Fault Tolerant and Secure Data Retrieval from Wireless Sensor Networks

Stefano CHESSA and Piero MAESTRINI

Abstract—An erasure encoding based on arithmetic residue codes with non-pairwise-prime moduli is introduced. Data are encoded with n residue digits, and can be reconstructed exactly from any subset of at least $n-z$ available digits not bearing errors. Data can also be reconstructed within a small δ from at least $n-z$ available digits bearing small errors, or from at least $n-z-2$ available digits bearing a single unrestricted error combined with small errors. Integers z and δ are depending on the actual moduli and redundancy, and small errors are those of magnitude not exceeding δ. Encoding and decoding of data requires simple arithmetic computation. The proposed encoding is suitable for application to wireless sensor networks, when data robustness and confidentiality are critical issues. To this purpose, data are independently collected by n replicated sensing nodes, each replica storing a different digit of the encoded data. This produces data dispersal without requiring wireless communication between nodes. Data retrieval tolerates failure of multiple sensor, as well as small errors arising from independent data collection, and unrestricted errors due to failures or intrusions. The proposed encoding reduces memory and energy requirements of nodes, and contributes to strengthened data security and confidentiality.

Index Terms— Error control codes, Fault tolerance, Security and privacy protection, Wireless sensor networks.

.

1. INTRODUCTION

Wireless Sensor Networks (WSN) are ideally suited to collect data with limited, or without, human intervention [1]. Applications may range from medical care, crop monitoring, inventory and quality management, natural emergency and battlefield surveillance. When data are to be gathered from remote, inaccessible, or hostile environments, there is no viable alternative to WNS.

A WSN is made of a (usually large) number of sensor nodes and one or several base station(s). Sensor nodes are equipped with sensing interface, a processing unit, program and data memory and a wireless transceiver, and are fed by batteries, possibly rechargeable from sunlight or other renewable sources. Processing, storage and power resources are scarce, and should carefully administered. The transmission range is limited by the scarcity of power resources. Base stations possess more substantial amounts of processing, storage and energy resources, and are able to accumulate data on relatively long term, until queried from the external world.

Sensors may stay on standby most of the time, to be activated periodically or on designated events, such as signals received from the communication interface. When active, a sensor

This work was supported in part by the Ministero dell'Istruzione, dell'Università e della Ricerca of Italy, under Project IsMANET.
The authors are with the Dipartimento di Informatica, Università di Pisa, Pisa, Italy, and with the Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo" (ISTI-CNR), Pisa, Italy. E-mail: Stefano Chessa <ste@ di.unipi.it>; Piero Maestrini <piero.maestrini@isti.cnr.it>.

gets data from the sensing interface, which it stores in the internal memory after some processing, and/or fetches from the internal memory data to be transmitted to a base station, which it places over the wireless channel.

Sensors and base stations are deployed over the sensing area, with a topology that should guarantee the network connectivity. As base stations may be outside the transmission range of most individual sensors, multi-hop routes may be needed to connect the source sensors to a destination base station. This increases the energy consumption in the intermediate sensor nodes that relay data, and contributes to network congestion. As radio channels lend themselves to eavesdropping, data confidentiality might somehow be compromised. If base stations are mobile, multi-hop routes can be avoided, as a sensor may delay data transmission until it detects a roving base station within its transmission range. However, sensor nodes may be unable to connect to base stations for relatively long time intervals, and this increases the memory requirements. A major problem with WSN is the potential loss of data, due to several reasons:

- sensors may fail, e. g. due to component failure, mechanical or thermal stress and battery depletion. Most failures are unrecoverable, although recovery may sometimes be possible, as it occurs in the case of batteries that are recharged from removable sources;
- wireless links may fail, due to insufficient transmission range, interposing obstacles, interferences, or intentional radio jamming by an adversary;
- overflow of local memory, when the input data rate from the sensing interface exceeds the output data rate toward base station(s).

Data losses can be prevented by data replication. Referring to the contents of the local memory of sensor node S as file F_S, a simple approach to replication consists in creating copies of F_S into the local memories of $r-1$ additional nodes (usually, every node plays both roles of sensing and storing data). With this approach, the global requirement of storage resources increases by a factor of r, and the activity of wireless channels also increases because of data transfers needed to create copies of the files. An alternate approach is *data fragmentation and dispersal* based on *erasure codes*, where, for every S, file F_S of size d is divided into b blocks, each of size d/b, which are encoded to produce $n= b+z$ fragments of size d/b, and the encoded fragments are stored in n different storage nodes. The encoding should ensure that the original file can be recovered from any m encoded fragments, with $b\leq m< b+z$. An erasure codes is called perfect if $m= b$. Replication with erasure codes increases the global memory requirements by a factor of $(b+z)/b$. Perfect or quasi-perfect erasure codes have been constructed from *Reed-Solomon* codes [2] or *Low-Density Parity-Check (LDPC)* codes [3].

Data fragmentation and dispersal based on erasure codes was originally introduced [4] aiming at reliability and security in distributed information storage and, dually, at fault-tolerant and fast data transmission in multiprocessors and networks. Subsequently, erasure codes have been widely investigated, mainly in view of application to distributed networked storage, serverless file systems and serverless video streaming. The computational cost of encoding and decoding, which is quite high in erasure codes based on Reed Salomon encoding, has been substantially reduced with the development of *Tornado* [5] and *Fountain* codes [6], both based on LPDC codes. The problem of reconstructing and replicating into spare nodes lost data fragments has also been addressed, and effective *regenerating codes* have been developed [7]. A comparative analysis of the main families of erasure LPDC codes, and an evaluation of respective performance in real-life applications to peer-to-peer and distributed file systems is reported in [8]. A comparison of simple replication and fragmented replication with erasure codes is reported in [9], showing that erasure encoding provides higher mean time to failures, and requires lesser memory size and bandwidth. Erasure codes constructed over a family of arithmetic residue codes, named RRNS [10], has

also been proposed for application to dependable and secure data storage in Ad-hoc Networks [11]. It should be stressed that, in all the above schemes, data produced and fragmented by sensing nodes need to be transmitted over wireless channels to be dispersed into storage nodes, and this implies increased storage and power requirements for nodes, and also increases the risk that data confidentiality is compromised.

With the development of computationally efficient encodings and the availability of sensor nodes equipped with more substantial processing and storage resources, it has been realized that erasure codes may also find a major application area in wireless sensor networks, especially in catastrophic scenarios such as monitoring of natural disasters and emergency management, where constructing reliable storage over unreliable nodes is a vital need [12]. Targeting robust distributed storage in wireless sensor networks, a decentralized erasure encoding with affordable computation and communication costs has been presented in [13].

Beside robust storage, data security is a major issue in wireless sensor networks to be deployed in hostile environments. Security requirements include *integrity* and *confidentiality* of data, *authentication* of communicating nodes, *availability* of services. The network should be able to withstand attacks aimed at threatening the network dependability and security; e.g., injection of false information from spoof nodes to the purpose of corrupting data or disrupting routes, or inducing congestion that may degrade the network performance. Among countermeasures, a major role is played by encryption with symmetric or asymmetric keys, and error encoding of data. An extensive survey of security issues and countermeasures is provided in [14].

In this paper we introduce a novel erasure code constructed over a family of arithmetic residue codes, named RNS-NPM, to be recollected in Section 3. As it occurs with the known erasure codes, data acquired by any sensor node are fragmented into n encoded fragments, which are stored into n distinct nodes, and data can be reconstructed from any n-z of the above fragments: in other words, up to z erasures can be tolerated. The new code also possesses the notable property of tolerating small errors of arbitrary multiplicity; that is, the information can be reconstructed within a small δ from n-z available fragments that were produced from different instances of the same data, each bearing an error not greater than δ. Further, the ability of tolerating erasures combined with small errors of arbitrary multiplicity is retained when unrestricted errors of bounded multiplicity also occur. In WSN application, the preceding properties allow independent acquisition of the same data by n replicated sensor nodes, each of which produces n encoded fragments from the local data instance and stores a single fragment, while discarding the others. As this occurs in every replicated sensor node, and different replicas store different fragments, the result is that n encoded fragments are dispersed into n nodes without involving inter-node communication. Memory resources are also spared since fragments, rather than whole data, need to be stored. The ability of tolerating small errors is essential, since it is unavoidable that the instances produced by independent data collection slightly deviate from the unknown, exact data value.

The remainder of this paper is organized as follows: Section 2 presents a scenario in WSN application which is ideally suited for the new erasure codes; Section 3 concisely recollects the residue arithmetic codes used to construct the new erasure code, and Sections 4, 5 and 6, respectively, derive the properties enabling toleration of erasures, toleration of erasures combined with small errors of arbitrary multiplicity, and toleration of erasures combined with a bounded number of unrestricted errors and small errors of arbitrary multiplicity. Section 7 draws conclusions, and the Appendix summarizes symbols and notations used throughout the paper.

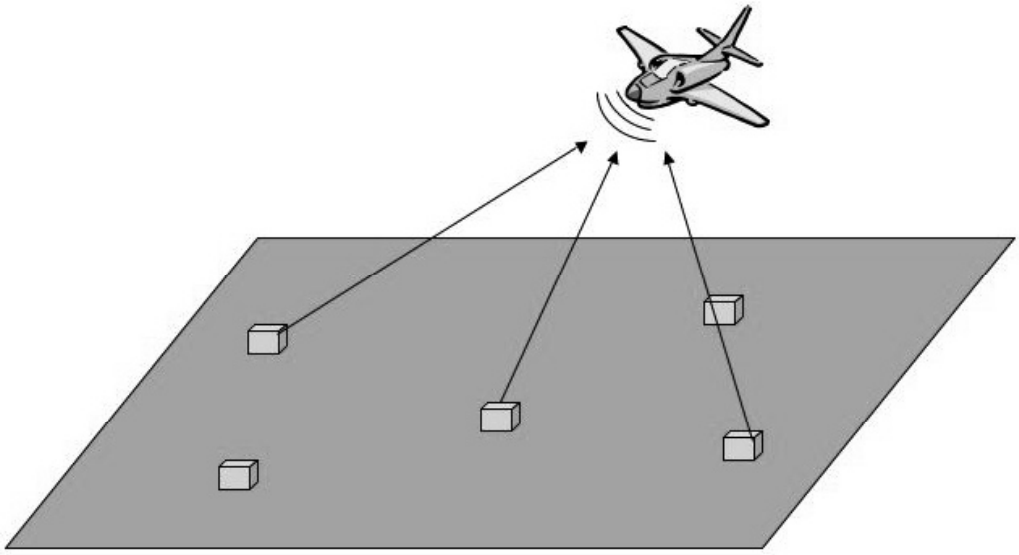

Fig. 1: A mobile base station collecting data from replicated sensor nodes

2. AN EXTREME SCENARIO IN WIRELESS SENSOR NETWORKS APPLICATION

Consider a scenario where a Wireless Sensor Network is deployed in a remote area deprived of communication infrastructures, and perhaps under hostile control. Static deployment of base stations is avoided for several reasons, including possible seizure by an adversary. Instead, data are collected by a mobile base station carried by a vehicle, most probably an aircraft or a drone. The mobile base station visits the area sporadically, and each time it polls the individual sensor nodes by establishing wireless communication (Fig. 1). It can be expected that some sensors, whose number is bounded by $z<n$, fail to respond due to hardware failures, permanent or temporary battery depletion, radio jamming, shadowing obstacles, or even because they were seized or destroyed by an adversary.

Every sensor collects data, which it encodes into an appropriate erasure code producing n fragments, and stores a unique fragment, out of the above n, in the internal memory. As sensor nodes store fragments, rather than whole data, the memory requirements are substantially decreased, and the probability of memory overflows occurring between visits of the mobile base stations is also decreased. Sensor nodes are replicated, and the same data are independently collected by n nodes, each of which stores a different encoded fragment. When it succeeds in establishing a wireless connection with the mobile base station, every sensor node fetches and uploads the locally resident fragment. There is no communication between sensor nodes, which stay silent except for the short time needed to transfer data to the mobile base station. The erasure code guarantees that data can be reconstructed, provided an arbitrary subset of $n-z$ encoded fragments is successfully uploaded.

However, it should be considered that replicated sensor nodes which independently collect the same data might be somehow apart from each other and under slightly different environmental conditions (e.g., temperature), and they might be activated at slightly different times. Further, in every sensing node, data transduction is within some non-zero tolerance. Thus, it is unavoidable that different sensor nodes acquire slightly different values for the same data; that is, under reasonable assumptions, that they produce slightly different integers. As every sensor node stores an encoded fragment of the locally acquired data, every fragment

may slightly deviate from the unknown, exact value; that is it could bear a small error. This imposes the requirement that the erasure code should be able to reconstruct the exact value, within a small tolerance, from fragments each of which may bear a small error; i. e., it should tolerate small errors of arbitrary multiplicity. The ability to tolerate erasures and small errors should be kept when a bounded number of fragments bear errors of unrestricted magnitude that cannot be otherwise detected. In fact, unrestricted errors may occur due to node or communication failures, or to intrusions. It will be shown that the preceding requirements are fulfilled by the erasure code that will be presented in the following of this paper.

Beside error tolerance and correction, the new erasure code also incorporates basic data safety: in fact, data reconstruction requires availability of an arbitrary subset of *n-z* encoded fragments, out of the set of *n* fragments that were generated, and there is no way to even guess the data from a smaller fragment subset. Further, every fragment is encoded with a key (actually a modulus in the residue code) which is tied to the encoding node and is known to the remote decoder, but can be kept secret otherwise. The above properties can be complemented with customary countermeasures, such as encryption of transmitted fragments, periodical scrambling of the node identifiers, tamper-resisting design of nodes to prevent extraction of secrets, intentionally seeded dummy nodes to disguise the adversary, and the like.

3. RESIDUE ENCODING WITH NON-PAIRWISE-PRIME MODULI

Let $\mathcal{M} \equiv \{m_1, m_2, \ldots, m_n\}$ be a set of positive integers, called *moduli*, $M = lcm(\mathcal{M})$ be the least common multiple of the moduli in set $\mathcal{M}$ and $d_{ij} = d_{ji} = gcd(m_i, m_j)$ be the greatest common divisor of the moduli m_i, m_j, with $d_{ij} > 1$ for at least one pair i,j. For any integer x, denote by $x_i = |x|_{mi}$ the residue of x modulo m_i $(1 \le i \le n)$. A number system representing integers as *n-tuples* of residues modulo $m_1, m_2, \ldots, m_n$ is called a *Residue Number System with Non-Pairwise-Prime Moduli (RNS-NPM).*

RNS-NPM were introduced in [15] and later rediscovered in [16]. It is known that the *RNS-NPM* with $\mathcal{M} \equiv \{m_1, m_2, \ldots, m_n\}$ provides unique representation of integers in the range $[0, M)$, called *legitimate range.* Integers in this range are called *legitimate.*

From the simultaneous congruences $x \equiv x_i \pmod{m_i}$ and $x \equiv x_j \pmod{m_j}$ it follows [17]:

$$x_i - x_j \equiv 0 \pmod{d_{ij}}. \tag{1}$$

N-tuples satisfying congruence (1) for every i, j with $1 \le i, j \le n: i \ne j$ are called *consistent n-tuples*; any other *n-tuple* is said to be *inconsistent*. Any integer in $[0, M)$ is represented by a n-tuple, which is unique. Conversely, every consistent n-tuple is the representation of a unique integer x in $[0, M)$.

Given any consistent n-tuple $X \equiv \{x_1, x_2, \ldots, x_n\}$, the integer x represented by X, denoted $x = \rho(X)$, can be reconstructed via the *Generalized Chinese Remainder Theorem* [18] as:

$$x = \left| \sum_{i=1,n} c_i x_i \frac{M}{m_i} \right|_M ,$$

with $c_i = \left(\frac{m_i}{\mu_i} \right) \cdot \left(\frac{M}{\mu_i} \right)_{inv}$, where $\mu_i > 1$ divides m_i, $\prod_{i=1,n} \mu_i = M$, and $\left(\frac{M}{\mu_i} \right)_{inv}$ denotes the

multiplicative inverse of $\frac{M}{\mu_i}$ modulo μ_i, .

From now on, we consider the notable class of *D-RNS-NPM*, also introduced in [15], where all integers in $\mathcal{D} \equiv \{d_{ij} \mid 1 \le i < n;\ i < j \le n\}$ are pairwise prime and greater than 1, and $m_i = \prod_{j=1,n;j\neq i} d_{ij}$. It is immediate that $M = \prod_{1\le i<n;i<j\le n} d_{ij}$ and $\prod_{i=1,n} m_i = M^2$, since every $d_{ij} = d_{ij}$ divides two moduli in $\mathcal{M}$.

An *error* borne by digit x_i $(0 \le i \le n)$ is an integer e_i, with $0 \le e_i \le m_i$, under which x_i is transformed into $\underline{x}_i = |x_i + e_i|_{mi}$. The *n-tuple* $E \equiv \{e_1, e_2, \ldots, e_n\}$ is called an *error n-tuple,* and the number of non-zero errors in E is called the *error multiplicity.*

From $\underline{x}_i = |x_i + e_i|_{mi}$, $\underline{x}_j = |x_j + e_j|_{mj}$ it follows [17]:

$$\underline{x}_i \equiv x_i + e_i \ (mod\ d_{ij});\quad \underline{x}_j \equiv x_j + e_j \ (mod\ d_{ij})$$

and, introducing *(1)*:

$$\underline{x}_i - \underline{x}_j \equiv e_i - e_j \ (mod\ d_{ij}) \qquad (2)$$

From *(2)* it is seen that the $\underline{X} \equiv \{\underline{x}_1, \underline{x}_2, \ldots \underline{x}_n\}$ is consistent if and only if $E \equiv \{e_1, e_2, \ldots, e_n\}$ is consistent. If E is inconsistent, the error is detected from the failure of the *consistency check* of $\underline{X}$; otherwise the error cannot be detected and reconstructing $\underline{X}$ yields integer $\underline{x} = |\rho(X) + \rho(E)|_M$, where $\rho(X) = x$ and $\rho(E) = 0$ only if $e_i = 0$ for every i. In [15] it was shown that *D-RNS-NPM's* are unable to detect all errors of given multiplicity, beyond multiplicity *1;* that is, the consistency check of $\underline{X}$ may not fail if the multiplicity of E is greater than *1*. However, errors of arbitrary multiplicity are detected with extremely high probability. In fact, the number l of error n-tuples that cannot be detected is equal to the number M of legitimate n-tuples, whereas the total number t of error n-tuples is $\prod_{i=1,n} m_i = M^2$, and thus, assuming random errors, the probability that an arbitrary error is detected is $1 - l/t = 1 - 1/M$.

The ability of *D-RNS-NPM* to reconstruct $x = \rho(X)$ from $\underline{X} \equiv \{\underline{x}_1, \underline{x}_2, \ldots \underline{x}_n\}$, was investigated in [15] assuming bounded error multiplicity. However, in view of the application sketched in Section 2, this paper is concerned with the ability of *D-RNS-NPM* to *tolerate* a bounded number of digit *erasures*, combined with *small errors* borne by an arbitrary number of digits and, possibly, *unrestricted errors* borne by a bounded number of digits. Erasures occur when l digits in X are lost, thus leaving an *available* (*n-l)-tuple A,* with $l > 0$. Erasures are said to be tolerated if $\rho(A) = \rho(X)$; i.e. the given number can be reconstructed exactly from the available (n-l)-tuple. If the available digits bear errors, either small or unrestricted, erasures combined with errors are said to be tolerated if $x = \rho(X)$ can be *guessed* from the available (n-l)-tuple $\underline{A}$, which may be inconsistent, within an approximation of $\pm\delta$ from x, where δ is a small integer. A precise definition of *small errors* and a bound to δ will be provided in the subsequent Sections.

4. TOLERATING ERASURES

Consider the *D-RNS-NPM* with $\mathcal{M} \equiv \{m_1, m_2, \ldots, m_n\}$ and the consistent n-tuple $X \equiv \{x_1, x_2, \ldots, x_n\}$ representing any legitimate integer x, and assume that l digits in this *n-tuple* are unavailable, while the remaining n-l digits are available and correct. The unavailable digits

are said to be *erased*, and the resulting error is called an *erasure* of multiplicity l. Equivalently, it is said that l erasures occur. The (n-l)-tuple of the available digits is denoted A.

Definition 1. *An erasure of multiplicity l is said to be tolerated if number $x = \rho(X)$ can be reconstructed exactly from the available (n-l)-tuple A.*

In order to derive the condition under which the given *D-RNS-NPM* tolerates erasures of bounded multiplicity, the following notations are introduced:

- $\#\mathcal{X}$ denotes the cardinality of set $\mathcal{X}$;
- $\mathcal{M}^p \subseteq \mathcal{M}$ denotes any subset of set $\mathcal{M}$ with $\#\mathcal{M}^p = p$;
- $\mathcal{F}^p \equiv \{\mathcal{M}^p \mid \mathcal{M}^p \subseteq \mathcal{M}; \#\mathcal{M}^p = p\}$ is the collection of all the subsets of cardinality p of set $\mathcal{M}$;
- $lcm\,(\mathcal{M}^p)$ is the least common multiple of the moduli in set $\mathcal{M}^p$.
- $\min_{\mathcal{M}^p \in \mathcal{F}^p} lcm(\mathcal{M}^p)$ is the minimum of $lcm(\mathcal{M}^p)$ over collection $\mathcal{F}^p$

The condition under which *D-RNS-NPM's* tolerate up to z erasures in any consistent n-tuple $X \equiv \{x_1, x_2, \ldots, x_n\}$ is stated by the following theorem:

Theorem 1. *The D-RNS-NPM with $\mathcal{M} \equiv \{m_1, m_2, \ldots, m_n\}$ and $M = lcm\,(\mathcal{M})$ tolerates erasures up to multiplicity z if the legitimate range is set to $\tilde{M}$, with $\tilde{M} = \min_{\mathcal{M}^{n-z} \in \mathcal{F}^{n-z}} lcm(\mathcal{M}^{n-z})$.*

Proof. Let $X \equiv \{x_1, x_2, \ldots, x_n\}$ be the consistent n-tuple representing an arbitrary integer x in the given *D-RNS-NPM,* and assume that l erasures occur, with $l \le z$. For the ease of notation and without any loss of generality assume that the erased digits are $x_{n-l+1}, \ldots, x_n$, and denote by $A \equiv \{x_1, x_2, \ldots, x_{n-l}\}$ the available (n-l)-tuple. As X is consistent, A is also consistent. Considering that the *RNS-NPM* with $\mathcal{M}_{av} \equiv \{m_1, m_2, \ldots, m_{n-l}\}$ has range $M_{av} = [0, lcm\,(\mathcal{M}_{av}))$ and $M_{av} \ge \tilde{M}$, this *RNS-NPM* is able to provide a unique representation of any integer in the range $[0, \tilde{M})$, and the given integer x can be reconstructed exactly as $\rho(A)$ via the Generalized Chinese Remainder Theorem. •

If $z = 1$, observe that $\tilde{M} = M$, since $\min_{\mathcal{M}^{n-1} \in \mathcal{F}^{n-1}} lcm(\mathcal{M}^{n-1}) = M$.

An insight in the redundancy structure enabling the *D-RNS-NPM's* to tolerate multiple erasures is provided by Fig. 2, where $n = 6$ and $\mathcal{M} \equiv \{m_1, m_2, m_3, m_4, m_5, m_6\}$. Letting $x_{ij} = |x_i|_{dij}$, and considering that $m_i = \prod_{j=1, 6; j \ne i} p_{ij}$ and all divisors in $\mathcal{D}$ are pairwise prime, the residue digit x_i can be given the residue representation $X_i \equiv \{x_{ij} \mid 1 \le j \le 6;\ j \ne i\}$, where X_i is a 5-tuple of *subdigits*. Since $x_{ij} = x_{ji}$, $\mathcal{X}' \equiv \{X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5 \cup X_6\}$, or equivalently $\mathcal{X}' \equiv \{x_{ij} \mid 1 \le i < 6;\ i < j \le 6\}$, is a $\binom{6}{2}$-uple providing an alternate residue representation of the given x, and this representation is non-redundant. Observe that every x_{ij} is replicated in X_i and X_j, since $x_{ij} = x_{ji}$, and that the redundancy of the given *D-RNS-NPM* resides in this replication. Assuming that digits x_4, x_5, x_6 are erased, x_{ij} is lost only if both replicas of it reside in the lost digits ; that is, if both $i \ge 4$ and $j \ge 4$. If $i \le 3$, x_{ij} is available from X_i for every j, and, if $i \le 3$ and

$j \le 3$, x_{ij} is available from both X_i and X_j. Thus, the given x can be reconstructed from the available subdigits if x is in the range $\left[0, \prod_{i=1,3;j=i,6;j\neq i} p_{ij}\right)$ or, equivalently, in the range *[0, lcm* (m_1, m_2, m_3)*)*. If a single digit, say x_6, is erased, then a replica of x_{i6} is available from X_i for every $1 \le i \le 5$, and single erasures are tolerated for every integer in the range *[0, M).*

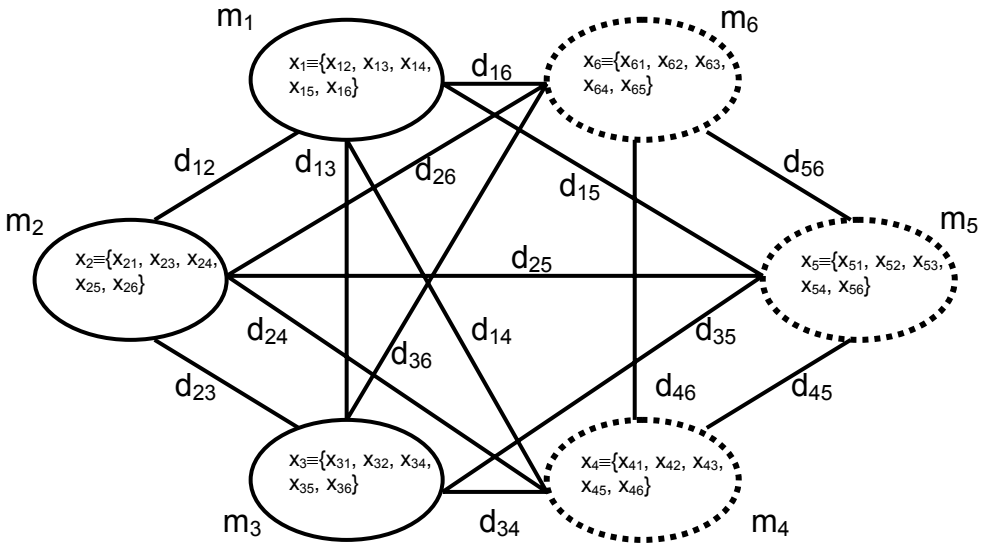

Fig. 2: A D-RNS-NPM with 6 moduli tolerating 3 erasures

5. TOLERATING SMALL ERRORS COMBINED WITH ERASURES

Consider the *D-RNS-NPM* with $\mathcal{M}\equiv\{m_1, m_2, \ldots, m_n\}$ and $M=lcm(\mathcal{M})$, and let $\tilde{M} = \min_{\mathcal{M}^{n-z}\in\mathcal{F}^{n-z}} lcm(\mathcal{M}^{n-z})$. From Theorem 1, the given *D-RNS-NPM* tolerates erasures up to multiplicity z. Assume that an erasure of multiplicity l occurs, with $0 \le l \le z$, and, for the ease of notation and without any loss of generality, that the erased digits are $x_{n-l+1}, x_{n-l+2}, \ldots, x_n$. Assume also that the erasure is combined with errors of unbounded multiplicity, and denote by $E\equiv\{e_1, e_2, \ldots, e_{n-l}\}$ the error (n-l)-tuple, with $e_i \neq 0$ for at least one i. Let $\underline{A}\equiv\{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$ be the (n-l)-tuple of the available digits, where $\underline{x}_j = |x_i + e_i|_{mi}$ bears error e_i. Although error correction is generally prevented by the unbounded error multiplicity [15], it will be shown that *small* errors of arbitrary multiplicity are alway*s tolerated.*

Definition 2. *Error* e_i *borne by digit* x_i *is said to be small if* $abs(e_i) \le \delta$*, with* $\delta < \frac{1}{4}\min_{d_{hk}\in\mathcal{D}} d_{hk}$.

Error (n-l)-tuple E is said to be small if inequality $abs(e_i) \le \delta$ *holds for every i with* $1 \le i \le n\text{-}l$.

Definition 3. *Error (n-l)-tuple E is said to be tolerated if there exists a legitimate number derived from* $\underline{A}\equiv\{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$*, which is within an approximation of* $\pm\delta$ *from* $x=\rho(X)$.

Reconsider congruence *(2),* equivalent to:

$$|\underline{x}_i - \underline{x}_j + 2\delta|_{dij} = |e_i - e_j + 2\delta|_{dij}, \qquad (2')$$

and let:

$$\gamma_{ij} = |\underline{x}_i - \underline{x}_j + 2\delta|_{dij} - 2\delta \qquad (3)$$

that is, from *(2')*:

$$\gamma_{ij} = |e_i - e_j + 2\delta|_{dij} - 2\delta. \qquad (4)$$

With the preceding notation:

Definition 4. *Set $\Gamma \equiv \{\gamma_{ij} : 0 \le i,j \le n\text{-}l;\ i \ne j\}$ is called the syndrome of error (n-l)-tuple E.*

Definition 5. *Given $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \dots, \underline{x}_{n-l}\}$, with $\underline{A}$ inconsistent, and any $\underline{x}_s \in \underline{A}$, called a seed, the guess G(s, $\underline{A}$) of $X \equiv \{x_1, x_2, \dots, x_{n-l}\}$ under error (n-l)-tuple E, constructed with seed $\underline{x}_s$, is defined as the (n-l)-tuple $G(s, \underline{A}) \equiv \{\xi_1^s, \xi_2^s, \dots, \xi_{n-l}^s\}$ with:*

$$\xi_i^s = |x_i + \varepsilon_i^s|_{mi}; \qquad (1 \le i \le n-l),$$

and:

$$\underline{\varepsilon}_i^s = e_i - \underline{e}_i^s; \quad \underline{e}_s^s = \left\lceil \frac{1}{n-l} \sum_{j=1,n-l;j\ne s} \gamma_{sj} \right\rceil; \quad \underline{e}_j^s = \underline{e}_s^s - \gamma_{sj} \ (j \ne s)$$

Under the hypothesis of small errors, $0 \le e_i - e_j + 2\delta \le 4\delta < d_{ij}$, from which $|e_i - e_j + 2\delta|_{dij} = e_i - e_j + 2\delta$. Thus *(4)* becomes :

$$\gamma_{ij} = e_i - e_j \qquad (5)$$

and:

$$abs(\gamma_{ij}) \le 2\delta; \qquad \gamma_{ij} = -\gamma_{ji}. \qquad (6)$$

The following Lemma provides a preliminary result to Theorem 2:

Lemma 2.1. *In the D-RNS-NPM with $\mathcal{M} \equiv \{m_1, m_2, \dots, m_n\}$ and $M = lcm(\mathcal{M})$, consider any $X \equiv \{x_1, x_2, \dots, x_n\}$ where $l \le z$ digits (without any loss of generality, digits $x_{n-l+1}, x_{n-l+2}, \dots, x_n$) are erased, and let $\mathcal{M}_{av} \equiv \{m_1, m_2, \dots, m_{n-l}\}$ with $M_{av} = lcm(\mathcal{M}_{av})$. If $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \dots, \underline{x}_{n-l}\}$ bears the small error (n-l)-tuple $E \equiv \{e_1, e_2, \dots, e_{n-l}\}$ and $\underline{A}$ is inconsistent, then the guess G(s, $\underline{A}$) of X is a consistent (n-l)-tuple for arbitrary $\underline{x}_s \in \underline{A}$, and the integer $\rho(G(s, \underline{A}))$ reconstructed in the D-RNS-NPM of moduli $\mathcal{M}_{av} \equiv \{m_1, m_2, \dots, m_{n-l}\}$ is equal to $|x + \varepsilon|_{Mav}$ with $abs(\varepsilon) \le \delta$.*

Proof. Select arbitrarily $\underline{x}_s \in \underline{A}$. From Definition 5, $\underline{e}_s^s = \left\lceil \frac{1}{n-l} \sum_{j=1,n-l;j\ne s} \gamma_{sj} \right\rceil$ and also, introducing (5) and $\varepsilon = \left\lfloor \frac{1}{n-l} \sum_{j=1,n-l} e_j \right\rfloor$:

$$\underline{e}_s^s = \left\lceil e_s - \frac{1}{n-l} \sum_{j=1,n-l} e_j \right\rceil = e_s - \varepsilon,$$

where $abs(\varepsilon) \le \delta$, since $\frac{1}{n-l}\sum_{j=1,n-l} e_j$ is the average of errors in $E \equiv \{e_1, e_2, \ldots, e_{n-l}\}$ and $abs(e_j) \le \delta$ for every j.

Combining $\underline{e}_j^s = \underline{e}_s^s - \gamma_{sj}$; $\gamma_{sj} = e_s - e_j$; $\underline{e}_s^s = e_s - \varepsilon$ yields $\underline{e}_j^s = e_j - \varepsilon$ for every j with $1 \le j \le n-l$; $j \ne s$, and since $\underline{e}_s^s = e_s - \varepsilon$ also holds, it follows that $\underline{\varepsilon}_j^s = e_j - \underline{e}_j^s = \varepsilon$ for every j with $1 \le j \le n\text{-}l$. Recalling from Definition 5 that $\xi_j^s = |x_j + \underline{\varepsilon}_j^s|_{mj}$ for every j with $1 \le j \le n\text{-}l$, this implies that $G(s, \underline{A}) \equiv \{\xi_1^s, \xi_2^s, \ldots, \xi_{n-l}^s\}$ is the sum of (n-l)-tuples $X \equiv \{x_1, x_2, \ldots, x_{n-l}\}$ and $E' \equiv \{\underline{\varepsilon}_j^s \mid \underline{\varepsilon}_j^s = \varepsilon\ (1 \le j \le n\text{-}l)\}$. It is immediate that $\rho(E') = \varepsilon$ and, since the given *D-RNS-NPM* tolerates z erasures and $l \le z$, $\rho(X) = x$. It follows that $\rho(G(s, \underline{A})) = |x + \varepsilon|_{Mav}$ with $abs(\varepsilon) \le \delta$. •

We are now ready to introduce the following theorem:

Theorem 2. *Consider the D-RNS-NPM with* $\mathcal{M} \equiv \{m_1, m_2, \ldots, m_n\}$, $M = lcm(\mathcal{M})$ *and let* $\tilde{M} = \min_{\mathcal{M}^{n-z} \in \mathcal{F}^{n-z}} lcm(\mathcal{M}^{n-z})$. *In this D-RNS-NPM, erasures of multiplicity* $l \le z$ *combined with small errors of arbitrary multiplicity are always tolerated, provided the legitimate range is set to* $[\delta, \tilde{M} - \delta)$.

Proof. Consider any $X \equiv \{x_1, x_2, \ldots, x_n\}$, with $\rho(X) \in [\delta, \tilde{M} - \delta)$, and let $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$ be the available (n-l)tuple, where error e_i borne by digit $\underline{x}_i$ is small for every i $(1 \le i \le n - l)$.

If $\underline{A}$ is consistent, from $abs(e_i) \le \delta$, $abs(e_j) \le \delta$ and $\delta < \frac{1}{4}\min_{d_{ij} \in \mathcal{D}} d_{ij}$, it follows $abs(e_i - e_j) < d_{ij}$ or $abs(e_j - e_i) < d_{ij}$, and $e_i - e_j \equiv 0 \pmod{d_{ij}}$ implies $e_i = e_j = \varepsilon$, where $\varepsilon < \delta$ for every i,j with $1 \le i,j \le n - l$. Hence $\rho(\{e_1, e_2, \ldots, e_{n-l}\}) = \varepsilon$ and, since $\underline{A}$ is the sum of (n-l)-tuples $X \equiv \{x_1, x_2, \ldots, x_{n-l}\}$ and $E \equiv \{e_1, e_2, \ldots, e_{n-l}\}$, $\rho(\underline{A}) = \left|\rho(\{x_1, x_2, \ldots, x_{n-l}\}) + \rho(\{e_1, e_2, \ldots, e_{n-l}\})\right|_{Mav}$; that is, $\rho = \rho(\underline{A}) = |x + \varepsilon|_{Mav}$, with $abs(\varepsilon) \le \delta$.

If $\underline{A}$ is inconsistent, let $G(s, \underline{A})$ be the guess of X constructed with arbitrary $\underline{x}_s \in \underline{A}$: from Lemma 2.1, $G(s, \underline{A})$ is consistent and can be reconstructed in the *D-RNS-NPM* with $\mathcal{M}_{av} \equiv \{m_1, m_2, \ldots, m_{n-l}\}$ and $M_{av} = lcm(\mathcal{M}_{av})$, yielding $\rho = \rho(G(s, \underline{A})) = |x + \varepsilon|_{Mav}$ with $abs(\varepsilon) \le \delta$.

In both cases, $x + \varepsilon$ is in the range $[0, \tilde{M})$ since x is in the range $[\delta, \tilde{M} - \delta)$ and $abs(\varepsilon) \le \delta$, and this implies $\rho = x + \varepsilon$ since $\tilde{M} \le M_{av}$. Letting $g = x + \varepsilon$ and redefining $g = \delta$ if $\rho < \delta$, or $g = \tilde{M} - \delta - 1$ if $\rho \ge \tilde{M} - \delta$, it is immediate that integer g is legitimate and $abs(g - x) \le \delta$. •

6. TOLERATING UNRESTRICTED ERRORS COMBINED WITH SMALL ERRORS AND ERASURES

The notable result of Theorem 2 relies on the assumption of small errors. This assumption will now be removed, and the combined occurrence of unrestricted errors, small errors and erasures will be considered. For the sake of simplicity, consideration will be limited to the case of a single unrestricted error.

Consider again the *D-RNS-NPM* with $\mathcal{M} \equiv \{m_1, m_2, \ldots, m_n\}$, $M = lcm(\mathcal{M})$ and $\tilde{M} = \min_{\mathcal{M}^{n-z} \in \mathcal{F}^{n-z}} lcm(\mathcal{M}^{n-z})$. Given integer $X \equiv \{x_1, x_2, \ldots, x_n\}$, assume that $l \le z$ digits are erased

and, for the ease of notation, that the available digits are those in set $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$, where $\underline{x}_i = |x_i + e_i|_{m_i}$ and $E \equiv \{e_1, e_2, \ldots, e_{n-l}\}$ is the error *(n-l)-tuple*. Assume also that $\underline{A}$ is inconsistent and that the unique unrestricted error is borne by the unidentified digit $\underline{x}_k$, with $0 \le k \le n-l$.

Consider the syndrome $\Gamma \equiv \{\gamma_{ij} \mid 0 \le i,j \le n-l;\ i \ne j\}$ of E, where γ_{ij} satisfies *(5)* and *(6)* if $i,j \ne k$, since e_i and e_j are small errors. However, if $i = k$, from $\gamma_{kj} = |e_k - e_j + 2\delta|_{d_{kj}} - 2\delta$, $\gamma_{jk} = |e_j - e_k + 2\delta|_{d_{kj}} - 2\delta$, the following equations hold for every j with $1 \le j \le n-l,\ j \ne k$:

$$\gamma_{kj} = e_k - e_j - p_{kj} d_{kj}; \quad \gamma_{jk} = e_j - e_k - p_{jk} d_{kj}; \quad (1 \le j \le n-l,\ j \ne k), \qquad (7)$$

where p_{kj} and p_{jk} are unique integers such that $0 \le e_k - e_j + 2\delta - p_{kj} d_{kj} < d_{kj}$ and $0 \le e_j - e_k + 2\delta - p_{jk} d_{kj} < d_{kj}$. Observe that inequalities $abs(\gamma_{kj}) \le 2\delta$, $abs(\gamma_{jk}) \le 2\delta$, as well as equation $\gamma_{kj} = -\gamma_{jk}$, may not hold. However, $\gamma_{kj} = -\gamma_{jk}$ holds if $abs(\gamma_{kj}) \le 2\delta$ and $abs(\gamma_{jk}) \le 2\delta$. In fact, $\gamma_{kj} + \gamma_{jk} = -(p_{kj} + p_{jk}) d_{kj}$ from *(7)*, and $p_{kj} + p_{jk} = 0$ since $abs(\gamma_{kj} + \gamma_{jk}) \le 4\delta < d_{kj}$.

Consider the guess $G(s, \underline{A})$ of $X \equiv \{x_1, x_2, \ldots, x_{n-l}\}$ constructed from $\underline{A}$ with seed $\underline{x}_s \in \underline{A}$, as defined in Definition 5: $G(s, \underline{A})$ may be inconsistent since Lemma 2.1 does not hold due to the unrestricted error borne by the unidentified digit $\underline{x}_k$. In other words, congruence $\xi_i^s - \xi_j^s \equiv 0 \ (mod\ d_{ij})$ may not hold for some i, j with $1 \le i,j \le n-l;\ i \ne j$.

The cases where $abs(\gamma_{ij}) > 2\delta$ for at least one $\gamma_{ij} \in \Gamma$, or where there exists at least one guess $G(s, \underline{A})$ which is inconsistent, are favourable ones, since digit $\underline{x}_k$ can be identified or, at least, confined within a small subset of set $\underline{A}$, called a *Suspect Set.* This result is stated by Lemma 3.1 and Lemma 3.2 which, respectively, construct the Suspect Set S_Γ implied by syndrome Γ and the Suspect Set S_G implied by some inconsistent guess $G(s, \underline{A})$.

Definition 6. *Let $\{\underline{x}_i, \underline{x}_j\}$ be any pair of digits in $\underline{A}$ with $1 \le i,j \le n-l;\ i \ne j$, such that $abs(\gamma_{ij}) > 2\delta$ or $abs(\gamma_{ji}) > 2\delta$, and Σ be the collection of all such pairs. Then the Suspect Set implied by syndrome Γ is a subset $S_\Gamma \subseteq \underline{A}$, defined as* $S_\Gamma = \bigcup_{\{\underline{x}_i, \underline{x}_j\} \in \Sigma} \{\underline{x}_i, \underline{x}_j\}$.

Lemma 3.1. *If there exist at least one pair $\{\underline{x}_i, \underline{x}_j\} \subseteq \underline{A}$ such that $abs(\gamma_{ij}) > 2\delta$ or $abs(\gamma_{ji}) > 2\delta$, then the cardinality of S_Γ is 1 or 2 and $\underline{x}_k \in S_\Gamma$.*

Proof. If $\underline{x}_i$ and $\underline{x}_j$ bear small errors, then $abs(\gamma_{ij}) \le 2\delta$ and $abs(\gamma_{ji}) \le 2\delta$ from (6). Thus, $abs(\gamma_{ij}) > 2\delta$ implies that either $\underline{x}_i = \underline{x}_k$ or $\underline{x}_j = \underline{x}_k$, where $\underline{x}_k$ is the unique, unidentified digit bearing an unrestricted error. Assume that there exists $\{\underline{x}_i, \underline{x}_j\}$ with $abs(\gamma_{ij}) > 2\delta$ or $abs(\gamma_{ji}) > 2\delta$: if such pair is unique, then $S_\Gamma \equiv \{\underline{x}_i, \underline{x}_j\}$, and $\underline{x}_k = \underline{x}_i$ or $\underline{x}_k = \underline{x}_j$. Otherwise, consider any $\{\underline{x}_p, \underline{x}_q\}$, distinct from $\{\underline{x}_i, \underline{x}_j\}$, such that $abs(\gamma_{pq}) > 2\delta$ or $abs(\gamma_{qp}) > 2\delta$: by the same reasoning, must be either $\underline{x}_p = \underline{x}_k$ or $\underline{x}_q = \underline{x}_k$, and $S_\Gamma = \{\underline{x}_i, \underline{x}_j\} \cap \{\underline{x}_p, \underline{x}_q\} = \{\underline{x}_k\}$ since pairs $\{\underline{x}_i, \underline{x}_j\}$ and $\{\underline{x}_p, \underline{x}_q\}$ are distinct. •

Definition 7. *Given $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$ and any guess $G(s, \underline{A})$ with $\underline{x}_s \in \underline{A}$ and $G(s, \underline{A})$ inconsistent, let $\{i, j\}$ be any pair with $1 \le i,j \le n-l;\ i \ne j$, such that $\xi_j^s - \xi_k^s \not\equiv 0 \ (mod\ d_{ij})$, and Σ' be the collection of all such pairs. Then the Suspect Set S_G implied by $G(s, \underline{A})$ is a subset $S_G \subseteq \underline{A}$, defined as* $S_G = \left(\bigcap_{\{i,j\} \in \Sigma'} \{\underline{x}_i, \underline{x}_j\} \right) \cup \{\underline{x}_s\}$.

Lemma 3.2. *Given* $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$, *assume that the unidentified digit* $\underline{x}_k$ *bears an unrestricted error, and that the guess* $G(s, \underline{A})$ *constructed with seed* $\underline{x}_s \in \underline{A}$ *is inconsistent. Then the cardinality of the Suspect Set* S_G *is at most 3 and* $\underline{x}_k \in S_G$.

Proof. Since d_{ij} divides both m_i and m_j, congruences $\xi_i^s \equiv x_i + \varepsilon_i^s \pmod{d_{ij}}$ and $\xi_j^s \equiv x_j + \varepsilon_j^s \pmod{d_{ij}}$ are immediate from Definition (5), and this implies $\xi_i^s - \xi_j^s \equiv \varepsilon_i^s - \varepsilon_j^s \pmod{d_{ij}}$ since $x_i - x_j \equiv 0 \pmod{d_{ij}}$. As a preliminary step in the proof, the following Propositions are introduced:

Proposition 3.2.1: *If* $G(s, \underline{A}) \equiv \{\xi_1^s, \xi_2^s, \ldots, \xi_{n-l}^s\}$ *is inconsistent and* $s \neq k$, *then* $\xi_i^s - \xi_j^s \not\equiv 0 \pmod{d_{ij}}$ *may hold only if* $i,j \neq s$ *and* $i = k$ *or* $j = k$.

If $i,j \neq s$ and $i,j \neq k$, $\varepsilon_i^s - \varepsilon_j^s = e_i - \underline{e}_s^s + \gamma_{si} - (e_j - \underline{e}_s^s + \gamma_{sj})$ from Definition (5) and $\gamma_{si} = e_s - e_i$, $\gamma_{sj} = e_s - e_j$ from (5): this implies $\varepsilon_i^s - \varepsilon_j^s = 0$, and also $\xi_i^s - \xi_j^s = 0$.

If $i = s \neq k$ and $j \neq k$, $\varepsilon_s^s - \varepsilon_j^s = e_s - \underline{e}_s^s - (e_j - \underline{e}_s^s + \gamma_{sj})$ from Definition (5) and $\gamma_{sj} = e_s - e_j$ from (5): this implies $\varepsilon_s^s - \varepsilon_j^s = 0$, and $\xi_i^s - \xi_j^s = 0$. Similarly if $j = s \neq k$ and $i \neq k$.

If $i = s + k$ and $j = k$, $\varepsilon_s^s - \varepsilon_k^s = e_s - \underline{e}_s^s - (e_k - \underline{e}_s^s + \gamma_{sk})$ from Definition (5) and $\gamma_{sk} = e_s - e_k - p_{sk} d_{sk}$ from (7), and thus $\varepsilon_s^s - \varepsilon_k^s = p_{sk} d_{sk}$: this implies $\varepsilon_s^s - \varepsilon_k^s \equiv 0 \pmod{d_{sk}}$, and $\xi_i^s - \xi_j^s \equiv 0 \pmod{d_{sk}}$. Similarly if $j = s \neq k$ and $i = k$.

In conclusion, $\xi_i^s - \xi_j^s \not\equiv 0 \pmod{d_{ij}}$ cannot hold, unless $i,j \neq s$ and $i = k$ or $j = k$.

Proposition 3.2.2: *If* $G(s, \underline{A}) \equiv \{\xi_1^s, \xi_2^s, \ldots, \xi_{n-l}^s\}$ *is inconsistent and* $s = k$, *then* $\xi_i^k - \xi_j^k \not\equiv 0 \pmod{d_{ij}}$ *only if* $i,j \neq k$.

If $i = k$, $\varepsilon_k^k - \varepsilon_j^k = e_k - \underline{e}_k^k - (e_j - \underline{e}_k^k + \gamma_{kj})$ from Definition (5) and, since error e_k is unrestricted, $\gamma_{kj} = e_k - e_j - p_{kj} d_{kj}$ from (7). It follows $\varepsilon_k^k - \varepsilon_j^k = p_{kj} d_{kj}$ and $\varepsilon_k^k - \varepsilon_j^k \equiv 0 \pmod{d_{kj}}$. Similarly if $j = k$. Since $\xi_i^k - \xi_j^k \equiv \varepsilon_i^k - \varepsilon_j^k \pmod{d_{ij}}$, $\xi_i^k - \xi_j^k \not\equiv 0 \pmod{d_{ij}}$ cannot hold unless $i,j \neq k$.

Now, assume that the guess $G(s, \underline{A})$ constructed with seed $\underline{x}_s \in \underline{A}$ is inconsistent, and that $\xi_i^s - \xi_j^s \not\equiv 0 \pmod{d_{ij}}$. Consider the following cases:

Case a): $s \neq k$. If $\xi_p^s - \xi_q^s \equiv 0 \pmod{d_{pq}}$ for every $\{p, q\}$ with $p \neq i, j$ or $q \neq i,j$, then $S_G \equiv \{\underline{x}_i, \underline{x}_j, \underline{x}_s\}$ by Definition 7 and, from Proposition 3.2.1, must be $\underline{x}_k = \underline{x}_i$ or $\underline{x}_k = \underline{x}_j$.

If there exists $\{p, q\}$ with $p \neq i, j$ or $q \neq i,j$ such that $\xi_p^s - \xi_q^s \not\equiv 0 \pmod{d_{pq}}$, by Proposition 3.2.1 must be either $\underline{x}_p = \underline{x}_k$ or $\underline{x}_q = \underline{x}_k$, and $\{\underline{x}_i, \underline{x}_j\} \cap \{\underline{x}_p, \underline{x}_q\} = \{\underline{x}_k\}$. This implies $S_G \equiv \{\underline{x}_k, \underline{x}_s\}$.

Case b): $s = k$. If $\xi_p^s - \xi_q^s \equiv 0 \pmod{d_{pq}}$ for every $\{p, q\}$ with $p \neq i, j$ or $q \neq i,j$, $S_G \equiv \{\underline{x}_i, \underline{x}_j, \underline{x}_k\}$ by definition (7), and $\underline{x}_i \neq \underline{x}_k$, $\underline{x}_j \neq \underline{x}_k$ from Proposition 3.2.1.

If there exists $\{p, q\}$ with $p \neq i, j$ or $q \neq i,j$ such that $\xi_p^s - \xi_q^s \not\equiv 0 \pmod{d_{pq}}$, by Proposition 3.2.1 $\underline{x}_p \neq \underline{x}_k$ and $\underline{x}_q \neq \underline{x}_k$ and, since $\{\underline{x}_i, \underline{x}_j\}$ and $\{\underline{x}_p, \underline{x}_q\}$ are distinct, either $\{\underline{x}_i, \underline{x}_j\} \cap \{\underline{x}_p, \underline{x}_q\} = \varnothing$, implying $S_G \equiv \{\underline{x}_k, \underline{x}_t\}$, or otherwise $\{\underline{x}_i, \underline{x}_j\} \cap \{\underline{x}_p, \underline{x}_q\} = \{\underline{x}_t\}$ for some $\{\underline{x}_t\} \neq \{\underline{x}_k\}$, implying $S_G \equiv \{\underline{x}_k, \underline{x}_t\}$. •

Given $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$, where the unidentified digit $\underline{x}_k$ bears an unrestricted error, assume that there exixts a consistent guess $G(s, \underline{A})$. Although $G(s, \underline{A})$ can be reconstructed in the *D-RNS-NPM* with $\mathcal{M}_{av} \equiv \{m_1, m_2, \ldots, m_{n-l}\}$, it cannot be expected that $\rho(G(s, \underline{A}))$ be a close approximation of $\rho(X)$, as Lemma 2.1 does not hold. Nevertheless, $\rho(G(s, \underline{A}))$ is strictly

related to $\rho(X)$, as stated by Lemma 3.3 and Lemma 3.4 which, respectively, consider the cases of $\underline{x}_s \in \underline{A}-\{\underline{x}_k\}$ and $\underline{x}_s=\underline{x}_k$.

Lemma 3.3. *Given $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$, where the unidentified digit $\underline{x}_k$ bears an unrestricted error, assume that the guess G(s, $\underline{A}$) constructed with seed $\underline{x}_s \in \underline{A}-\{\underline{x}_k\}$ is consistent. Then $\rho(G(s, \underline{A}))$, reconstructed from G(s, $\underline{A}$) in the D-RNS-NPM with $\mathcal{M}_{av} \equiv \{m_1, m_2, \ldots, m_{n-l}\}$ and $M_{av}=lcm(\mathcal{M}_{av})$, is equal to $|x + \varepsilon^s + h\, lcm(\mathcal{M}_{av}-\{m_k\})|_{Mav}$, where $abs(\varepsilon^s) \le \delta$ and h is an integer with $0 \le h < \dfrac{\mathrm{lcm}(\mathcal{M}_{av})}{\mathrm{lcm}(\mathcal{M}_{av}-\{m_k\})}$.*

Proof. If *G(s, $\underline{A}$)* is consistent, congruences $\xi_j^s - \xi_k^s \equiv 0 \pmod{d_{jk}}$ and $\varepsilon_j^s - \varepsilon_k^s \equiv 0 \pmod{d_{jk}}$ hold for every *j* with $1 \le j \le n-l;\ j \ne k$. If $j \ne s$, from Definition 5, $\varepsilon_j^s - \varepsilon_k^s = e_j - \underline{e}_s^s + \gamma_{sj} - (e_k - \underline{e}_s^s + \gamma_{sk})$ and, replacing γ_{sj} and γ_{sk} from (5) and from (7), it is immediate that $\varepsilon_j^s - \varepsilon_k^s = p_{sk}\, d_{sk}$. Similarly, $\varepsilon_s^s - \varepsilon_k^s = p_{sk}\, d_{sk}$.

It follows that $p_{sk}\, d_{sk} \equiv 0 \pmod{d_{kj}}$ holds for every *j* with $1 \le j \le n-l,\ j \ne k$, and thus [17] $p_{sk} d_{sk} \equiv 0 \pmod{\underset{j=1,n-l;\, j\ne k}{lcm}(d_{kj})}$; that is, $p_{sk}\, d_{sk} \equiv 0 \pmod{\prod_{j=1,n-l;\, j\ne k} d_{kj}}$. Letting $\hat{m}_k = \prod_{j=1,n-l;\, j\ne k} d_{kj}$, the preceding congruence is equivalent to $p_{sk}\, d_{sk} = w\, \hat{m}_k$ for some integer *w*.

On the other hand, from $\varepsilon_i^s - \varepsilon_k^s = p_{sk}\, d_{sk}$ and $\varepsilon_j^s - \varepsilon_k^s = p_{sk}\, d_{sk}$, it follows $\varepsilon_i^s = \varepsilon_j^s$ for every *i,j* with $1 \le i,j \le n-l;\ i,j \ne k$. Introducing ε^s with $\varepsilon_j^s = \varepsilon^s$ for every $j \ne k$, and replacing $\underline{e}_s^s$ from Definition 5 in $\varepsilon^s = e_s - \underline{e}_s^s$, yields $\varepsilon^s = e_s - \left\lceil \dfrac{1}{n-l} \sum_{j=1,n-l;\, j\ne s,k} \gamma_{sj} + \dfrac{1}{n-l}\gamma_{sk} \right\rceil$ and also:

$$\varepsilon^s = e_s - \left\lceil e_s - \frac{1}{n-l}\left(2e_s + \sum_{j=1,n-l;\, j\ne s,k} e_j\right) + \frac{1}{n-l}\gamma_{sk} \right\rceil,$$

$-\lceil number \rceil = \lfloor -number \rfloor$, yields:

$$\varepsilon^s = \left\lfloor \frac{1}{n-l}\left(2e_s + \sum_{j=1,n-l;\, j\ne s,k} e_j\right) - \frac{1}{n-l}\gamma_{sk} \right\rfloor,$$

from which $abs(\varepsilon^s) \le \delta$, since $abs\left(\dfrac{1}{n-l}\left(2e_s + \sum_{j=1,n-l;\, j\ne s,k} e_j\right)\right) \le \delta$ and $abs\left(\dfrac{1}{n-l}\gamma_{sk}\right) < \delta$ for $n-l > 2$.

Consider (n-l)-tuple $\{\varepsilon_1^s, \varepsilon_2^s, \ldots, \varepsilon_{n-l}^s\}$, where $\varepsilon_j^s = \varepsilon^s$ for every $j \ne k$, and $\varepsilon_k^s = \varepsilon^s - w\, \hat{m}_k$ from $\varepsilon^s - \varepsilon_k^s = p_{sk}\, d_{sk}$ and $p_{sk}\, d_{sk} = w\, \hat{m}_k$. This (n-l)-tuple is the sum of (n-l)-tuples $E' \equiv \{e'_i \mid e'_i = \varepsilon^s\ (1 \le i \le n-l)\}$ and $E'' \equiv \{e''_i \mid e''_i = 0\ (1 \le i \le n-l;\ i \ne k);\ e''_k = -w\, \hat{m}_k\}$. Reconstructing *E'* and *E''* in the *D-RNS-NPM* with $\mathcal{M}_{av} \equiv \{m_1, m_2, \ldots, m_{n-l}\}$ and $M_{av}=lcm(\mathcal{M}_{av})$, yields $\rho(E') = \varepsilon^s$ and $\rho(E'') \equiv 0 \pmod{lcm(\mathcal{M}_{av}-\{m_k\})}$; that is $\rho(E'') = h.lcm(\mathcal{M}_{av}-\{m_k\})$, where *h* is an integer with $0 \le h < \dfrac{\mathrm{lcm}(\mathcal{M}_{av})}{\mathrm{lcm}(\mathcal{M}_{av}-\{m_k\})}$.

This concludes the proof, since $\xi_i^s = |x_i + \varepsilon_i^s|_{mi}$ and $\rho(G(s, \underline{A})) = |\rho(\{x_1, x_2, \ldots, x_{nl}\}) +$

$\rho(\{\varepsilon_1^s, \varepsilon_2^s, ..., \varepsilon_{n-l}^s\})|_{Mav}$; from which $\rho(G(s, \underline{A})) = |x + \varepsilon^s + h.lcm(\mathcal{M}_{av} - \{m_k\})|_{Mav}$, with $abs(\varepsilon^s) \leq \delta$ and integer h satisfying $0 \leq h < \dfrac{\text{lcm}(\mathcal{M}_{av})}{\text{lcm}(\mathcal{M}_{av} - \{m_k\})}$. •

Lemma 3.4. *Given $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$, where the unidentified digit $\underline{x}_k$ bears an unrestricted error, assume that $abs(\gamma_{ij}) \leq 2\delta$ for every i,j with $1 \leq i,j \leq n-l$; $i \neq j$, and that guess $G(i, \underline{A})$ is consistent for every $1 \leq i \leq n-l$. Then $\rho(G(k, \underline{A}))$, reconstructed from guess $G(k, \underline{A})$ in the D-RNS-NPM of moduli $\mathcal{M}_{av} \equiv \{m_1, m_2, \ldots, m_{n-l}\}$, with $M_{av} = lcm(\mathcal{M}_{av})$ is equal to $|x + \varepsilon^s + h.lcm(\mathcal{M}_{av} - \{m_k\})|_{Mav}$, where $abs(\varepsilon^s) \leq \delta$ and h is an integer with $0 \leq h < \dfrac{\text{lcm}(\mathcal{M}_{av})}{\text{lcm}(\mathcal{M}_{av} - \{m_k\})}$.*

Proof. If $G(k, \underline{A})$ is consistent, congruences $\xi_i^k - \xi_j^k \equiv 0 \pmod{d_{ij}}$ and $\varepsilon_i^k - \varepsilon_j^k \equiv 0 \pmod{d_{ij}}$ hold for every i,j with $1 \leq i,j \leq n-l$; $i,j \neq k$. From Definition 5, $\varepsilon_i^k - \varepsilon_j^k = e_i - \underline{e}_k^k + \gamma_{ki} - (e_j - \underline{e}_k^k + \gamma_{kj})$ and also, from (7), $\varepsilon_i^k - \varepsilon_j^k = p_{kj} d_{kj} - p_{ki} d_{ki}$. Further, from $\varepsilon_i^k - \varepsilon_j^k = e_i - \underline{e}_k^k + \gamma_{ki} - (e_j - \underline{e}_k^k + \gamma_{kj})$ and $abs(e_i) \leq \delta$, $abs(e_j) \leq \delta$, $abs(\gamma_{ki}) \leq 2\delta$, $abs(\gamma_{kj}) \leq 2\delta$, inequality $abs(\varepsilon_i^k - \varepsilon_j^k) \leq 6\delta$ also holds.

Given that $G(i, \underline{A})$ is consistent, $\varepsilon_j^i - \varepsilon_k^i \equiv 0 \pmod{d_{kj}}$ for every $j \neq i,k$ and, from Definition 5, $\varepsilon_j^i - \varepsilon_k^i = e_j - \underline{e}_i^i + \gamma_{ij} - (e_k - \underline{e}_i^i + \gamma_{ik})$, where $\gamma_{ik} = -\gamma_{ki}$ because $abs(\gamma_{ki}) \leq 2\delta$ and $abs(\gamma_{ik}) \leq 2\delta$. Replacing $\gamma_{ij} = e_i - e_j$ from (5) and $\gamma_{ki} = e_k - e_i - p_{ki} d_{ki}$ from *(7)*, the preceding equation becomes $\varepsilon_j^i - \varepsilon_k^i = - p_{ki} d_{ki}$, from which $- p_{ki} d_{ki} \equiv 0 \pmod{d_{kj}}$. Combining the preceding congruence with $\varepsilon_i^k - \varepsilon_j^k = p_{kj} d_{kj} - p_{ki} d_{ki}$ yields $\varepsilon_i^k - \varepsilon_j^k \equiv 0 \pmod{d_{kj}}$. Considering $G(j, \underline{A})$, with $j \neq i,k$, a similar reasoning yields $- p_{kj} d_{kj} \equiv 0 \pmod{d_{ki}}$ and $\varepsilon_i^k - \varepsilon_j^k \equiv 0 \pmod{d_{ki}}$.

From simultaneous congruences $\varepsilon_i^k - \varepsilon_j^k \equiv 0 \pmod{d_{ij}}$, $\varepsilon_i^k - \varepsilon_j^k \equiv 0 \pmod{d_{kj}}$, $\varepsilon_i^k - \varepsilon_j^k \equiv 0 \pmod{d_{ki}}$, congruence $\varepsilon_i^k - \varepsilon_j^k \equiv 0 \pmod{d_{ij}\, d_{kj}\, d_{ki}}$ also holds [17], and thus $\varepsilon_i^k - \varepsilon_j^k = w\, d_{ij}\, d_{kj}\, d_{ki}$, where must be $w = 0$ since $abs(\varepsilon_i^k - \varepsilon_j^k) \leq 6\delta$ and $d_{ii}\, d_{kj}\, d_{ki} > 6\delta$. This implies $\varepsilon_i^k = \varepsilon_j^k$ and also $p_{ki} d_{ki} = p_{kj} d_{kj}$ for arbitrary i,j with $i,j \neq k$, since equations $p_{ki} d_{ki} = \varepsilon_k^k - \varepsilon_i^k$ and $p_{kj} d_{kj} = \varepsilon_k^k - \varepsilon_j^k$ are immediate from $\varepsilon_i^k = e_i - \underline{e}_k^k + \gamma_{ki}$ (or $\varepsilon_j^k = e_j - \underline{e}_k^k + \gamma_{kj}$) combined with $\gamma_{ki} = e_k - e_i - p_{ki} d_{ki}$ (or $\gamma_{kj} = e_k - e_j - p_{kj} d_{kj}$). Letting $\varepsilon^k = \varepsilon_j^k$ and $p_k d_k = p_{kj} d_{kj}$ and replacing into $\varepsilon_k^k - \varepsilon_j^k \equiv 0 \pmod{d_{kj}}$ and $p_{kj} d_{kj} \equiv 0 \pmod{d_{kj}}$, yields congruences $\varepsilon_k^k - \varepsilon^k \equiv 0 \pmod{d_{kj}}$ and $p_k d_k \equiv 0 \pmod{d_{kj}}$, which hold for every j. Letting $\hat{m}_k = \prod_{j=1,n-l} d_{kj}$, congruences $\varepsilon_k^k \equiv \varepsilon^k \pmod{\hat{m}_k}$ and $p_k d_k \equiv 0 \pmod{\hat{m}_k}$ also hold [17], from which $\varepsilon_k^k = \varepsilon^k + w \hat{m}_k$ and $p_k d_k = w \hat{m}_k$ for some integer w.

On the other hand, considering $\varepsilon^k = e_j - \underline{e}_k^k + \gamma_{kj}$, which holds for arbitrary $j \neq k$, and replacing $\underline{e}_k^k$ from Definition 5, yields $\varepsilon^k = e_j + \gamma_{kj} - \left\lceil \dfrac{1}{n-l} \sum_{i=1,n-l;i\neq k} \gamma_{ki} \right\rceil$ and also, rearranging and introducing $-\lceil number \rceil = \lfloor -number \rfloor$, $\varepsilon^k = \left\lfloor e_j + \gamma_{kj} - \dfrac{1}{n-l} \sum_{i=1,n-l;i\neq k} \gamma_{ki} \right\rfloor$. Replacing $\gamma_{kj} = e_k - e_j - p_k d_k$ and $\gamma_{ki} = e_k - e_i - p_k d_k$ from *(7)* yields:

$$\varepsilon^k = \left\lfloor e_j + \frac{1}{n-l}\gamma_{kj} + \frac{n-l-1}{n-l}\left(e_k - e_j - p_k d_k\right) - \frac{1}{n-l} \sum_{i=1,n-l;i\neq k} \left(e_k - e_j - p_k d_k\right) \right\rfloor,$$

that is:

$$\varepsilon^k = \left\lfloor \frac{1}{n-l}\gamma_{kj} + \frac{1}{n-l}\left(e_j + \sum_{i=1,n-l;i\neq k} e_i\right) \right\rfloor,$$

which implies $abs(\varepsilon^k) \leq \delta$, as $abs\left(\frac{1}{n-l}\left(e_j + \sum_{i=1,n-l;i\neq k} e_i\right)\right) \leq \delta$ and $abs\left(\frac{1}{n-l}\gamma_{kj}\right) < \delta$ for $n\text{-}l > 2$.

Consider now the (n-l)-tuple $\{\varepsilon_1^k, \varepsilon_2^k, ..., \varepsilon_{n-l}^k\}$, representing an integer in the *D-RNS-NPM* with $\mathcal{M}_{av} \equiv \{m_1, m_2, \ldots, m_{n-l}\}$ and $M_{av} = lcm(\mathcal{M}_{av})$. This (n-l)-tuple is the sum of (n-l)-tuples $E' \equiv \{e'_i \mid e'_i = \varepsilon^k \ (1 \leq i \leq n\text{-}l)\}$ and $E'' \equiv \{e''_i \mid e''_i = 0 \ (1 \leq i \leq n\text{-}l;\ i \neq k;\ e''_k = w\,\hat{m}_k\}$. Reconstructing E' and E'' in the *D-RNS-NPM* with $\mathcal{M}_{av} \equiv \{m_1, m_2, \ldots, m_{n-l}\}$ and $M_{av} = lcm(\mathcal{M}_{av})$, yields $\rho(E') = \varepsilon^k$ and $\rho(E'') \equiv 0 \ (mod\ lcm(\mathcal{M}_{av} - \{m_k\}))$; that is, $\rho(E'') = h.lcm(\mathcal{M}_{av} - \{m_k\})$, with integer h satisfying $0 \leq h < \frac{\text{lcm}(\mathcal{M}_{av})}{\text{lcm}(\mathcal{M}_{av} - \{m_k\})}$. This concludes the proof, since $\xi_i^k = |x_i + \varepsilon_i^k|_{mi}$ and $\rho(G(s, \underline{A})) = |\rho(\{x_1, x_2, \ldots, x_{n-l}\}) + \rho(\{\varepsilon_1^k, \varepsilon_2^k, ..., \varepsilon_{n-l}^k\})|_{Mav}$; that is $\rho(G(s, \underline{A})) = |x + \varepsilon^k + h\ lcm(\mathcal{M}_{av} - \{m_k\})|_{Mav}$, where $abs(\varepsilon^k) \leq \delta$ and h is an integer with $0 \leq h < \frac{\text{lcm}(\mathcal{M}_{av})}{\text{lcm}(\mathcal{M}_{av} - \{m_k\})}$. •

Now, consider the *D-RNS-NPM* with $\mathcal{M} \equiv \{m_1, m_2, \ldots, m_n\}$, $M = lcm(\mathcal{M})$, and define the legitimate range as $[\delta, \tilde{M} - \delta)$, with $\tilde{M} = \min_{\mathcal{M}^{n-z} \in \mathcal{F}^{n-z}} lcm(\mathcal{M}^{n-z})$. Given any legitimate $X \equiv \{x_1, x_2, \ldots, x_n\}$, assume l erasures, with $l \leq z\text{-}2$, and a single unrestricted error $\underline{e}_k$ combined with an arbitrary number of small errors in the available (n-l)-tuple $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$. As pointed out in Section 3, with extremely high probability $\underline{A}$ is inconsistent, and the error is detectable. In this hypotesis, reconstruct the available (n-l)-tuple $\underline{A}$ with the *Decoding Algorithm* reported in *Table 1*, which returns an integer ρ. It is claimed that ρ is in the legitimate range $[\delta, \tilde{M} - \delta)$, and ρ is within $\pm\delta$ from $x = \rho(X)$, implying that the assumed error situation is tolerated. This notable result is stated by the following Theorem.

Theorem 3. *The D-RNS-NPM with* $\mathcal{M} \equiv \{m_1, m_2, \ldots, m_n\}$, $M = lcm(\mathcal{M})$, $\tilde{M} = \min_{\mathcal{M}^{n-z} \in \mathcal{F}^{n-z}} lcm(\mathcal{M}^{n-z})$ *and legitimate range* $[\delta, \tilde{M} - \delta)$ *tolerates up to z-2 erasures combined with any detectable error (n-l)-tuple E where at most one error is unrestricted and the remaining errors are small.*

Proof. Given any $X \equiv \{x_1, x_2, \ldots, x_n\}$ with $x = \rho(X)$ in the range $[\delta, \tilde{M} - \delta)$, assume that l digits are erased, with $l \leq z\text{-}2$, and, without any loss of generality, that the set of the available digits is $\underline{A} \equiv \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_{n-l}\}$. If all errors in E are small, the claim is immediate from Theorem 2. Otherwise, assume that the unidentified digit $\underline{x}_k \in \underline{A}$ bears an unrestricted error, while any other error is small. Let $\mathcal{M}_{av} \equiv \{m_1, m_2, \ldots, m_{n-l}\}$, $\Gamma \equiv \{\gamma_{ij} : 0 \leq i,j \leq n\text{-}l;\ i \neq j\}$ and consider the *Decoding Algorithm*.

TABLE 1: DECODING ALGORITHM

Decoding Algorithm

*/ * x≡ {$x_1, x_2, \ldots, x_n$}; $\delta \le x < \tilde{M} - \delta$; I≤ z-2 digits are erased / **

input $\underline{A}$; **let** $\Gamma \equiv \{\gamma_{ij} \mid \underline{x}_i, \underline{x}_j \in \underline{A}; i \neq j\}$; */ * #$\underline{A}$≥ n- z +2; Γ is the syndrome / **

let $\rho = \tilde{M}$;

if there exists $\gamma_{ij} \in \Gamma$ **with** abs(γ_{jj})> 2δ { */ *case 1 / **

construct S_Γ;

*/ * S_Γ is the Suspect Set implied by syndrome Γ; #S_Γ= 1 or #S_Γ= 2 / **

select arbitrarily $\underline{x}_s \in \underline{A}$- S_Γ ;

while $S_\Gamma \neq \varnothing$ {

select arbitrarily $\underline{x}_i \in S_\Gamma$; **let** $S_\Gamma = S_\Gamma - \{\underline{x}_i\}$;

if G(s, $\underline{A}$- { $\underline{x}_i$ }) is consistent {

if ρ(G(s, $\underline{A}$- { $\underline{x}_i$ }) < $\tilde{M}$ **let** $\rho = \rho(G(s, \underline{A} - \{\underline{x}_i\}))$;

*/ *ρ(G(s, $\underline{A}$- {$\underline{x}_i$})) is reconstructed with the moduli in $\mathcal{M}_{av} - \{m_i\}$ / **

}

}

}

else */ * abs(γ_{jj})≤ 2d for every $\gamma_{ij} \in \Gamma$ / * { */ *case 2 / **

if there exists $\underline{x}_s \in \underline{A}$ **with** G(s, $\underline{A}$) inconsistent {

construct S_G from G(s, $\underline{A}$);

*% S_G is the Suspect Set implied by the guess G(s, $\underline{A}$); 1 ≤ #S_G ≤ 3 / **

select arbitrarily $\underline{x}_s \in \underline{A}$- S_G;

while $S_G \neq \varnothing$ {

select arbitrarily $\underline{x}_i \in S_G$; **let** $S_G = S_G$- { $\underline{x}_i$ };

if G(s, $\underline{A}$- { $\underline{x}_i$ }) is consistent {

if ρ(G(s, $\underline{A}$- { $\underline{x}_i$ }) < $\tilde{M}$ **let** $\rho = \rho(G(s, \underline{A} - \{\underline{x}_i\}))$;

*/ * ρ(G(s, $\underline{A}$- {$\underline{x}_i$})) is reconstructed with moduli in $\mathcal{M}_{av} - \{m_i\}$ / **

}

}

}

else */ * G(s, $\underline{A}$) consistent for every $\underline{x}_s \in \underline{A}$ / * { */ *case 3 / **

let S= $\underline{A}$; */ * S is a trivial Suspect Set / **

select arbitrarily $\underline{x}_s \in S$, */ * might be $\underline{x}_s = \underline{x}_k$ / **

do {

select arbitrarily $\underline{x}_i \in$ S- { $\underline{x}_s$ } ; **let** S= S- { $\underline{x}_i$ };

let $\rho = \rho(G(s, \underline{A} - \{\underline{x}_i\}))$;

let $\underline{x}_s \in \underline{x}_i$; */ * $\underline{x}_s \neq \underline{x}_k$ in next iteration / **

}

while $\rho \ge \tilde{M}$ **and** S ≠ ∅

}

}

if ρ(G(s, $\underline{A}$- { $\underline{x}_i$ }) < $\tilde{M}$ {

if $\rho < \delta$ **let** $\rho = \delta$;

else if $\rho \ge \tilde{M} - \delta$ **let** $\rho = \tilde{M} - \delta$;

return ρ */ * ρ is within ≠δ from x / **

}

else Algorithm Failure */ * hypothesis violated / **

Observe preliminarly that all digits in $\underline{A}$-{$\underline{x}_k$} bear small errors and thus, from Lemma 2.1, reconstructing $\rho(G(s, \underline{A}-\{\underline{x}_k\}))$ in the *D-RNS-NPM* of moduli $\mathcal{M}_{av}^k = \mathcal{M}_{av}-\{m_k\}$ with $M_{av}^k = lcm(\mathcal{M}_{av}^k)$ yields $\rho(G(s, \underline{A}-\{\underline{x}_k\}) = |x+\varepsilon|_{M_{av}^k}$. Since $abs(\varepsilon) \le \delta$, $0 \le x+\varepsilon < \tilde{M}$, and $M_{av}^k > \tilde{M}$, the preceding equation becomes $\rho(G(s, \underline{A}-\{\underline{x}_k\})) = x+\varepsilon$, with $0 \le \rho(G(s, \underline{A}-\{\underline{x}_k\})) < \tilde{M}$.

The *Decoding Algorithm* runs through one case among *1, 2* or *3* and, in any case, iterates evaluation of $\rho(G(s, \underline{A}-\{\underline{x}_i\}))$ in the *D-RNS-NPM* of moduli $\mathcal{M}_{av}^i = \mathcal{M}_{av}-\{m_i\}$ with $M_{av}^i = lcm(\mathcal{M}_{av}^i)$, each time with a different $\underline{x}_i$ in the Suspect Set S_Γ, S_G or S. As, under the hypothesis, $\underline{x}_k$ is in every one of the above Suspect Sets, *Decoding Algorithm* will eventually pick $\underline{x}_i = \underline{x}_k$ and exits from the case with $\rho(G(s, \underline{A}-\{\underline{x}_k\})) < \tilde{M}$, unless inequality $\rho(G(s, \underline{A}-\{\underline{x}_i\})) < \tilde{M}$ also holds for some $\underline{x}_i \neq \underline{x}_k$ that was picked before.

If $\underline{x}_i \neq \underline{x}_k$ and $s \neq k$, then by Lemma 3.3 $\rho(G(s, \underline{A}-\{\underline{x}_i\})) = \left| x + \varepsilon^s + h \cdot lcm(M^i_{av} - \{m_k\}) \right|_{M^i_{av}}$, where $abs(\varepsilon^s) \leq \delta$ and h is an integer with $0 \leq h \leq \frac{\text{lcm}(\mathcal{M}^i_{av})}{\text{lcm}(\mathcal{M}^i_{av} - \{m_k\})} - 1$. If $s = k$, the same result holds by Lemma 3.4. Observe that equality $s = k$ may only occur in the first iteration of case 3, whereas in all subsequent iterations, as well as in cases 1 and 2, $s \neq k$ always holds. Replacing the preceding inequality for h yields $x + \varepsilon^s + h \cdot lcm(M^i_{av} - \{m_k\}) \leq x + \varepsilon^s + lcm(M^i_{av}) - lcm(M^i_{av} - \{m_k\})$, from which $x + \varepsilon^s + h \cdot lcm(M^i_{av} - \{m_k\}) \leq lcm(M^i_{av})$, as $\# \mathcal{M}^i_{av} - \{m_k\} = n\text{-}l\text{-}2 \leq n\text{-}z$, and thus $lcm(M^i_{av} - \{m_k\}) \geq \tilde{M}$. Given that $0 \leq x + \varepsilon^s < \tilde{M}$ and $lcm(M^i_{av} - \{m_k\}) \geq \tilde{M}$, in the preceding inequality must be $h = 0$ and thus $\rho(G(s, \underline{A}-\{\underline{x}_i\})) = x + \varepsilon^s$ with $abs(\varepsilon^s) \leq \delta$.

Combining this result with equation $\rho(G(s, \underline{A}-\{\underline{x}_k\})) = x + \varepsilon$ with $abs(\varepsilon) \leq \delta$, holding when $\underline{x}_i = \underline{x}_k$, it is concluded that *Decoding Algorithm* always exits from the occurring case with $\rho = x + \varepsilon$ and $abs(\tilde{\varepsilon}) \leq \delta$, and thus $0 < \rho \leq \tilde{M}$. As ρ is subsequently redefined as $\rho = \delta$ if $\rho < \delta$, or $\rho = \tilde{M} - \delta$ if $\rho \geq \tilde{M} - \delta$, the integer ρ eventually returned is in the legitimate range $[\delta, \tilde{M} - \delta)$ and it is within $\pm\delta$ from integer x. •

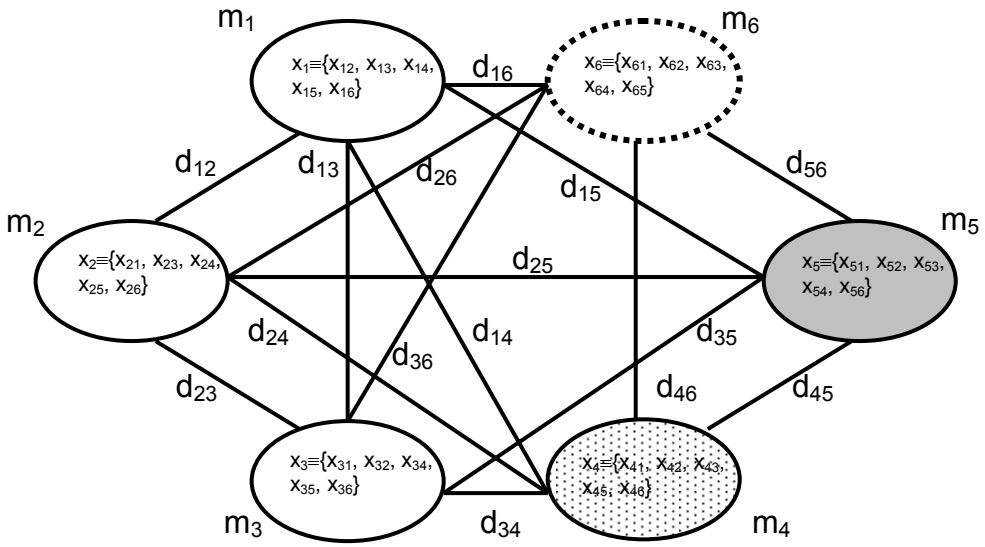

Fig. 3: A D-RNS-NPM with 6 moduli tolerating 1 erasure and a single unrestricted error combined with small errors

As an example, consider the *D-RNS-NPM* of Fig. 3, with $\mathcal{M} \equiv \{m_1, m_2, m_3, m_4, m_5, m_6\}$, and let $z = 3$ and $\tilde{M} = \min_{\mathcal{M}^3 \in \mathcal{F}^3} lcm(\mathcal{M}^3)$. Let x be any integer in the range $[\delta, \tilde{M} - \delta)$, represented by $X \equiv \{x_1, x_2, x_3, x_4, x_5, x_6\}$, and assume that one digit, namely x_6, is erased and one available digit, namely x_5, bears an unrestricted error, while the remaining available digits bear small errors.

If the *Decoding Algorithm* picks $\underline{x}_i = \underline{x}_5$, it reconstructs the (n- 2)-tuple $\{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_4\}$ with the moduli in $\{m_1, m_2, m_3, m_4\}$ as if digit x_5 were also erased. Since digits in $\{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_4\}$ bear small errors and $lcm(m_1, m_2, m_3, m_4) > \tilde{M}$, the algorithm returns ρ with $\delta \leq \rho < \tilde{M} - \delta$ and $abs(x - \rho) < \delta$.

If the Decoding Algorithm picks $\underline{x}_i \neq \underline{x}_5$, say $\underline{x}_i = \underline{x}_4$, and, for some $s \in \{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_5\}$, inequality $\rho(G(s, \{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_5\})) < \tilde{M}$ holds, then the 4-tuple $\{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_5\}$ is reconstructed with the moduli in $\{m_1, m_2, m_3, m_5\}$, yielding $\rho(\{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_5\}) = x + \varepsilon^s + h \cdot lcm(m_1, m_2, m_3\})$ with $abs(\varepsilon^s) < \delta$ and $h = 0$ by Theorem 3. Thus, although $\underline{x}_5$ bears an unrestricted error, the Decoding Algorithm returns ρ with $\delta \leq \rho < \tilde{M} - \delta$ and $abs(x - \rho) < \delta$.

7. CONCLUSION

The Residue Number Systems with Non-Pairwise-Prime Moduli lend themselves to construction of erasure codes with properties that are highly desirable in Wireless Sensor Networks, when data robustness and confidentiality are critical issues. Assuming n non-pairwise-prime moduli, the codewords are n-tuples of residue digits encoding integers in the legitimate range of the code. Denoting by z a non-negative integer depending on the code redundancy, and by δ a small integer depending on the actual moduli, the following properties have been demonstrated:

1. if l digits are erased, and the available digits are exempt from errors, then the encoded integer can be reconstructed exactly from the available digits, provided $l \leq z$;
2. if l digits are erased, and the available digits bear an unbounded number of errors of magnitude less than δ (otherwise said, small errors), then the encoded integer can be reconstructed from the available digits within an approximation of $\pm \delta$, provided $l \leq z$;
3. if l digits are erased, and the available digits bear a single unrestricted error combined with an unbounded number of errors of magnitude less than δ, then with extremely high probability the encoded integer can be reconstructed from the available digits within an approximation of $\pm \delta$, provided $l \leq z - 2$.

Encoding and decoding require simple arithmetic computation; namely calculation of n residues for encoding, and evaluation of a linear polynomial for decoding via the Generalized Chinese Remainder Theorem.

In the application to Wireless Sensor Networks, sensing nodes are replicated, with n replicate nodes independently collecting and encoding the same data. Every sensing node stores a single digit of the encoded data, with different nodes storing different digits. This way, the code digits are dispersed over the set of the replicated nodes, without requiring wireless communication between nodes. Avoiding communication contributes to energy conservation and to data safety, as wireless channels lend themselves to eavesdropping. Memory requirements of individual nodes are also reduced, since every node stores a residue digits, rather than the entire encoding of data. To reconstruct the data, it is sufficient that at least $n - z$ digits are retrieved from any subset of at least n-z duplicate nodes. The tolerance of erasures is complemented with the ability to reconstruct the data within an approximation of $\pm\delta$ when the available digits bear small errors of unbounded multiplicity, and this is a vital property, since it is unavoidable that replicate sensing nodes collect slightly different values for the same data. It has been shown that the ability to tolerate erasures combined with small errors is kept, with extremely high probability, when a single available digit bears an unrestricted error, that may arise from faults or intrusions. The latter property could be extended to multiple unrestricted errors, with the number of allowable unrestricted errors to be traded with the number of tolerable erasures.

The newly introduced erasure codes also provide basic data confidentiality, since decoding of the available digits requires that the set of moduli is known, as well as the association of the moduli with the available digits, and there is no way to even guess the data from less than $l - z$ digits. Although an adversary may attempt to guess the moduli, determining the actual

association with the available digits adds considerable difficulty. Further, data security can be reinforced with a number of countermeasures, such as encryption of the residue digits. A deep analysis of the security aspects is the matter of further research.

APPENDIX

The following is a summary of the notations used in the paper:

- *abs(integer)*: the absolute value of *integer;*
- $\lfloor number \rfloor$: equal to *number* - *f*, with *number* - *f* integer and $0 \le f < 1$;
- $\lceil number \rceil$: equal to *number* + *f*, with *number* + *f* integer and $0 \le f < 1$;
- m_i : a *modulus* (positive integer);
- $\mathcal{M} \equiv \{m_1, m_2, \ldots, m_n\}$: a n-tuple of *moduli;*
- $M = lcm(\mathcal{M})$*:* the least common multiple of the integers in set $\mathcal{M}$*;*
- $d_{ij} = gcd(m_i, m_j)$: the greatest common divisor of m_i and m_j;
- $\mathcal{D}$*:* given $M \equiv \{m_1, m_2, \ldots, m_n\}$, $\mathcal{D} \equiv \{d_{ij} : 1 \le i < n;\ i < j \le n\}$;
- δ: a non-negative integer with $\delta < \frac{1}{4} \min_{d_{hk} \in \mathcal{D}} d_{hk}$;
- *x:* a non-negative integer to be represented in a RNS;
- $x_i = |x|_{mi}$ *:*the *residue* of *x modulo* m_i;
- $X \equiv \{x_1, x_2, \ldots, x_n\}$: the residue representation of *x* with the moduli in $\mathcal{M}$*;*
- $\rho(X)$*:* the integer *x* represented by *X*;
- $y \equiv w \pmod m$*:* integers *y* and *w* are *congruent modulo m*;
- $y \not\equiv w \pmod m$*:* congruence $y \equiv w \pmod m$ does not hold;
- e_i : *error* borne by digit x_i;
- $E \equiv \{e_1, e_2, \ldots, e_n\}$*:* the *error n-tuple* borne by $X \equiv \{x_1, x_2, \ldots, x_n\}$;
- $\underline{x}_i$*:* a residue digit bearing an error;
- $\underline{X} \equiv \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_n\}$: a residue representation bearing an error n-tuple;
- $\Gamma \equiv \{\gamma_{ij} : 0 \le i,j \le n\text{-}l;\ i \ne j\}$: the *syndrome* of error (n-l)-tuple *E;*
- *A*: an *available (n-l)-tuple* of residue digits, resulting from *l erasures;*
- $\underline{A}$: an *available (n-l)-tuple* of residue digits, resulting from *l erasures* and an error (n-l)-tuple*;*
- $G(s, \underline{A})$*:* the *guess* of $X \equiv \{x_1, x_2, \ldots, x_{n-l}\}$ constructed from $\underline{A}$ with *seed* $\underline{x}_s \in \underline{A}$;
- $\#\mathcal{X}$: the cardinality of set $\mathcal{X}$*;*
- $\mathcal{M}^p$: a subset of set $\mathcal{M}$ with $\#\mathcal{M}^p = p$;
- $\mathcal{F}^p \equiv \{\mathcal{M}^p \mid \mathcal{M}^p \subseteq \mathcal{M};\ \#\mathcal{M}^p = p\}$: the collection of all the subsets of set $\mathcal{M}$*,* each of cardinality *p;*
- $lcm(\mathcal{M}^p)$: the least common multiple of the moduli in set $\mathcal{M}^p$;
- $\min_{\mathcal{M}^p \in \mathcal{F}^p} lcm(\mathcal{M}^p)$: the minimum of $lcm(\mathcal{M}^p)$ over collection $\mathcal{F}^p$.

REFERENCES

[1] Paolo Baronti, Prashant Pillai, Vince Chook, Stefano Chessa, Alberto Gotta, and Y. Fun Hu, Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards, Computer Communications, vol. 30, no. 7, 2007, pp. 1655-1695.

[2] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.
[3] R. G. Gallager, *Low-Density Parity-Check Codes,* MIT Press, Cambridge, MA, 1963.
[4] M. O. Rabin. Efficient Dispersal of Information for Security, Load Balancing and Fault Tolerance. *Journal of the ACM,* vol 36 , no. 2, 1989, pp. 335-348.
[5] M. Luby, M. Mitzenmacher, A. Shokrallahi, D. Spielman, and V. Stemann. Practical Loss-Resilient Codes, *Proc. of the 29th Annual ACM Symposium on Theory of Computing*, 1997, pp. 150-159.
[6] M. Luby, M. Mitzenmacher, A. Shokrallahi, and V. Stemann. Efficient Erasure Correcting Codes, *IEEE Trans. Inf. Theory,* vol 47, no. 2, Feb. 2001, pp. 569-58
[7] A.G. Dimakis, P. B. Brighten Godfrey, Y. Wu, M. O. Wainwright, and K. Ramchandran. Network Coding for Distributed Storage Systems, *Proc. 26th IEEE International Conference on Computer Communications*, May 2007, pp. 2000-2008.
[8] J. S. Plank and M.G. Thomason. A Practical Analysis of Low-Density Parity-Chech Erasure Codes for Wide-Area Storage Application, *Proc. of the 2004 International Conference on Dependable Systems and Networks*, 2004, pp. 115-124.
[9] H. Wheatherspoon and J. Kubiatowicz. Erasure Codes vs. Replication: A Quantitative Comparison, *Proc. of the 1st International Workshop on Peer-to-Peer Systems*, 2002.
[10] F. Barsi and P. Maestrini. Error Correcting Properties of Redundant Residue Number Systems, *IEEE Trans. Comput,* vol. C-21 (6), June 1972, pp. 307-515.
[11] S. Chessa and P. Maestrini. Dependable and Secure Data Storage and Retrieval in Mobile, Wireless Networks, *Proc. of the 2003 International Conference on Dependable Systems and Networks*, 2003, pp. 207-216.
[12] A. Kamra, J. Feldman, V, Misra, and D. Rubenstein. Growth Codes: Maximizing Sensor Network Data Persistence, *ACM SIGCOMM Computer Communication Review,* vol. 36 (4), Oct.)2006, pp. 255-266.
[13] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran. Decentralized Erasure Codes for Distributed Networked Storage, *IEEE Trans Inf, Theory,* vol IT-52 (6), June 2006, pp. 2809-2816.
[14] Y. Zhou and Y. Fang. Securing Wireless Sensor Networks: A Survey, *IEEE Communication Surveys and Tutorial,* vol. 10 no. 3. pp. 6-28.
[15] F. Barsi and P.Maestrini. Error Codes Constructed in Residue Number Systems with Non-Pairwise-Prime Moduli, *Information and Control*, vol. 46, no. 1, July 1980, pp. 16-25.
[16] R. S. Katti. A New Residue Arithmetic Error Correction Scheme, IEEE Trans. Comput, vol. C-45, no. 1, Jan. 1996, pp. 13-19.
[17] I. M. Vinogradov. *Elements of Number Theory,* Dover, New York, 1954.
[18] O. Ore. The General Chinese Remander Theorem, *Amer. Math. Montly,* 1952, pp. 365-370.