Whitenoise Encryption Implementation with Increased Robustness against Side-Channel Attacks

Mihai Sima
University of Victoria
P.O. Box 1700 Stn CSC, Victoria
British Columbia V8W 2Y2, Canada
Email: msima@ece.uvic.ca

André Brisson
Whitenoise Laboratories Canada Inc.
#701–1736 West 10th Street, Vancouver
British Columbia V6J 2A6, Canada
Email: abrisson@wnlabs.com

***Abstract*—Two circuit design techniques improve the robustness of Whitenoise encryption algorithm implementation against side-channel attacks based on dynamic and/or static power consumption. The first technique aims to conceal the power consumption and has linear cost. The second technique aims to randomize the power consumption and has quadratic cost. These techniques are not mutual exclusive; their synergy provides a good robustness against power analysis attacks. Other circuit-level protection can be applied on top of the proposed techniques, opening the avenue for generating very robust implementations.**

I. Introduction

In the challenge of securing Internet communications, Whitenoise Laboratories has proposed a stream-cipher algorithm [1], [2], [5], [6]. As claimed by Traore and Liu, the Whitenoise encryption algorithm survived a large number of brute force attacks [3], [4]. As a result, the algorithm can be considered to be highly secure.

The physical implementation is a weak chain in computer security today, as it can provide side-channel information that attackers can use to reveal the secret key. As the activity in a cryptosystem is dependent on the secret key, attacks based on power analysis [7], [8], [20] exploit the correlation between the data, operations, and power consumption. Field-Programmable Gate Arrays (FPGA) are notable for their large power consumption, and that leads to particularly vulnerable implementations [17]–[19], [21]. The cost needed to mount power attacks ranges from hundreds of dollars in the case of simple cryptosystems, to thousands (or even tens or hundred of thousands) dollars for more complex cryptosystems. In any case, this vulnerability is subject of major concerns for the builders of cryptosystems.

There are two main techniques to increase the robustness of cryptographic implementations [9]: (i) hiding (or concealing), which makes the power consumption data and/or operation independent, and (ii) masking, which randomizes the power consumption. In this paper both techniques are considered in securing the Whitenoise algorithm implementation.

Whitenoise algorithm consists of a number of Line-Feed Shift Registers (LFSR) of different lengths, whose outputs are XOR'ed and sent to an S-box for deliniarization [1], [2]. Whitenoise brute-force implementation has been shown to be weak to attacks based on the LFSR power consumption and Hamming distance [10]. It is the goal of this paper to propose an implementation technique that remove this weakness, rendering an encryption implementation with increased robustness against such attacks. To summarize, the paper contributions are as follows.

1) A design technique based on cell replication, which conceals the dynamic power consumption of the line-feed shift registers.
2) A design technique based on signal polarity inversion, which conceals the static power consumption of the shift registers.
3) A design technique based on running fake keys, which further randomizes the power consumption of the shift registers.

The paper is organized as follows. Section II summarizes the Whitenoise encryption algorithm. Section III discloses a power concealment technique, whereas Section IV discloses a power masking technique. Section V provides a detailed discussions of the achieved security versus the cost. Section VI concludes the paper.

II. Whitenoise Encryption Algorithm

As shown in Figure 1, the Whitenoise encryption algorithm includes a number of line-feed shift registers (LFSR), whose lengths and bit values are defined by the secret key (the mentioned figure shows only fours registers with lengths equal to 3, 5, 7, and N, respectively). The registers loop infinitely, their outputs being XOR'ed. The XOR output is sent to an S-box for deliniarization.

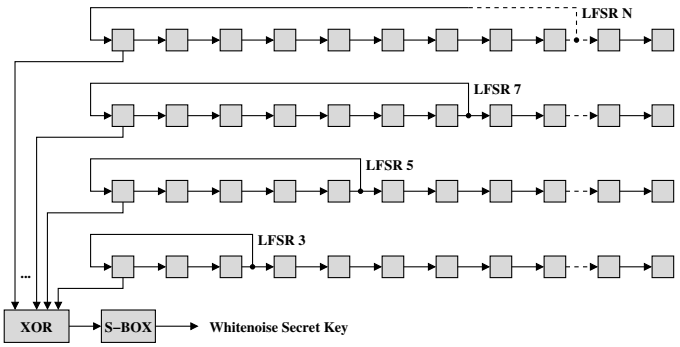

Fig. 1: The Whitenoise encryption algorithm.

For the sake of presentation, we assume that the maximum configurable length of a shift register in the Whitenoise algorithm is 11. Assume a line-feed shift register with seven cells, whose configured bit values are A, B, C, D, E, F, and G. In this case, at it is apparent in Figure 2, a stub of four (pink) cells operates in parallel with the main (blue) loop, a feature that generates a periodic power consumption (ABCD, GABC, FGAB, EFGA, DEFG, CDEF, BCDE) having the period equal to the length of the main line-feed shift register. This is a major leak of side-channel information that can be used to find the number and the lengths of the line-feed shift registers, and ultimately determine the secret key [10].

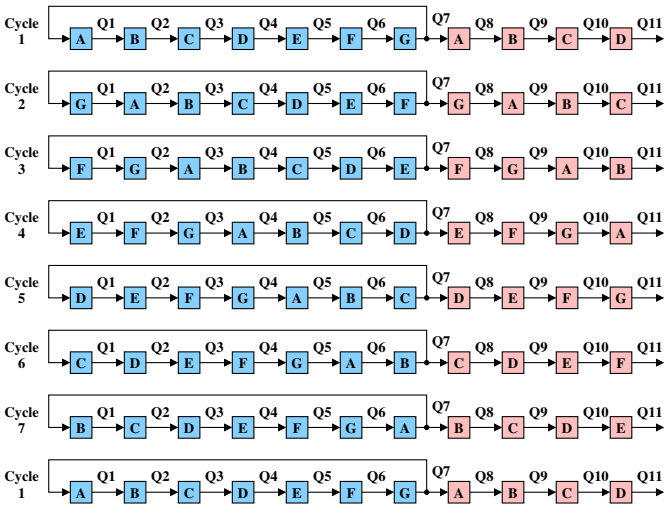

Fig. 2: An 11-bit register with 7-cell feedback.

The attempt of deactivating of the pink stub (for example, by forcing it in an idle state), in order to eliminate the periodic component of the power consumption, does not solve the problem, as the static power consumption of the main (blue) loop still depends on the loop Hamming distance. Attacks based on leakage have been proven successful on cryptosystems [8], [12]–[14]. As leakage power reaches a large fraction of the total power consumption in modern technology nodes, this problem can no longer be neglected.

In the next section, we present a circuit technique that conceals both the static and dynamic power consumption, with beneficial effects in robustness against power attacks.

III. Techniques to Conceal Power Consumption

To conceal the periodic power consumption of the pink stub, we propose to deploy a second (green) stub, such that the total number of cells in the pink and green stubs equals the number of cells in the blue (main) shift register. This is shown in Figure 3. This way, the total dynamic power consumption of the pink and green part equals the dynamic power consumption of the blue part, which is itself a constant (which means it does not carry any side-channel information). Unfortunately, both the static power consumptions of the blue and pink+green parts depend on Hamming distances and, therefore, constitute a source of information leak. As mentioned in the previous section, this is a serious implementation problem in modern technology nodes.

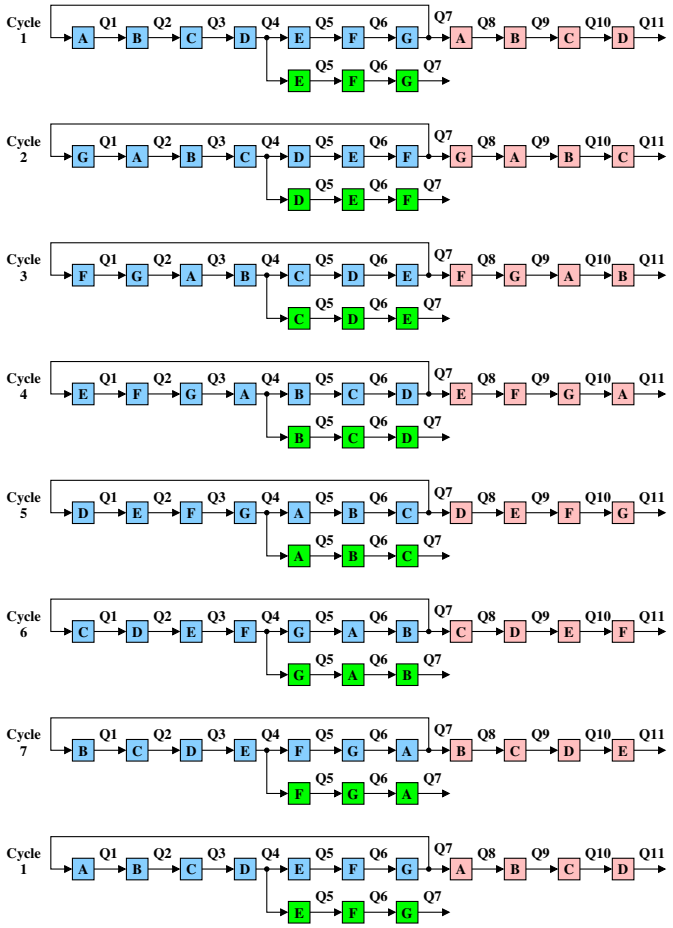

Fig. 3: A secured 11-bit register with 7-cell feedback.

A way to conceal the static power consumption, is to drive the pink+green part with inverted signals, as shown in Figure 4. This way, the number of cells in logic '1' equals the number of cells in logic '0', which breaks the dependence of the static power consumption on the key bits. At this point, the attacker is no longer able to obtain side-channel information by simply stopping the clock and measuring the leakage power consumption.

IV. Techniques to Mask Power Consumption

This technique consists in replicating each register $N-1$ times (where N is the total number of registers), such as the original register runs its own key bits o produce real scrambling data, and all its replicas run the key bits of all the other registers to produce fake scrambling data. This technique is exemplified in Figure 5, where Registers 1 and 2 are replicated. Register 1 replica runs the key bits of the original Register 2, and Register 2 replica runs the key bits of the original Register 1. Note that Bits H1 and H1 in the Register 2 replica (typed in slanted fonts) are dummy data; they are needed since the Register 2 feedback is longer than the Register 1 feedback.

Assume $N = 10$. Then, there will be $N \times N = 10 \times 10 - 10 = 90$ registers running fake data. As a result, the power consumption will generate 90% fake side-channel information

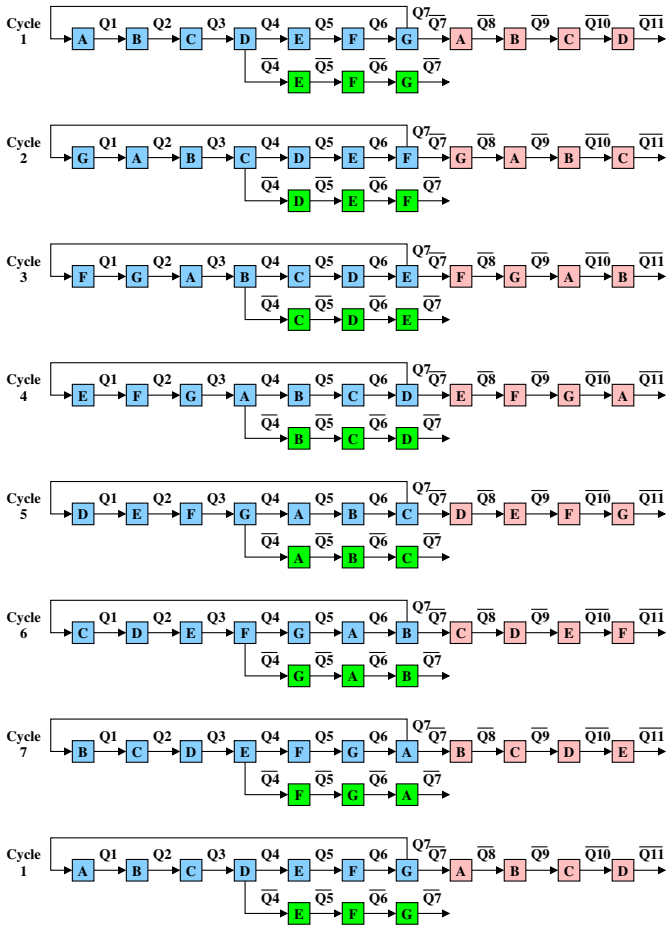

Fig. 4: A highly secured 11-bit register with 7-cell feedback.

misleading the attacker. This represents an order of magnitude improvement in robustness at a quadratic cost. At this point it should be mentioned that adding the *masking* technique on top of the hiding technique requires further investigation, as the efficiency of combining *hiding* with *masking* is still under intense debate [23].

To summarize, the following transformations are proposed to build a secured-by-design Whitenoise implementation.

- The addition of a second (green) stub to force the total power consumption of the two stubs constant. This technique aims to conceal the dynamic power consumption of the shift registers.
- The change in signal polarity for both stubs, which aims to conceal the total dynamic and static power consumption.
- The replication of the shift registers, such that they run fake key bits. This technique aims to mask both the dynamic and static power consumptions.

It is important to mention that the proposed circuits can be easily augmented with other security techniques. For example, dual-rail logic can be an interesting option for more advanced implementations [11], [15], [16], [22]. This is left for future work.

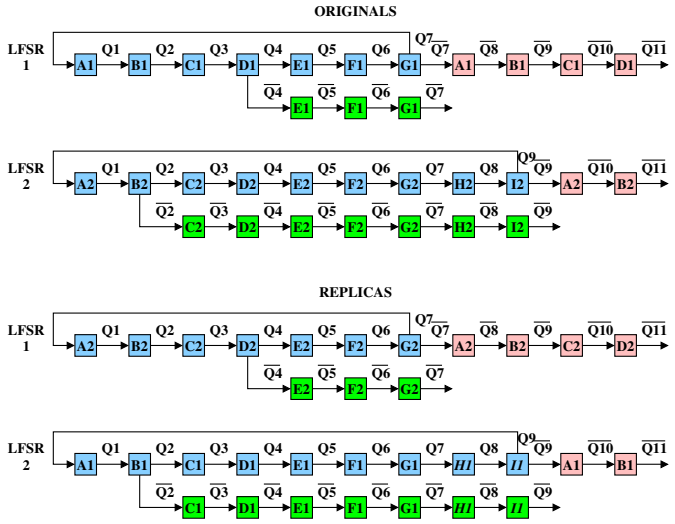

Fig. 5: A masked implementation.

V. Discussions

There is a known vulnerability of the straightforward (which is also the cheapest) implementation due to the periodic activity within shift registers [10]. Depending on the application cost and required security level, measures can be taken to defend the implementation. A number of defending techniques based on concealing and masking the power consumption have been presented. From a business perspective, it is possible to choose one of the following options:

- The straightforward (non-secured) implementation, which is the cheapest one and offers the lowest level of security. This implementation is appropriate for applications in which the equipment for power signal acquisition is more expensive than the gains that can be obtained from breaking the cryptosystem (such as bus passes or museum passes), or when the attacker does not have access to the physical implementation of the system.
- The power concealment protection, which has a linear cost (in the worst case scenario all the shift registers are duplicated, doubling the silicon area). Possible applications include mobile devices, wearable electronics, etc.
- The power masking protection, which has a quadratic cost, where each of the N registers is replicated $N-1$ times. It should be emphasized that this technique opens up the avenue for further research, as circuit-level countermeasures, such as WDDL, are likely to be required. Possible applications would include hard-disks with encryption.

VI. Conclusion

A circuit design technique based on replication improves the robustness of Whitenoise encryption algorithm implementation against side-channel attacks based on dynamic and/or static power consumption. The first technique conceals

the power consumption and has linear cost. The second technique randomizes the power consumption and has quadratic cost. These techniques are not mutual exclusive; their synergy provides a good robustness against power analysis attacks. Other circuit-level protection can be applied on top of the proposed techniques, opening the avenue for generating very robust implementations.

ACKNOWLEDGMENT

The authors would like to thank ...

REFERENCES

[1] A.J. Brisson, "The Whitenoise Algorithm – A Visual Look," Technical Report, Whitenoise Laboratories, Vancouver, British Columbia, Canada, Nov. 2011. [Online]. Available: http://www.wnlabs.com/pdf/WhitenoiseAlgorithmVisualLook.pdf

[2] S. Coram-Mekkey, "Whitenoise Laboratories – An Overview," White Paper, Whitenoise Laboratories, Vancouver, British Columbia, Canada, June 2015. [Online]. Available: http://www.wnlabs.com/papers/Whitenoise_Overview_Short.pdf

[3] I. Traoré and M.Y. Liu, "Evaluation of Whitenoise Cryptosystem. Part 1: Encryption Algorithm," Technical Report ECE03-3, University of Victoria, British Columbia, Canada, Feb. 2003.

[4] D. Wagner, "A Security Evaluation of Whitenoise," ..., Oct. 2003. [Online]. Available: http://www.wnlabs.com/pdf/Wagner_Security_Analysis.pdf

[5] S.L. Boren and A.J. Brisson, "Dynamic Distributed Key System and Method for Identity Management, Authentication Servers, Data Security and Preventing Man-in-the-Middle Attacks," U.S. Patent Application 2009/0106551 A1, Apr. 2009.

[6] A.J. Brisson, "Dynamic Identity Verification and Authentication, Dynamic Distributed Key Infrastructures, Dynamic Distributed Key Systems and Method for Identity Management, Authentication Servers, Data Security and Preventing Man-in-the-Middle Attacks, Side Channel Attacks, Botnet Attacks, and Credit Card and Financial Transaction Fraud, Mitigating Biometric False Positives and False Negatives, and Controlling Life of Accessible Data in the Cloud," U.S. Patent Application 2013/0227286 A1, Aug. 2013.

[7] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proc. 19th Annual Int. Cryptology Conf. (CRYPTO '99)*. Santa Barbara, California: Dec. 1999, pp. 388–397.

[8] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *Proc. 6th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004)*. Cambridge, Massachusetts: Aug. 2004, pp. 16–29.

[9] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer Science+Business Media, 2010.

[10] B. Zakeri, *On Studying Whitenoise Stream-Cipher Robustness against Power Analysis Attacks*, MASc Thesis, University of Victoria, British Columbia, Canada, Dec. 2012.

[11] K. Tiri, M. Akmal, and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards," in *Proc. 28th European Solid-State Circuits Conf. (ESSCIRC 2002)*. Florence, Italy: Sept. 2002, pp. 403–406.

[12] L. Lin and W. Burleson, "Leakage-Based Differential Power Analysis (LDPA) on Sub-90nm CMOS Cryptosystems," in *Proc. IEEE Int. Symp. on Circuits and Systems (ISCAS 2008)*. Seattle, Washington: May 2008, pp. 252–255.

[13] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits," *IEEE Tran. on Circuits and Systems-I: Regular Papers*, vol. 57, no. 2, pp. 355–367, Feb. 2010.

[14] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Trifiletti, "Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations," *IEEE Tran. on Circuits and Systems-I: Regular Papers*, vol. 61, no. 1, pp. 429–442, Feb. 2014.

[15] D. Suzuki and M. Saeki, "Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style," in *Proc. 8th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006)*. Yokohama, Japan: Oct. 2006, pp. 255–269.

[16] S. Guilley, S. Chaudhuri, L. Sauvage, T. Graba, J.-L. Danger, P. Hoogvorst, V.-N. Vong, M. Nassar, and F. Flament, "Shall we trust WDDL?" in *Proc. First Int. Conf. Future of Trust in Computing 2008*. Berlin, Germany: June/July 2008, pp. 208–215.

[17] S. B. Örs, E. Oswald, and B. Preneel, "Power-Analysis Attacks on an FPGA – First Experimental Results," in *Proc. 5th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2003)*. Cologne, Germany: Sept. 2003, pp. 35–50.

[18] F.-X. Standaert, S. B. Örs, J.-J. Quisquater, and B. Preneel, "Power Analysis Attacks Against FPGA Implementations of the DES," in *Proc. 14th Int. Conf. on Field Programmable Logic and Applications (FPL 2004)*. Leuven, Belgium: Aug.-Sept. 2004, pp. 84–94.

[19] F.-X. Standaert, F. Mace, E. Peeters, and J.-J. Quisquater, "Updates on the Security of FPGAs Against Power Analysis Attacks," in *Proceedings of the 2nd Int. Workshop on Reconfigurable Computing: Architectures, Tools and Applications (ARC 2006)*. Delft, The Netherlands: Mar. 2006, pp. 335–346.

[20] Y. Lu, M. P. O. (née McLoone), and J. V. McCanny, "Differential Power Analysis of a SHACAL-2 Hardware Implementation," in *Proc. IEEE Int. Symp. on Circuits and Systems (ISCAS 2008)*. Seattle, Washington: May 2008, pp. 2933–2936.

[21] L. Sauvage, M. Nassar, S. Guilley, F. Flament, J.-L. Danger, and Y. Mathieu, "DPL on Stratix II FPGA: What to Expect?" in *Proc. IEEE Int. Conf. on Reconfigurable Computing and FPGAs (ReConFig 2009)*. Cancun, Mexico: Dec. 2009, pp. 243–248.

[22] K. Tiri and I. Verbauwhede, "Design Method for Constant Power Consumption of Differential Logic Circuits," in *Proc. Design, Automation, & Test in Europe Conf. and Exposition (DATE'05)*. Munich, Germany: Mar. 2005, pp. 628–633.

[23] K. Tiri and P. Schaumont, "Changing the Odds Against Masked Logic," in *Proc. 13th Int. Workshop on Selected Areas in Cryptography (SAC 2006)*. Montreal, Canada: Aug. 2006, pp. 134–146.