



HAL
open science

A Probabilistic Parallel Bit-Flipping Decoder for Low-Density Parity-Check Codes

Khoa Le, Fakhreddine Ghaffari, Lounis Kessal, David Declercq, Emmanuel
Boutillon, Chris Winstead, Bane Vasic

► **To cite this version:**

Khoa Le, Fakhreddine Ghaffari, Lounis Kessal, David Declercq, Emmanuel Boutillon, et al.. A Probabilistic Parallel Bit-Flipping Decoder for Low-Density Parity-Check Codes. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2018. hal-01700298v1

HAL Id: hal-01700298

<https://hal.science/hal-01700298v1>

Submitted on 3 Feb 2018 (v1), last revised 25 Sep 2018 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Probabilistic Parallel Bit-Flipping Decoder for Low-Density Parity-Check Codes

Khoa Le, Fakhreddine Ghaffari, *Member, IEEE*, Lounis Kessal, *Member, IEEE*,
David Declercq, *Senior Member, IEEE*, Emmanuel Boutillon, *Senior Member, IEEE*,
Chris Winstead, *Senior Member, IEEE* and Bane Vasić, *Fellow, IEEE*

Abstract—This paper presents a new Bit Flipping (BF) decoder, called Probabilistic Parallel Bit Flipping (PPBF) for Low-Density Parity-Check (LDPC) codes on the Binary Symmetric Channel. In PPBF, the flipping operation is proceeded with a probabilistic behavior which is shown to improve significantly the error correction performance. The advantage of PPBF comes from the fact that, no global computation is required during the decoding process and from that, all the computations can be executed in the local computing units and in-parallel. PPBF provides a considerable improvement of the decoding frequency and complexity, compared to other known BF decoders, while obtaining a significant gain in error correction. One improved version of PPBF, called non-syndrome PPBF (NS-PPBF) is also introduced, in which the global syndrome check is moved out of the critical path and a new terminating mechanism is proposed. In order to show the superiority of the new decoders in terms of hardware efficiency and decoding throughput, the corresponding hardware architectures are presented in the second part of the paper. The ASIC synthesis results confirm that, the decoding frequency of the proposed decoders is significantly improved, much higher than the BF decoders of literature while requiring lower complexity to be efficiently implemented.

Index Terms—Low-Density Parity-Check, probabilistic Bit Flipping decoding, high decoding throughput, low-complexity implementation.

I. INTRODUCTION

Low-Density Parity-Check (LDPC) codes were introduced by Gallager in 1963 and they have been adopted as a part of several standards, such as IEEE 802.11n, 802.16a, *etc.* due to their outstanding error correction capability [1][2]. LDPC codes can be decoded by two classes of decoding algorithms: *soft-information* message passing algorithms, *e.g.* Min Sum (MS), Sum Product (SP) [3], or *hard-decision* algorithms, *e.g.* Bit Flipping (BF), Gallager-A,B [4]. The soft-information

decoding algorithms provide a very good decoding performance, being close to the capacity, but require an intensive computation. They exhibit, therefore, very high complexity in hardware realization [3]. On the contrary, the hardware implementations of hard-decision decoders were shown to be very low complexity thanks to the simple computation units and smaller connection networks, but they are weak in error correction. The increasing demand of massive data rates in several applications, such as optical communications, high-speed Ethernet [5], data storage devices [6][7][8] or the New Radio of 5G enhanced mobile broadband (eMBB) [9], will require higher decoding throughput. In such applications, hard decision decoders become the promising candidates thanks to their simple computations and hence, low complexity and high decoding throughput, given that, the decoding performance is improved. This paper focuses on the Bit Flipping (BF) hard decision decoder to not only enhancing the decoding throughput and reducing the decoder complexity but also improving the error correction performance. Furthermore, we focus on the decoders which require only the hard information from the channel. These decoders could be used when the channel soft-information is unable to obtain or requires a long latency to be generated, such as the storage system [10][11].

The BF decoding concept is firstly introduced by Gallager [4], in which the binary information is iteratively passed between two groups of nodes: the Variable Nodes (VNs) and the Check Nodes (CNs), and it uses the channel hard-information as the input values. The CN operation is the exclusive-OR (XOR) operations and at each iteration, a VN is flipped if the number of unsatisfied neighboring CNs is higher than a predefined threshold. This BF is a very low complexity decoder but providing a very weak error correction, compared to the soft-decision decoders. Several BF decoders have been latter proposed in literature, in which Gradient Descent Bit Flipping (GDBF) and Probabilistic Gradient Descent Bit Flipping (PGDBF), introduced by Rasheed *et al.* in [12], could be seen as the most promising algorithms, in term of error correction. In GDBF, the CN operation is the XOR calculation as in the standard BF decoder, while VN computes a function called *inversion* or *energy* function derived from a gradient descent formulation. A VN is flipped when its energy value is a maximum, compared to all other energies. GDBF provides a very good error correction and it is better than the prior-introduced deterministic BF decoders. PGDBF is a variant of GDBF, introduced also in [12]. PGDBF follows precisely the decoding steps of GDBF and differs only

This work was funded by the french ANR under grant number ANR-15-CE25-0006-01 (NAND project).

Khoa Le, Fakhreddine Ghaffari, David Declercq and Lounis Kessal are with ETIS, UMR8051/ Université Paris Sein/ Université de Cergy-Pontoise/ ENSEA/ CNRS, 95014 Cergy-Pontoise, France (email: {khoa.letrung,fakhreddine.ghaffari,declercq,kessal}@ensea.fr).

Emmanuel Boutillon is with the lab-STICC, UMR 6285, Université de Bretagne Sud, 56321 Lorient, France, (email: emmanuel.boutillon@univ-ubs.fr).

Chris Winstead is with the Department of Electrical and Computer Engineering, Utah State University, UT 84322-4120 USA, (email: chris.winstead@usu.edu).

Bane Vasić is with Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ, 85719 USA, (email: vasic@ece.arizona.edu).

A part of this work was presented at the International Conference on Advanced Technologies for Communication, Quynhon, Vietnam, Oct. 2017.

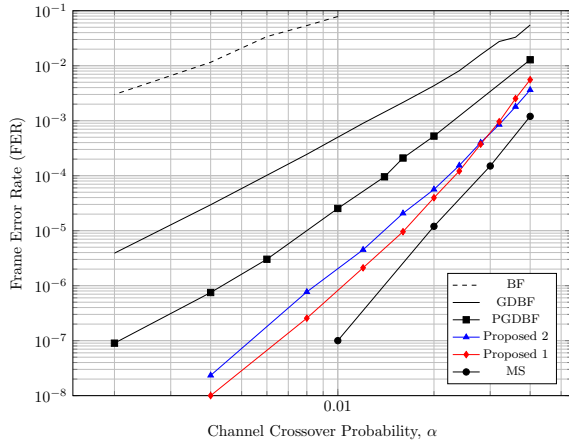


Fig. 1: The evolution in term of decoding performance of BF decoders on the Tanner code [14].

from the VN flipping operations. All the flipping candidates in GDBF are only flipped with a probability of p ($p < 1$) in PGDBF. This probabilistic behavior interestingly improves the decoding performance, far better than the original GDBF and very close to MS [13]. The evolution of BF performance improvement is shown in Fig. 1 on the well-known Tanner code [14]. Another newly proposed BF decoder is introduced by J. Jung in 2017 [10], called Multi-Bit Flipping (MBF). The MBF scenario is in line with our target in which the decoder requires only hard information from the channel for decoding. The VNs of MBF also compute at each iteration the energy value basing on its neighbor CN values. The novelty comes from the fact that, at each iteration of MBF, only a constant number of VNs are allowed to flip to avoid the overcorrection. For example, only 4 VN are flipped at each iteration. This truly helps the MBF avoid VN miss-flipping and offers a considerable improvement in error correction.

GDBF and PGDBF implementations can be found in [13] and MBF is implemented in [10]. A drawback of these BF decoders is that, a global operation (the Maximum Finder - MF in [13] and N-to-4 sorter in [10]) is required to identify the maximum among the VN energy values. This global operation operates on the large number of energy values and in the hardware implementations, it lengthens the decoder data path and limits the maximum achievable frequency, especially when the codeword length is extended. Although the reported decoding throughput of the above decoders is very promising, the global operation are the main obstacle for further improving the operating frequency and therefore, limit the maximization of the decoding throughput.

Another global computing block, which also limits the maximization of the operating frequency, is the Syndrome Check (SC) module. During the decoding process, the SC module verifies all the CN values and indicates at its output the stopping signal when all of them are satisfied, *i.e.* when all of CN values are 0's. We show in this paper that, the SC is an important module for prior-introduced BF decoders to obtain the decoding success but it can not be fully pipelined to improve the decoding speed. The hardware implementation

of the SC module has all of the CN outputs as its inputs and the data path becomes significantly long when the number of CNs is large. A BF decoder in which the SC is eliminated (or pipelined) from the data path, would provide a significant improvement in operating frequency but a special stopping mechanism is required.

This paper presents a new probabilistic parallel BF decoder (PPBF) in which no global operation is required. The flipping decision in each VN of PPBF is made locally in the VN basing only on its channel value, neighbor CN values and a probabilistic binary signal. In PPBF, depending on the computed energy value, the VN will be flipped with the corresponding probability. Therefore, at each iteration, all VNs in PPBF could be flipped (with different probabilities) and it is different from the PGDBF decoder where only the VNs having the maximum energy are the flip candidates. The data path is significantly shortened which results an enhancement of decoding throughput. More interestingly, by eliminating the global operation, PPBF is very low-complexity, even be equivalent to that of the deterministic GDBF decoder, while having a better decoding performance than PGDBF and being very close to the MS performance. An improved version of PPBF, called Non-Syndrome Probabilistic Parallel Bit Flipping (NS-PPBF), is then introduced, further shortening the critical path by moving the global SC module out of the data path. In NS-PPBF, when converging to a correct codeword, the decoder will stop flipping thanks to a specific flipping mechanism. NS-PPBF additionally improves the decoding frequency, compared to PPBF while maintaining the good error correction capability.

The rest of the paper is organized as following. In section II, the notations of LDPC codes and LDPC decoding algorithms are firstly introduced. The PPBF algorithm is then presented. The analysis of PPBF in improving of decoding performance and operating frequency is also provided. The improved version PPBF (the NS-PPBF) is introduced in section III. In section IV, the implementation architectures for PPBF and NS-PPBF are presented with detailed circuit for the probabilistic signal generator and processing units. In section V, the hardware synthesis results and the simulated error correction performance are presented. These results confirm that, the proposed decoders significantly improve the operating frequency, reduce the decoder complexity while improving the error correction capability, better than all known BF decoders in literature. The good decoding performance along with the high throughput and low complexity lead PPBF and NS-PPBF decoders to become the promising candidates for the next generation of communication and storage standards. Section VI concludes the paper.

II. THE PROBABILISTIC PARALLEL BIT FLIPPING DECODERS

A. Notations

LDPC code is defined by a sparse parity-check matrix $H(M, N)$, $N > M$. Each row represents a parity check function, computed by a CN, on the VNs represented by the columns. The VN v_n ($1 \leq n \leq N$) is checked by the CN

c_m ($1 \leq m \leq M$) if the entry $H(m, n) = 1$ and they are called neighbors. LDPC code can also be represented by a bipartite graph called Tanner graph composing two groups of nodes, the CNs c_m , $m = 1, \dots, M$, and the VNs v_n , $n = 1, \dots, N$. The VN v_n ($1 \leq n \leq N$) connects to the CN c_m ($1 \leq m \leq M$) by an edge in the Tanner graph if the entry $H(m, n) = 1$. We denote the set of CNs connecting to the VN v_n (the so-called, neighbor set) as $\mathcal{N}(v_n)$ and $|\mathcal{N}(v_n)|$ is called the degree of VN v_n . Similarly, $\mathcal{N}(c_m)$ denotes all VNs connecting to CN c_m and $|\mathcal{N}(c_m)|$ is the degree of CN c_m . This paper works on the regular LDPC code, *i.e.* $|\mathcal{N}(v_n)| = d_v$ and $|\mathcal{N}(c_m)| = d_c$, $\forall n, m$. A vector $\mathbf{x} = \{x_n\} = \{0, 1\}^N$ is called a codeword if and only if $H\mathbf{x}^T = \mathbf{0}$. \mathbf{x} is sent through a transmission channel and we denote $\mathbf{y} = \{y_n\} = \{0, 1\}^N$ as the channel output. The decoders presented in this paper are applied on the Binary Symmetric Channel (BSC) where each bit $x_n \in \mathbf{x}$ is flipped with a probability α , called channel crossover probability, when being transmitted, *i.e.*, $\Pr(y_n = x_n) = 1 - \alpha$ and $\Pr(y_n = 1 - x_n) = \alpha$, $1 \leq n \leq N$. We use the superscript (k) together with the node notations, *e.g.* $c_m^{(k)}$, $v_n^{(k)}$, to denote the nodes values at the k -th iteration. Also, the nodes values vector at the k -th iteration are denoted as $\mathbf{v}^{(k)} = (v_1^{(k)}, v_2^{(k)}, \dots, v_N^{(k)})$ and $\mathbf{c}^{(k)} = (c_1^{(k)}, c_2^{(k)}, \dots, c_M^{(k)})$.

B. The proposed Probabilistic Parallel Bit Flipping decoder

The proposed PPBF decoding algorithm follows the decoding procedure as in other introduced BF algorithms, in which the binary messages are iteratively passed between the VNs and CNs via the decoding iterations. The CN messages are simply the parity information and its computation is formulated as in Equ. 1 where \oplus is the bit-wise Exclusive-OR (XOR) operation. The BF decoding process is stopped either when all CNs equations are satisfied, *i.e.* $\mathbf{c}^{(k)} = \mathbf{0}$, in this case, the decoding process is declared as success and the $\mathbf{v}^{(k)}$ are the decoded codeword, or k reaches to the maximum number of iterations (denoted by It_{max}). In the latter case, the decoding process is declared as failure.

$$c_m^{(k)} = \bigoplus_{v_n \in \mathcal{N}(c_m)} v_n^{(k)} \quad (1)$$

When the above stopping conditions are not satisfied, all CN computation results, $c_m^{(k)}$, $1 \leq m \leq M$, are sent to neighbor VNs (called CN messages) and the VN operations are then proceeded. The computation of VN are summarized as following. Firstly, each VN evaluates its energy (reliability) value $E_n^{(k)}$, using Equ. 2, where the energy value is the summation of two terms. The first term is the similarity between its current value, $v_n^{(k)}$, and its channel output, y_n (computed by \oplus function). The second term is the number of its unsatisfied neighbor CNs, *i.e.* the neighbor CNs having $c_m^{(k)} = 1$. It is clear that, the energy value for a VN is an integer and varies between 0 to $d_v + 1$, ($0 \leq E_n^{(k)} \leq d_v + 1$). Secondly, basing on the computed energy value $E_n^{(k)}$, a random bit with Bernoulli distribution, $\mathcal{B}(\cdot)$, (denoted as $R_n^{(k)}$) is drawn in each VN such that $\Pr(R_n^{(k)} = 1) = \mathbf{p}(E_n^{(k)})$ and $\Pr(R_n^{(k)} = 0) = 1 - \mathbf{p}(E_n^{(k)})$ where \mathbf{p} is a pre-defined vector

of real values, $\mathbf{p} = (p_0, p_1, \dots, p_{d_v+1})$, $|\mathbf{p}| = d_v + 2$ and $\mathbf{p}(\ell)$ returns the ℓ -th element of \mathbf{p} , ($0 \leq \ell \leq d_v + 1$), $p_0 = \mathbf{p}(0) = 0$, $0 < p_\ell = \mathbf{p}(\ell) \leq 1, \forall \ell = 1, \dots, d_v + 1$. Finally, each VN will determine its new value basing on the generated random bit $R_n^{(k)}$. If $R_n^{(k)} = 1$, the VN will update its values by inverting the current value $v_n^{(k)}$, otherwise, it keeps the current value. All the VN values are sent to the neighbor CNs and a new decoding iteration will start. The PPBF decoding algorithm is described in algorithm 1.

$$E_n^{(k)} = v_n^{(k)} \oplus y_n + \sum_{c_m \in \mathcal{N}(v_n)} c_m^{(k)} \quad (2)$$

Algorithm 1 The PPBF decoding algorithm

```

1: Initialization  $k = 0$ ,  $\mathbf{v}^{(0)} = \mathbf{y}$ ,  $\mathbf{p} = (p_0, p_1, \dots, p_{d_v+1})$ 
2: while  $k \leq It_{max}$  do
3:   for  $1 \leq m \leq M$  do ▷ CN processing
4:     Compute  $c_m^{(k)}$ , using Equ. (1).
5:   end for
6:   if  $\mathbf{c}^{(k)} = \mathbf{0}$  then ▷ Check syndrome
7:     exit while
8:   end if
9:   for  $1 \leq n \leq N$  do ▷ VN processing
10:    Compute  $E_n^{(k)}$  using Equ. (2).
11:    Generate  $R_n^{(k)}$  from  $\mathcal{B}(\mathbf{p}(E_n^{(k)}))$ .
12:    if  $R_n^{(k)} = 1$  then
13:       $v_n^{(k+1)} = v_n^{(k)} \oplus 1$ 
14:    end if
15:  end for
16:   $k = k + 1$ 
17: end while
18: Output:  $\mathbf{v}^{(k)}$ 

```

It is interesting to make the comparisons between the PPBF and the state-of-the-art PGDBF decoding algorithm which can be found in [12][13] as the best BF decoder in term of error correction. The VN and global operations of PGDBF (the main differences between PPBF and PGDBF) are recalled in algorithm 2 where $R_n^{(k)}$ also denotes the random bit generated for v_n but differs from the fact that, $\Pr(R_n^{(k)} = 1) = p$, $\Pr(R_n^{(k)} = 0) = 1 - p$ (p is a pre-defined value). The VN processing of PGDBF can be divided into 2 parts. At the first part, each VN computes its energy value $E_n^{(k)}$ using also the Equ. (2). These computed energy values are sent to a global module to find the maximum energy $E_{max}^{(k)} = \max_n(E_n^{(k)})$. At the second part, each VN will generate a random bit $R_n^{(k)}$. Then, the value of each VN will be flipped if and only if its energy equals to the maximum energy ($E_n^{(k)} = E_{max}^{(k)}$) and the generated random bit $R_n^{(k)} = 1$. It can be seen that, the PPBF and PGDBF decoding algorithms have the same decoding steps as well as the CN and VN energy computation formulations. They also apply the probabilistic flipping of the VN values in each iteration. The differences between them are two folds. First, PPBF does not require the maximum energy value in making flipping selection and therefore, no global operation (the global sorting) is required. This comes from the

fact that, in PPBF each VN flips its value basing only on its own energy and the random signal value regardless the energy of other VNs. Second, in the binary random generating step of PPBF, the probability of generated bit, $R_n^{(k)}$, is dynamically changed on the VNs and on the decoding iterations. This probability is controlled by the VN energy values at each iteration while in PGDBF, it is fixed for all iterations and is equal for all VNs. Therefore, all VNs in PPBF are the flipping candidates (rather than only the energy-maximum VNs as in PGDBF) and they are actually flipped with different probabilities. This property helps PPBF be more advantageous in error correction than the PGDBF, presented in the next section.

Algorithm 2 The VN and global operation in PGDBF decoder

```

1: for  $1 \leq n \leq N$  do                                ▷ VN processing part 1
2:   Compute  $E_n^{(k)}$ , using Equ. (2).
3: end for
4: Sort  $E_{max}^{(k)} = \max_n(E_n^{(k)})$                     ▷ Global operation
5: for  $1 \leq n \leq N$  do                                ▷ VN processing part 2
6:   Generate  $R_n^{(k)}$  from  $\mathcal{B}(p)$ .
7:   if  $E_n^{(k)} = E_{max}^{(k)}$  and  $R_n^{(k)} = 1$  then
8:      $v_n^{(k+1)} = v_n^{(k)} \oplus 1$ 
9:   end if
10: end for

```

C. The PPBF improves the BF state-of-the-art error correction capability

The PPBF is proposed with the probabilistic strategy in flipping the VN, which provides an ability known as *oscillation breaking* to improve error correction, with respect to the deterministic BF decoders [15][16]. Indeed, when we consider the case of the GDBF, the failure comes from the fact that, during the decoding process, GDBF decoder falls into the infinite oscillations (or loops) between the tentative states of \mathbf{v} , which prevent GDBF converging to the correct codeword [13][15]. The probabilistic flip of PPBF helps break this oscillation and converge. For illustrating, we conducted a statistical analysis on the failures of GDBF decoder and the oscillation breaking of PPBF on the Tanner code. The results are plotted in Fig. 2. In Fig. 2A, we classified all the failure cases of GDBF into the t -iterations oscillation types, *i.e.* the positions of erroneous bits stay the same after t iterations, $\mathbf{v}^{(k+t)} = \mathbf{v}^{(k)}$, for several values of α and $It_{max} = 300$. It is confirmed by Fig. 2A that, all of the decoding failures of GDBF are due to the infinite oscillation between states of \mathbf{v} and furthermore, the 2-iterations oscillation dominates other types, especially in the low error rate region. We then re-decoded the GDBF failure cases by PPBF (and also by PGDBF for comparison). The results are plotted in Fig. 2B. It is remarked that, the PPBF corrects almost the failure cases of GDBF, especially in low error rate region. This above interesting property is the source of PPBF error correction improvement.

The error correction of PPBF in the above statistics is even better than that of the PGDBF decoder. This is because

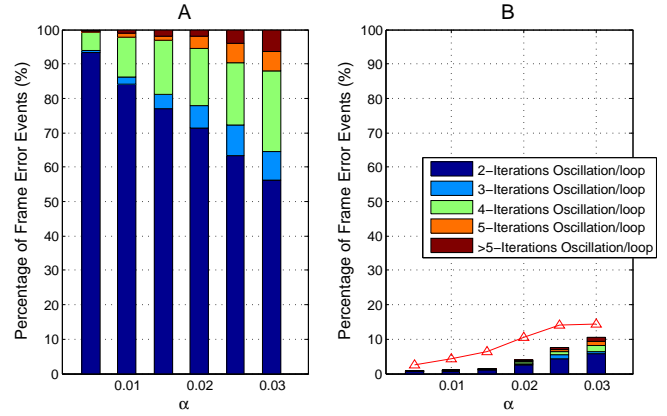


Fig. 2: The statistical analysis of decoding failure of BF decoders on the Tanner code: A. The failure types in error correction of GDBF decoder, B. The remaining after re-decoding the error codewords in (A) by PPBF (bars) and by PGDBF (red triangle-marked line).

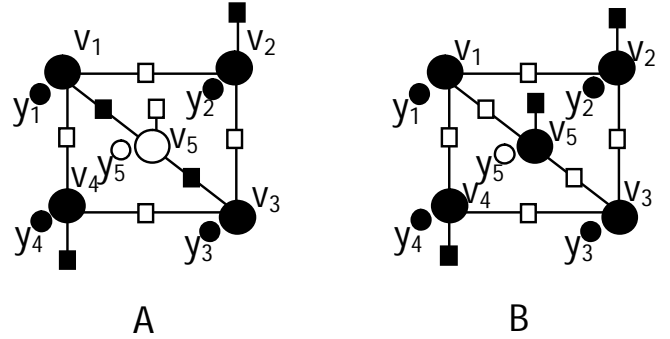


Fig. 3: The error pattern with which PGDBF failed to correct while PPBF can correct.

of the fact that, there are certain error patterns with which PGDBF failed to correct while PPBF could correct. We show an example of these error patterns in Fig. 3 where there are 4 bits in error allocated in a Trapping Set (5, 3) [13]. Fig. 3A describes the error positions initially received from the channel. The correct VNs (satisfied CNs) are denoted as white-filled circles (squares), the erroneous VNs (unsatisfied CNs) are the black-filled circles (squares). When decoding this error pattern by PGDBF decoder, the VN v_5 has maximum energy ($E_5^{(1)} = 2$) (other VNs have energy of 1) and v_5 becomes the only flip candidate. The PGDBF will either flip v_5 (if $R_5^{(1)} = 1$) or not flip v_5 (if $R_5^{(1)} = 0$). In the latter case, PGDBF keeps the same error pattern for the next iteration. In the case PGDBF flips v_5 , the error locations are illustrated in Fig. 3B and in the next iteration, v_5 is again the only flipping candidate since it has energy of 2 while others have either 1 or 0. The PGDBF may again flip or not flip v_5 depending on $R_5^{(2)}$. It can be seen that, the PGDBF is always in the two cases (Fig. 3A and Fig. 3B) for all subsequent iterations. Therefore, the PGDBF is trapped between the 2-iterations oscillation and never correct all erroneous VNs due to its maximum-energy

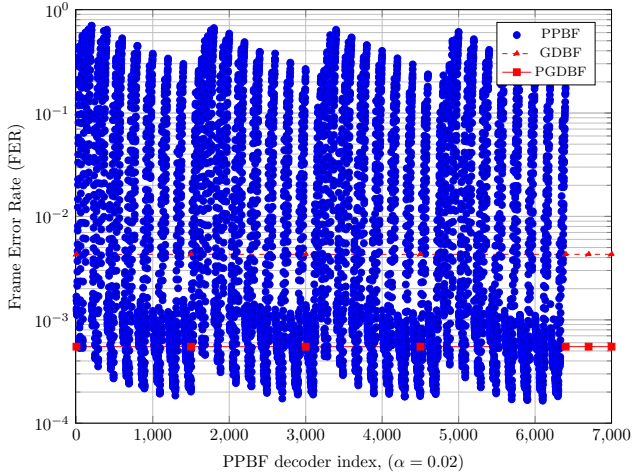


Fig. 4: The statistical analysis of PPBF decoding performance with different realization of \mathbf{p} on the Tanner code at $\alpha = 0.02$.

VN flip constraint. It is contrary in the case of PPBF where all VNs are the flipping candidates. With the above error pattern, at the first iteration, PPBF not only flips v_5 with $\mathbf{p}(2)$ (because $E_5^{(1)} = 2$) but also other erroneous VNs (v_1, v_2, v_3 and v_4) with $\mathbf{p}(1) > 0$ (because $E_1^{(1)} = E_2^{(1)} = E_3^{(1)} = E_4^{(1)} = 1$). For example, PPBF can correct this error pattern in a single iteration with probability $(\mathbf{p}(1))^4(1 - \mathbf{p}(2)) > 0$ where it flips 4 erroneous energy-1 VNs and does not flip other VNs. Using the analyzing method in [24], it is shown that PPBF will eventually correct this error pattern in a subsequent number of iterations.

The PPBF superiority in term of error correction is controlled by the values of \mathbf{p} . We show that it is feasible to choose \mathbf{p} such that PPBF provides the significant decoding gain by the following experiment. A statistics on the Frame Error Rate (FER) as a function of \mathbf{p} was conducted on the Tanner code ($d_v = 3, d_c = 5$). The testing values of \mathbf{p} were chosen with the ranges and steps as in the table I and they are explained as following. It is obvious to choose $p_0 = \mathbf{p}(0) = 0$ since the VN having all neighbor CN satisfied and being similar to the channel received value, should not be flipped. In principle, the VN that has higher energy values should have higher probability of flip. The VN that has all neighbor CN unsatisfied and its value disagrees with the channel received value (in the Tanner code, its energy is 4), should be flipped with high probability ($p_4 = \mathbf{p}(4)$ should be close to 1). The VN that has energy of 1 should be flipped with a smallest probability ($p_1 = \mathbf{p}(1)$ should be close to 0) to avoid flip too many correct VNs unintentionally since there may exist many correct VNs having the energy of 1. $p_2 = \mathbf{p}(2)$ and $p_3 = \mathbf{p}(3)$ were chosen to cover a large ranges. Table 4 shows all of the studied configurations. A nested loops are formed to cover all combinations where p_1 is in the most inner loop, p_4 is the most outer loop. There are 6400 combinations and they are marked by an index i ($0 \leq i \leq 6399$) from $\mathbf{p}^{[0]}$ to $\mathbf{p}^{[6399]}$. We run the PPBF decoder with those values of $\mathbf{p}^{[i]}$ at $\alpha = 0.02$, $It_{max} = 300$ and plot the results in Fig. 4. We also show the decoding performance of GDBF and PGDBF decoders (also

at $\alpha = 0.02$, $It_{max} = 300$) to make the comparisons.

TABLE I: The probability ranges for the statistical experiment.

	min	max	step	number of testing cases
p_0	0	0	0	1
p_1	0	0.039	0.001	40
p_2	0.1	0.5	0.1	5
p_3	0.3	1.0	0.1	8
p_4	0.7	1.0	0.1	4
Total testing cases				6400

It can be seen that, there are many values of \mathbf{p} with which PPBF decoder outperforms PGDBF decoder. This number is even larger when comparing to the GDBF decoder. Some of them may have 1.4 decade better than GDBF and 0.6 decade better than PGDBF such as $\mathbf{p}^{[5898]} = (0, 0.18, 0.3, 0.8, 1.0)$, $\mathbf{p}^{[6099]} = (0, 0.19, 0.3, 0.9, 1.0)$, etc. The numerous options of \mathbf{p} providing a good decoding performance, are very promising since they facilitate the choice of PPBF to have the good decoding performance and simplify the hardware implementation, as shown in section IV.

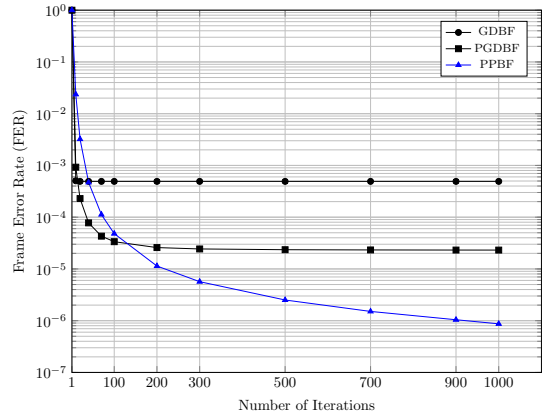


Fig. 5: The FER of GDBF, PGDBF and PPBF decoders as function of iterations on the Tanner code, $\alpha = 0.01$.

It is observed that the performance of PPBF decoder is continuously improved when increasing the number of decoding iterations. Indeed, as seen in Fig. 5 where we plot the FER as a function of the number of iterations, the PGDBF tends to saturate in correcting errors after 200 decoding iterations while the GDBF is saturated even after 10 decoding iterations. Running GDBF and PGDBF after those numbers of iterations will not provide any gain in error correction. However, this is not the case of PPBF decoder which continues to decrease the FER after the first 200 iterations. It can be seen that, when PPBF runs up to $It_{max} = 1000$ iterations, it provides around 1 decade more in FER compared to the one at 200 iterations. The PPBF is, therefore, very favorable in the applications where error correction is more privileged than the decoding time constraint.

As a conclusion of this section, our statistical analysis reveals that PPBF is a very promising decoder in term of error correction. It is even more interesting since PPBF is shown to improve significantly the decoding frequency when

being implemented, which is presented in the next section. Some research directions may be opened, *e.g.*, the theoretical optimization and the systematic choice of \mathbf{p} where it may be considered as a function of α or even a function of decoding iterations. PPBF may be optimized for the additive white gaussian noise (in which PPBF may converge to the Noisy GDBF in [27]) channel and/or on irregular LDPC codes. These interesting directions are kept as our future works.

D. The PPBF improves the decoding throughput and reduces the BF decoder complexity

Typically, the average decoding throughput of a hardware implemented BF decoder, θ (in bits/s), is computed using the Equ. 3 where f_{max} denotes the maximum decoding frequency, N_c denotes the number of clock cycles required for each decoding iteration and It_{ave} is the number of iterations in average.

$$\theta = \frac{N \cdot f_{max}}{It_{ave} \cdot N_c} \quad (3)$$

In a hardware implemented LDPC decoder, the maximal operating frequency is limited by the length of the longest data path (the so-called, critical path) and f_{max} should be inferior to $1/t_D$, ($f_{max} < 1/t_D$), where t_D is the length of the critical path to avoid the timing error when operating [25]. In order to improve the decoding throughput (assuming to keep N , It_{ave} and N_c as the constants), the hardware implementations of LDPC decoders tend to be parallelized to shorten the critical path [22], heightening maximally the achievable operating frequency f_{max} . However, the maximization of the operating frequency in some reported BF decoders in the literature such as GDBF, PGDBF [13] or MBF [10] may be limited since the global operation is required in these decoders, dramatically increasing the critical path [17]. In order to clarify the effect of the global operation on the critical path as well as the decoder complexity, we choose to analyze the architecture of PGDBF decoder in [13] (presented in Fig. 6). The operation of PGDBF decoder on this architecture may be found in that paper. The longest data path in PGDBF implementation is shown by the dashed green path in Fig. 6. This critical path starts from the output of D-FlipFlop storing $v_n^{(k)}$ and passes to the CNU, the energy computation (summation block), the Maximum Finder (MF) block, several computing units and ends at the input-D of the D-FlipFlop (the updated VN value for the next iteration, $v_n^{(k+1)}$). Many implementing methods of the MF can be found in [17]. We illustrate the implementation of MF in Fig. 6 by the binary tree of the Compare-And-Swap Units (CASUs) [10]. The CASU passes at its output the larger value of the 2 input values. The latency of the MF module can be formulated as $t_{MF} = t_c \lceil \log_2(N) \rceil$ where t_c is the delay of a single CASU module. This critical path may become longer when longer code is used. The ASIC synthesis results of the PGDBF decoder on the $d_v = 3$, $d_c = 6$, $N = 1296$, $M = 648$, code rate $R = 0.50$ regular LDPC code (dv3R050N1296) show that, the MF is more than 40% of the total length of the critical path (the details of synthesis setup are introduced in section V). The MF is also a large part of PGDBF in term of complexity since

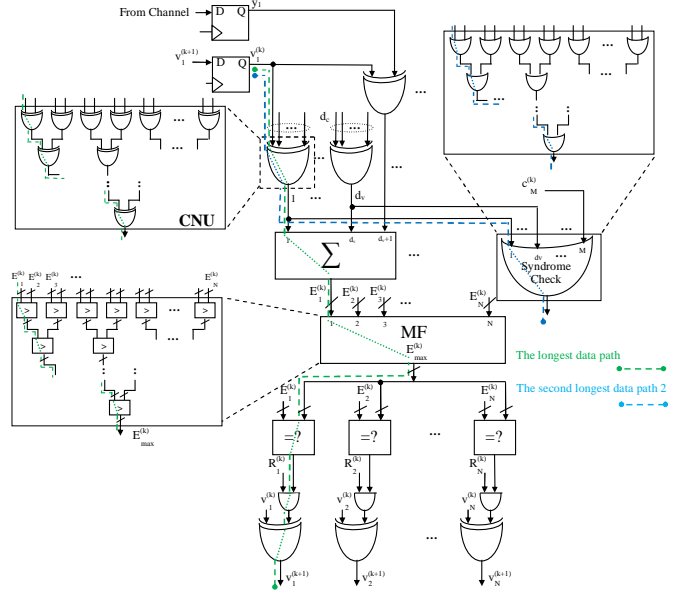


Fig. 6: The critical paths in PGDBF decoder.

it requires approximately $N - 1$ CASUs. The synthesis shows also that, the MF is responsible for 20% of the total PGDBF decoder area.

The VNs of PPBF do not require the maximum energy value in their operations. This is the source of the improvement in the term of operating frequency of PPBF. For example, it is expected that, PPBF will decrease 40% of the critical path when designed and synthesized on the same dv3R050N1296 LDPC code. Since the MF is not implemented, the decoder complexity may also be reduced, compared to that of the PGDBF.

III. THE NON-SYNDROME PROBABILISTIC PARALLEL BIT FLIPPING DECODER

The PPBF is expected to have an improvement in operating frequency since the critical path is significantly reduced (which is proven by the synthesis results in section V). In the synthesized PPBF decoder, it is observed that, the critical path of PPBF starts from the output of the D-FlipFlop storing $v_n^{(k)}$ and passes to the CNU, the SC module and ends at this SC module output (which controls the enable-input of D-FlipFlop to store $v_n^{(k+1)}$ into the place of $v_n^{(k)}$). This critical path is similar to the second longest data path in PGDBF implementation, illustrated in Fig. 6 by the dashed blue path. We target to further improve the operating frequency of PPBF by eliminating the SC module from the data path, further shortening the critical path of PPBF. This modified version of PPBF is named as NS-PPBF decoder.

In some LDPC decoding algorithms such as MS, OMS, Sum-Product or Gallager-A/B, the decoding process may continue to run when the decoder already converges to the correct codeword. This extra updating of the A-Posteriori-Probability (APP) will make the hard-decision even more solid. This property provides the possibilities that, the early stopping condition (the SC module) may not need to be implemented

(the decoding process will stop after It_{max} iterations), or may be fully pipelined to other computing process (the SC may raise the stopping signal in a subsequent number of clocks or iterations after converging) [23]. It is different in the case of BF decoders such as GDBF, PGDBF, PPBF *etc.* where the SC module plays an important role in ensuring the finding of correct codewords. Indeed, when converging to the correct codeword (all CN values are zeros), the computed energy in these BF decoders is either 0 (of the correctly received VNs from channel) or 1 (of the incorrectly received VNs from channel, the value of 1 comes from the term $v_n^{(k)} \oplus y_n$ in energy computation of Equ. 2). If the SC result is not verified to stop the decoding process, the BF decoders tend to flip the energy-1 VNs in the next iteration (GDBF will flip all energy-1 VNs while PPBF and PGDBF flip a random part of them). These decoders are re-entering to the incorrect-codeword states and the correct codeword may not be found after It_{max} iterations or in a subsequent number of iterations after converging. Because of this flipping principle, the SC can not be fully pipelined when implementing the BF decoders (note further that, since the computations are simple, in the literature, these BF decoders are usually implemented such that they take only $N_c = 1$ clock cycle for 1 decoding iteration). In PPBF, SC module becomes a part of the critical path. Moreover, the SC is a global operation which verifies all the values of M CNs in each iteration. It occupies, therefore, a noticeable part of that critical path in PPBF. In fact, SC delays a period of $t_{SC} = t_o \lceil \log_2(M) \rceil$, where t_o is the delay of a single OR gate, when being implemented as a binary tree of OR gates (as in Fig. 6). The hardware synthesis of PPBF shows that, the delay of SC module is around 20% of the PPBF critical path length. We propose in NS-PPBF decoder a new flipping mechanism which does not depend on the SC result.

Algorithm 3 The VN operations of the NS-PPBF decoder

```

1: for  $1 \leq n \leq N$  do ▷ VN processing
2:   Compute  $E_n^{(k)}$ , using Equ. (2).
3:   if  $E_n^{(k)} \neq 1$  or  $v_n^{(k)} \neq y_n$  then
4:     Generate  $R_n^{(k)}$  from  $\mathcal{B}(\mathbf{p}(E_n^{(k)}))$ .
5:     if  $R_n^{(k)} = 1$  then
6:        $v_n^{(k+1)} = v_n^{(k)} \oplus 1$ 
7:     end if
8:   end if
9: end for

```

The proposed flipping mechanism targets to automatically stop the NS-PPBF decoding process when all the CNs are satisfied (all CNs are 0's). The VN operation of NS-PPBF is described in Algorithm 3. It can be seen that, the flipping of NS-PPBF decoder is almost similar to that of the PPBF decoder and the difference is on the flipping when the VN energy is 1. In fact, it is sufficient to consider only the case that $E_n^{(k)} = 1$ because when the codeword is found, the VN produces only the values 1 or 0 as its energy. In NS-PPBF, when the energy $E_n^{(k)} = 1$, it separates the case where the value 1 is because of the term $v_n^{(k)} \oplus y_n$ and the case where the value 1 is because of the term $\sum_{c_m \in \mathcal{N}(v_n)} c_m^{(k)}$. NS-PPBF

then flip the VN having $E_n^{(k)} = 1$ with probability $p_1 = \mathbf{p}(1)$ only in the latter case. It means that, NS-PPBF will not flip the VNs having energy 1 coming from the disagreement between the current value and the channel value. By using this principle, whenever a correct codeword is found, all the CNs are satisfied, the NS-PPBF will not flip any VNs and the current $\mathbf{v}^{(k)}$ is preserved. The decoding process will stop either when It_{max} iterations have been reached (if the SC is not implemented), or the pipelined implemented SC produces the stopping signal. $\mathbf{v}^{(k)}$ is then declared as the decoded codeword.

It can be seen that, the NS-PPBF decoding process will terminate without using the signal from the SC module. The SC contribution to the critical path have been eliminated, which will improve the operating frequency of the decoder. However, with the constraint applied in energy-1 flipping, it may reduce the decoding dynamic and leads to a small degradation in error correction, compared to the PPBF decoder. This decoding degradation will be discussed in the section V.

IV. THE HARDWARE IMPLEMENTATION ARCHITECTURE

In order to verify the efficiency of the proposed BF decoders in terms of decoding frequency and decoder complexity, the hardware architectures implementing these decoders are introduced in this section. These hardware architectures are then synthesized on the Application-Specific Integrated Circuit (ASIC). The synthesis results and discussions are presented in the next section.

The first proposed hardware architecture to implement PPBF decoder is presented in Fig. 7. Similarly to the architecture of PGDBF decoder, the CN operations is realized by the d_c -input XOR gates. The VN energy value is computed by the summation block whose inputs are the CN computation results and the XOR1 (computing the term $v_n^{(k)} \oplus y_n$). The key feature of this architecture is that, the computed energy values will control the threshold input of a random generator (RG). This threshold input is used to control the probability of the generated bit and by doing that, the probability of the generated bit is adapted for each VN and each iteration. One RG method could be used is the Linear Feedback Shift Register (LFSR) as in [18]. The VN value for the next iteration, $v_n^{(k+1)}$, is computed by the XOR2 gate basing on the generated bit and the VN current value $v_n^{(k)}$. The $v_n^{(k+1)}$ is an inversion of $v_n^{(k)}$ if the generated bit $R_n^{(k)} = 1$ since $X \oplus 1 = \mathbf{NOT}(X)$, $\forall X$. When the generated bit $R_n^{(k)} = 0$, $v_n^{(k+1)} = v_n^{(k)}$ since $X \oplus 0 = X$, $\forall X$. The SC module is implemented to stop the decoder when the correct codeword is found. This architecture can fully execute the operations of the PPBF decoder and can also be adapted for the NS-PPBF. However, the results reported in [18] revealed that, this method may be costly since each VN requires an LFSR module and the decoder complexity may be increased due to these RGs, especially when the LDPC code with large N is used. We leave aside this architecture and focus on a low-complexity solution to generate the binary random signals, introduced in [13], called Cyclic Shift Truncated Sequence (CSTS).

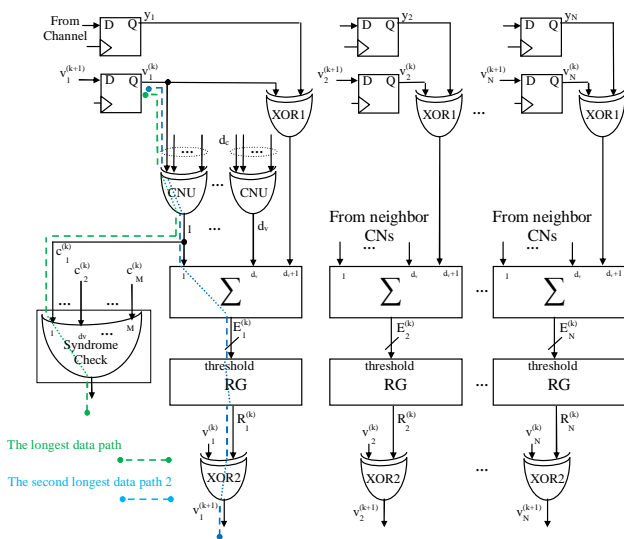


Fig. 7: The LFSR-based implementation of PPBF decoder.

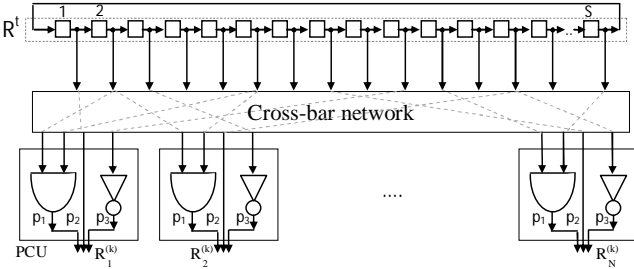


Fig. 8: The proposed probabilistic signal generator (random generator - RG) for PPBF decoder.

A. The probabilistic signal generator for PPBF and NS-PPBF decoders

Inspired by the results of [13] where the correlation in the random generation may not much affect the error correction of the probabilistic BF decoders, we apply that CSTS approach to implement the RGs for PPBF and NS-PPBF decoders, to reduce the hardware resources. In CSTS, a short D-FlipFlop sequence, R^t with size $|R^t| = S < N$, is allocated. R^t initially stores the generated bits where the 1's are with the ratio of p_r on the total of bits, and they are distributed in an arbitrary order. For each clock cycle, R^t is cyclically shifted. It can be approximated that, in S clock cycles, each output of R_t produces the 1's with probability p_r . The outputs of D-FlipFlops in R^t have been used as a random bit, triggered to the Variable Node Processing Units (VNUs) and one output can be used for multiple VNUs of the PGDBF without degrading the decoding performance [13].

The RGs of the PPBF and NS-PPBF decoders require to generate the random bits with different probabilities. In order to produce these desired probabilities, we use the logic gates as introduced in [18] and its principle is briefly recalled as following. Let a and b be two binary values with $\Pr(a = 1) = p_r$ and $\Pr(b = 1) = p_r$, it can be shown that, $\Pr(a \text{ AND } b = 1) = p_r^2$, $\Pr(\text{NOT}(a) = 1) = 1 - p_r$ and $\Pr(a$

OR $b = 1) = 2p_r - p_r^2$. Other logic functions such as XOR *etc.* can also be formulated. We design the Probability Controlling Units (PCUs), composed by the logic gates, to produce the random bits for our PPBF and NS-PPBF decoders. The PCU has the binary values from R^t as its inputs through the crossbar network and has several binary outputs. Each output has different probability to be 1, which is transformed from the probability p_r from R^t .

In this paper, we target to implement PPBF and NS-PPBF decoders for the Tanner and the dv3R050N1296 LDPC codes which have the $d_v = 3$. The extension for other LDPC codes which have higher VN degree, *i.e.* $d_v \geq 4$, is straightforward. As shown in the statistical analysis, several values of \mathbf{p} may be used to provide the good decoding performance gain. We use $\mathbf{p}^{[5689]} = (0, 0.09, 0.3, 0.7, 1)$ as an example to implement since it provides a good error correction while facilitating the hardware implementation. In fact, it can be shown that, $\mathbf{p}^{[5689]} \neq (0, p_r, p_r, 1 - p_r, 1)$ where $p_r = 0.3$. The designed RG is shown in Fig. 8 where N PCUs are designed for N VNUs. Each PCU has $d_v = 3$ outputs (internally named as p_1, p_2 and p_3). The outputs have the value of 1 with the probability correspondingly to p_1, p_2 and p_3 . The outputs of each PCU are triggered to the corresponding implemented VNU of the PPBF and NS-PPBF, presented in the next section.

B. The computing units of PPBF decoder

PPBF decoder is realized in hardware by two connection networks connecting two groups of processing units: the VNUs and CNU. The proposed architecture to implement PPBF decoder is presented in Fig. 9. The connection network 1 transmits the messages from VNUs to CNU and the connection network 2 is to transfer the messages from CNU to VNUs. The CNU in PPBF decoder are also the d_c -inputs XOR gates, computing the parity check on the VN messages. The CNU outputs are transmitted to the VNU inputs and we denote (as in Fig. 9) c_m as the group of messages of $c_m \in \mathcal{N}(v_n), 1 \leq n \leq N$. In each VNU, the summation block computes the VN energy value and this computed energy controls the selection of the multiplexer MUX5to1 module. The MUX5to1 module is a key module which results to flip or not the VN current value, $v_n^{(k)}$, by producing 1's or 0's at its output. When the output of MUX5to1 is 1's, the VN current value, $v_n^{(k)}$, is XOR-ed by 1 by the XOR2 and is flipped, otherwise, $v_n^{(k+1)} = v_n^{(k)} \oplus 0 = v_n^{(k)}$. The flipping probability of $v_n^{(k)}$ is, therefore, controlled its energy. Indeed, the input 0 of MUX5to1 is always reset to 0 while the input 4 is set to 1 which results the fact that, the VN which has energy of 0 is not flipped and the VN having energy of 4 is flipped with probability of 1. When the energy is from 1 to 3, the corresponding flipping probability is arranged as p_1, p_2 and p_3 , controlled by the RG. The SC is implemented by M -inputs OR gate whose inputs are the outputs of the CNU. The decoder will stop when SC produces 0.

It should be noted that, this PPBF architecture requires $N_c = 1$ clock cycle for each decoding iteration. The critical path of the PPBF is denoted by the dashed green path and the second longest data path is shown by the dashed blue path in

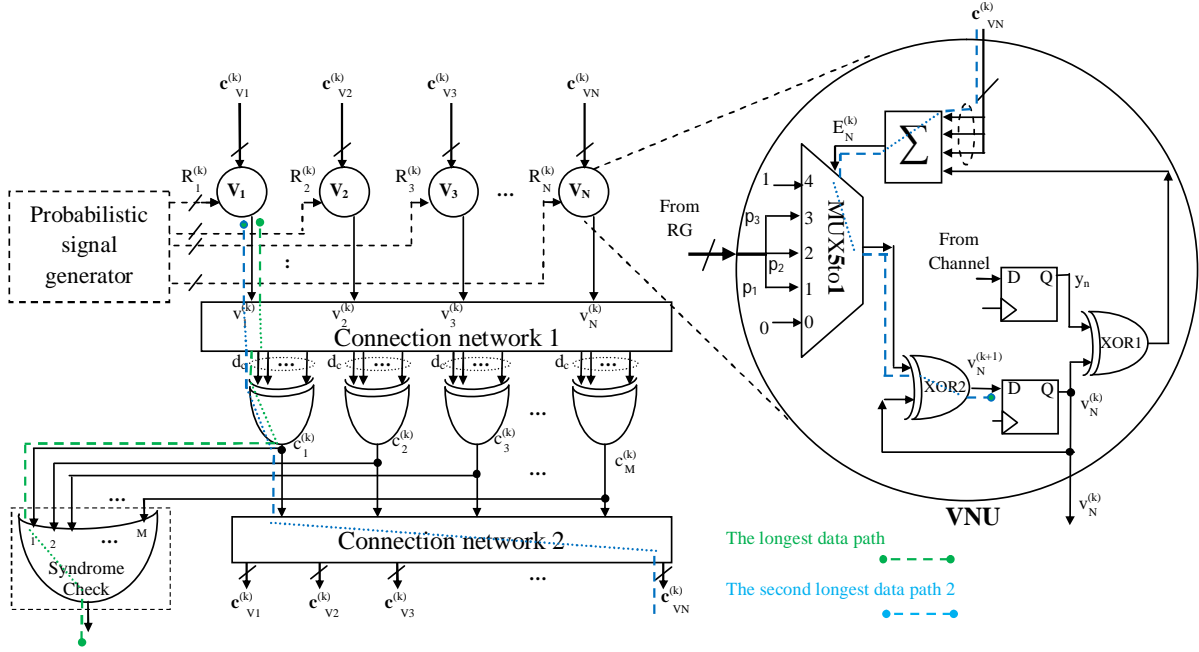


Fig. 9: The proposed architecture for the realization of PPBF decoder for $d_v = 3$ LDPC codes.

Fig. 9.

C. The computing units of NS-PPBF decoder

The implementation architecture of NS-PPBF decoder is presented in Fig. 10, in which it follows mostly the principle of PPBF architecture. The difference comes from the added multiplexer MUX2to1. The MUX2to1 is controlled by the output of the XOR1 which indicates the similarity between the $v_n^{(k)}$ and y_n . This added MUX2to1 contributes to the flipping feature of NS-PPBF in the case when the energy-1 appears. In fact, when $E_n^{(k)} = 1$ and $v_n^{(k)}$ differs from y_n , XOR2 always receives 0's from MUX5to1 and $v_n^{(k)}$ will not be flipped. When $E_n^{(k)} = 1$ and $v_n^{(k)}$ equals to y_n , XOR2 receives signal from the RG with the probability p_1 to be equal to 1.

In the NS-PPBF hardware architecture, the SC is not implemented and the decoder will stop after It_{max} iterations. The critical path of NS-PPBF in the synthesized decoder is shown by the dashed green path in Fig. 10.

V. SYNTHESIS RESULTS AND DECODING PERFORMANCE

A. Synthesis results

In this section, we report the ASIC synthesis results of our decoder implementations. The proposed decoders are implemented using the Digital Standard Cell Library SAED-EDK90-CORE, Process 1P9M 1.2v/2.5v. The hierarchical design flow is followed with the Synopsys Design Platform: Synopsys Design Compiler is used for VHDL synthesis, Synopsys VCS tool for simulation and DVE, a graphical user interface for debugging and viewing waveforms. Synopsys Prime Time tool is used for timing analysis, power and energy estimation, and Synopsys IC Compiler (ICC) is used for floor planning, place and route.

We make the first synthesis of our decoders on the Tanner code ($d_v = 3, d_c = 5, N = 155, M = 93$). Our strategy is to look for the minimum timing constraint to which the synthesizer can pass (which indicates the maximum achievable frequency that the decoders can operate) after place-and-route synthesizing processing. The GDBF and PGDBF decoders are implemented following the architecture described in [13]. The synthesis results are reported in Table II. It can be seen, as expected, that PPBF increases more than 43% in the operating frequency compared to GDBF and PGDBF while NS-PPBF is even more than 64%. The average decoding throughput at $\alpha = 0.012$ is also provided. It is shown that, the PPBF and NS-PPBF are faster in decoding speed than PGDBF (with 28.1 Gbps and 32.5 Gbps compared to 25.3 Gbps). In term of hardware complexity, PPBF reduces 3.4% and NS-PPBF reduces 1.4% compared to the PGDBF. This complexity reduction is interesting since PPBF and NS-PPBF provide a better error correction (shown in the next sub-section) while requiring less hardware resources. The complexity reduction is modest because of the fact that, our decoders do not require the MF (which significantly reduces the complexity). However, their RGs are more costly than that of the PGDBF, which diminishes the advantage of the MF removal. Our decoders consume more energy than other BF decoders. PPBF needs 0.59 pJ to decode 1 bit while NS-PPBF requires 0.6 pJ, compared to 0.33 pJ of PGDBF and 0.24 pJ of GDBF. It is because of the fact that, the proposed decoders operate at higher frequency. Also, more switching activities may be produced in PPBF and NS-PPBF due to the randomness injection in all levels of VN energy.

In the second synthesis, we implement the proposed decoders for the longer code (the dv3R050N1296 LDPC code). We put them on comparisons with other BF-based decoders

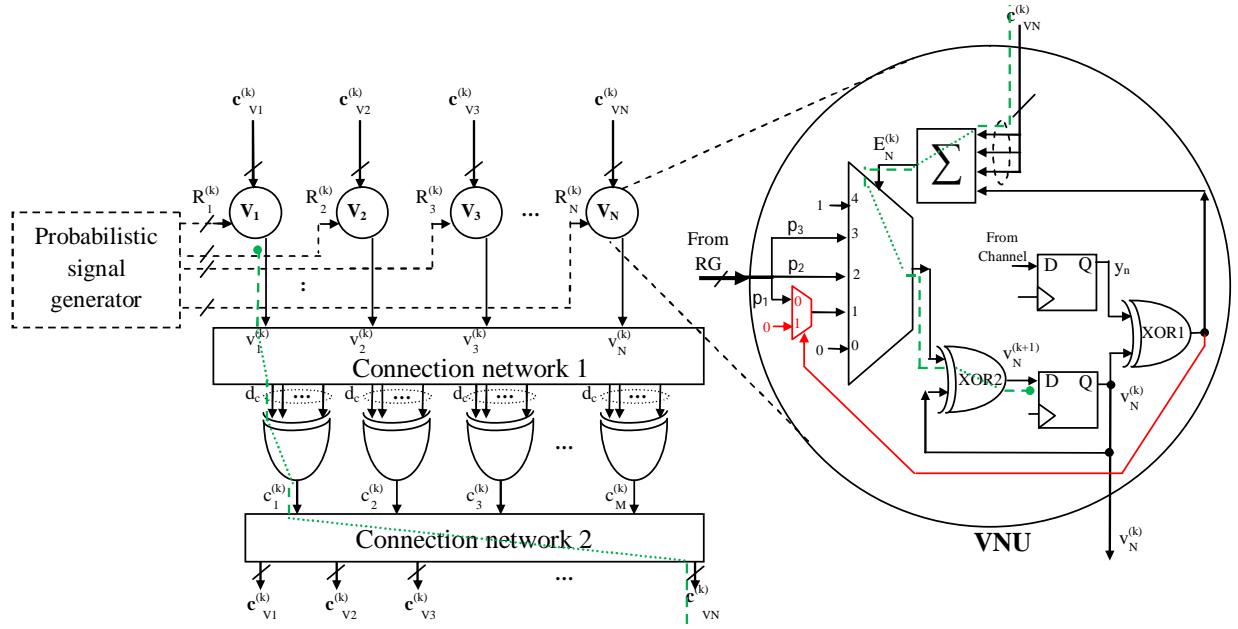


Fig. 10: The proposed architecture for the realization of NS-PPBF decoder for $d_v = 3$ LDPC codes.

TABLE II: The synthesis results of PPBF and NS-PPBF in the comparisons to GDBF and PGDBF decoders on the Tanner Code. All the RGs are the CSTS-based implementations with $S = 155$. PGDBF is with $p = 0.7$. The average throughput θ and the average power consumption (energy/bit) are computed at $\alpha = 0.012$.

	Area (μm^2)	f_{max} (MHz)	θ (Gbps)	Energy/bit (pJ)
GDBF	39528 (-17.6%)	435 (+0%)	30.4	0.24
PGDBF	46472 (-0.0%)	435 (+0%)	25.2	0.33
PPBF	44881 (-3.4%)	625 (+43.7%)	28.1	0.59
NS-PPBF	45814 (-1.4%)	714 (+64.1%)	32.5	0.60

as well as the MS benchmark on the literature. It can be seen in the table III that, PPBF and NS-PPBF provide a significant gain in decoding frequency. PPBF can operate at $f_{max} = 476$ MHz and NS-PPBF is at $f_{max} = 556$ MHz, compared to 385 MHz of GDBF and 357 MHz of PGDBF. PPBF and NS-PPBF are much faster than MS (250 MHz) and ATBF (250 MHz). In term of hardware complexity, the proposed decoders require the smaller hardware resource to be implemented. The required area is from $0.35 - 0.37 mm^2$ which is equivalent to that of the GDBF (and PGDBF) decoder. It is only 1/5 of SBF, 1/4 of MS and 1/2 of ATBF decoders. In term of decoding throughput, we compute θ in the worst case (where It_{max} is used) and in the average case (where It_{ave} at $FER = 10^{-5}$ is used). In the former case, the proposed decoders provide the throughput from 2 to 2.5 Gbps which are higher than the GDBF (1.44 Gbps), PGDBF (1.35 Gbps) and MS (1.95 Gbps). The better decoding throughput is also observed in the average throughput to maintain the FER at 10^{-5} . In order to make the comparison in the hardware efficiency, we produce the throughput area ratio (TAR) of all the synthesis results and make comparison to other decoders.

It can be seen that, the TAR of PPBF and NS-PPBF (218–272 $Gbps/mm^2$) are much higher than the other decoders such as ATBF (34.6 $Gbps/mm^2$), SBF (18.8 $Gbps/mm^2$) and MS (16.7 $Gbps/mm^2$).

B. Decoding performance

The decoding performance of the PPBF and NS-PPBF decoders, simulated on several LDPC codes, is shown in this section. The values of \mathbf{p} are chosen by empirical experiments. On the illustrating figures, we show the decoding performance comparisons with other hard decision decoders such as the conventional BF, GDBF, PGDBF and Gallager-B (GaB). All hard decision decoders are run with $It_{max} = 300$. The performance of the quantized soft-decision MS decoder, implemented in layered scheduling with 4 bits for LLR and 6 bits for APLLR [21], is also added, with the $It_{max} = 20$.

Fig. 11 shows the decoding performance on the Tanner code. It can be seen that, the PPBF is the best error correction compared to all other BF decoders. NS-PPBF is better than the PGDBF especially in the low-error rate region. With a small degradation compared to PPBF, NS-PPBF is at the gains of decoding throughput as shown in the previous section. We also extend the simulation of PPBF and NS-PPBF on this Tanner code to run up to $It_{max} = 1000$. Our proposed decoders provide a significant gain in the decoding performance as shown in the statistical analysis. At $\alpha = 0.004$, PPBF provides around 2 decades gain in FER compared to PGDBF, 3.3 decades when compared to GDBF. With $It_{max} = 1000$, PPBF gains around 1 decade in FER when compared to itself with $It_{max} = 300$, which confirms the superiority of PPBF when increasing the number of decoding iterations. It is also shown that, the decoding performance of PPBF and NS-PPBF is very close to that of the MS decoder.

TABLE III: Comparison between the proposed BF decoders and the state-of-the-art LDPC decoders.

	This work		K.Le'17[26]		M.Ismail'13[20]	J.Cho'10[28]	Nguyen-Ly'16[21]
(N, M)	(1296, 648)		(1296, 648)		(1008, 504)	(1057, 813)	(1296, 648)
Decoder	PPBF	NS-PPBF	GDBF	PGDBF	ATBF	SBF	MS(4, 6)
Technology	90nm		90nm		90nm	180nm	65nm
Frequency (MHz)	476	556	385	357	250	345	250
Area (mm^2)	0.367	0.349	0.360	0.367	0.729	7.4	0.72
Area scaled to 90nm (mm^2)	0.367	0.349	0.360	0.367	0.729	1.85	1.38
It_{max}	300	300	300	300	—	40	20
Throughput @ It_{max} (Gbps)	2.06	2.45	1.44	1.35	—	$\theta_{min} = 0.253$	2.7
Tput scaled to 90nm (Gbps)	2.06	2.45	1.44	1.35	—	0.506	1.95
It_{ave} @ FER= 10^{-5}	7.71	7.58	2.24	5.48	—	—	2.34 [26]
	@ $\alpha \approx 0.012$	@ $\alpha \approx 0.012$	@ $\alpha \approx 0.005$	@ $\alpha \approx 0.011$			@ $\alpha \approx 0.025$
Average throughput @ FER= 10^{-5} (Gbps)	80	95.1	222.8	84.4	25.2 @ $It = 10$	$\theta_{max} = 17.37$	-
Average throughput scaled to 90nm (Gbps)	80	95.1	222.8	84.4	25.2	34.74	23.1 [26]
Average TAR ($Gbps/mm^2$) (90nm)	218	272.4	618.9	230	34.6	18.8	16.7

The decoding performance on other LDPC codes with different (VN and CN) node degrees and code rates, are shown in Fig. 12, 13 and 14. Fig. 12 shows the performance on the dv3R050N1298 ($d_v = 3, d_c = 6, N = 1296$, code rate $R = 0.5$) LDPC code. With the chosen value of \mathbf{p} , PPBF and NS-PPBF have the equivalent error correction and they are better than PGDBF when $FER > 1e^{-5}$. Compared to GDBF decoder, PPBF and NS-PPBF provide a significant gain in performance, half-way approaching the MS, while requiring the equivalent hardware complexity and 1.5 times faster in decoding speed, as shown in the previous section.

The good decoding performance of PPBF and NS-PPBF are also observed on $d_v = 3, d_c = 6, N = 1296$, code rate $R = 0.75$ code (Fig. 13) and $d_v = 4, d_c = 8, N = 1296$, code rate $R = 0.5$ (Fig. 14). Especially, PPBF and NS-PPBF are very close to the MS performance for the latter code.

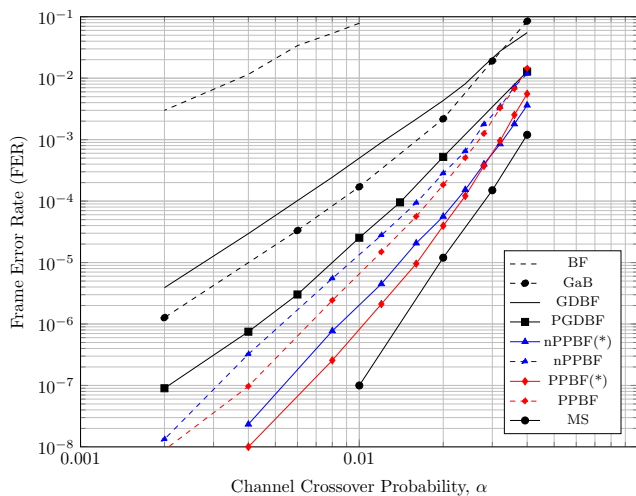


Fig. 11: The decoding performance of PPBF and NS-PPBF with $\mathbf{p} = (0, 0.019, 0.3, 0.9, 1.0)$, on comparison to other BF decoders and to the MS on the Tanner code. (*) are the decoding performance with $It_{max} = 1000$.

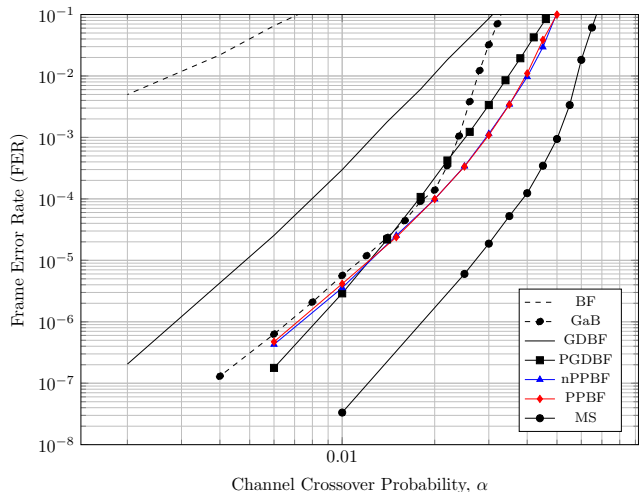


Fig. 12: The decoding performance of PPBF and NS-PPBF with $\mathbf{p} = (0, 0.004, 0.3, 0.9, 0.7)$, on comparison to other BF decoders and to the MS on the $d_v = 3, d_c = 6, N = 1296$, code rate $R = 0.5$ LDPC code.

VI. CONCLUSION

In this paper, we propose a new high-throughput, low-complexity Bit Flipping decoder for Low-Density Parity-Check (LDPC) codes on Binary Symmetric Channel (BSC), called Probabilistic Parallel Bit Flipping (PPBF). The PPBF is more advantageous than other state-of-the-art BF decoders such as the Gradient Descent Bit Flipping and Probabilistic Gradient Descent Bit Flipping decoders, in terms of operating frequency and decoder complexity, thanks to the elimination of the global operation which helps shorten the critical path and reduce the decoder hardware cost. Furthermore, in PPBF, the probabilistic flipping of the Variable Node is introduced for all levels of its energy value rather than only on the maximum values as in PGDBF. PPBF provides, therefore, a very good error correction capability and in some cases, overcomes some error patterns with which PGDBF can not correct. One improved version of PPBF, named as non-syndrome Proba-

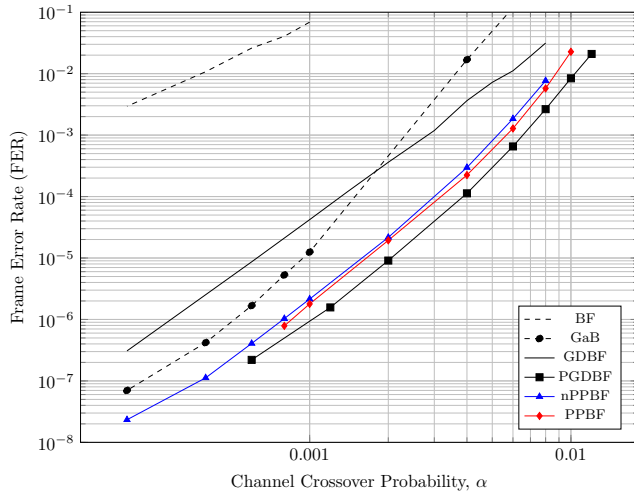


Fig. 13: The decoding performance of PPBF and NS-PPBF with $\mathbf{p} = (0, 0.001, 0.1, 1.0, 1.0)$, on comparison to other BF decoders on the $d_v = 3, d_c = 6, N = 1296$, code rate $R = 0.75$ LDPC code.

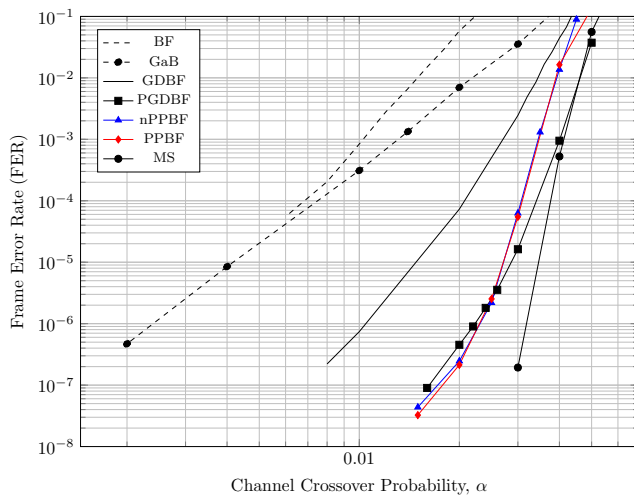


Fig. 14: The decoding performance of PPBF and NS-PPBF with $\mathbf{p} = (0, 0.001, 0.05, 0.3, 0.95, 0.95)$, on comparison to other BF decoders and to the MS on the $d_v = 4, d_c = 8, N = 1296$, code rate $R = 0.5$ LDPC code.

bilistic Parallel Bit Flipping (NS-PPBF), is then introduced in which the critical path is further shortened by eliminating the global Syndrome Check module from the data path. The operating frequency of the NS-PPBF is heightened while a negligible error correction degradation observed, with respect to those of the PPBF. The hardware architectures to implement the PPBF and NS-PPBF decoders are introduced with the detailed circuits of the random generator and computing units. The ASIC synthesis results of the proposed architectures re-confirm as expected that, PPBF and NS-PPBF are high hardware-efficiency and high decoding throughput. The proposed PPBF and NS-PPBF appear as the very low-complexity, high throughput decoders with the significant improvement in error correction, which can be seen as the competitive

candidates for the next communication and storage standards.

ACKNOWLEDGMENT

This work was funded by the french ANR under grant number ANR-15-CE25-0006-01 (NAND project).

REFERENCES

- [1] "Wireless lan medium access control and physical layer specifications: Enhancements for higher throughput, p802.11n/d3.07," *IEEE-802.11n*, Mar. 2008.
- [2] "Local and metropolitan area networks - part 16, ieee std 802.16a-2003," *IEEE-802.16*.
- [3] D. Declercq, M. Fossorier, and E. Biglieri, "Channel coding: Theory, algorithms, and applications," *Academic Press Library in Mobile and Wireless Communications, Elsevier, ISBN: 978-0-12-396499-1*, 2014.
- [4] R. G. Gallager, "Low density parity check codes," *MIT Press, Cambridge, 1963, Research Monograph series*, 1963.
- [5] "Ieee standard for information technology - corrigendum 2: Ieee std 802.3an-2006 10gbase-t correction," *IEEE Std 802.3-2005/Cor 2-2007 (Corrigendum to IEEE Std 802.3-2005)*, Aug. 2007.
- [6] S. Jeon and B. V. K. V. Kumar, "Performance and complexity of 32 k-bit binary ldpc codes for magnetic recording channels," *IEEE Transactions on Magnetics*, vol. 46, no. 6, pp. 2244–2247, June 2010.
- [7] K. C. Ho, C. L. Chen, Y. C. Liao, H. C. Chang, and C. Y. Lee, "A 3.46 gb/s (9141,8224) ldpc-based ecc scheme and on-line channel estimation for solid-state drive applications," in *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2015, pp. 1450–1453.
- [8] G. Dong, N. Xie, and T. Zhang, "On the use of soft-decision error-correction codes in nand flash memory," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 58, no. 2, pp. 429–439, Feb 2011.
- [9] G. document, "Ldpc codes for the enhanced mobile broadband (embb) data channel in the 3gpp 5g new radio," [Online]. Available: http://www.3gpp.org/ftp/tsg_ran/WG1_RL1/TSGR1_88/Report/.
- [10] J. Jung and I. C. Park, "Multi-bit flipping decoding of ldpc codes for nand storage systems," *IEEE Communications Letters*, vol. PP, no. 99, pp. 1–1, 2017.
- [11] Y. Du, Q. Li, L. Shi, D. Zou, H. Jin, and C. J. Xue, "Reducing ldpc soft sensing latency by lightweight data refresh for flash read performance improvement," in *2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2017, pp. 1–6.
- [12] O. A. Rasheed, P. Ivanis, and B. Vasić, "Fault-tolerant probabilistic gradient-descent bit flipping decoder," *IEEE Communications Letters*, vol. 18, no. 9, pp. 1487–1490, Sept 2014.
- [13] K. Le, F. Ghaffari, D. Declercq, and B. Vasić, "Efficient hardware implementation of probabilistic gradient descent bit-flipping," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 4, pp. 906–917, April 2017.
- [14] M. Tanner, D. Srkdhara, and T. Fuja, "A class of group-structured ldpc codes," in *Proc. 5th Int. Symp. Commun. Theory App.*, July 2001.
- [15] D. Declercq, C. Winstead, B. Vasic, F. Ghaffari, P. Ivanis, and E. Boutillon, "Noise-aided gradient descent bit-flipping decoders approaching maximum likelihood decoding," in *2016 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC)*, Sept 2016, pp. 300–304.
- [16] B. Vasić, P. Ivanis, and D. Declercq, "Approaching maximum likelihood performance of ldpc codes by stochastic resonance in noisy iterative decoders," in *Information Theory and Applications Workshop*, Feb. 2016.
- [17] B. Yuçe, H. F. Ugurdag, S. Goren, and G. Dunder, "Fast and efficient circuit topologies for finding the maximum of n k-bit numbers," *IEEE Transactions on Computers*, vol. 63, no. 8, pp. 1868–1881, Aug 2014.
- [18] K. Le, D. Declercq, F. Ghaffari, C. Spagnol, E. Popovici, P. Ivanis, and B. Vasić, "Efficient realization of probabilistic gradient descent bit flipping decoders," in *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2015, pp. 1494–1497.
- [19] G. Sundararajan, *Noisy Gradient Descent Bit Flip Decoding of Low Density Parity Check Codes: Algorithm and Implementation*. Doctoral dissertation, Utah State University, Logan, Utah, 2016, 2016.
- [20] M. Ismail, I. Ahmed, , and J. Coon, "Low power decoding of ldpc codes," *ISRN Sensor Networks*, vol. 2013, no. 650740, 2013.
- [21] T. T. Nguyen-Ly, T. Gupta, M. Pezzin, V. Savin, D. Declercq, and S. Cotozana, "Flexible, cost-efficient, high-throughput architecture for layered ldpc decoders with fully-parallel processing units," in *2016 Euromicro Conference on Digital System Design (DSD)*, Aug 2016, pp. 230–237.

- [22] T. T. Nguyen-Ly, V. Savin, K. Le, D. Declercq, F. Ghaffari and O. Boncalo, "Analysis and Design of Cost-Effective, High-Throughput LDPC Decoders," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. PP, No. 99, pp. 114, 2017.
- [23] D. Declercq, V. Savin, O. Boncalo and F. Ghaffari, "An Imprecise Stopping Criterion Based on In-Between Layers Partial Syndromes," in *IEEE Communications Letters*, Vol. 22, No. 1, pp. 1316, Jan. 2018.
- [24] B. Vasić, P. Ivanis, D. Declercq and K. LeTrung, "Approaching maximum likelihood performance of LDPC codes by stochastic resonance in noisy iterative decoders," in *2016 Information Theory and Applications Workshop (ITA)*, La Jolla, CA, 2016, pp. 1-9.
- [25] F. Leduc-Primeau, F. R. Kschischang and W. J. Gross, "Modeling and Energy Optimization of LDPC Decoder Circuits with Timing Violations," in *IEEE Transactions on Communications*, vol. PP, no. 99, pp. 1-1, 2017.
- [26] K. Le, D. Declercq, F. Ghaffari, L. Kessal, O. Boncalo and V. Savin, "Variable-Node-Shift Based Architecture for Probabilistic Gradient Descent Bit Flipping on QC-LDPC Codes," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. PP, no. 99, pp. 1-1, 2018.
- [27] G. Sundararajan, C. Winstead and E. Boutillon, "Noisy Gradient Descent Bit-Flip Decoding for LDPC Codes," in *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3385-3400, Oct. 2014.
- [28] J. Cho, J. Kim and W. Sung, "VLSI Implementation of a High-Throughput Soft-Bit-Flipping Decoder for Geometric LDPC Codes," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 5, pp. 1083-1094, May 2010.



Khoa Le received his bachelor and Master of science degrees in Electronics Engineering from Ho Chi Minh City University of Technology (HCMUT), Vietnam in 2010 and 2012, respectively. He received the Ph.D degree from the University of Cergy-Pontoise, France in 2017. Khoa is currently a post-doctoral researcher in ETIS laboratory, ENSEA, France. His research interests are in error correcting code algorithms, analysis and their implementations in FPGA/ASIC.



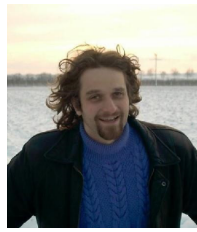
Fakhreddine GHAFARI received the Electrical Engineering and Master degrees from the National School of Electrical Engineering (ENIS, Tunisia), in 2001 and 2002, respectively. He received the Ph.D degree in electronics and electrical engineering from the University of Sophia Antipolis, France in 2006. He is currently an Associate Professor at the University of Cergy Pontoise, France. His research interests include VLSI design and implementation of reliable digital architectures for wireless communication applications in ASIC/FPGA platform and

the study of mitigating transient faults from algorithmic and implementation perspectives for high-throughput applications.



Lounis Kessal received his PhD degree of micro-electronics in 1987 from the Paris-XI University. He is currently associate professor at ENSEA engineering school and doing research activities at ETIS laboratory. His research interests are essentially on real-time image processing. His previous research works lead him to study the interest of the dynamic reconfiguration approach in architectures dedicated to signal and image processing. Lounis Kessal is also working on Reconfigurable Systems on Chip (RSoC) and ASIC/FPGA implementations of error

correcting code algorithms.



David Declercq was born in June 1971. He graduated his PhD in Statistical Signal Processing 1998, from the University of Cergy-Pontoise, France. He is currently full professor at the ENSEA in Cergy-Pontoise. He is the general secretary of the National GRETSI association, and Senior member of the IEEE. He has held the junior position at the "Institut Universitaire de France" from 2009 to 2014. His research topics lie in digital communications and error-correction coding theory. He worked several years on the particular family of LDPC codes, both from the code and decoder design aspects. Since 2003, he developed a strong expertise on non-binary LDPC codes and decoders in high order Galois fields GF(q). A large part of his research projects are related to non-binary LDPC codes. He mainly investigated two aspects: (i) the design of GF(q) LDPC codes for short and moderate lengths, and (ii) the simplification of the iterative decoders for GF(q) LDPC codes with complexity/performance tradeoff constraints. David Declercq published more than 40 papers in major journals (IEEE-Trans. Commun., IEEE-Trans. Inf. Theo., Commun. Letters, EURASIP JWCN), and more than 120 papers in major conferences in Information Theory and Signal Processing.



Emmanuel Boutillon was born in Chatou, France in 1966. He received the Engineering Diploma from the Telecom Paris Tech, Paris, France in 1990. In 1991, he worked as an assistant professor in the Ecole Multinationale Supérieure des Tlcommunications in Africa (Dakar). In 1992, he joined Telecom Paris Tech as a research engineer where he conducted research in the field of VLSI for digital communications. He obtained his Ph.D in 1995. In 1998, he spent a sabbatical year at the University of Toronto, Ontario, Canada. In 2000, he moved to the University of Bretagne Sud as a professor. He headed the LESTER lab from 2005 up to end of 2007 and the CACS department between 2008 up to 2015. He is currently the scientific adviser of the lab-STICC. In 2011, he had a sabbatical year at INICTEL-UNI, Lima (Peru).

His research interests are on the interactions between algorithm and architecture in the field of wireless communications and high speed signal processing. In particular, he works on Turbo Codes and LDPC decoders.



Chris Winstead received the B.S. degree in Electrical and Computer Engineering from the University of Utah in 2000, and the Ph.D. degree from the University of Alberta in 2005. He is currently with the ECE Department at Utah State University, where he holds the rank of Associate Professor. Dr. Winstead's research interests include algorithms for probabilistic error correction and inference, particularly Bayesian networks and Hidden Markov Models; implementation of high-performance forward error correction techniques, especially Low-

Density Parity Check (LDPC) codes; mixed-signal circuit design for reliable wireless communication; low-power and fault-tolerant VLSI circuits; theory of stochastic computation with applications in electronics and synthetic biology. In 2010, Dr. Winstead received the NSF Career award for research in low-energy wireless communication circuits, and in 2013-14 he was a Fulbright Visiting Professor at Université de Bretagne Sud in Lorient, France. Dr. Winstead is a Senior Member of the IEEE and a member of the Tau Beta Pi engineering honor society.



Bane Vasić is a Professor of Electrical and Computer Engineering and Mathematics at the University of Arizona. He is affiliated with BIO5, the Institute for Collaborative BioResearch, and is a Director of the Error Correction Laboratory. Dr. Vasić is an inventor of the soft error-event decoding algorithm, and the key architect of a detector/decoder for Bell Labs data storage chips which were regarded as the best in industry. Dr. Vasić is a Chair of the IEEE Data Storage Technical Committee, Editor of the IEEE JSAC Special Issues on Data Storage Channels

and Member of the Editorial Board of the IEEE Transactions on Magnetics. He is da Vinci Circle and Fulbright Scholar and founder and Chief Scientific Officer of Codelucida.