International Symposium on Information Theory and its Applications, ISITA2008
Auckland, New Zealand, 7-10, December, 2008

An Information-Theoretic Cryptanalysis of Network Coding – is Protecting the Code Enough?

Luísa Lima[†], João P. Vilela[†], João Barros[†] and Muriel Médard[‡]

[†] Instituto de Telecomunicações
Departamento de Ciência de Computadores
Universidade do Porto
Rua Campo Alegre, 1021/1055, 4169-007 Porto, Portugal
E-mail: {luisalima, joaovilela, barros}@dcc.fc.up.pt

[‡] Massachusetts Institute of Technology
77 Massachusetts Ave Bldg 32-D626
Cambridge, MA 02139-4301, USA
E-mail: medard@mit.edu

Abstract

We consider the issue of confidentiality in multicast network coding, by assuming that the encoding matrices, based upon variants of random linear network coding, are given only to the source and sinks. Based on this assumption, we provide a characterization of the mutual information between the encoded data and the two elements that can lead to information disclosure: the matrices of random coefficients and, naturally, the original data itself. Our results, some of which hold even with finite block lengths, show that, predicated on optimal source-coding, information-theoretic security is achievable for any field size without loss in terms of decoding probability. It follows that protecting the encoding matrix is generally sufficient to ensure confidentiality of network coded data.

1. INTRODUCTION

We are intrigued by the inherent security properties of Random Linear Network Coding (RLNC) [1], a fully distributed method for performing network coding, in which each node in the network independently and randomly selects a set of coefficients and uses them to form linear combinations of the data symbols it receives. If the coefficients are chosen at random from a large enough field, it is very likely that this matrix will be invertible, which explains why this approach is capable of achieving the multicast capacity of a network. Each symbol or packet is sent along with the global encoding vector [2], which, provided that the received matrix has full rank, enables the receivers to decode the original data using Gaussian elimination.

If one assumes that the global encoding vector is hidden from any node in the network other than the sinks and the source nodes, then all that intermediate nodes have access to is the encoded data in the payload of packets, to which the fact that the encoding is performed uniformly at random adds a natural degree of secrecy. One scheme that relies in this concept is SPOC [3] (Secure Practical Network Coding). SPOC is a lighweight security scheme to ensure confidentiality in network coding, which leverages the inherent security provided by RLNC to reduce the overhead in comparison to end-to-end encryption of the entire data flow, as explained in detail in the next section.

Assuming that the full payload of all encoded packets in the network is available to an eavesdropper, there are two natural ways of attack: (1) deduce the source coefficients from the payload and decode the data regularly, and (2) deduce the original data directly from the payload. We thus analyze the mutual information between the payload and the two elements that we aim to protect: the encoding matrix (because it leads to the recovery of the original data), and the original data itself. We consider a generic setting with optimal source encoding and devise several coding strategies that provide RLNC with information-theoretic security. Our main contributions are as follows:

- We show a general result for the mutual information between the payload and the encoding matrix, which goes to zero with the size of the field;
- We show that, according to the coding scheme used at the source, it is possible to achieve zero mutual information, either between the payload and the encoding matrix or between the payload

Part of this work was done while the first two authors were visiting students and the third author a visiting scholar at the Laboratory for Information and Decision Systems at the Massachusetts Institute of Technology. This work was partly supported by the Fundação para a Ciência e Tecnologia (Portuguese Foundation for Science and Technology) under grants SFRH/BD/24718/2005 and SFRH/BD/28056/2006, by the USA Air Force Office of Scientific Research Grant No. FA9550-06-1-0155, by DARPA under grant 6916804, and by the European Community under grant FP7-INFSO-ICT-215252 (N-Crave Project).

and the original information. Furthermore, the mutual information between the payload and, respectively, the original information or the encoding matrix tends to zero with the size of the field;

- We evaluate the impact of the reuse of the same set of source coefficients in the security of RLNC based protocols;
- We illustrate our analytical results through the use of numerical simulation for finite block length and small field sizes.

We believe that these contributions can help pave the way for highly efficient cryptographic schemes for network coding.

2. SECURITY ISSUES IN PRACTICAL NETWORK CODING

A framework for packetized network coding (*Practical Network Coding*, PNC) is presented in [4]. The packet format consists of the *global encoding vector* (kept in the header) and the payload, which is divided into vectors according to the field size (2^8 or 2^{16}, i.e. each symbol has 8 or 16 bits, respectively). Each of these symbols is then used as a building block for the linear operations performed by the nodes. PNC also includes a buffering model which divides the stream of packets into *generations* of size h, such that packets in the same generation are tagged with a common generation number. When there is a transmission opportunity at an outgoing edge, the sending node generates a new packet, which contains a random linear combination of all packets in the buffer that belong to the *current* generation.

SPOC (Secure Practical Network Coding) [3] is a lightweight security scheme for confidentiality in RLNC, which provides a simple yet powerful way to exploit the inherent security of RLNC in order to reduce the number of cryptographic operations required for confidential communication. This is achieved by protecting (or "locking") only the source coefficients required to decode the linearly encoded data, while allowing intermediate nodes to run their network coding operations by way of "unlocked" coefficients which provably do not compromise the hidden data. In this case, the threat model is one in which the attacker has access to all the information being transmitted in the network, with the exception of the secret keys shared among the legitimate parties in the network. A summary of the protocol operation is presented in *Table 1.*

3. MODEL AND ABSTRACTIONS

Let $\mathbf{A} = (a_{ij})$ be the $n \times n$ encoding matrix used for performing coding at the source. Each of the coefficients a_{ij} is uniformly distributed over all elements of a finite field $\mathbb{F}_q$, $q = 2^m$, and mutually independent. Let the original data, or plaintext, be $\underline{b} = (b_1, b_2, \ldots, b_n)^T$, uniformly distributed over all elements of $\mathbb{F}_q$, mutually independent, and independent of $\mathbf{A}$. The case in which the data, that is, $\underline{b}$, is not perfectly uniformly distributed is beyond the scope of this paper. The payload of the packets is represented by $\underline{\gamma} = (\gamma_1, \ldots, \gamma_n)^T$, where $\gamma_i = \sum_{j=1}^{n} a_{ij} b_j$. Without loss of generality, we abstract the network structure and consider the payload of all packets together. An algorithm for the considered setting is presented in *Algorithm 1.*

Table 1: Summary of SPOC Protocol

Initialization (source nodes):

- A key management mechanism is used to exchange shared keys with the sink nodes, which are used for the encryption of the locked coefficients.
- The source node stores the message packets $w_1, w_2, ..., w_h$ in its memory;
- The source node forms a random linear combination of the h packets in its memory (the current generation) and puts it in a packet to be sent;
- The coefficients corresponding to a distinct line of the $h \times h$ identity matrix are added to the header of each coded packet. These correspond to the *unlocked* coefficients;
- The packet's global encoding vector is encrypted with the shared keys and also placed in the header of each packet. These correspond to the *locked* coefficients.

Operation at intermediate nodes:

- When a packet is received by a node, the node stores the packet in its memory;
- To transmit on an outgoing link, the node produces a packet by forming a random linear combination of the packets in its buffer, modifying both the unlocked and locked coefficients without distinction, according to the rules of standard RLNC based protocols.

Decoding (sink nodes):

- When *sufficient packets are received*:
  - Using the unlocked coefficients, which store the operations performed upon the locked coefficients throughout the network (see also [3]), the receiver reverts those operations thus obtaining the original locked coefficients;
  - The receiver then decrypts the locked coefficients using the shared keys;
  - The receiver determines the decoding matrix by computing the product of the unlocked coefficients and the corresponding locked coefficients;
  - Gaussian elimination is then performed to recover the original packets.

We denote the fact that a vector $\underline{v}$ has x zeros by $Z(\underline{v}) = x$. The following lemma follows from the results in [1] and shall be useful in the proofs for our results.

Lemma 1 (From [1]): In Random Linear Network Coding, the conditional entropy of the payload $\underline{\gamma}$ given the encoding matrix $\mathbf{A}$ is lower bounded by:

Algorithm 1 Abstraction of the SPOC Protocol

```
**Alice:** Through the use of a source coding algorithm, transform sequence $x^k$ into a uniform random sequence $b_1, \ldots, b_l$ according to the specifications in the following sections;
**Alice:** Divide $b_1, \ldots, b_l$ into $1 \times n$ vectors $\underline{b}_K = (b_1, \ldots, b_n)$;
**Alice:** Generate a $n \times n$ encoding matrix $\mathbf{A} = (a_{ij})$ in which $P(a_{ij}) = q^{-1}, \forall i, j$;
**Alice:** Compute $\underline{\gamma} = \mathbf{A}\underline{b}_K$, where $\underline{b}_K = (b_1, \ldots, b_n)^T$;
**Alice:** Send the encoding matrix $\mathbf{A}$ through the secret channel and $\underline{\gamma}$ through the public channel;
**Bob:** Compute $\mathbf{A^{-1}}\underline{b}_K$ to obtain $\underline{b}_K$; repeat for each $\mathbf{A}\underline{b}_K$ received.
**Bob:** Concatenate $b_1 \ldots b_l$ and reverse the source coding algorithm to obtain $x^k$.
```

$$H(\underline{\gamma}|\mathbf{A}) \geq n \log(q)\left(1 - f(q))\right), \text{where } O(f(q)) = O\left(\frac{1}{q}\right).$$

4. SECURITY ANALYSIS

The following theorem provides a general bound for the mutual information between the encoding matrix and the payload.

Theorem 1: The mutual information between the payload $\underline{\gamma}$ and the encoding matrix $\mathbf{A}$ is upper bounded by:

$$I(\underline{\gamma}; \mathbf{A}) \leq f(n, q)$$

where $f(n, q)$ is a function such that $O(f(n, q)) = O\left(\frac{n \log(q)}{q}\right)$.

Proof: The result follows from considering that $I(\mathbf{A}; \underline{\gamma}) = H(\underline{\gamma}) - H(\underline{\gamma}|\mathbf{A})$, where $H(\underline{\gamma})$ is upper bounded by $n \log(q)$ and $H(\underline{\gamma}|\mathbf{A})$ is lower bounded by the expression given by *Lemma 1.* ■

The following corollaries provide tighter bounds for the case in which only invertible matrices $\mathbf{A}$ are considered.

Corollary 1: The mutual information between the payload $\underline{\gamma}$ and the encoding matrix $\mathbf{A}$, given that $\mathbf{A}$ is invertible and that $b_i \in \mathbb{F}_q \backslash \{0\}, 0 \leq i \leq n$, is upper bounded by:

$$\begin{aligned} I(\underline{\gamma}; \mathbf{A} | \{\det(\mathbf{A}) \neq 0\}, \{b_i \in \mathbb{F}_q \backslash \{0\}\}) \\ \leq n(\log(q) - \log(q-1)) \end{aligned}$$

Corollary 2: The mutual information between the payload $\underline{\gamma}$ and the encoding matrix $\mathbf{A}$, given that $\mathbf{A}$ is invertible and that $b_i \in \mathbb{F}_q, 0 \leq i \leq n$, is equal to 0:

$$I(\underline{\gamma}; \mathbf{A} | \{\det(\mathbf{A}) \neq 0\}, \{b_i \in \mathbb{F}_q\}) = 0$$

4.1. Case-by-case bounds for $I(\mathbf{A}; \underline{\gamma})$ and $I(\underline{b}; \underline{\gamma})$

Since the derivation of a general bound for the mutual information between the payload and $\underline{b}$ is infeasible without further assumptions, we consider the following restrictions on coding: (1) source encoding of the plaintext where the source symbols exclude the codeword zero and (2) traditional source encoding, with random matrices that do not include the coefficient 0. Reference [5] contains an analysis on the impact of 0's in diagonalization properties of partial matrices in RLNC: in fact, the distribution of 0's in the payload of RLNC is not uniform, since 0 is the absorbent element for the multiplication. This introduces some dependencies on the result, which we evaluate next. The following lemma will be useful.

Lemma 2: The probability of the sum $S_k = \sum_{i=0}^{k} \sigma_i$, where $\sigma_i \in \mathbb{F}_q \backslash \{0\}$ and $P(\sigma_i) = (q-1)^{-1} \forall i$ yielding the result $\phi \in F_q$, can be recursively characterized by:

$$\begin{cases} z_0 = 0, z_1 = (q-1) \\ P(S_k = 0 | (\sigma_1, \ldots, \sigma_k), \sigma_i \neq 0) = p_0 \\ P(S_k = \phi | (\sigma_1, \ldots, \sigma_k), \sigma_i \neq 0)_{\forall \phi \neq 0} = p_\phi \\ (p_0, p_\phi)_k = \left(\frac{(q-1)^{k-1} - z_{k-1}}{(q-1)^k}, \frac{(q-1)^k - z_k}{(q-1)^{k+1}}\right) \end{cases}$$

Proof: See *Appendix.* ■

4.1.1. Source coding on $\underline{b}$

In what follows, we consider the quantities of our interest in the case where source coding is performed such that $\underline{b}$ excludes the zero codeword.

Theorem 2: The mutual information between the payload $\underline{\gamma}$ and the plaintext $\underline{b}$ for the case in which b_i is uniformly i.i.d and $b_i \in \mathbb{F}_q \backslash \{0\}$ is:

$$I(\underline{\gamma}; \underline{b}) = 0$$

Proof: See *Appendix.* ■

Theorem 3: The mutual information between the payload $\underline{\gamma}$ and the encoding matrix $\mathbf{A}$, for the case in which b_i is uniformly i.i.d and $b_i \in \mathbb{F}_q \backslash \{0\}$ is upper bounded by:

$$\begin{aligned} & I(\underline{\gamma}; \mathbf{A}) \\ & \leq n\left(\log(q) - \sum_{i=0}^{n} \binom{n}{i} \frac{(q-1)^{(n-i)}}{q^n} H(\gamma_i | Z(\underline{a}_i) = i)\right) \end{aligned}$$

where $H(\gamma_i | Z(\underline{a}_i) = i) = -p_{0i} \log p_{0i} - (q-1) p_{\phi i} \log p_{\phi i}$, and the values for $(p_0, p_\phi)_i$ are given by the expression in *Lemma 2.* It follows that $\lim_{q \to \infty} I(\underline{\gamma}; \mathbf{A}) = 0$.

Proof: See *Appendix.* ■

4.1.2. Variants of the encoding matrix

The following results consider the quantities of our interest in the case where the entries of the encoding matrix $\mathbf{A}$ are chosen uniformly i.i.d among the non-zero elements of the finite field, $\mathbb{F}_q\backslash\{0\}$.

Theorem 4: The mutual information between the payload $\underline{\gamma}$ and the plaintext $\underline{b}$, for the case in which b_i is uniformly i.i.d and $a_{ij} \in \mathbb{F}_q\backslash\{0\}$ is bounded by:

$$\begin{aligned} &I(\underline{\gamma};\underline{b}) \\ &\leq \left(n\log(q) - \sum_{i=0}^{n} \binom{n}{i} \frac{i(q-1)^{(n-i)}}{q^n} H(\gamma_i|Z(\underline{b})=i) \right) \end{aligned}$$

where $H(\gamma_i|Z(\underline{b})=i)) = -p_{0i}\log p_{0i} - (q-1)p_{\phi i}\log p_{\phi i}$, and the values for $(p_0,p_\phi)_i$ are given by the expression in *Lemma 2*. It follows that $\lim_{q\to\infty} I(\underline{\gamma};\underline{b}) = 0$.

Sketch of Proof: The proof uses the same arguments as the ones in *Theorem 3*.

Theorem 5: The mutual information between the payload $\underline{\gamma}$ and the encoding matrix $\mathbf{A}$, for the case in which b_i is uniformly i.i.d and $a_{ij} \in \mathbb{F}_q\backslash\{0\}$ obeys to:

$$I(\underline{\gamma};\mathbf{A}) = 0$$

Sketch of Proof: The proof uses the same arguments as the ones in *Theorem 2*.

4.2. Impact of reuse of the coding matrix

We now consider the impact of the reuse of the coding matrix, that is, the information that a possible attacker could obtain by observing $(\underline{\gamma}_1,\underline{\gamma}_2,\ldots,\underline{\gamma}_n) = (\mathbf{A}\underline{b}_1,\mathbf{A}\underline{b}_2,\ldots,\mathbf{A}\underline{b}_n)$, where $\mathbf{A}$ is a matrix generated once at random according to the cases considered so far. This analysis is relevant to allow the reuse of encoding matrices at each generation. Due to lack of space, we only include the results referring to the cases considered in *Theorems 2* and *4*. The results for the remaining cases are similar.

Theorem 6: The information obtained about $\mathbf{A}$ given $(\underline{\gamma}_1,\underline{\gamma}_2,\ldots,\underline{\gamma}_w) = (\mathbf{A}\underline{b}_1,\mathbf{A}\underline{b}_2,\ldots,\mathbf{A}\underline{b}_w)$, for the case in which b_i is uniformly i.i.d and $a_{ij} \in \mathbb{F}_q\backslash\{0\}$ is given by:

$$I(\underline{\gamma}_1,\underline{\gamma}_2,\ldots,\underline{\gamma}_w;\mathbf{A}) \quad = \quad 0$$

Sketch of Proof: The result follows by considering standard entropy inequalities.

Theorem 7: The information obtained about $(\underline{b}_1,\ldots,\underline{b}_w)$ given $(\underline{\gamma}_1,\underline{\gamma}_2,\ldots,\underline{\gamma}_w) = (\mathbf{A}\underline{b}_1,\mathbf{A}\underline{b}_2,\ldots,\mathbf{A}\underline{b}_w)$, for the case in which b_i is uniformly i.i.d and $b_i \in \mathbb{F}_q\backslash\{0\}$, satisfies:

$$I(\underline{\gamma}_1,\ldots,\underline{\gamma}_w;\underline{b}_1,\ldots,\underline{b}_w) \quad = \quad 0,$$

Sketch of Proof: The result follows by considering standard entropy inequalities.

4.3. Discussion

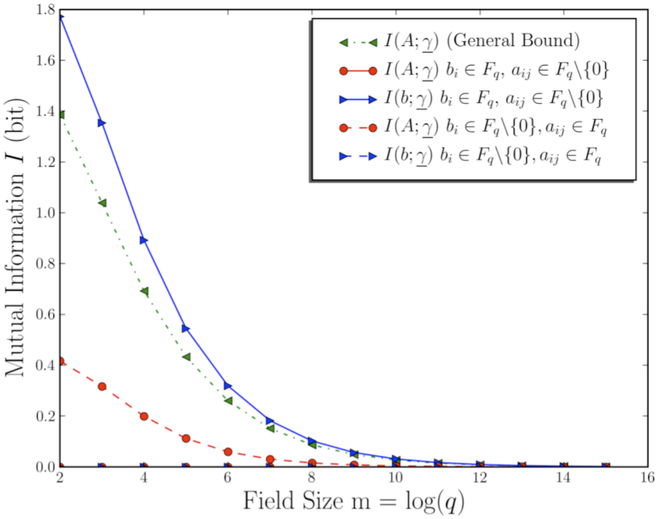

Figure 1: Mutual information in function of field size, for several coding strategies for RLNC and $n = 4$.

The results, illustrated in *Figure 1*, provide fundamental insights with respect to the confidentiality of the information secured by protecting the code used in RLNC. One remarkable consequence is that, independently of the encoding matrix, and as long as source coding is optimal, benefits are achieved simultaneously in terms of security and in terms of decoding probability. In fact, both the mutual information between the payload and the original plaintext or the coefficients and the decoding error probability decrease as the field size increases [1].

Another interesting observation from our results is the dichotomy between including the zero symbol in $\mathbf{A}$ or $\underline{b}$. In fact, one can achieve zero mutual information either between the payload and the original information – by performing source-coding that excludes the codeword zero – or zero mutual information between the coefficients of the encoding matrix and the original information – by generating random matrices with coefficients chosen among the non-zero elements of the finite field under consideration.

This trade-off suggests some implications on the number of reutilizations of the encoding matrix in secure practical protocols. This number is typically proportional to the size of the generation and of the packets in practical RLNC based protocols, and should be carefully chosen if b_i's are chosen to belong to $\mathbb{F}_q\backslash\{0\}$, since some information is leaked about the encoding matrix in each reutilization. On the other hand, if one chooses b_i among all the elements in the finite field and the encoding matrix not to include zeros, there is leakage of information about each $\underline{b}$, but not about $\mathbf{A}$, and the size of the generation is no longer relevant in terms of security.

5. NUMERICAL SIMULATION

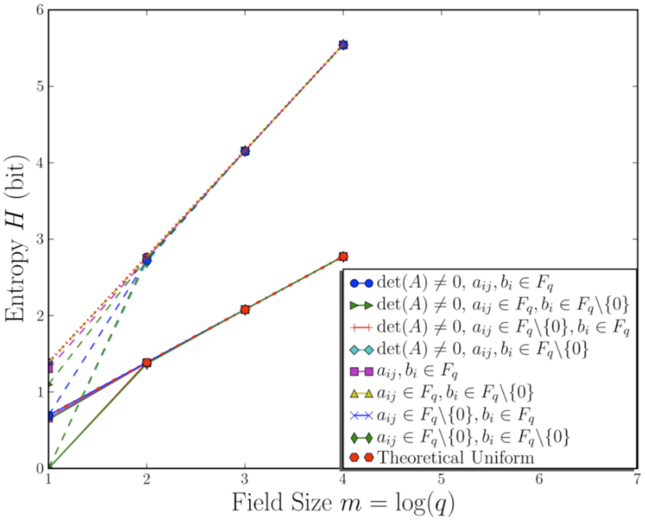

Figure 2: Evolution of $H(\underline{\gamma})$ and $H(\gamma_i), 1 \leq i \leq 2$, with the size of the field, for $n = 2$. Full lines represent the entropy of γ_i (that is, the entropy of the resulting symbols), while dashed lines represent the entropy of $\underline{\gamma}$ (that is, the entropy of the resulting vectors).

With the goal of verifying both the impact of the invertibility of $\mathbf{A}$ and the impact of the choice of 0's in the coefficients of $\mathbf{A}$ and $\underline{b}$ in the entropy of $\underline{\gamma}$, we consider several scenarios for the evolution of the entropy with the size of the field, as shown in *Figure 2*. Due to computational complexity, we restrict ourselves to 2×2 matrices, yet we consider several field sizes. We determine the entropy numerically, both on a sequence basis ($H(\underline{\gamma})$, for all possible $\underline{\gamma}$) and on a symbol basis ($H(\gamma_i)$, for all possible γ_i) , and compare it to the theoretical entropy of the uniform distribution for both.

The results presented in *Figure 2* show that both quantities approach maximum entropy very fast with the size of the field, even for small fields. Both entropies show a similar behavior. As predicted, most cases are far from maximum entropy for $m = 1$ (since in a field with 2 elements, many matrices are not invertible, and the results are thus far from uniform) and approach maximum entropy very fast from $m = 2$ onwards. Notice that in the cases we consider, both $H(\gamma_i)$ and $H(\underline{\gamma})$ are maximum, for all field sizes considered.

6. CONCLUSIONS AND FURTHER WORK

We obtained bounds for the mutual information between the payload of packets encoded with RLNC and either the coefficient matrix or the original plaintext, for several choices of source coding and matrix restrictions. Our bounds indicate that it is possible to guarantee information-theoretic security for the payload by compressing without the zero symbol. Alternatively, we can exclude the zero symbol from the encoding matrix and achieve the same goal. Provided that the source coding stage offers optimal compression, protecting the code is generally sufficient. This observation is likely to have a strong impact on the design of secure RLNC protocols, most strikingly with respect to the choice of generation size and security constraints.

As part of our ongoing work, we are considering the evaluation of the impact of non-uniformities caused by imperfect source coding and modes of encryption for secure network coding protocols, using both information-theoretic tools and state of the art cryptanalysis techniques.

References

[1] T. Ho, M. Médard, R. Koetter, D.R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[2] Ralf Koetter and Muriel Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, 2003.

[3] J. P. Vilela, L. Lima, and J. Barros, "Lightweight Security for Network Coding," *Proc. of the IEEE International Conference on Communications (ICC 2008), Beijing, China*, May 2008.

[4] P.A. Chou, Y. Wu, and K. Jain, "Practical network coding," *Allerton Conference on Communication, Control, and Computing*, 2003.

[5] Luísa Lima, Muriel Médard, and João Barros, "Random linear network coding: A free cypher?," in *IEEE International Symposium on Information Theory, Nice, France*, June 2007.

APPENDIX

Sketch of Proof for Lemma 2

Let S_i represent the result of the sum of i elements. We represent all the possibilities of results by a q-ary tree, in which each the i^{th} level of depth represents the possibilities for S_i. By using this representation, we consider the probabilities for obtaining each symbol in

$\mathbb{F}_q$ at each "step" of the sum, that is, $S_{i+1} = \sigma_{i+1} + S_i$, where $\sigma_{i+1} \neq 0$. Let Z_i represent the number of zeros at level i of the tree. It is clear that $Z_1 = 0$, since $\sigma_1 \in \mathbb{F}_q \backslash \{0\}$. At each step $i > 1$, each non-zero element contributes to the tree with one 0, while each zero element contributes to the sum tree with no zeros. This can be easily representable by a recursive expression:

- The number of zeros at step i is the subtraction of the number of elements at level i of the tree by the number of non-zeros from the last iteration, that is, $Z_{i-1}(q-1)$ and hence $Z_i = (q-1)^i - Z_{i-1}(q-1)$;
- The number of non-zeros at step i is simply the subtraction of the total number of elements of the level i of the tree with Z_i.

The result follows. ■

Sketch of Proof for Theorem 2

We start by noting that since $H(\underline{\gamma}) \leq n\log(q)$, then $I(\underline{b}; \underline{\gamma}) \leq n\log(q) - H(\gamma|\underline{b})$. We now consider $H(\underline{\gamma}|\underline{b})$ in detail.

We analyse the result $\underline{\gamma} = \mathbf{A}\underline{b}$ first by considering the multiplication operation, since it precedes the sum operation. We introduce an auxiliary matrix $\mathbf{C} = (c_{ij})$, where $c_{ij} = a_{ij}b_j$. Since a_{ij} and b_j are chosen independently of one another, it is clear that each column in $\mathbf{C}$ is independent of each other.

To analyse the dependency among the elements in the same column, that is, $a_{lj}b_j$ and $a_{kj}b_j$, we note that

$$\forall b_j, P(a_{ij}b_j = \alpha | b_j = \beta, b_j \neq 0) = \frac{1}{q},$$

because of the properties of the multiplicative group of a finite field.

Also, since each a_{ij} is independent of the others, it is clear that c_{ij} is independent of c_{lj}, $\forall i \neq l$, that is, there are no dependencies among the elements of the same column.

We now consider the sum operation. At each intermediate sum operation, $c_{il} + \sum_{j=1}^{l-1} c_{ij}, l \leq n$, c_{ij} is uniformly i.i.d. with $P(c_{il}|b_l) = \frac{1}{q}$. By an induction-like argument, with the inductive basis $P(c_{l1}+c_{l2} = \tau) = \frac{1}{q}$, we reach the final result, that is, $P(\gamma_l = \tau) = \frac{1}{q}$, and $H(\gamma_l) = \log(q)$. Since each element in the vector $\underline{\gamma}$ is independent of one another, it follows that

$$H(\underline{\gamma}|\underline{b}) = nH(\gamma_l|\underline{b}) = n\log(q),$$

and $I(\underline{\gamma}|\underline{b}) = 0$. ■

Sketch of Proof for Theorem 3

The proof uses the same arguments as in *Theorem 2*. We start by noting that $I(\mathbf{A}; \underline{\gamma}) \leq n\log(q) - H(\underline{\gamma}|\mathbf{A})$ and consider $H(\underline{\gamma}; \mathbf{A})$ in detail, by analysing one element γ_i of $\underline{\gamma}$ at a time.

We consider beforehand the multiplication operation and use the auxiliary matrix $\mathbf{C} = (c_{ij})$, where $c_{ij} = a_{ij}b_j$ and $\gamma_i = \sum_{j=1}^{n} c_{ij}$. By using the same arguments as in the proof for *Theorem 2*, we note that each column of $\mathbf{C}$ is independent of each other.

We now consider, without loss of generality, $c_{1j} = a_{1j}b_j$. It is clear that $P(c_{1j} = 0 | a_{1j} = 0) = 1$. If $c_{1j} \neq 0$, then

$$P(c_{1j} = \theta | a_{1j} = \alpha_{1j})_{\theta, \alpha_{1j} \neq 0} = (q-1)^{-1}.$$

By using the same arguments as in the proof for *Theorem 2*, it follows that the lines of $\mathbf{C}$ are mutually independent of each other.

We now consider the addition operation, by considering $\underline{c}_1$. Let $S_i = \sum_{j=1}^{i} c_{1i}$ and $\gamma_1 = S_n$. Since the multiplication of a number by a zero always yields the zero result and zero is the neutral element of addition, we can rearrange $\underline{c}_1$ and $\underline{a}_1$ in the following way:

$$\begin{aligned} & P(S_n = \phi | Z(\underline{a}_1) = l)) \\ & \quad = \quad P(S_n = \phi | \underline{a}_1 = (\alpha_1, ..., \alpha_l, \overbrace{0, ..., 0}^{n-l}))_{\alpha_j \neq 0, \forall j} \\ & \quad = \quad P(S_l = \phi | \underline{a}_1 = (\alpha_1, \ldots, \alpha_l))_{\alpha_j \neq 0, \forall j} \end{aligned}$$

The probability $P(S_l = \theta | \underline{a}_1 = (\alpha_1, \ldots, \alpha_l))_{\alpha_j \neq 0, \forall j}$ is given by $S_l = \sum_{i=0}^{l} c_{1i}$, where $\alpha_i, c_{1i} \in \mathbb{F}_q \backslash \{0\}$ and $P(c_{1i}) = (q-1)^{-1}$, which are given by *Lemma 2*.

We now subdivide the computation of $H(\gamma_1|\underline{a}_1)$ in sets, each corresponding to $\underline{a}_1$ having i zero elements:

$$\begin{aligned} & H(\gamma_1|\underline{a}_1) \\ & \quad = -\sum_{i=0}^{n} \binom{n}{i} \frac{(q-1)^{(n-i)}}{q^n} \left((q-1)f(\phi, \underline{a}_1) + f(0, \underline{a}_1)\right), \end{aligned}$$

where $f(\theta, \underline{v}) = p(\gamma_1 = \theta|\underline{v}) \log p(\gamma_1 = \theta|\underline{a}_1)$ and $\underline{a}_1 = (\alpha_1, \ldots, \alpha_{n-i}, 0, \ldots, 0)$.

Since each line of $\mathbf{C}$ is mutually independent of the others, $H(\gamma|\mathbf{A}) = nH(\gamma_1|\underline{a}_1)$ and it follows that

$$\begin{aligned} & I(\gamma; \mathbf{A}) \\ & \quad = n\left(\log(q) - \sum_{i=0}^{n} \binom{n}{i} \frac{(q-1)^{(n-i)}}{q^n} H(\gamma_i|Z(\underline{a}_i) = i)\right), \end{aligned}$$

where

$$(H\gamma_i|Z(\underline{a}_i) = i) = -p_{0i}\log p_{0i} - (q-1)p_{\phi i}\log p_{\phi i},$$

and the values for $(p_0, p_{\theta i})$ are given by the expression in *Lemma 2*. ■