Towards a Self-Organizing Deciphering System based on a Wave Digital Emulator

Karlheinz Ochs, Enver Solan, Dennis Michaelis, and Leon Schmitz

Ruhr-University Bochum
Chair of Digital Communication Systems
Bochum, Germany
Email: {karlheinz.ochs, enver.solan, dennis.michaelis, leon.schmitz}@rub.de

***Abstract*—Current cryptographic systems are based on functions that are easy to compute, yet finding the inverse operation is computationally complex. One of these functions is the prime factorization which is utilized in modern communication systems. Memristive circuits are challenging these standards because they enable self-organizing logic gates (SOLGs) which can be operated in reverse mode, where every node can electively be used as an input or output. So far, only investigations with idealized memristor models have been done. That is because manufacturing costs of real memristors are high. Thus, our goal is to create a highly flexible emulator for an universal SOLG to aid future investigations. We therefore exploit the wave digital algorithm to obtain an emulator which preserves stability, allows for exchangeable memristor models, and enables parameter optimization and sensitivity analyses during runtime for future research.**

I. Introduction

Asymmetric cryptography is of fundamental importance in modern communication systems. These cryptosystems frequently depend on public key cryptography [1]. The underlying algorithms depends on the use of so called "one-way functions", i.e. functions whose inverse cannot be calculated in a reasonable period of time. Due to their sequential nature, today's algorithms are not able to solve this problem in polynomial time.

The aim is to use the massively and intrinsic parallelism of electrical hardware in order to solve such dedicated problems more efficiently. By utilizing SOLGs [2], which can operate in reverse, one could use this intrinsic parallelism in order to solve computationally complex problems, such as the subset sum problem [3] efficiently. In this work we focus on a path towards a self-organizing prime factorization, which is a common one way function in digital communication cryptography. In general, a proper reverse operation mode means that an appropriate configuration is adjusted at the input terminals when exciting the output with a particular signal. The main electrical components included in order to achieve the self-organization feature are memristors, which are nonlinear resistors with a memory. The fact, that only ideal memristor models were used may indicate that a hardware realization of the systems presented in [2] is still a challenging task.

The aim of this paper is to introduce an emulation technique which highly corresponds to a possible hardware realization of the SOLG in order to facilitate the transformation of the concept to electrical hardware. Due to several benefits, like flexibility, robustness and massive algorithmic parallelism, we emulate the SOLG with the wave digital method [4]. The latter is real-time capable and preserves especially underlying energetic properties, like passivity, which is important when it comes to incorporate software emulators in real circuits [5]. The concept is demonstrated by a wave digital model of a self-organizing (SO) 2-bit multiplier that incorporates SO-AND and SO-XOR gates. Therefore an universal logic gate [2] is discussed that can adopt different logic gate functions by a simple adjustment in parameters. Negations are realized by interchanging nodes at the corresponding port.

In the following, the concept of self-organizing logic gates is briefly recapitulated. After that, the wave digital model of the universal logic gate is introduced. Subsequently, the functionality of the emulator is demonstrated by emulation results. Main results of the work is summarized in the conclusion at the end of the manuscript.

II. Self-Organizing Universal Gates

Universal SOLGs are introduced in [2], where the term universal indicates that with those devices several logic functions can be realized only by adapting particular parameters. Such an SOLG with three ports is shown in Fig. 1.

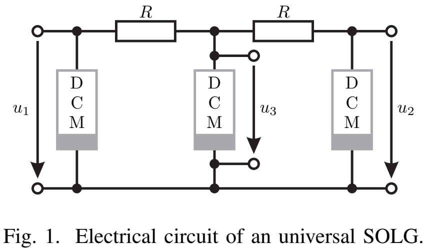

Fig. 1. Electrical circuit of an universal SOLG.

Besides two resistors, it is formed by so called dynamic correction modules (DCM) which are memristive one-ports including additional controlled-sources. A detailed composition of a dynamic correction module is shown in Fig. 2. Since

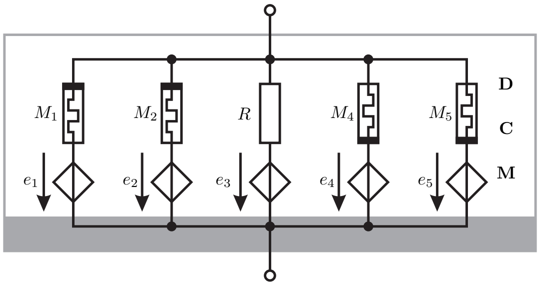

Fig. 2. Eelectrical circuit of the DCM with memristive devices.

the polarity of memristive devices must be taken into account, the DCM one-ports can also be interpreted as one-ports with a particular polarity. The voltage-controlled voltage sources (VCVS) are described by

$$e_\mu = \alpha_0 + \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 \,, \quad \mu = 1, \ldots, 5, \tag{1}$$

where the coefficients α_ν, $\nu = 0, \ldots, 3$ lead to different logic functions of the SOLG, such as SO-AND and SO-XOR, cf. [2]. Consequently, every possible logic gate can be realized.

A. Memristive Device

In this work, we utilize the nonlinear dopant-drift model [6] to realize the emulator of the universal SOLG. This model erroneously remains in an internal state whenever it reaches the boundary values. To overcome this boundary-lock problem an enhanced window function is used in the presented approach [7]. The voltage-current relationship is

$$u(t) = M(z)\, i(t), \quad \text{with} \quad M(z) = R_1\,[1 - z] + zR_0 \,, \tag{2a}$$

where M is the memristance value, z is the internal state and R_0 and R_1 are the low and high resistance state, respectively. The underlying differential equation is

$$\dot{z}(t) = \mu_v R_0 D^{-2} w(z) i(t), \quad \text{with} \tag{2b}$$

$$w(z) = [1 - 2w_0]\left[1 - [1 - 2z]^{2p}\right] + w_0, \tag{2c}$$

with the window function w, window function offset w_0, mobility coefficient μ_v, device width D and exponent p, which controls the steepness of the window function.

B. Self-Organizing Logic Circuits (SOLC)

So far the distinct SOLG has been discussed. However, in order to obtain as self-organizing logic circuit for solving dedicated problems, such logic gates have to be connected together. This connection is realized through special two-ports consisting of a voltage-controlled differential current source (VCDCS) [2], cf. Fig 3.

The VCDCSs j are characterized by

$$j(t) = j_0 + \int_{t_0}^{t} \gamma\left(u\left(\tau\right)\right) \mathrm{d}\tau \,,$$

$$\gamma\left(u\right) = \frac{I_0}{\tau_0}\left[-\frac{1}{2} + \sum_{k=0}^{2} \frac{[-1]^k}{1 + \mathrm{e}^{-\frac{1}{U}[u + [k-1]u_\mathrm{L}]}}\right],$$

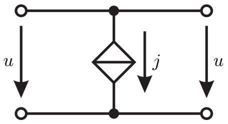

Fig. 3. Connection two-port for interconnecting SOLGs to SOLCs containing a voltage-controlled differential current source.

with initial injected current j_0, normalization constants I_0, τ_0, U with the units of a current, time and a voltage, and logic voltage level u_L (u_L is a logical 1, 0 V a logical 0). Their purpose is to ensure that invalid configurations at the SOLGs do not occur. A graphical representation of the voltage-dependent function $\gamma\left(u\right)$ is shown in Fig. 4.

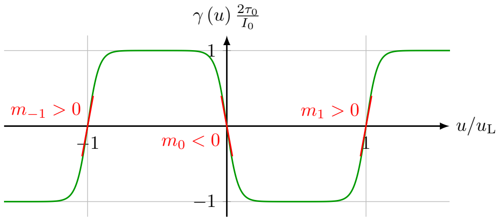

Fig. 4. Characteristic curve of the differential current source γ.

If $\gamma(u) > 0$, that corresponds to a positive change in the current $j(t)$ which will decrease u, while $\gamma(u) < 0$ increases u. Therefore, $u = 0$ V ($m < 0$) corresponds to an unstable operating point, while $u = \pm u_L$ are stable operating points.

III. Wave Digital Model

In order to obtain an emulator of SOLGs, we deploy the wave digital concept [4] as an emulation technique. It converts the underlying physical system into an algorithmic model with particular features that make it suitable as an intermediate step towards a hardware realization. The relevant benefit of the wave digital emulation approach in this context is its parameter flexibility, making it suitable for live optimization and sensitivity analyses [8], [9].

Next, the process of deriving a wave digital emulator is in principle explained. First, by numerical integration using the trapezoidal rule, differential equations become difference equations with remaining implicit functions [5], [10]. Second, voltages u and currents i are replaced by wave quantities as independent variables, so that implicit relationships are explicit equations in wave domain

$$a = u + R\,i \,, \quad b = u - R\,i \,, \quad R > 0. \tag{3}$$

Here, a and b denote the incident and reflected wave of an arbitrary port, respectively, and R denotes the port resistance being a positive constant. For a detailed review [4] is recommended. In the following the wave digital model of the specific one- and two-ports used in this paper are introduced.

A. Memristive Voltage Source

Considering the DCMs shown in Fig. 2, memristive voltage sources are needed in the SOLG, cf. Fig. 1. It is described by

$$u = e - M(z)\, i, \tag{4}$$

with $M(z)$ as in (2a)–(2c). The electrical circuit of a memristive voltage source is shown on the left-hand side of Fig. 5. A general approach for wave digital realizations of memristive devices has been introduced recently [10]. Based on these insights and plugging (3) into (4), the corresponding wave flow diagram of the memristive voltage source can be modeled as shown in Fig. 5 (right) since

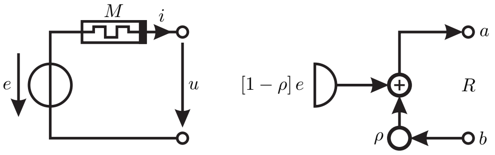

Fig. 5. Electrical circuit of a memristive voltage source (left) and corresponding wave flow diagram (right).

$$a = e + \rho\,[b - e]\ , \quad \rho = \frac{M - R}{M + R}. \tag{5}$$

For a matched resistive voltage source ($\rho = 0$) this correspondence degenerates to

$$M = R_0\ , \quad R_0 = R \Rightarrow a = e, \tag{6}$$

which is also a part of the DCM of Fig. 2. In order to get a wave digital formulation for the matched constant resistor, as it is needed for the interconnection of the DCMs, the voltage source is set to zero $e = 0$, leading to $a = 0$.

B. Dynamic Correction Modules

As can be seen from Fig. 2, these memristive or resistive voltage sources are interconnected by Kirchhoff's parallel interconnections, which correspond to parallel adaptors with adaption coefficients $\gamma_1, \dots, \gamma_5$ in the wave digital domain, cf. [4]. The resulting wave digital model of a dynamic correction module is shown in Fig. 6. Since wave digital models of memristive devices lead to parametric loops, the composition of the memristive voltage sources also contain these loops [10]. We solve them by applying fix-point iterations [11].

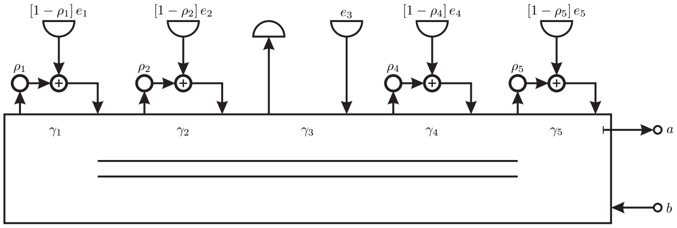

Fig. 6. Wave flow diagram of the DCM in Fig. 2.

A wave digital realization of the universal logic gate as in Fig. 1 is depicted in Fig. 7, deploying parallel and series adaptors with adaption coefficients $\gamma_{11}, \dots, \gamma_{33}$. The arrows indicates the ability of the circuit to use all three ports as input and output ports simultaneously. A unique benefit of the wave digital method is that the logic function can also be changed during runtime only by changing the parameters of the VCVSs, see (1).

IV. Emulation Results

In this section we investigate a fundamental setup that is a building block towards a self-organizing deciphering system. The circuit of interest is shown in Fig. 8 and displays a 2-bit multiplier except that all logic gates are SOLG as described in the previous section. The emulation parameters are specified in Table I. With standard 2-bit multipliers one would apply the binary representations of

Emulation parameters					
R_0	=	1 Ω	μ_v	=	10^{-5}
R_1	=	100 Ω	w_0	=	10^{-4}
u_L	=	5 V	p	=	1
D	=	1 μm			

TABLE I
Parameters for the emulation results in Fig. 9.

$$[u_{10}\ u_{11}] = \alpha \cdot u_L, \quad \alpha = [\alpha_{10}\ \alpha_{11}]_2, \tag{7}$$
$$[u_{20}\ u_{21}] = \beta \cdot u_L, \quad \beta = [\beta_{20}\ \beta_{21}]_2, \tag{8}$$

respectively, at the left-hand ports to observe the binary representation of the 4-bit solution of

$$\gamma = \alpha \cdot \beta = [\gamma_0\ \gamma_1\ \gamma_2\ \gamma_3]_2 = \frac{[v_0\ v_1\ v_2\ v_3]}{u_L}, \tag{9}$$

at the right-hand ports with $\alpha_\mu, \beta_\nu, \gamma_\omega \in \{0, 1\}$. In contrast, the self-organizing setup in Fig. 8 allows for applying the binary representation of the 4-bit solution $v_0, \dots, v_3$ as an input. We are interested in signals $u_{10}, \dots, u_{21}$ which are the two 2-bit factors relevant for multiplication. Doing so is essentially operating the 2-bit multiplier in reverse mode. The emulation results show

$$\begin{array}{l} v_0 = v_4 = 0, \\ v_1 = v_2 = u_L, \end{array} \quad \Leftrightarrow \quad \gamma = [0\ 1\ 1\ 0]_2 = 6, \tag{10}$$

which is the binary representation of the number 6, are shown in Fig. 9. After $t \approx 60\ ms$ it can be observed that

$$\begin{array}{lcl} u_{10} = u_L,\ u_{11} = 0 & \Leftrightarrow & \alpha = [1\ 0]_2 = 2, \\ u_{20} = u_L,\ u_{21} = u_L & \Leftrightarrow & \beta = [1\ 1]_2 = 3, \end{array} \tag{11}$$

where indeed $\alpha \cdot \beta = 6$. It should be noted that α and β in this example are the prime factorization of γ, a very commonly used concept that is used in cryptography. For this reason we understand this work as a path towards self-organizing deciphering systems.

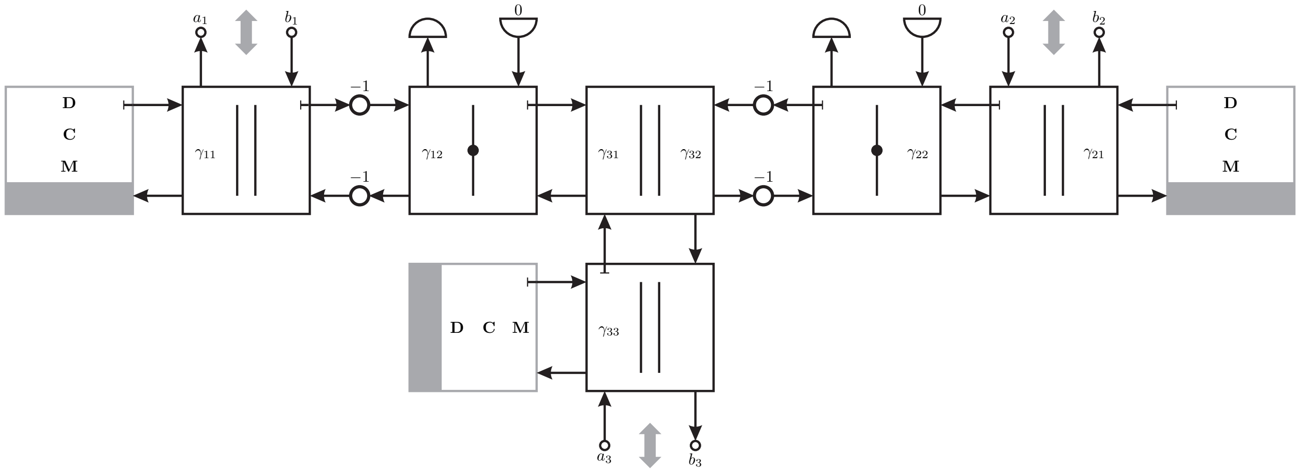

Fig. 7. Wave flow diagram of the universal SOLG with DCMs as in Fig. 1.

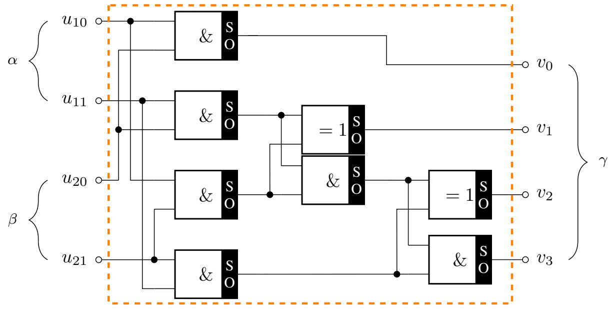

Fig. 8. SO 2-bit multiplier consisting of SO-XOR and SO-AND gates.

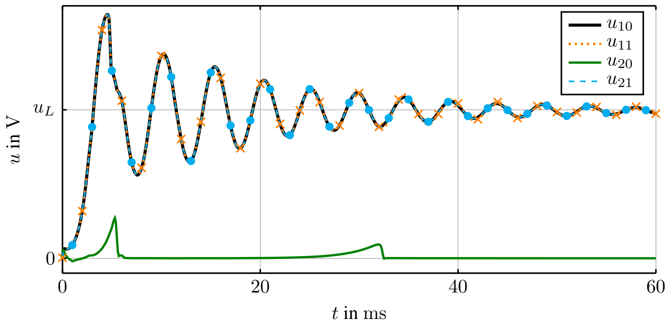

Fig. 9. Emulation results with $v_0, \ldots, v_3$ as in (10). After $t \approx 60$ ms the configuration represents $\alpha = 2$ and $\beta = 3$ which is the prime factorization of $\gamma = 6$.

V. Conclusion and Outlook

In the proposed approach a powerful emulator of SOLGs based on the wave digital concept has been shown, which offers electrical interpretable parameters that are easily adjustable. The functionality of the emulator has been demonstrated by operating a SO 2-bit multiplier in reverse mode to obtain a simple prime factorization of a 4-bit number. This emulator is not only a significant step forward considering the hardware realization of SOLGs, since live parameter optimizations and live sensitivity analyses are possible, but is also a path towards self-organizing deciphering systems.

The proposed emulator can be used in order to emulate different logic functions only by adjusting the corresponding parameters. Other parameters, e.g. for faster convergence, can then be improved through optimization during runtime and aid the development for manufacturing.

Acknowledgment

The financial support by the German Research Foundation (Deutsche Forschungsgemeinschaft - DFG) through FOR 2093 and DFG-404291403 is gratefully acknowledged.

References

[1] D. Shah *et al.*, "Revisting of elliptical curve cryptography for securing Internet of Things (IOT)," in *Advances in Science and Engineering Technology International Conferences*. Abu Dhabi, UAE: IEEE, Feb. 2018, pp. 1–3.

[2] F. Traversa *et al.*, "Polynomial-time solution of prime factorization and NP-complete problems with digital memcomputing machines," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 27, no. 2, pp. 023 107–1 – 023 107–22, 2017.

[3] K. Ochs *et al.*, "Towards Wave Digital Memcomputing with Physical Memristor Models," *accepted for International Symposium on Circuits and Systems*, Jan. 2019.

[4] K. Meerkötter, "On the Passivity of Wave Digital Networks," *IEEE Circuits and Systems*, vol. 18, no. 4, pp. 40–57, Oct. 2018.

[5] K. Ochs, "Passive integration methods: Fundamental theory," *AEÜ International Journal of Electronics and Communications*, vol. 55, no. 3, pp. 153–163, May 2001.

[6] Z. Biolek *et al.*, "SPICE model of memristor with nonlinear dopant drift," *Radioengineering*, vol. 18, no. 2, pp. 210 – 214, 2009.

[7] E. Solan *et al.*, "An enhanced lumped element electrical model of a double barrier memristive device," *Journal of Physics D: Applied Physics*, vol. 50, no. 19, p. 195102, 2017.

[8] K. Ochs *et al.*, "Sensitivity analysis of memristors based on emulation techniques," in *IEEE 59th International Midwest Symposium on Circuits and Systems*. IEEE, Oct. 2016, pp. 1–4.

[9] E. Solan *et al.*, "Parameter identification of a double barrier memristive device," in *IEEE 60th International Midwest Symposium on Circuits and Systems*, Aug. 2017, pp. 851–854.

[10] E. Solan *et al.*, "Wave Digital Emulation of General Memristors," *International Journal of Circuit Theory and Applications*, vol. 46, no. 11, pp. 1–17, 2018.

[11] T. Schwerdtfeger *et al.*, "A multidimensional signal processing approach to wave digital filters with topology-related delay-free loops," in *IEEE International Conference on Acoustics, Speech and Signal Processing*. Florence, Italy: IEEE, 2014, pp. 389–393.