# Secure Network Coding: Overview and State-of-the-art.

**J. de Curtó i Díaz**, **I. de Zarza i Cubero**, and **M. A. Vázquez**.

**Bellaterra, 2012.**

**Universitat Autònoma de Barcelona**

# Secure Network Coding: Overview and State-of-the-art

J. de Curtó i Díaz*, I. de Zarza i Cubero*, and M. A. Vázquez.
Universitat Autònoma de Barcelona.
c@decurto.tw, z@dezarza.tw
*Both authors contributed equally.

## I. Introduction

Network coding is one of the most important breakthroughs on the theory of information transmission and processing. It is based on a simple, yet powerful, idea: in a packet network, instead of simply routing packets, intermediate nodes may compute and transmit functions of the packets they receive.

Network coding allows network routers to mix the information content such that incoming packets are combined before forwarding them. Which is indeed an effective way to improve both throughput and robustness.

However, what happens when the network contains malicious nodes? Such nodes might intercept the network in order to eavesdrop an ongoing communication, and/or might pretend to forward packets originating from the source, while actually they inject fake packets into the information flow so as to cause a decoding error.

Since routers combine packets' content, just a single corrupted packet can contaminate all the information reaching a certain destination. As a result, unless this problem is solved, network coding cannot perform better than pure forwarding when such malicious adversaries are present. Thus, research in Secure Network Coding has become essential.

Now we are going to introduce a basic model of network coding.

## II. Model of the Network

The next graph-theoretical model, while not the most general possible, will be enough to model the major ideas involved in the next sections.

A combinational packet network $N = (V, E, S, T, A)$ comprises:

- A finite directed acyclic multigraph $G = (V, E)$ where $V$ is the set of vertices and $E$ is the multiset of directed edges;
- A distinguished set $S \subset V$ of sources;
- A distinguished set $T \subset V$ of sinks;
- And a finite packet alphabet $A$ with $|A| \geq 2$.

Vertices model communication nodes within the packet network, while directed edges model error-free communication channels between the nodes. An edge $(u, v)$ has unit capacity $(C)$ in the sense that it can be used to reliably deliver one packet from $u$ to $v$.

The above model is illustrated in Figure 1, where the classical butterfly network is exposed and a secure network code is depicted. Next we are going to introduce the basic setting of network coding.

## III. Threat model

There is a source, $A$, who communicates using a wired or wireless network to a receiver $B$, Figure 2. There is also an attacker $C$, hidden in the network.

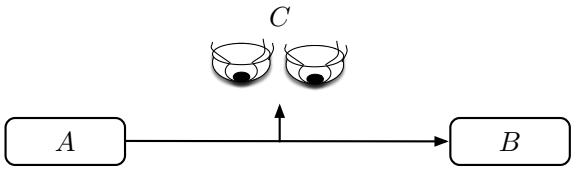


Figure 2: Threat model.

$C$ aims to prevent or minimize the transfer of information from $A$ to $B$, and/or to eavesdrop on it. He can observe some or all of the transmissions, and can inject his own. When he injects his own packets, he pretends it is part of the information flow from $A$ to $B$.

## IV. Classification

The state-of-the-art of secure network coding can be classified using two general distinct approaches: computational security (cryptographic) and information-theoretic.

Whereas in computational security, architectures are based on (unproven) assumptions of intractability of certain functions, typically done at upper layers of the protocol stack, in information-theoretic there are no computational assumptions and it is based on the fact that an eavesdropper cannot infer anything from message $M$ when observing packet $X$ $(I(X; M) = 0)$, furthermore, it is implementable at the physical-layer.

The approach information-theoretic is based on introducing redundancy so as to enable recovery from malicious adversaries. This technique does not rely on any computational assumption but it is limited to offer security against certain adversaries. In fact, these settings place constraints on the adversary's computational power, the number of nodes the adversary can corrupt and/or the number of links at which the adversary can eavesdrop.

The approach cryptographic is based on providing a way for honest nodes to verify authenticity of individual packets. This approach focus only in protecting against a computationally bounded adversary. It is important to note that this cannot be done using classical signatures, since intermediate nodes apply functions to input packets. This technique can offer security against an adversary who eavesdrop on the entire network and controls an arbitrary number of nodes, as long as the sink node receives $m$ correct and linearly independent vectors. Moreover, they also allow to recover a portion of the original file if less than $m$ vectors are received. Another important feature is that intermediate nodes can verify if an individual packet is correct and reject an incorrect one. All existing research focuses on public-key architecture, rather than symmetric-key.

This classification can be more generally described using the passive or active nature of the adversary (see Médard [2012]). Where approaches cryptographic and information-theoretic are classified

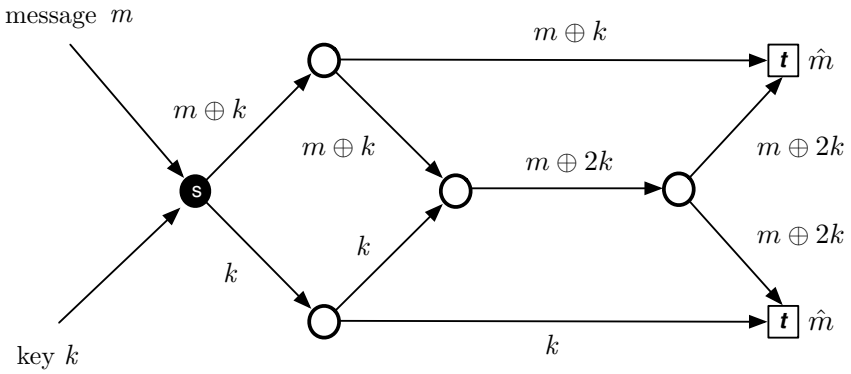


Figure 1: A secure network code.

within it, as it is shown in Figure 3.

Based on Médard [2012] we can classify the lines of research using the passive or active nature of the adversaries.

We consider communication in the presence of passive adversaries who only wishes to learn the information transmitted over the network (eavesdropping). In this case, the main objective of current research is to enable secrecy.

On the other hand, we consider communication in the presence of active adversaries who have not only eavesdropping but also jamming capabilities. Whose objective is to cause a decoding error at the terminal nodes. In this case, we can divide current research into two categories: the first one which looks for reliability, that is to say, correct decoding, and the second one which looks for both reliability and secrecy.

The communication in the presence of both passive and active adversaries can be classified in two settings: coherent, where the terminal nodes are assumed to know the topology of the network throughout the architecture of communication used, and non-coherent, where no knowledge of the topology and/or code being used is assumed to be present at the terminal nodes. Current research activity involves the study of these two branches. Both architectures coherent and non-coherent are included inside the approach information-theoretic (mentioned earlier in this section), where there are no computational assumptions on the adversary.

In the case of an active adversary, there is also an approach cryptographic where we assume the adversary to be computationally limited. Current research involves schemes which are conditioned on certain cryptographic assumptions.

We are going to see in detail the current lines of research involving the topics above.

### A. *Secrecy in architecture coherent and passive adversary*

Secure communication in the context of coherent network coding with a passive adversary has been addressed in several works over the last decade. Now we are going to do an overview of the main lines of research:

Initiated by Cai and Yeung [2002], this line of study considers improving any linear network code (which allows communication at a rate $C$ in the absence of an eavesdropper) to one which is secure. The main idea here is to use redundancy in order to enable secrecy. The presence of an eavesdropper is dealt by using a better encoding at the source and a better decoding at terminal nodes. To illustrate this, in Cai and Yeung [2002], the source appends to the information $X$ (with $C - z_1$ characters) a uniformly distributed random vector $R$ ($z_1$ characters) to obtain $(X, R)$. This goes over a certain invertible linear transform $T$ resulting in the message $M$. Which is transmitted using the original scheme of network coding. The terminal, on decoding, recovers $M$ and then through $T$ recovers $X$.

The matrix $T$ needs to be designed such that any $z_1$ linear combinations of $M$ do not reveal information on the value of $X$.

Other research takes a different approach in which they concentrate on the design of the internal architecture of network coding instead of the design of $T$, Rouayheb and Soljanin [2007]; Rouayheb et al. [2012].

Furthermore, ongoing research also involves mixing block error correcting codes with architectures of network coding in order to characterize pre-encoding schemes $T$ that allow secure communication when combined with a scheme of network coding Ngai et al. [2009].

Moreover, there is also research involving perfect/weak security of a random linear network code without any pre-encoding via $T$. Here, a random linear network code is one in which the linear coefficients governing the coding scheme are all chosen uniformly and independently at random from the underlying field $F$ and the actions of the eavesdropper are independent of these random choices.

The works mentioned above all focuse on acyclic networks, however, there is also research in the general (not necessarily acyclic) setting, for instance Jain [2004]. Where the necessary and sufficient condition for secure communication is the existence of a single path not seen by the adversary from sender to receiver.

### B. *Secrecy in architecture non-coherent and passive adversary*

We focus on two lines of work: schemes with randomized source encoding, and those with deterministic source encoding.

As for schemes with randomized source encoding, we can illustrate the main idea using two examples. Both the construction mentioned

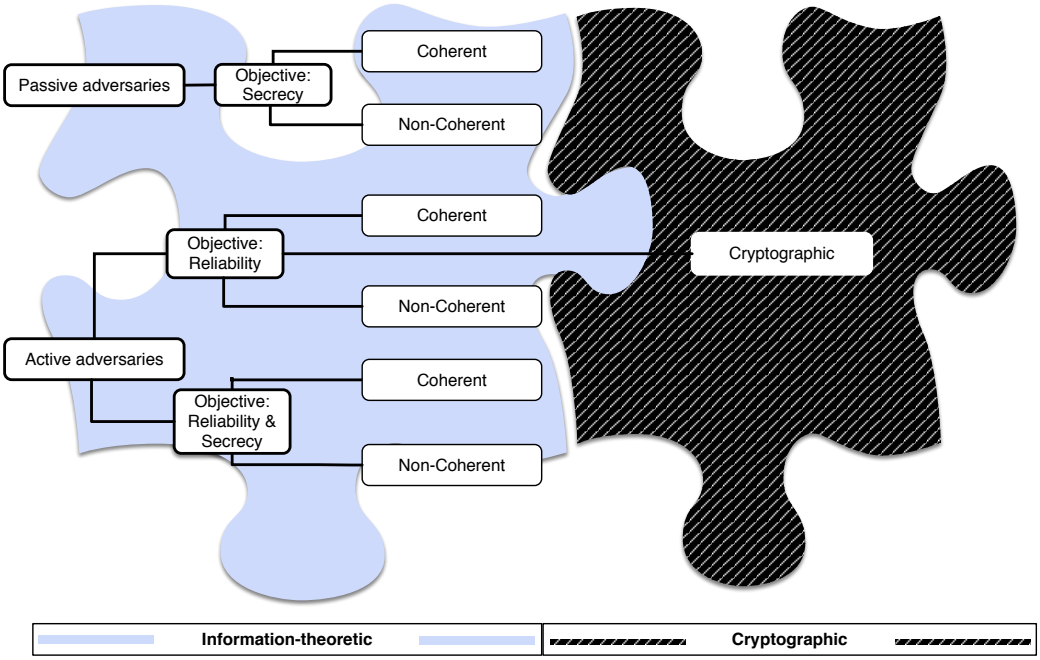


Figure 3: Classification.

in Feldman et al. [2004], where the linear filter that the source uses to generate the message is obtained by randomly choosing a matrix of the correct dimension, and the distributed random linear scheme of network coding Ho et al. [2006], where interior nodes perform random linear combinations over sufficiently large finite fields, can be unified to generate a linear network code perfectly secure against eavesdropping by any adversary that can wiretap at most $z_1$ links.

As for deterministic source encoding, the second line of work under consideration, we can illustrate the main idea with the work in Silva and Kschischang [2009b]. They use a deterministic source encoder placed over a random linear non-coherent network code (for example the used in Ho et al. [2006]). The formulation of the wiretap network is utilized and they propose a coset coding based on maximum rank-distance (MRD) codes, that does not impose any constraints on the underlying network code. In other words, for any linear network code that is possible to multicast, secure communication at the maximum possible rate is achieved with a fixed outer code. The essence of this approach is to use a vector outer code over a block length $n$, which is also a linear code.

### C. *Reliability in architecture coherent and active adversary*

In this case we are focused on the design of network codes that enable reliable error-detection and communication in the presence of active adversaries that have both eavesdropping and jamming capabilities.

If we suppose the adversary can jam $z_0$ links of the network and observe all links of the network it is shown that the rate is $(C-2z_0)^+$.

The problem of error correction in network coding is studied in Yeung and Cai [2006] and Cai and Yeung [2006], where the fundamental coding bounds are obtained.

These works draw an analogy between HAMMING bound (it holds for all types of errors; random or adversarial), SINGLETON bound (for sufficiently large alphabet sizes this bound is tighter than HAMMING bound), and GILBERT-VARSHAMOV bound, in coherent network coding.

Finally, last but not least, an important work of error correction was done by Ngai and Yeung [2009]. They present a construction of secure error-correcting (SEC) network codes that can protect the source message from wiretapping, random errors, and errors injected by the wiretapper. Furthermore, they also proved the optimality of their construction.

### D. *Reliability in architecture non-coherent and active adversary*

In this architecture neither the network topology nor the network code are known in advance. It considers the rate of reliable communication in the setting non-coherent in the presence of a hidden active jammer that can jam $z_0$ links of the network. It is shown that in this setting, the same rate of $(C-2z_0)^+$ is achievable as in the case coherent. Here, all the complexity is absorbed into the encoder and decoder. The key to understand this is that if the network performs linear network coding, the relationship between the source information $X$, the fake information $Z$ injected by the adversary, and the information received by the receiver can be expressed as:

$$Y = TX + T'Z.$$

In Kötter and Kschischang [2007, 2008] it is indicated a strategy for good design of codes for the operator channel (the relationship between $X$ and $Y$, $T$), closely paralleling classical algebraic designs (such as Reed-Solomon). They demonstrate computationally efficient encoding and decoding of such codes via codes based on linearized polynomials (analog to Reed-Solomon from classic algebraic theory). In Silva and Kschischang [2007, 2009a]; Silva et al. [2008b] they demonstrate alternative methods of decoding by using rank-metric decoding algorithms.

Other lines of research consider the problem of detecting (instead of correcting) adversarial network errors in an architecture non-

coherent, which is more straightforward. In Ho et al. [2008] the source appends a non-linear hash to each packet of the data contained within it. They show that as long as there is even one uncorrupted path from source to destination, then arbitrary errors by the adversary can be detected with high probability, using a low-complexity scheme.

Other work also considers the case of random errors on links rather than adversarial errors. In this model $Z$ is chosen uniformly at random from the set of matrices, instead of deliberately chosen by an adversary in order to decrease the rate at which sender and receiver can communicate. In Montanari and Urbanke [2007] and Silva et al. [2008a] they demonstrate that there is a higher rate in this case than with adversarial errors.

An alternate architecture for efficient non-coherent network error correction is proposed in Jaggi et al. [2007, 2008]. Although the parameters are generally inferior to those in Kötter and Kschischang [2007, 2008], they allow for a new line of research: computationally efficient "linear list-decoding", which is useful in a variety of settings. For instance, in Jaggi et al. [2007, 2008] this result is used as the first stage of a non-coherent network error correcting code.

### *E. Reliability in architecture cryptographic and active adversary*

We consider adversarial jammers that are computationally bounded. In this line of research, one assumes that certain computational tasks are intractable (such as factoring), and based on these constraints design an achievable architecture of communication.

It can be shown that it is possible to communicate at rate $C - z_0$ in the presence of a computationally bounded adversary that can corrupt up to $z_0$ links of the network, which improves on the rate of $C - 2z_0$ achieved in the architecture coherent (in which the jammer has no computational limitations).

We can divide the works into two different lines of research: authentication in-network and authentication end-to-end.

In the first one, the architecture in-network, internal nodes of the network may identify and reject information packets that have been corrupted by the jammer using a mechanism of authentication. This changes the jammer setting into a situation where some links of the network are not able to transmit information and no jammer is present. An example of this are the schemes of standard random linear network coding in Ho et al. [2006].

In this line of research there are several open lines of study. Which include designing efficient signature schemes closed under linear coding operations (referred to as homomorphic Johnson et al. [2002]; Micali and Rivest [2002]) and designing signature schemes which do not need a complex infrastructure to support key distribution between internal nodes of the network. It is important to note that authentication in-network guarantees communication at rate $C - z_0$, however, in many cases a higher rate is possible (it depends on the number of links the jammer is controlling).

In the second line of research, authentication end-to-end, internal nodes are not aware of the presence of an adversarial jammer and standard coding protocols are used. Hence, to deal with the presence of this malicious adversary, improved encoding and decoding are applied to source and terminal nodes, respectively.

Authentication end-to-end is better than authentication in-network in terms of coding. Moreover, it also guarantees a rate $C - z_0$. However, using the same architecture as in-network, it may be true that authentication end-to-end obtains a lower rate (this is because it assumes that the adversary locates itself in the worst-case manner, that is to say, it is a pessimistic assumption).

*1) **Architecture in-network**:* A function of hashing $h$ is homomorphic if for $x = \sum x_c$ it holds that $h(x) = \sum h(x_c)$. Functions of hashing that are homomorphic can be used typically in a random scheme (non-coherent) of network coding as in Ho et al. [2006]. Current research involves studying the requirements from the local information $h(x_c)$.

In Krohn et al. [2004] and Gkantsidis and Rodríguez [2006], the hashes of the source information $h(x_c)$ are assumed to be reliably communicated to internal nodes of the network. Thus, a centralized trusted authority is assumed to provide theses hashes. In Gkantsidis and Rodríguez [2006]; Krohn et al. [2004] the communication scheme suggested is based on the hardness of the problem Discrete-Log. In Boneh et al. [2009]; Charles et al. [2006]; Médard et al. [2007] the need to distribute the values of hashing is obviated using public-key cryptography. Charles et al. [2006] is based on the hardness of Discrete-Log problem and the computational security of CO-DIFFIE-HELLMAN problem on elliptic curves. Médard et al. [2007] is based on linear subspace authentication, also based on the hardness of Discrete-Log. Boneh et al. [2009] presents two settings based on the idea presented in Médard et al. [2007]. The first setting is homomorphic and based on the computational security of the DIFFIE-HELLMAN assumption, while the second scheme is non-homomorphic and based on the Discrete-Log, using the same ideas as in Krohn et al. [2004] and Médard et al. [2007].

*2) **Architecture end-to-end**:* As in the previous architecture, this line of research also starts by improving a scheme non-coherent of network coding such as the work in Ho et al. [2006], this is done in Nutman and Langberg [2008]. However, the only changes applied here are in the encoding and decoding of the source terminals. The protocol presented in Nutman and Langberg [2008] is based on Jaggi et al. [2007, 2008]. In these the rate $C - z_0$ is obtained under the assumption that source and terminal nodes share a low rate side channel in which they communicate a short secret. It is based on allowing list decoding (rather than unique decoding) at terminal nodes. Once such a list is obtained, each terminal may pick the correct element from its list using the secret side information. The secrecy of the side information is crucial to avoid the jammer from causing a decoding error. With this in mind, Nutman and Langberg [2008] instead of transmitting the side information over a side channel, encrypts this information using an architecture of public-key encryption and transmits the encrypted information over the network. If we assume the jammer cannot break the encryption, the side information remains secret. It is also important to consider that this information still needs to be transmitted reliably. In order to do this, they use a reliable scheme of encoding.

### *F. Reliability and Secrecy in case coherent*

We are going to consider the interplay between eavesdropping and jamming. When we want to protect a message against an eavesdropper (who can see $z_I$ links), we can achieve a secrecy rate of $C - z_I$. This is done by linearly combining a random message (of rate $z_I$) with the source message (of rate $C - z_I$). Hence, these architectures can be understood as a one-time-pad combined with

network coding.

Now we have a network with a hidden adversarial jammer who can observe all transmissions, and can jam $z_0$ links, in this case we have seen that the rate at which information can be transmitted reduces to $C - 2z_0$. This architecture can be seen as converting operator channels with errors of capacity $C$ into error-free operator channel of capacity $C - 2z_0$.

If the adversary can only observe $z_I$ transmissions in the network and jam $z_0$ links, one question arises: what is the best achievable rate of secret and reliable communication? The answer to this question is an important line of research. The work in Ozarow and Wyner [1985] (zero errors and single-letter coding) answers the question by combining the results in the two above paragraphs: an overall rate of $C - 2z_0 - z_I$. This bound is later extended in Silva and Kschischang [2010, 2011] to zero-error block length coding. Moreover, algorithms that achieve these bounds have been studied for the case coherent in Ngai and Yang [2007]; Ngai and Yeung [2009] (block decoding and single letter coding, respectively). These two algorithms work by first converting an operator channel with errors into an error-free operator channel of rate $C - 2z_0$, and over this channel they overlay a one-time pad + network coding, which ensures secrecy against a wiretapping adversary, and reduces the rate to $C - 2z_0 - z_I$.

Finally, another line of research consists on relaxing the requirement from zero-error to one of small error (meaning asymptotically small). Here, the upper bound of $C - 2z_0 - z_I$ no longer holds, and only a bound of $C - z_0 - z_I$ can be derived. This higher rate is indeed achievable with low-complexity codes.

### G. *Reliability and Secrecy in case non-coherent*

The results in Silva and Kschischang [2010, 2011] extends the previous setting coherent to non-coherent codes. Given an arbitrary linear network code, Silva and Kschischang [2010, 2011] gives a scheme end-to-end that treats the network code as an operator channel and achieves the same result of $C - 2z_0 - z_I$ obtained in the latter section. They use rank-metric codes which are good not only for error correction but also for achieving secrecy.

In Yao et al. [2010] it is shown that as long as the sum of the adversary's jamming rate $z_0$ and his eavesdropping rate $z_I$ is less than network capacity $C$ ($z_0 + z_I < C$) there exist codes with low complexity that can communicate a single bit correctly and without leaking any information to the adversary. Furthermore, this result is combined with a secret sharing result of Jaggi et al. [2007, 2008] to design codes that allow communication at the optimal source rate of $C - z_0 + z_I$ while keeping the message secret.

The idea in Jaggi et al. [2007, 2008] can be described as follows: the source node generates a small secret linear hash of its information and sends it to the receiver over a secret and reliable channel. Then, using linear list decoding, the receiver is able to infer a single element from the list with high probability.

Finally, it is also important to mention the work in Yao et al. [2010], where a protocol to secretly and reliably share a bit over the network is described. This protocol emulates a secret and reliable channel using a straightforward rank modulation protocol.

## REFERENCES


D. Boneh, D. Freeman, J. Katz, and B. Waters. 2009. Signing a linear subspace: Signature schemes for network coding. 12th International Conference on Practice and Theory in Public Key Cryptography. 4

N. Cai and R. W. Yeung. 2002. Secure network coding. IEEE International Symposium on Information Theory. 2

N. Cai and R. W. Yeung. 2006. Network error correction, part II: Lower bounds. Communications in Information and Systems. 3

D. Charles, K. Jain, and K. Lauter. 2006. Signatures for network coding. 40th Annual Conference on Information Sciences and Systems. 4

J. Feldman, T. Malkin, C. Stein, and R. A. Servedio. 2004. On the capacity of secure network coding. 42nd Annual Allerton Conference on Communication, Control, and Computing. 3

C. Gkantsidis and P. Rodríguez. 2006. Cooperative security for network coding file distribution. IEEE International Conference on Computer Communications. 4

T. Ho, B. Leong, R. Kötter, M. Médard, M. Effros, and D. R. Karger. 2008. Byzantine modification detection in multicast networks using randomized network coding. IEEE Transactions on Information Theory. 4

T. Ho, M. Médard, R. Kötter, D. R. Karger, M. Effros, J. Shi, and B. Leong. 2006. A random linear network coding approach to multicast. IEEE Transactions on Information Theory. 3, 4

S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard. 2007. Resilient network coding in the presence of Byzantine adversaries. IEEE International Conference on Computer Communications. 4, 5

S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Médard, and M. Effros. 2008. Resilient network coding in the presence of Byzantine adversaries. IEEE Transactions on Information Theory. 4, 5

K. Jain. 2004. Security based on network topology against the wiretapping attack. IEEE Wireless Communications. 2

R. Johnson, D. Molnar, D. Song, and D. Wagner. 2002. Homomorphic signature schemes. Topics in Cryptology. 4

R. Kötter and F. R. Kschischang. 2007. Coding for errors and erasures in random network coding. IEEE International Symposium on Information Theory. 3, 4

R. Kötter and F. R. Kschischang. 2008. Coding for errors and erasures in random network coding. IEEE Transactions on Information Theory. 3, 4

M. N. Krohn, M. J. Freedman, and D. Mazires. 2004. On-the-fly verification of rateless erasure codes for efficient content distribution. IEEE Symposium on Security and Privacy. 4

M. Médard. 2012. Network Coding: Fundamentals and Applications. Elsevier. 1, 2

M. Médard, F. Zhao, T. Kalker, and K. J. Han. 2007. Signatures for content distribution with network coding. IEEE International Symposium on Information Theory. 4

S. Micali and R. Rivest. 2002. Transitive signature schemes. Topics in Cryptology. 4

A. Montanari and R. Urbanke. 2007. Coding for network coding. arXiv:0711.3935. 4

C. K. Ngai and S. Yang. 2007. Deterministic secure error-correcting (SEC) network codes. IEEE Information Theory Workshop. 5

C. K. Ngai and R. W. Yeung. 2009. Secure error-correcting (SEC) network codes. Workshop on Network Coding, Theory and Applications. 3, 5

C. K. Ngai, R. W. Yeung, and Z. Zhang. 2009. Network Generalized Hamming Weight. Workshop on Network Coding, Theory, and Applications. 2

L. Nutman and M. Langberg. 2008. Adversarial models and resilient schemes for network coding. IEEE International Symposium on Information Theory. 4

L. H. Ozarow and A. D. Wyner. 1985. Wiretap channel II. Advances in Cryptology. 5

S. E. Rouayheb and E. Soljanin. 2007. On Wiretap Networks II. IEEE International Symposium on Information Theory. 2

S. E. Rouayheb, E. Soljanin, and A. Sprintson. 2012. Secure network coding for wiretap networks of type II. IEEE Transactions on Information Theory. 2

D. Silva and F. R. Kschischang. 2007. Using rank-metric codes for error correction in random network coding. IEEE International Symposium on Information Theory. 3

D. Silva and F. R. Kschischang. 2009a. Fast encoding and decoding of Gabidulin codes. IEEE International Symposium on Information Theory. 3

D. Silva and F. R. Kschischang. 2009b. Universal weakly secure network coding. Information Theory Workshop on Networking and Information Theory. 3

D. Silva and F. R. Kschischang. 2010. Universal secure error control schemes for network coding. IEEE International Symposium on Information Theory. 5

D. Silva and F. R. Kschischang. 2011. Universal secure network coding via rank-metric codes. IEEE Transactions on Information Theory. 5

D. Silva, F. R. Kschischang, and R. Kötter. 2008a. Capacity of random network coding under a probabilistic error model. 24th Biennial Symposium on Communications. 4

D. Silva, F. R. Kschischang, and R. Kötter. 2008b. A rank-metric approach to error control in random network coding. IEEE Transactions on Information Theory. 3

H. Yao, D. Silva, S. Jaggi, and M. Langberg. 2010. Network codes resilient to jamming and eavesdropping. Workshop on Network Coding Theory and Applications. 5

R. W. Yeung and N. Cai. 2006. Network error correction, part I: Basic concepts and upper bounds. Communications in Information and Systems. 3