{ut}{m} \rfloor r \bmod (q)$. Also, note that if t is a solution of $j = \lfloor \frac{ut}{m} \rfloor r \bmod (q)$, then so are $t+s$, where s takes m/u contiguous integer values, such that $-m/u < s < m/u$. Moreover, if t is a solution, then so is $t_y = \lfloor \frac{j'm+yqm}{u} \rfloor$. The number of values y can take is $u/2-1$, as we need $t_y < k$. Thus, for each $j < q$, there are $(u/2)(m/u) = m/2$ lists in which j appears. By lemma 9, we have an $\Omega(k)$ lower bound.

  If $v \neq 0$, and $(ur+vm) = 1 \bmod (q)$ then as mentioned in section 5.2.3 the lower bound is untenable.

6 Acknowledgements and Future Work

The bounds in this paper are in terms of 2-input XOR gates. An interesting question to ask is whether using arbitrary 2-input logic gates help in general matrix-vector multiplication over $GF(2)$. This question in turn is equivalent to asking if using AND gates help [9]. The latter is an open question [20].

The authors would like to thank Don Coppersmith for the proof of the Regularity Lemma. We would also like to thank Anna Gal for pointing out [1] and [20], and for helpful discussion on the complexity of matrix-vector multiplication; and Shuhong Gao for very helpful information and comments about irreducible binomials.

References

[1] N. Alon, M. Karchmer and A. Wigderson "Linear Circuits over GF(2)". In *SIAM J. of Comput.* Vol. 19, No. 6, pp. 1064-1067, December 1990

[2] B. Benjauthrit, I.S. Reed, "Galois Switching functions and their Applications". In *IEEE Trans. Comput.*, Vol. C-25, pp.78-86, January 1976.

[3] I.S. Reed and T.K. Truong ,"The Use of Finite Fields to Compute Convolutions, "In *IEEE Trans. Infrom. Theory*, vol. IT-21, No.2, pp.208-213, March 1975.

[4] R.E. Blahut, *Theory and Practice of Error Control Codes*, Reading, MA: Addison-Wesley, 1984.

[5] D. Coppersmith, *Personal Communication.*

[6] R. Crandall, K. Dilcher and C. Pomerance, " A search for Wieferuch and Wilson primes," *Math. Comp.*, **66**:217 (1997), Pages 433-449.

[7] W. Diffie and M. Hellman, "New Directions in Cryptography", *IEEE Trans. Info. Th.*, 22 (1976).

[8] T. ElGamal, " A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Trans. Info. Th.*, 31, (1985)

[9] A. Gal, *Personal Communication.*

[10] B. S. Kaliski Jr. and M. Liskov, "Efficient finite field basis conversion using dual bases," In *CHES*, 1999.

[11] B. S. Kaliski Jr. and Y. L. Yin, "Storage-efficient finite field basis conversion", In *Selected Areas of Cryptography*, LNCS 1556, Pages 81-93, 1998.

[12] N. Koblitz "Elliptic Curve Cryptosystems", *Math. Comp.*, 48, (1987)

[13] R. Lidl and H. Niederrieter, *Introduction to finite fields and their applications.* Cambridge University Press, Ma., 1986.

[14] F.J. MacWilliams and N.J. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam:North-Holland 1986.

[15] J.H. McClellan, C.M. Rader, *Number Theory in Digital Signal Processing*, Englewood Cliffs: Prentice Hall, 1979.

[16] A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone and T. Yaghoobian, *Applications of Finite Fields*. Kluwer Academic Publishers, Boston, 1992.

[17] V. Miller, "Uses of Elliptic curves in cryptography", Crypto 85, LNCS 218

[18] C. Paar, "Efficient VLSI Architectures for bit-parallel computations in Galois Fields", *PhD Thesis*, Inst. Experimental Mathematics, Univ. of Essen, Germany, 1994

[19] C. Paar and P. Soria-Rodriguez, "Fast Arithmetic architectures for public-key algorithms over Galois fields $GF((2^n)^m)$," In *EUROCRYPT 97*, 1997.

[20] P. Pudlak, "Communication in bounded depth circuits," *Combinatorica*, 14(2) 1994 203-216.

[21] A. Rudra, P. Dubey, C. Jutla, V. Kumar, J. Rao, P. Rohatgi, "Efficient Rijndael Encryption IMplementation with Compsite Field Arithmetic", CHES 2001, LNCS 2162

[22] R. Schroeppel, H. Orman, S. O'Malley and O. Spatscheck, "Fast Key Exchange with elliptic curve systems," In *CRYPTO 95*, 1995.

[23] A. Satoh, S. Morioka, K. Takano and S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization," in *ASIACRYPT01*, 2001.

[24] J.H. Silverman, "Wieferich's criterion and the abc-conjecture," *J. Number Theory*, **30**:30 (1988), Pages 226–237.

[25] J.H. Silverman, "Fast multiplication in finite field $GF(2^N)$," In *CHES*, 1999.

[26] H.C.A. van Tilborg, *An Introduction to Cryptology*, Boston:Kluwer Academic Publ., 1988.

[27] E. De Win, A. Bosselaers, S. Vandenberghe, P. De Gersem and J. Vandewalle, "A fast software implmentation for arithmetic operations in $GF(2^n)$," In *ASIACRYPT 96*, 1996.

[28] Advanced Encryption Standard, AES, http://www.nist.gov/aes

A General lower bound proof

For the general version of Corollary 2 we use the following notation — let $P_j(x)$ denote the field polynomial corresponding to d_j where $k = \prod_{j=1}^{v} d_j$. Also let $P_j(\alpha_j) = 0$.

Consider a (k,t)-column transformation matrix T' that maps elements of $GF(2^k)$ to the isomorphic composite $GF((...((2^{d_1})^{d_2})...)^{d_v})$. Let H' denote the isomorphism, and $\mathcal{T}'$ the set $\{\beta^{r'_1}, \beta^{r'_2}, \cdots, \beta^{r'_t}\}$. Then, $\exists r'_1, r'_2, ..., r'_t \in \{1,..,k\}$ such that

$$H(\beta^l) \begin{cases} \Sigma_{i_1=0}^{d_1-1}\Sigma_{i_2=0}^{d_2-1}\cdots\Sigma_{i_v=0}^{d_v-1} c^l_{i_1 i_2 \cdots i_v} \Pi_{p=0}^{v-1}(\alpha_p)^{i_p}, & \text{where alteast two } c^l_{i_1 i_2 \cdots i_v} = 1, \\ & \text{if } \beta^l \in \mathcal{T}' \\ \Pi_{p=0}^{v-1}(\alpha_p)^{i_{p,l}}, & \text{for some unique v-tuple } (i_{1,l}, i_{2,l}, \cdots, i_{v,l}) \\ & \text{where } \forall p \in [1..v]\ i_p < d_p, \\ & \text{if } \beta^l \in \mathcal{B} - \mathcal{T}'. \end{cases}$$

Let $\sqrt{\mathcal{T}'} \subseteq \mathcal{B}$ denote the set $\{\beta^j \mid \beta^{2j} \in \mathcal{T}'\}$. Let $\mathcal{Z}' = (\sqrt{\mathcal{T}'} \cup \mathcal{T}') \cap \mathcal{S}$. Note that $|\mathcal{Z}'| \leq 2|\mathcal{T}'| = 2t$. Further, for any set A, let $H'(A) = \{H'(x) | \ x \in A\}$.

It can be seen that Claim 1 can be generalised to the following claim –

Claim 2 *If $H(\beta) \neq \Pi_{j=0}^{v}\alpha_j^{u_j}$ for any $u_j \in [0 \cdots (\mathcal{O}(P_j)-1)]$ and $\Sigma_{j=0}^{v} u_j \neq 0$, then $s(T) = \Omega(k)$.*

If $H(\beta) = \Pi_{j=0}^{v}\alpha_j^{u_j}$, then $\mathcal{U}_j = \{u_j, 2u_j \bmod (\mathcal{O}(P_j)), \cdots, (k-1) \bmod (\mathcal{O}(P_j))\}$ and ρ_j is the minimum value such that $\rho_j u_j = 0 \bmod (\mathcal{O}(P_j))$.

Again we consider three cases.

Case G.1 : All the $P_j(x)$ are *good* polynomials .

Lemma 15 *For any $t < (2^{v-1}-1)k/2^{v+1}$ there cannot exist a (k,t)-column transform that performs an isomorphic mapping from $GF(2^k)$ to a composite field $GF((...((2^{d_1})^{d_2})...)^{d_v})$, where $k = \prod_{j=1}^{j=v} d_j$.*

Proof: Consider $\beta^{s'} \in (\mathcal{S} - \mathcal{Z}')$, i.e. $H'(\beta^{s'})$ is of the form $\Pi_{p=0}^{v-1}(\alpha_p)^{i_{p,s'}}$. A proof along the same lines as the proof for Lemma 8 shows that $|H(\mathcal{S} - \mathcal{Z}') - \{1\}| \leq k/2^v - 1$ (as the number of unique $(i_{1,s'}, i_{2,s'}, ...i_{v,s'})$ v-tuples is $\prod_{j=1}^{j=v}(d_j/2) - 1 = k/2^v - 1$). The proof is complete by noting that H' is a one-to-one mapping and that $|\mathcal{S} - \mathcal{Z}' - \{1\}| \geq k/2 - 2t - 1$. ■

Case G.2 : Exactly d out of v $P_j(x)$ are *good* polynomials .

Without loss of generality assume $P_1(x), \cdots, P_d(x)$ are *good.*

Lemma 16 *In Case G.2, $s(T) = \Omega(k)$.*

Proof: If the condition of Claim 2 holds, then we are done. Thus, $H(\beta) = \Pi_{j=0}^{v}\alpha_j^{u_j}$. There are $\min(k-1, \rho_l)$ distinct values in $\mathcal{U}_l$ for $l \in [1 \cdots d]$. If $\rho_l \geq (3/2)^{v/d-1} d_l$, then we are done (as there are atmost d_l distinct is such that α_l^i is a singleton and hence, T is a $(k, O(k))$-column transform).

For each $e \in [d+1 \cdots v]$, assume $\gcd(u_e, \mathcal{O}(P_e)) > 1$. $\mathcal{U}_e$ has atmost ρ_e distinct values. By Observation 1, $\rho_e < \mathcal{O}(P_e)/3$. Thus, $|H(\beta)| < \Pi_{j=1}^{v}\rho_j < k$ which is a contradiction. Without loss of generality $\gcd(u_v, \mathcal{O}(P_v)) = 1$. Lemma 10 completes the proof[4]. ■

Case G.3 All the $P_j(x)$ are not *good* polynomials .

A simple generalisation of the proof of Lemma 12 gives the following lemma –

Lemma 17 *In Case G.3, $s(T) = \Omega(k)$.*

■

B Galois Field Essentials

For a detailed treatment of the material presented here see [13, 18].

A Finite field, $\mathbb{F}$ is defined by two parameters- its prime characteristic p and its dimension k over $\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the set of integer modulo the prime p. The field $\mathbb{F}$ has p^k elements and is isomorphic to any other field having p^k elements. The field $\mathbb{F}$ is often written as $GF(p^k)$, where GF stands for $GaloisField$. The additive identity of $\mathbb{F}$ is denoted by 0. The multiplicative group of $\mathbb{F}$ is denoted by $\mathbb{F}^*$ (or alternatively as $GF^*(p^k)$). A *primitive element* or *generator* of $\mathbb{F}^*$ is any element that generates the multiplicative group. Specifically, if $\gamma \in \mathbb{F}^*$ is a primitive element then $\mathbb{F}^* = \{1, \gamma, \cdots, \gamma^{p^k-2}\}$.

Let $\mathbb{Z}_p[x]$ denote the polynomial ring in one unknown. A polynomial $r \in \mathbb{Z}_p[x]$ is said to be *irreducible* if $r = gh$ implies that either g or h is a constant that is, $g(x)$ or $f(x) \in \mathbb{Z}_p$. Further an irreducible polynomial r of degree k is said to be primitive if some root (and hence each root), β

[4] In the proof of Lemma 10 substitute $P, \mathcal{U}$ and m by $P_v, \mathcal{U}_v$ and d_v respectively .

of r generates $GF^*(p^k)$. Typically $GF(p^k)$ is represented as the quotient ring $\mathbb{Z}_p[x]/(r)$, where r is an irreducible polynomial of degree k. $\{1, \beta, \cdots, \beta^{k-1}\}$ is the *standard basis* of $GF(p^k)$, that any $A \in GF(p^k)$ can be represented as $\sum_{i=0}^{k-1} a_i \beta^i$, where $a_i \in \mathbb{Z}_p$.

Let $k = nm$ and let $q \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree n. Further let $GF(p^n)$ be represented as the quotient ring $\mathbb{Z}_p[x]/(q)$. Further let $s \in GF(p^n)[x]$, where $GF(p^n)[x]$ is the ring of polynomials where the coefficient are in $GF(p^n)$, be an irreducible poynomial[5] over $GF(p^n)$ of degree m. The quotient ring $GF(p^n)[x]/(s)$ is denoted by $GF((p^n)^m)$, it is isomorphic to $GF(p^k)$ and is called a *composite field*. Let α be a root of s, then $\{1, \alpha, \cdots, \alpha^{m-1}\}$ is the standard basis of $GF((p^n)^m)$, that is, for any $B \in GF((p^n)^m)$, $B = \sum_{i=0}^{m-1} b_i \alpha^i$ where $b_i \in GF(p^n)$.

In our setting, $p = 2$. For the base field, $GF(2)$ or $\mathbb{Z}_2$(note that this field just contains 2 elements 0 and 1), "addition" is the *exclusive-or* operation while "multiplication" is the boolean *and*. Let H be the isomophism from $GF(2^k)$ to $GF((2^n)^m)$, where k=nm. By the defintion of isomorphism, H maps identity to identity.

Let $R(z)$ be the irreducible polynomial of degree k for $GF(2^k)$ and let $R(\beta) = 0$. Let $Q(y)$ be the irreducible polynomial of degree n for $GF(2^n)$ and $Q(\omega) = 0$. Finally $P(x)$ be the irreducible polynomial of degree m for $GF((2^n)^m)$ and let $P(\alpha) = 0$. Thus for any $A = \sum_{i=0}^{k-1} a_i \beta^i \in GF(2^k)$ there exists $H(A) \in GF((2^n)^m)$. Consider the $k \times k$ binary matrix, M, such that the i^{th} coloumn is the additive representation[6] of $H(\beta^i)$. It is easy to see that the following matrix-vector multiplication represents $H(A)$: $M \begin{bmatrix} b_{k-1} \\ b_{k-2} \\ \vdots \\ b_1 \\ b_0 \end{bmatrix}$

In this paper we give a lower bound on the number of 2-input *exclusive-or* gates required to implement the above matrix-vector.

[5]A polynomial $f \in GF(p^n)[x]$ is irreducible if $f = gh$ implies $g(x)$ or $f(x) \in GF(p^n)$.

[6]Additive representation of of any $B \in GF((2^n)^m)$ is of the form $B = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} c_{i,j} \alpha^j \omega^i$.