A Secure Memristor Replicator Architecture with Physical Uncloneability

X. Yang, S. Khandelwal and A. Jabir

We present a lightweight and highly versatile architecture for replicating the resistance of a source memristor into a destination memristor. This can be useful for storing or backing up sensed analogue information, e.g. sensed resistance, voltage, etc, in a single memristor. The architecture, which is simple and power efficient, is also able to produce non-linear digital codes during the replication process for added security by taking advantage of the non-linear behaviour of memristors. The generated codes can also be used to retrieve the analogue value within acceptable conversion errors, with circuit elements already built into the replicator. We also show that the architecture demonstrates physical uncloneable properties.

Introduction: A memristor is a non-volatile resistive memory postulated by Leon Chua in 1971 [1] and fabricated by the HP group in 2008 [2]. Since then, there has been significant interests in exploiting this technology in the designs of high density non-volatile memory, neuromorphic systems, logic design, and most recently in sensors and solar cells [3, 5]. There are several existing techniques for tuning a memristor's conductivity to a predetermined value, e.g. [3, 4]. Most of these techniques require complex circuitry, while some require external processing and others are unable to perform well for devices with high OFF- to ON-resistance ratios. To this end, we propose an accurate and efficient lightweight architecture for replicating the resistance of a source memristor into a destination memristor by repeatedly applying programming pulses, but without much of the drawbacks of the existing techniques. Such a circuit can be crucial for backing up analogue data, e.g. from a memristor sensor [5], before or during conversion to digital form. We show that the proposed architecture is extremely versatile and can be used not only for replicating memristors, but also for generating non-linear digital code and decoding the code back to the source memristance/voltage (within quantisation limits). Owing to this non-linear encoding, the architecture also provides a certain level of inherent security features. Our experimental results also demonstrate that it offers physical uncloneability [6], which can be critical in applications such as chip tagging/identification as well as for preventing unauthorised fabrications.

Fabricated memristive devices are non-linear. Any change in the tunnel barrier width exponentially changes its memristance. Let R_{off} and R_{on} be the High and Low Resistive States respectively, $\lambda = \ln(\frac{R_{\text{off}}}{R_{\text{on}}})$, $x_{\text{on}} \leq x \leq x_{\text{off}}$, where x_{on} and x_{off} are the lower and upper bounds of the undoped region. Then the instantaneous memristance, $R_{\text{M}} = R_{\text{on}} \cdot e^{\lambda \cdot (x - x_{\text{on}})/(x_{\text{off}} - x_{\text{on}})}$, which is clearly non-linear in x [7].

Fig. 1(a) shows the symbol of a memristor. The state of a memristor shifts non-linearly towards R_{off} when a write voltage V_{W} $>$ a threshold voltage V_{off} is applied across it and it shifts non-linearly towards R_{on} when $V_{\text{W}} <$ a threshold voltage V_{on} is applied across it [7]. The state of the memristor remains unchanged for any voltage applied in between V_{on} and V_{off}. Hence, the state of a memristor can be read by applying a read-voltage, V_{R}, such that $V_{\text{on}} \leq V_{\text{R}} \leq V_{\text{off}}$ and $V_{\text{R}} \neq 0$.

Proposed Architecture: Fig. 1(b) shows our proposed architecture for replicating a source memristor M_{S} to a destination memristor M_{D} within quantisation limits. M_{S}, M_{D} and the load resistors, R_{SL} and R_{DL}, form two voltage dividers. R_{SL} and R_{DL} are assumed to be closely matched. The output of the voltage dividers V_{INS} and V_{IND} are continually compared by the comparator.

1. Replication and Encoding: Let f_{rep} be the replication frequency of the clock (clk) and $T_{\text{rep}} = T_{\text{prog}} + T_{\text{hold}} = 1/f_{\text{rep}}$ be the clock cycle. Voltages V_{prog} and V_{hold} are alternatively applied during T_{prog} and T_{hold} respectively. V_{prog} is adjusted to be sufficiently high so that V_{W} appears across M_{D} only even with the load R_{DL}. Similarly, V_{hold} is adjusted to be sufficiently high such that a V_{R} appears across both M_{S} and M_{D} simultaneously. Hence resistance of M_{S} is copied to M_{D} by repeatedly applying the programming pulses. During each T_{prog}, V_{prog} shifts the barrier of M_{D} from the R_{on} region towards the R_{off} region by a small amount, but non-linearly, and during the following T_{hold}, M_{D} and M_{S} are compared. The counter at the top counts the number of clock pulses required to replicate.

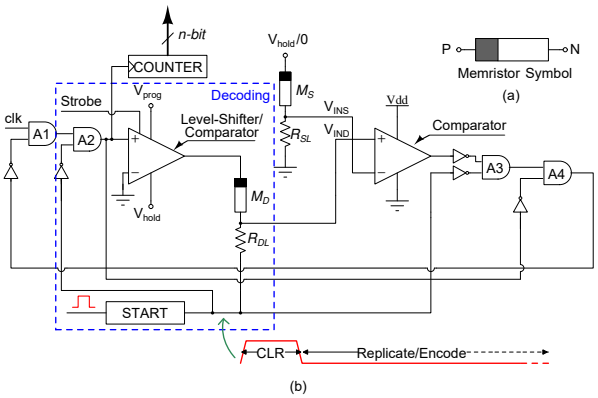

Fig. 1: Proposed memristor replicator architecture.

The replication starts by first resetting the counter and a 'CLR' pulse applied to the negative (N) terminal of M_{D}. This pulse is of sufficient amplitude such that a very short duration resets M_{D} to R_{on}. The first stage of the counter is used to generate the pulse and once CLR is complete the counter is reused for encoding. During CLR: (i) the level-shifter is disabled with the strobe input; (ii) AND gates A_2 and A_3 block the inputs and produce a constant zero. Hence, clk is prevented from reaching the level shifter. As a result, the level-shifter produces 0 at the P-terminal of M_{D} and the high CLR pulse at its N-terminal resets M_{D} to R_{on}.

When CLR returns to 0, the level-shifter and the AND gates A_2 and A_3 are enabled and the replication starts. A_2 passes clk to the level-shifter which switches between V_{prog} and V_{hold} in the same cycle (T_{rep}). V_{prog} shifts the barrier of M_{D} during T_{prog}, and the resulting voltage is compared with that across M_{S} during T_{hold} by the comparator. During T_{hold} the comparator keeps producing a 1 until the voltage across M_{D} exceeds M_{S}. This forces A_3 and A_4 to produce a 0, which lets A_1 pass clk through to the level-shifter. As a result the voltage across M_{D} gradually increases during each clock cycle, until it exceeds that across M_{S} at which point the comparator produces a 0 during T_{hold}. This forces A_3 and A_4 to produce a 1 and the level-shifter is disabled via the strobe. This stops A_1 from letting clk through thereby indicating an end of replication. Essentially the circuit enters a 'locked' state which is controlled by the voltage across M_{D}. During replication, the counter counts the number of clock cycles required to replicate, which is the encoded digital value corresponding to the analogue voltage (resistance) of M_{S}. Hence, the proposed architecture performs non-linear encoding of the analogue voltage/resistance while the replication takes place. It is assumed that V_{INS} remains steady during the conversion process. However, if V_{INS} increases during the conversion, then V_{IND} will follow V_{INS}. If this is undesirable then adding a single latch between A_4 and A_1 will ensure that the conversion stops the first time V_{IND} matches V_{INS}.

2. Decoding: Let us assume that while replicating, the counter registered digital value C. Decoding is achieved by first clearing M_{D} with CLR and by 'programming' it with the same V_{prog} and V_{hold} at the same frequency $f_{\text{rep}} = 1/(T_{\text{prog}} + T_{\text{hold}})$ for C number of cycles. A part of the decoder logic appears in the blue boundary in Fig. 1. A down counter, initialised to C, is used to count the number of clock cycles. After decoding, $V_{\text{hold}} - V_{\text{DL}}$, where V_{DL} is the voltage drop across R_{DL}, divided by the current gives the corresponding encoded resistance within quantisation limits.

3. Security and Physical Uncloneability: The proposed architecture provides a certain level of inherent security by virtue of non-linear encoding. The encoded value C is a function of V_{W}, T_{prog}, T_{hold}, and M_{D} itself. Hence, it is extremely challenging to guess what resistance or voltage C represents without having full knowledge of these quantities. Additionally, access to an almost exact matching memristor to M_{D} provides further challenge and difficulty.

The architecture also provides physical unclonability [6] by virtue of non-linearity as well as its sensitivity to process and parametric variations. As revealed by our experimental results, the non-linear code depends heavily on the physical parameters of M_D, e.g. the physical length of a memristor D, threshold voltage, etc. Any small variations in these are amplified by the counting based encoding mechanism and results in different codes (Fig. 2). Hence, any two fabricated chips are likely to produce different codes for the same input voltage/resistance thereby making it very hard to clone.

While this architecture is geared towards replicating memristors, it can also be used for non-linear encoding/decoding and for Challenge-Response-Pair (CRP) based authentication [6]. Instead of M_S, in Fig. 1(b) V_{INS} can be an input voltage serving as a challenge. After encoding, the contents of the counter can serve as a unique non-linear response. Additionally, this response will vary from chip-to-chip owing to its physical uncloneability thereby also offering provisions for chip identification/tagging. An analogue voltage at V_{INS} can be obtained from a lightweight encryption hardware or a hash function generator, e.g. a linear feedback shift register, for ad

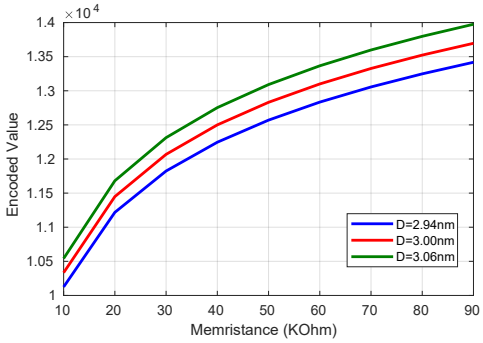

Fig. 2: Variations in encoded digital output with $\pm 2\%$ variation in process parameter D for the same resistive values.

Experimental Results: For the experimental results, the memristors were coded in Spice based on the model and parameters in [7] and the systems were designed and simulated in LTSpice. We used the 32 nm technology node for the MOS-transistors and assumed V_{prog}= 41mV, V_{hold}= 20mV, T_{prog}= 2.5ns, R_{SL}=R_{DL}= 1KΩ, R_{on}=1KΩ, R_{off}=100KΩ, D=3nm, V_{on}=−0.2V and V_{off}=0.02V. Table 1 summarises the results as M_S was varied from 10KΩ to 90KΩ. Clearly, the encoded value is non-linear and maintains low percentage error in copying the resistance of M_S to the destination M_D.

The proposed architecture inherently provides non-linear encoding as shown in Fig. 2. This figure also shows that a small variation in the physical parameters of M_D results in different analogue-to-digital transfer characteristics.

Fig. 3 and Fig. 4 show the results of varying V_{prog} and T_{prog} respectively while keeping the other parameters fixed. As we see the behaviour of the proposed architecture is non-linear throughout, i.e. it is non-linear for specific V_{prog} or T_{prog} and also for their diffe

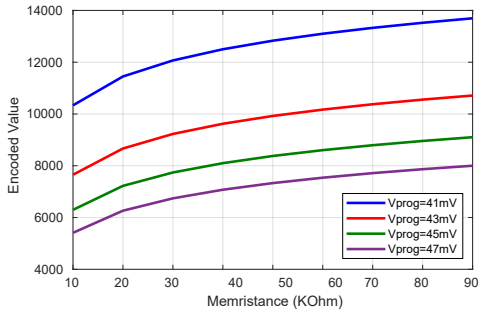

Fig. 3: Effects of varying V_{prog} on the encoded values.

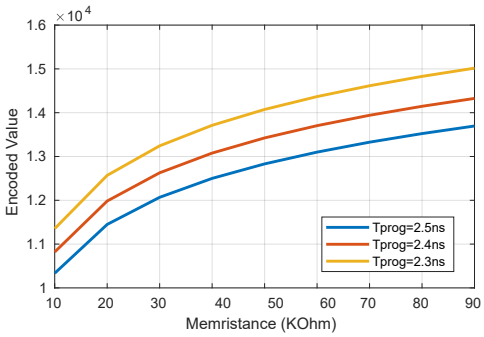

Fig. 4: Effects of varying T_{prog} on the encoded values.

Table 1: Replication/Encoding (R_{on} = 1KΩ, R_{off} = 100KΩ).

V_{prog}=41mV,V_{hold}=20mV,T_{prog} = 2.5ns,R_{SL} = R_{DL} = 1KΩ				
M_S KΩ	M_D KΩ	Time μsec	% Err	Enc Val
10	10.0555	51.6685	0.555	10334
30	30.051	60.3387	0.170	12068
50	50.070	64.1536	0.140	12831
70	70.0653	66.6337	0.0933	13327
90	90.068	68.4787	0.0756	13696

Conclusions: We proposed a highly versatile architecture for replicating a source memristor to a destination memristor, which can also be used for generating non-linear digital codes for added security, physical uncloneability, and also for decoding the analogue value from the digital codes. The proposed architecture is lightweight and relies only on a few logic components, two comparators, and a counter. The simulation results demonstrated its non-linear behaviour and its sensitivity to process and parametric variations. The latter can be extremely useful for designing physical uncloneable functions. We envisage that the proposed architecture can be used for backing up analogue data (e.g. sensed information [5]) especially in remote sensor nodes while securely digitising the information, chip tagging/identification, as well as for preventing unauthorised chip fabrications.

X. Yang, S. Khandelwal and A. Jabir (*School of ECM, Oxford Brookes University, UK*)

E-mail: skhandelwal@brookes.ac.uk

References

1 Chua, L. O.: 'Memristor-the missing circuit element', *IEEE Trans. Circuit Theory*, 1971, **CT-18**, (5), pp. 507-519
2 Strukov, D. B., Snider, G. S., Stewart, D. R. and Williams, R. S.: 'The missing memristor found', *Nature*, 2008, **453**, pp. 80-83
3 Olumodeji, O. A., Bramanti, A. P., and Gottardi, M.: 'A memristor-based pixel implementing light-to-resistance conversion', *Opt. Eng.*, 2016, **55**, (2), p. 020501
4 Olumodeji, O. A. and Gottardi, M.: 'Emulating the physical properties of HP memristor using an arduino and a digital potentiometer', *2016 12th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME)*, Lisbon, 2016, pp. 1-4.
5 Adedotun, A., Mathew, J., Jabir, A., Natale, C. D., Martinelli, E. and Ottavi, M.: 'Efficient Sensing Approaches for High-Density Memristor Sensor Array,' *Journal of Computational Electronics*, 2018, **17**, (3), pp. 1285-1296
6 Vijayakumar, A. and Kundu, S.: 'A novel modeling attack resistant PUF design based on non-linear voltage transfer characteristics', *Design, Automation & Test in Europe Conference & Exhibition*, Grenoble, 2015, pp. 653-658
7 Kvatinsky, S., Ramadan, M., Friedman, E. G. and Kolodny, A.: 'VTEAM: A General Model for Voltage-Controlled Memristors', *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2015, **62**, (8), pp. 786-790