

# Whitenoise Encryption Implementation with Increased Robustness to 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 design techniques improve the robustness of Whitenoise encryption algorithm implementation to 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 mutually exclusive; their synergy provides a good robustness to 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], [6], [7]. This technology can be used in applications such as identity management, secure network access, dynamic authentication, intrusion detection, automatic revocation, as well as encryption. The Whitenoise algorithm is rather simple; thus, its implementation will need only reduced silicon area or a low-end microcontroller (such as, PIC from Microchip Tech [3]), and exhibit low power consumption, being particularly suitable for use in portable electronics. The Whitenoise encryption algorithm survived a large number of brute force attacks mounted on a computer array during a performance analysis conducted by Traoré and Liu [4] at the University of Victoria, Canada. As described by Wagner [5], no mathematical attack breaking Whitenoise was found in his security analysis at the University of California at Berkeley. As a result, the algorithm is considered to be highly secure.

The deployment of a cryptosystem introduces new physical variables. Its physical implementation provides side-channel information that attackers can use to reveal the secret key and fixed data therein. As the encryption activity depends on the secret key, attacks based on power analysis [8], [9], [19] exploit the correlation between the data, operations, and power consumption. The popular Field-Programmable Gate Arrays (FPGA) are notable for their large power consumption, and that leads to vulnerable implementations [17], [18]. It is worth mentioning that the

cost needed to mount power attacks ranges from thousands of dollars in the case of simple cryptosystems to tens or hundreds of thousands of dollars for more complex cryptosystems. In any case, this vulnerability is a major concern for the builders of cryptosystems.

There are two main techniques to increase the robustness to side-channel attacks of cryptosystems [10]: (i) hiding (or concealing), which makes the power consumption independent relative to the processed data and/or operations, and (ii) masking, which randomizes the power consumption. In this paper, both techniques are considered in securing the Whitenoise hardware implementation or as an adjunct to randomize the power consumption of other cryptosystems.

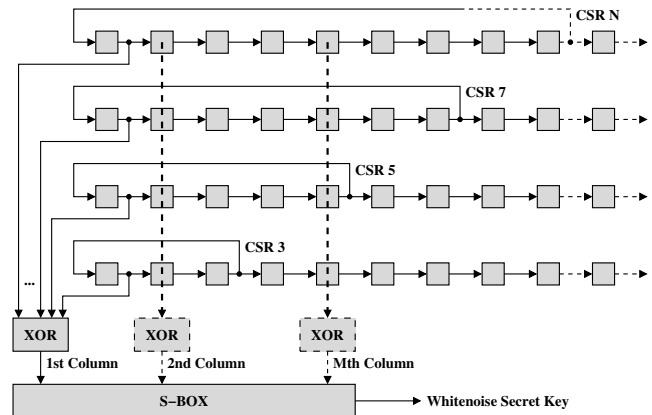


Figure 1: Common Whitenoise algorithm implementation.

Figure 1 shows a common implementation of the Whitenoise algorithm, which consists of prime-length Circular Shift Registers (CSR) storing randomized subkey data, whose outputs are XOR'd and sent to an S-box for delinearization [1], [2]. The number of CSRs, their lengths, and their byte values are configurable, being populated and re-populated from a Master Key. It is a concern that this *implementation* might be vulnerable to attacks based on power consumption and Hamming distance (defined as the number of bits which differ between two binary strings)

[11]. In this paper we propose design techniques that remove this weakness, rendering an encryption implementation with increased robustness to such attacks. Our contributions are as follows.

- 1) A design technique based on cell replication, which provides a high degree of concealment of the CSR power consumption.
- 2) A design technique based on signal polarity inversion, which further removes the power consumption dependence on the Hamming distance.
- 3) A design technique based on fake keys, which randomizes the power consumption of the CSRs.

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 detailed discussions of the achieved security versus the cost of the implementation. Section VI concludes the paper.

## II. WHITENOISE ENCRYPTION ALGORITHM

The implementation of the Whitenoise algorithm shown in Figure 1 is based on Circular Shift Registers (CSR), which store randomized subkeys whose number, lengths, and byte values are defined by the secret master key (for clarity, only four registers with 3, 5, 7, and N cells, respectively, are shown). These registers loop infinitely, their outputs being XOR'd. The XOR outputs are sent to an S-box for delinearization.

In a common hardware implementation scenario, each CSR is manufactured with the largest number of cells allowed by the algorithm and cost of the chip. Based on randomized data from the master key, a set of selectors (not figured) will define the length and byte values of each CSR. For the sake of presentation, assume that the maximum configurable length of a subkey in the implementation is 11. Also assume that one of the circular shift registers has seven cells, whose configured byte values are A, B, C, D, E, F, and G (the letters are used in ascending order for clarity only, as they do not represent static values). Figure 2 presents the evolution of the 7-cell CSR over seven cycles. Due to the circular operation, only the position of the bytes stored into main (blue) loop change, not their values. Thus, main loop's total power consumption does not change from cycle to cycle (but it can change when its subkey is reloaded). On the other hand, the stub of four (red) cells, which operates in parallel with the main (blue) loop, exhibits a periodic power consumption (ABCD, GABC, FGAB, EFGA, DEFG, CDEF, BCDE) having the period equal to the length of the CSR. This is a major leak of side-channel information that can be used to reveal the number and the lengths of the circular shift registers, and ultimately a static secret key [11].

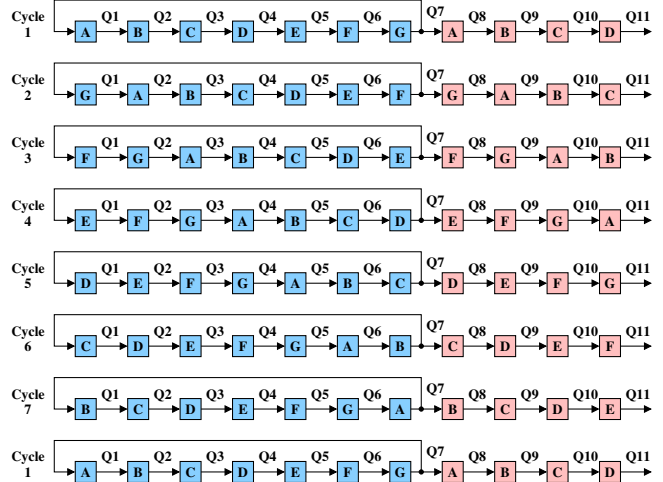


Figure 2: A 7-cell circular shift.

By deactivating the red stub (e.g., by forcing it in an idle state), the periodic component of the power consumption is eliminated. However, this approach only slightly improves the robustness to power attacks. As the levels of the dynamic and static (leakage) power consumptions of the main (blue) loop still depend on the Hamming distance, they can change when the secret key is reloaded. In particular, leakage-based attacks have been proven highly successful [9], [13]–[15]. As leakage power is a large fraction of the total power consumption in modern technologies, this problem cannot be neglected.

We next present a technique that conceals the static and dynamic power consumptions. It has strong beneficial effects in Whitenoise robustness to power-based attacks.

## III. TECHNIQUES TO CONCEAL POWER CONSUMPTION

To conceal the periodic component of the power consumption of the red stub, we propose to deploy a second (green) stub, such that the total number of cells in the red and green stubs equals the number of cells in the blue (main) loop. This technique is illustrated in Figure 3. It is apparent that the byte values in the red+green part are identical to those in the blue part; thus, the power consumption of the red and green part equals the power consumption of the blue part, which, as described, is itself a constant due to the circular operation. Unfortunately, the static power consumptions of both the blue and red+green parts depend on Hamming distances, being a source of information leak. As mentioned in the previous section, this is a serious security threat.

The dynamic and static power consumptions are concealed by driving the red+green part with inverted signals (Fig. 4). This way, since the number of cells in logic '1' equals the number of cells in logic '0' at any time instance, the dependence of the power consumption on Hamming

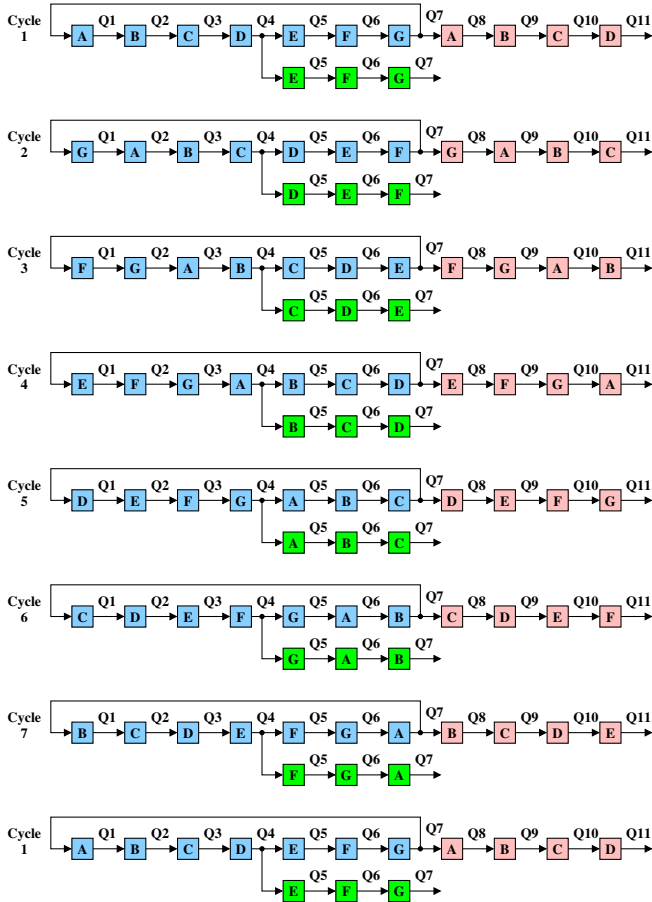


Figure 3: A secured 7-cell circular shift register.

distance is removed with no hardware overhead. Since the power consumption is now independent of the secret key, the attacker is no longer able to obtain side-channel information by stopping the clock and measuring the leakage.

The manufacturing technology exhibits variations with process and temperature. Since component mismatches will always exist, different cells in the implementation will not have equal power consumptions. As a result, security techniques based on power concealment suffer from technological limitations. The next section addresses this issue, and proposes an additional layer of protection based on power masking.

#### IV. TECHNIQUES TO MASK POWER CONSUMPTION

We propose to replicate each register  $N - 1$  times (where  $N$  is the total number of registers), such as the original register runs its own subkey to produce real randomized data, whereas its replicas run the subkeys of the other registers to produce fake randomized data. This technique is exemplified in Figure 5, where the Register 1 replica runs the key bytes of the original Register 2, and the Register 2 replica runs the key bytes of the original Register 1 (note that Bytes H1

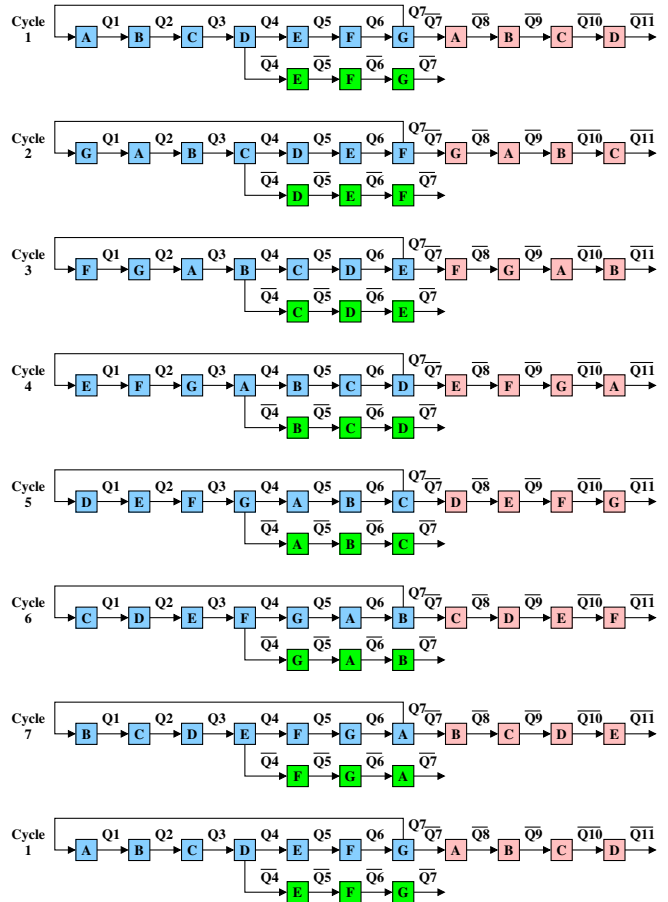


Figure 4: A highly secured 7-cell circular shift register.

and H1 in the Register 2 replica are dummy data; they are needed since the Register 2 feedback is longer than the Register 1 feedback). The reasoning behind this technique is to run each of the subkey byte values with every CSR length, thereby decorrelating the items of information they may carry.

It should be observed that the attacker does not have access to any of the replicas' outputs, as they are not routed to circuit's pins. Without knowledge on these outputs, it is very difficult (if not impossible) to launch side-channel attacks on replicas themselves; this makes the masking technique highly secure.

Assume  $N = 10$ . Then, there will be  $N \times N - N = 10 \times 10 - 10 = 90$  registers running fake data. As a result, the residual power consumption due to mismatching will generate 90% fake side-channel information misleading the attacker. This represents an order of magnitude improvement in robustness achieved 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 effectiveness of combining *hiding* with *masking* is under intense debate [21].

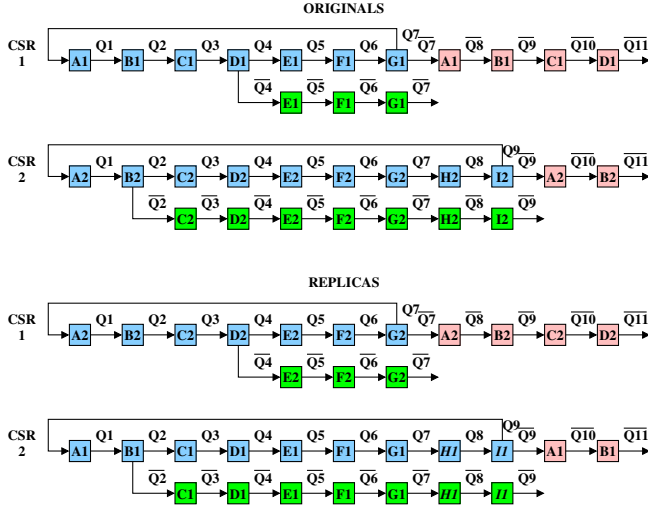


Figure 5: A masked implementation.

To summarize, the following physical transformations are proposed to build a Whitenoise implementation, which is robust to attacks based on power consumption.

- The addition of a second (green) stub to force the total power consumption of the red+green part constant. This technique aims to conceal the power consumption of the circular shift registers and their stubs.
- The change in signal polarity for both stubs, which aims to remove the dependence on both dynamic and static power consumptions on Hamming distance.
- The replication of the circular shift registers, such that the replicas will run fake subkeys. This technique aims to randomize the power consumption, thereby misleading the attacker.

It is important to emphasize that the proposed techniques address the security problem at the conceptual level. Other security techniques at the circuit level can be used on top of the presented techniques. For example, dual-rail logic can be an interesting option for more advanced implementations [12], [16], [20]. This is left for future work.

## V. DISCUSSIONS

There are concerns that the straightforward (which is also the cheapest) Whitenoise implementation might be vulnerable due to the periodic activity within CSRs [11]. Depending on the application cost and required security level, measures can be taken to *defend the implementation*. Techniques based on concealing and masking the power consumption have been presented. From a fabrication perspective, this opens the avenue of trading the security level for the cost of implementation. Possible scenarios are described below.

The **straightforward (non-secured) implementation** is the cheapest one and offers the lowest level of robustness to power attacks. It is appropriate when the equipment for power signal acquisition is more expensive than the gains to be obtained from breaking the cryptosystem (such as bus or museum passes), or when the attacker does not have physical access to the cryptosystem (for example, when Whitenoise is either behind secure perimeters or it is used to randomize the power consumption of different cryptosystems like AES NI from Intel or PAX from Princeton University).

The **power concealment protection**, which has a linear cost (in the worst case scenario all the shift registers are duplicated, doubling the silicon area), can be used to protect portable electronics devices. Possible applications include smartphones, wearable electronics, etc.

The **power masking protection** has a quadratic cost, as each of the  $N$  registers is replicated  $N - 1$  times. This technique opens up the avenue for further research, as the efficiency of combining *hiding* with *masking* is still an open question [21]. Possible applications would include, for example, hard-disks and USB memory keys with hardware encryption.

It is mentioned that the robustness of a cryptosystem *implementation* is difficult to achieve and has been a weak chain in the efforts of providing a trusted computing platform for many years [8], [10]. Power concealment through replication has been previously attempted; see, for example, the dual-rail logic family [20]. Although our replication technique is specific to Whitenoise, it only requires the duplication of a part of the chip (namely, the stubs), whereas the dual-rail logic doubles the chip area. Due to its two-phase operation (precharge, evaluate), the dual-rail logic significantly increases the dynamic power consumption. In contrast, our technique can be implemented in standard logic, thereby maintaining the dynamic power consumption at acceptable levels.

## VI. CONCLUSION

Circuit design techniques based on replication improve the robustness of Whitenoise encryption algorithm implementation to side-channel attacks based on power consumption. The first technique conceals the power consumption and has linear cost. The second technique randomizes the power consumption and has quadratic cost. The synergy of these two techniques provides a good robustness to power analysis attacks. Other circuit-level protection can be applied on top of the proposed techniques, opening the avenue for generating very robust implementations at a reasonable cost. It should be investigated whether these techniques can be used against other attacks relying on electromagnetic radiation, chip temperature, etc.

## 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] C. 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](http://www.wnlabs.com/papers/Whitenoise_Overview_Short.pdf)
- [3] \*\*\*, "PIC10F200/202/204/206 6-Bit, 8-Pin Flash Microcontrollers," Microchip Technology, Arizona, USA, Mar. 2014.
- [4] 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.
- [5] D. Wagner, "A Security Evaluation of Whitenoise," University of California, Berkeley, Oct. 2003. [Online]. Available: [http://www.wnlabs.com/pdf/Wagner\\_Security\\_Analysis.pdf](http://www.wnlabs.com/pdf/Wagner_Security_Analysis.pdf)
- [6] 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.
- [7] 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.
- [8] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proceedings of the 19th Annual International Cryptology Conference (CRYPTO '99)*. Santa Barbara, California: Dec. 1999, pp. 388–397.
- [9] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004)*. Cambridge, Massachusetts: Aug. 2004, pp. 16–29.
- [10] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer Science+Business Media, 2010.
- [11] B. Zakeri, *On Studying Whitenoise Stream-Cipher Robustness against Power Analysis Attacks*, MASC Thesis, University of Victoria, British Columbia, Canada, Dec. 2012.
- [12] 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 *Proceedings of the 28th European Solid-State Circuits Conference (ESSCIRC 2002)*. Florence, Italy: Sept. 2002, pp. 403–406.
- [13] L. Lin and W. Bureson, "Leakage-Based Differential Power Analysis (LDPA) on Sub-90nm CMOS Cryptosystems," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS 2008)*. Seattle, Washington: May 2008, pp. 252–255.
- [14] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits," *IEEE Transactions on Circuits and Systems-I: Regular Papers*, vol. 57, no. 2, pp. 355–367, Feb. 2010.
- [15] 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 Transactions on Circuits and Systems-I: Regular Papers*, vol. 61, no. 1, pp. 429–442, Feb. 2014.
- [16] D. Suzuki and M. Saeki, "Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style," in *Proceedings of the 8th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006)*. Yokohama, Japan: Oct. 2006, pp. 255–269.
- [17] S. B. Örs, E. Oswald, and B. Preneel, "Power-Analysis Attacks on an FPGA – First Experimental Results," in *Proceedings of the 5th International 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 *Proceedings of the 14th International Conference on Field Programmable Logic and Applications (FPL 2004)*. Leuven, Belgium: Aug.-Sept. 2004, pp. 84–94.
- [19] Y. Lu, M. P. O. (née McLoone), and J. V. McCanny, "Differential Power Analysis of a SHACAL-2 Hardware Implementation," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS 2008)*. Seattle, Washington: May 2008, pp. 2933–2936.
- [20] K. Tiri and I. Verbauwhede, "Design Method for Constant Power Consumption of Differential Logic Circuits," in *Proceedings of the Design, Automation, & Test in Europe Conference and Exposition (DATE'05)*. Munich, Germany: Mar. 2005, pp. 628–633.
- [21] K. Tiri and P. Schaumont, "Changing the Odds Against Masked Logic," in *Proceedings of the 13th International Workshop on Selected Areas in Cryptography (SAC 2006)*. Montreal, Québec, Canada: Aug. 2006, pp. 134–146.