On Quaternary 1-of-4 ID Generator Circuits

Julian Murphy and Gareth Howells
School of Engineering and Digital Arts
University of Kent
Canterbury United Kingdom (UK)
{ j.murphy-2060@kent.ac.uk, w.g.j.howells@kent.ac.uk }

Klaus D McDonald-Maier
School of Computer Science and Electronic Engineering
University of Essex
Colchester, United Kingdom (UK)
{ kdm@essex.ac.uk }

***Abstract*—A quaternary 1-of-4 ID generator circuit is presented. It exploits the properties of quaternary metastability to provide stable n-bit IDs tolerant to the effects of nanoscale process scaling and temperature variations, which is achieved by increasing the margin between threshold voltage and metastability voltage via quaternary metastability. A 128-bit ID generator hardware implementation and electrical evaluation yields an average of 26.6% uniqueness of ID bits and 100% stability rate over a $10°C$ to $40°C$ temperature range.**

Introduction

Recent security trends have led to a need for ID bit generator circuits capable of delivering stable and predicable sequences of n ID bits (e.g., 128-bits). Here a n-bit ID is formed from many single or tuples of ID bits via concatenation of the outputs of n identical ID bit generator circuits. Such circuits exploit the fact lithography fabrication differences—known as process variability—cause variations in circuit-level switching threshold voltages (V_{th}) due to transistor doping imbalances. This in turn makes one integrated circuit (IC) unique compared to another.

The most common and practical ID generator circuit design exploits *binary metastability*. Here, the ID generator circuit will output a binary zero or one due to bias in the circuit's V_{th} with respect to the binary metastable settling state. However, since a n-bit ID generator (n identical ID bit generator circuits) is attempting to extract, manipulate and use digitally in a security setting, the naturally analogue and asynchronous metastability properties of an IC, they always output noisy bit values as a proportion of a given n-bit ID. In other words, certain bits will be unstable and different each time a n-bit ID is requested, rather than giving the same n-bit ID each time (e.g., 20 bits will be unstable for a 128-bit ID).

This problem, termed *stability*, is two-fold as follows. Firstly, it is due to environmental temperature changes, given the macro-block level (IP core) voltage is fixed, if not precisely clamped, by the power management circuitry on an IC. Since in nanoscale IC processes circuits operate in temperature inversion, where the effect of decreasing temperature increases V_{th} to slow circuits and vice-versa. Notably, other temperature effects are also at play here, such as Negative Bias Temperature Instability (NBTI). All of which affect V_{th}, meaning it is possible an ID generator circuit may toggle from its calibrated and known values, which occurs when the equality between V_{th} and the binary metastable settling state reverses.

And, secondly, as supply voltage reduces with smaller nanoscale IC process geometries, circuit V_{th} threshold voltages do not decrease proportionally. This means a circuit's metastable voltage level gets closer to V_{th}, since binary metastability occurs at $V_{dd}/2$; and so, the gain of the circuit is reduced and it takes longer to transition out of metastability. As a consequence, the likelihood of an ID generator circuit toggling is increased.

All ID generator circuits also suffer from a statistical bias effect, termed *uniqueness*, insomuch as a n-bit ID from one IC will not be completely random and unique versus another from a different IC. Typically, improvements in stability come at the cost of uniqueness, which gives a catch twenty-two situation. However, it can be observed by simply induction, that if an ID generator is perfectly stable within its temperature operating parameters (assuming the core voltage is fixed), uniqueness can be guaranteed through simple cryptographic functions. For instance, using a one-way hash such as SHA-2 or 3, where if one bit is different, a completely different binary hash string will result.

We have observed, at the cost of a drop in uniqueness, that stable ID generator circuits can be implemented in nanoscale processes if the effect of process scaling is addressed by increasing (fractionally) the margin between a ID circuit's V_{th} and metastable settling state, which at the same time will give tolerance to temperature variations.

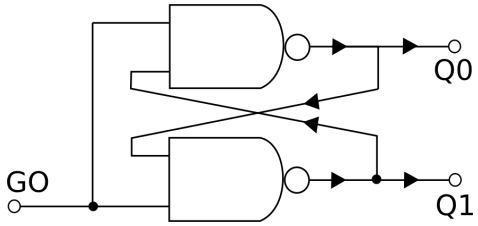

Fig. 1. 1-of-2 ID Generator

As such, in this paper, we present a quaternary 1-of-4 ID generator aimed at meeting this requirement. It exploits quaternary metastability to increase the margin between V_{th} and the metastable setting state, and is capable of generating 2-bits of an ID at a time rather than just 1-bit.

QUATERNARY ID CIRCUIT DESIGN

The most frequently used ID generator circuit is based on a 1-of-2 cross-coupled 2-input NAND gate arbiter design, termed here a 1-of-2 ID generator circuit, and as shown in Fig. 1. Such a design is usually used to control access to two concurrent resources asynchronously on a bus (e.g., different memory IP blocks), or as a bistable and Set-Reset latch.

Here, two inputs are wired together as a *go* signal, while the other two inputs are fed back by its opposing outputs and works as follows. When *go* is low, it is in a reset state {11}; and when *go* is high, it has two 1-of-2 codeword stable equilibrium states {01, 10} separated by a single unstable metastability point (i.e., saddle equilibrium).

In metastability, we have $V(q_0) = V(q_1) = V_F$, where V_F denotes the fix-point voltage output of a two-input NAND with one input high and other input at V_F (i.e., $V_{dd}/2$). When the voltage difference $|V(q_0) - V(q_1)|$ exceeds V_{thp} (the pMOS threshold voltage) either Q_0 or Q_1 will pull to V_{dd}, since the gate's feedback input will now be at gnd. The other NAND gate will now have its other input pulled high turning on its second nMOS series transistor, making its output transition low ($V_F \rightarrow gnd$), thus giving a 10 or 01 output.

The bias towards which rail (Q_0 or Q_1) is decided by the equality between the ID generator circuit's V_{th} and the metastable voltage level; which, in turn, is governed by the closeness of the metastability point and V_{th} due to nanoscale voltage scaling, process variability and temperature variations as discussed. For instance, the V_{th} of a circuit can be approximated by $V_{th} \approx (r \cdot V_{dd})/(1 + r)$ [4]. Here r is ratio of the relative drive strengths of the nMOS and pMOS transistors, typically sized such that $r \leq 1$. This puts V_{th} exactly at $V_{dd}/2$, which is a 1-of-2 ID generator circuit's metastable point.

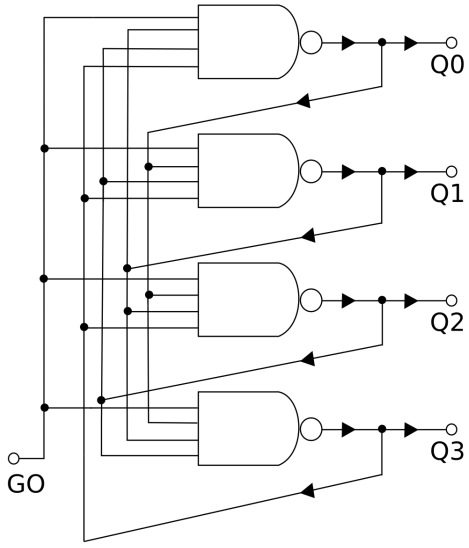

Fig. 2. 1-of-4 ID Generator

But, it can be noted, metastability is a function of a given ID circuit's gate-level design which allows it to be controlled; while V_{th} of a circuit is fixed and its value dependent on process variability and temperature (uncontrollable). Therefore, these two properties are actually mutually exclusive, which gives the opportunity to directly address instability issues. We propose to do this using a quaternary 1-of-4 ID generator circuit instead as shown in Fig. 2. It has the interesting property of multiple metastability states distributed between gnd and V_{dd}; one of which lies above $V_{dd}/2$ the metastable voltage point of a 1-of-2 ID generator. Thus, this alternative design allows the margin between V_{th} and an ID generator circuit's metastable voltage point to be increased.

The quaternary 1-of-4 ID generator in Fig. 2 encodes 2-bits as four states on four wires $\{00 \rightarrow 1110, 01 \rightarrow 1101, 10 \rightarrow 1011, 11 \rightarrow 0111\}$. It adds two extra feedback paths and requires four 4-input NAND gates compared to the 1-of-2 ID generator. Such a design is usually used to arbitrate between four concurrent masters requesting access to the same resource, and such 1-of-n designs were first proposed by Sutherland in [1]; and, later identified as having special metastability properties in [2] and [3]. Note, it would also be possible to use a 1-of-3 ID generator design, however, a 1-of-3 design is impractical due to being ternary, whereas quaternary encoding will map directly to 2-bit binary.

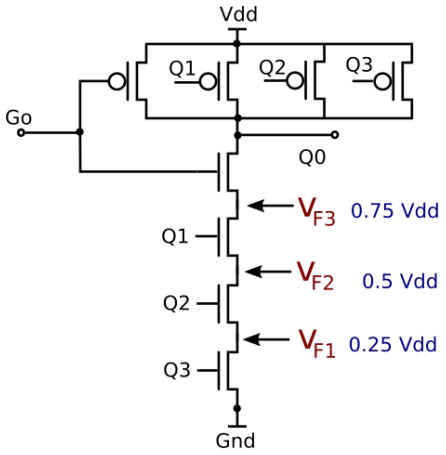

Fig. 3. 1-of-4 ID generator circuit NAND transistor structure and voltages

Its operation is as follows. When go is low, it is in a reset state and gives an all-ones $\{1111\}$ output. Conversely, when go transitions low it becomes metastable before it resolves to a 1-of-4 codeword. Let V_{Fi} be the fixed point voltage that, when applied to i inputs of one of the NANDs (keeping the other $4 - i$ inputs high), produces V_{Fi} at the output. With four nMOS transistors in series, we have $V_{F1} < V_{F2} < V_{F3} < V_{F4}$, which is illustrated in Fig. 3.

Since all the actual inputs are wired together as go and in what would be normally be four request signals only one actual metastability state is possible, a quaternary metastable state. The other metastability states would be possible if the circuit was being used as a regular arbiter via the various input combinations. Therefore, in quaternary metastability, we have $V(q_0) = V(q_1) = V(q_2) = V(q_3) = V_{F3}$ when go is high, since one of the nMOS transistors is on from the go signal V_{F3} represents the voltage across the remaining three nMOS transistor stack and thus $\approx 0.75 \cdot V_{dd}$. Eventually, the quaternary metastability state is broken and the circuit will proceed towards a stable state with three outputs high and one low.

It should be noted that the transient behavior of quaternary metastability is less regular compared to binary metastability when resolving, if the circuit is sufficiently symmetric, the quaternary metastable state may evolve into V_{F2} and then potentially even V_{F1}before reaching a stable state. This occurs as the remaining nMOS transistors turn on as the feedback inputs transition high—this behavior is highly unlikely due to parasitics and process variability, however.

```
1
2  module arb( a, q );
3  input  [2:0] a;
4
5  output [2:0] q;
6
7  (* ALLOW_COMBINATORIAL_LOOPS = "true", KEEP = "true" *) wire [2:0] p;
8
9  nand nand3_i0( p[0], a[0], p[1], p[2] );
10 nand nand3_i1( p[1], a[1], p[0], p[2] );
11 nand nand3_i2( p[2], a[2], p[0], p[1] );
12
13 assign q[2:0] = p[2:0];
14
15 endmodule
```

Fig. 4. Verilog 1-of-4 ID generator implementation

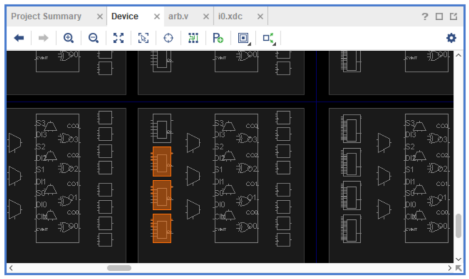

Fig. 5. 1-of-4 ID generator placement

Electrical Evaluation

To test the validity of increasing the margin between a circuit's metastable voltage and V_{th} by using a quaternary 1-of-4 ID generator circuit design, a 128-bit version was designed and implemented via a Xilinx Arty-A7 Artix-35T FPGA-based development board. The Artix-35T IC is manufactured in a 28nm TSMC nanoscale lithography process and uses a 0.9 volt core voltage (inherently giving a very small margin between V_{th} and a binary metastable voltage point).

First, a 1-of-4 ID generator circuit was implemented in a Verilog module together with a explicit Xilinx Vivado timing constraint (`"ALLOW_COMBINATIONAL_LOOPS"`) to ensure feedback paths were not removed during logic synthesis, as shown in Fig. 4. This module was then further constrained using Xilinx XDC macro commands (`create_macro` and `update_macro`) to ensure the four NAND gates forming one 1-of-4 ID generator were placed in the same slice—each Artix-35T slice features four look-up tables allowing all four NANDs to be placed in one slice. This placement technique is shown in Fig. 5. Xilinx's placement and routing tool placed the macros where it chose, rather than locking the 1-of-4 ID macros to a particular site on the FPGA layout, and routed wiring interconnects using its internal algorithms. This is because Xilinx XDC

macros do not allow routing-fixed macro construction as was possible in older Xilinx FPGAs (i.e., before 3D transistor lithography processes).

Next, a 128-bit 1-of-4 ID block was implemented in Verilog instantiating the base ID Verilog module and macro (64 times), which was interfaced as an IP core (32-bit AXI bus interface) to allow use with Xilinx's EDK software. While multiple software addressable 32-bit registers read the 1-of-4 output (256-bit wide) and control the *go* signal, where one 32-bit result register can store 16 1-of-4 codewords (i.e., 16 binary ID bits). Actual conversion to binary was not performed in hardware so the 1-of-4 codewords could be inspected for the reset state {1111} and possible erroneous codewords. The IP core was then included as a peripheral in a 32-bit Microblaze SoC design in Xilinx's EDK software—a UART IP code was used for I/O—and then exported to Eclipse. Drivers and software were then written to read and write from the IP core and to transfer the raw 1-of-4 ID output to a connected PC for analysis.

We first evaluated the uniqueness of the implemented 128-bit 1-of-4 ID generator at room temperature (nominal operating conditions). Ten identical Arty-A7 Artix-35T FPGA boards were used to extract their individual IDs using the same programming bitstream. The values were read from the boards multiple times in 1-of-4 and converted to binary on a PC to ensure ID consistency. Then the number of differing bits (Hamming Distance) between identifiers found, which resulted in an average of 26.6% and means that approximately 34 bits differ out of 128 bits for each 128-bit ID compared to another ID. This is not the ideal of 50%, which indicates a ID generators output is highly random and uniformly distributed. But, the result, and as expected, is the cost of attempting to increase stability by increasing the margin between an ID circuit's metastability point and V_{th}.

Given approximately 34 bits were shown to differ between IDs, next in software to test generating cryptographic-suitable IDs, the IDs were passed through a bit mixing stage and then passed through a S-box function stage from AES. As expected, this gave a 50% difference between IDs, which could be recreated consistently after repeated stress testing at room temperature. Note, hashing could also be used for higher ID lengths e.g. 256 or 512; and cryptographic post-processing could be embedded directly in the IP core too.

Next, we evaluated the stability of the ID generator under varying temperature conditions. One of the boards was placed in a digitally temperature selectable Peltier thermoelectric cooler and warmer chamber. A temperature sweep was performed over a $10°C$ to $40°C$ temperature range to simulate a likely climate profile variation, and readings taken at $1°C$ intervals via the boards integrated temperature sensor and chamber's digital controls. To implement a feasible and meaningful stress test, this temperature sweep experiment was repeated multiple times over a number of hours and individual days. The IDs reading were consistent for every reading taken, thus yielding a 100% stability rate. The experiment was also repeated with another five FPGA boards to verify the stability result was the same. This outcome was identical and validates the observation increasing the margin between a ID circuit generator's metastability voltage and V_{th} is of benefit in gaining stable IDs.

Conclusion

A quaternary 1-of-4 ID generator that gives stable and reliable IDs has been introduced, its correct implementation presented and an evaluation in terms of uniqueness and stability over a $10°C$ to $40°C$ temperature range. It seeks to address the instability caused by nanoscale process scaling and temperature variations by increasing the margin between a circuit's V_{th} and metastability voltage via quaternary metastability. We conclude from a 100% stability rate over a $10°C$ to $40°C$ temperature range, such an ID generator circuit design can facilitate the use of n-bit IDs directly and reliably in cryptographic applications or protocols. The cost, as noted, is reduced uniqueness of the IDs generated at 26.6%.

Acknowledgment

This work has been supported by the European CHIST-ERA SPIRIT Project funded in the UK by the Engineering and Physical Sciences Research Council (EPSRC) [grant numbers EP/P016006/1 and EP/P015956/1].

References

[1] Sutherland, I. E., et al.: 'The trimosbus', Proc. First Caltech Conf. on Very Large Scale Integration, Pasadena, California, January 1979, pp. 395-427, caltechconf.library.caltech.edu/193 accessed November 2017

[2] van Berkel, C.H. and Molnar, C.E.: 'Beware the three-way arbiter', *J. Solid-State Circuits*, 1999, **34**, (6), pp. 840-848, doi: 10.1109/4.766818

[3] Davies, A.C.: 'Dynamic Properties of a Multiway Arbiter', IEEE Int. Symp. on Circuits and Systems (ISCAS), Geneva, Switzerland, May 2000, pp. 221-224, doi: 10.1109/ISCAS.2000.856036

[4] Rabaey, J. M.: 'Digital Integrated Circuits: A Design Perspective', (Prentice Hall Electronics and VLSI Series, NJ, US, 1996, second edition)