Reversible cryptographic hardware with optimized quantum cost and delay.

Anindita Banerjee
Department of Physics and Material Science Engineering, Jaypee Institute of Information Technology
A-10, Sector-62, Noida, Uttar Pradesh, PIN -201307, INDIA
Email: anindita.phd@gmail.com

***Abstract*—In order to defend the power analysis attack reversible logic is a good candidate as it ideally does not dissipate any heat and today reversible logic is an emerging research area. In literature different designs for reversible hardware cryptography have been proposed but they have been implemented using complex gate libraries and further theorems have been proposed defining lower limit of implementation cost which is quantum cost. We have proposed novel designs for reversible ALU of a cryptoprocessor which have been implemented in standard gate library and the quantum cost reported here are better than the lower bounds reported in literature. Further we have calculated delay of the proposed designs. We have verified that our proposed designs are minimal with respect to gate count which is circuit cost by simulating it in RevKit. This is for the first time that the optimization algorithms to optimize quantum cost and delay have been applied to improvise on the cost metric in reversible ALU design.**

***Index Terms*—hardware cryptography, quantum cost, delay, garbage bits, reversible ALU.**

I. Introduction

Today security in digital computing and communications is of prime importance and therefore cryptographic protocols play a major role. These cryptographic protocols have to be robust against numerous attacks such as software attacks [1], microprobing/physical attacks [2] and side-channel attacks [3]. Here, we are interested in protection of cryptoprocessor against power attacks which use the power dissipation characteristics from the cryptoprocessor. There are two types of power attack which are Simple power analysis (SPA) and Differential power analysis (DPA), of these two attacks the DPA is the most powerful attack and it is used to attack the smart card, it utilizes power traces gathered from several runs and relies on the power consumption variation due to data dependency to break the key. Recently Thapliyal [4] and Nayeem *et al.* [5] have proposed reversible logic to thwart attacks against cryptographically secure hardware based on DPA. According to Landauer's principle irreversible logic computation results in energy dissipation due to power loss. In 1973 Bennet [6] had shown that energy dissipation problem of VLSI circuits can be circumvented by using reversible logic. This is so because reversible computation does not require to erase any bit of information and consequently it does not dissipate any energy for computation. Thus if reversible hardware is utilized for cryptography then power analysis attack can be prevented. The most common modular arithmetic operation to be widely used in public key cryptography like RSA, Diffie-Hellman key exchange, Digital Signature Standard and more recent Elliptic Curve Cryptography (ECC) is the Montgomery's modular algorithm [7]. Thapliyal [4] and Nayeem *et al.* [5] have proposed a reversible architecture of ALU and Montgomery's multiplier. However the design proposed by Nayeem is better mainly because as reported in [5] it requires less area as it reuses it's Carry Save Adder (CSA) design, it does not use carry propagation logic and thus fast summation is possible, it's architecture is simple and efficient as it requires only two CSA and does not require substraction operation. In this paper we improvise on the lower bound of quantum cost set in [5]. We have also reported delay of our circuit designs. In next section we briefly discuss the background, in Section III we will present our work and finally we conclude in Section IV.

II. Background

Reversible gate: The gates used in conventional circuit or digital designing is irreversible (except Not gate) that means the input cannot be traced from output. For example the AND gate, OR gate, NAND gate etc. are irreversible gates. A gate is reversible if it has equal number of inputs and outputs and the boolean function that maps the input in output is bijective.

Garbage bit: A garbage bit is the additional output to make a function reversible and it is not used for further computations. Therefore large number of garbage bits are undesirable in a reversible circuit. In a reversible function let q be the maximum number of times an output pattern is repeated then minimum number of garbage bits required for minimality is $\lceil log_2(q) \rceil$ [8].

Reversible circuit: A classical reversible circuit is represented by network of wires that carry bit values to gates that perform elementary operations on the bits. The input bits are written on the left side of the circuit and the output bits are written on the right side of the circuit. The target appear as $\oplus$ and control appear as $\bullet$ on the bit line.

Gate library: Gate count is the total number of gates in a circuit, but it is not unique. If one is allowed to introduce a new gate or if a complex gate library is used then the gate count can be considerably reduced.

978-1-4244-9074-5/10/$26.00 2010 IEEE

There are several universal reversible gate libraries [9], [10] and among these libraries NCT gate library is the smallest complete set. Consequently NCT is a good choice of gate library. Further, these gates can be experimentally realized using low power CMOS [11] and simple optics [12].

Quantum cost: The quantum cost [13] of a reversible gate is the number of primitive quantum gates needed to implement the gate. All (1×1) and (2×2) are considered as quantum primitive gates and the cost of all quantum primitive gates or quantum gates are considered as one. Since Toffoli gate is not a quantum primitive gate, an NCT circuit can not be used directly to determine the quantum cost. But Toffoli gate can be constructed using square root of not gate (V) and C gate and the quantum cost of Toffoli gate is five. Quantum cost is used to measure the implementation cost of a quantum circuit and it is used not only with respect to quantum circuits but also reversible circuit technology [9], [14], [15], moreover, today quantum technology is best candidate for implementing reversible logic.

Delay: Delay [16] is considered as an important measure to evaluate a logic design but not much work have been reported except [16], [17] in reversible logic design. Kaye [18] has defined that a reversible circuit design can be visualized as a sequence of discrete time slices and depth is summation of total time slices. Mohammadi [16] has reported that delay is directly proportional to depth. Interestingly in [14] an algorithm is prescribed to optimize the depth of a circuit (level compaction) but unfortunately none of the reported work have implemented his algorithm.

III. Proposed work

The arithmetic logic unit (ALU) of a cryptoprocessor leak information through power consumption and therefore is the major source of power consumption in the hardware cryptography. An ALU comprises of carry propagate adders; carry save adders, multipliers, squares, registers, multiplexes and accumulators. In public key cryptography like RSA, ECC, DSA etc require arithmetic modular multiplication of large integers and for this the widely used technique is the Montgomery's modular multiplication [7]. Recently Nayeem *et al.* [5] have proposed reversible CSA architecture implementation of Montgomery multiplier and reported lower bound of the quantum cost and garbage bits. We have proposed new designs and the reported quantum cost is lower than the ones reported in literature. In this paper we present reversible designs of each component of ALU. We start with a reversible CSA and a very common operation in the cryptosystem like RSA is the 1024 bit addition which requires carry propagate adder and carry save adder. The design process of our circuits is given in the following steps:

1) Obtain the augmented truth table.
2) Obtain a a reversible circuit using transformation based algorithm and apply local optimization tools [14] to optimize the gate count. The gate count of gated D latch is minimal as it was re synthesized by exact synthesis algorithm [19] using RevKit [20] and it resulted in same design.
3) Obtain an elementary circuit by converting the Toffoli gate into elementary gate.
4) Apply the quantum cost optimization algorithm [15] to obtain the optimized quantum cost.
5) Apply the level compaction algorithm [14] to obtain the optimized delay.

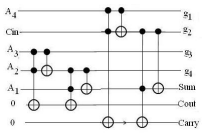

Fig. 1. Reversible four-to-two CSA adder

TABLE I
Comparison of different reversible four-to-two CSA adder where N stands for Not gate, C stands for Cnot gate and T stands for Toffoli gate.

	Nayeem *et al.* [5]	Thapliyal [4]	Proposed
Quantum cost	12	28	12
Garbage bits	4	4	4
Gates	MTSG	TSG	N, C and T

In Fig. 1 we have presented a reversible four-to-two carry save adder. To briefly discuss the existing reversible CSA architecture [4] requires TSG gate which has quantum cost of 14. The TSG gate can perform adder operation. In [5] a full adder operation is realized by a MTSG gate which is not a unique gate and we have proved in [21] that several such gates can be proposed. Therefore TSG and MTSG gates belong to complex gate library for which no experimental realization is present in literature. In Table I we have compared the quantum cost and garbage bits of reversible four-to-two CSA adder and the proposed design has a delay of 9. Apart from CSA adders this multiplier requires sequential elements like register and shift registers. In Fig. 2 we have presented gated D Latch using Toffoli gate and a Cnot gate with circuit cost of 3, quantum cost of 5 and delay of 5.

The n-bit reversible register is designed from n gated D latch as shown in Fig. 3. In [5] according to Lemma 2 the quantum cost of an n-bit reversible register is at least 6n but present designs show that the quantum cost can be reduced to 5n. Therefore though the Theorem 1 in [5] stands the same

Fig. 2. Reversible D latch

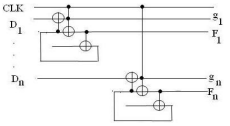

Fig. 3. Reversible n bit register

TABLE II
COMPARISON OF DIFFERENT REVERSIBLE N BIT REGISTER.

	Nayeem *et al.* [5].	Thapliyal [4]	Proposed
Quantum cost	6n	6n	5n
Garbage bits	2n	n+1	n+1
Gates	F and C	F and C	N, C and T

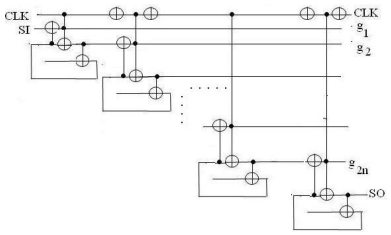

Fig. 4. Reversible SISO register.

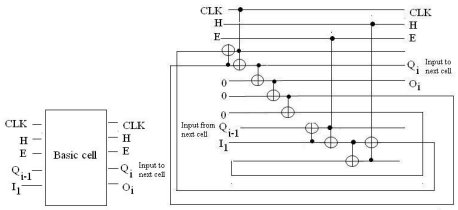

Fig. 5. Reversible PIPO register (a) basic cell (b) NCT circuit

TABLE IV
COMPARISON OF DIFFERENT REVERSIBLE N BIT PIPO REGISTER.

	Nayeem *et al.* [5]	Proposed
Quantum cost	18n	15n
Garbage bits	3n+3	3n+3
Gates	F and HNFG	N, C and T

provided we consider Fredkin gate as 1 therefore Fredkin gate library but if we consider other gate library then it is not applicable but the Lemma 2 should stand the same for all gate libraries as it provides a comparison with the quantum cost. It is observed that present design has lower quantum cost than the lower bound in Lemma 2 [5]. In Table II we have compared the proposed design with [5]. The delay for the reversible n-bit register is 5n.

Modified Theorem 1: In NCT gate library an n-bit reversible register can be realized by at least 3n gates and n+1 garbage outputs.

Modified Lemma 2: The quantum cost of an optimized n-bit reversible register is at least 5n.

In serial in serial out register (SISO), data is shifted one bit right with every clock pulse. In Fig. 4 we have presented n bit reversible SISO shift register comprising of D flip flop (master slave), it comprises of 6n +1 gates in NCT gate library and 2n + 2 garbage bits. Theorem 3 in [5] as we have already mentioned that each Fredkin gate is gated D latch and considered as 1 gate, but their design can be improvised by considering a single bit line for clock and then another bit line for inverted clock pulse. The quantum cost of n bit SISO shift register is 10n +1 while the quantum cost reported in [5] is 12n and optimized delay of present design is 10n. In Table III we have compared the proposed design with with [5].

Modified Theorem 3: In NCT gate library an n-bit reversible SISO shift register using master-salve D flip-flops can be realized by at least 8n-1 gates and 2n+1 garbage outputs.

Modified Lemma 4: The quantum cost of an optimized n-bit reversible SISO shift register is at least 10n.

A parallel in parallel out register (PIPO) is one where the data input for example $(I_1, I_2....I_n)$ are entered into the register at once with the next clock pulse, it shifts parallel and it appears at the parallel output $(O_1, O_2....O_n)$ at the end. In Fig. 5 we have presented the PIPO shift register it consist of D flip flop that executes the output depending on the value of Hold and Enable bit lines. When the Hold bit line is low and the Enable bit line is high then the input value I_1 is loaded into the register and if Enable is low then input is shifted right. When the Hold bit line is High then the register retains its present value. The present design improves over the Lemma 7in [5] because the quantum cost of the present design of n bit reversible PIPO shift register is at least 15n and the delay is 14n. In Table IV we have compared the proposed design with with [5].

Modified Theorem 6: In NCT gate library an n-bit reversible PIPO shift register using clocked D flip-flops can be implemented by 9n reversible gates and 3n+3 garbage outputs.

Modified Lemma 7: The quantum cost of an optimized n-bit reversible PIPO shift register is at least 15n.

In Fig. 6 a reversible multiplexer is presented which has 2n gates, 4n quantum cost and 3n+1 delay. Here S is the Select bit line that selects between the two inputs A_{1-n} and B_{1-n}, to be precise when $S = 0$ then $Z_{1-n} = A_{1-n}$ and when $S = 1$ then $Z_{1-n} = B_{1-n}$. In Table V we have compared the proposed design with with [5].

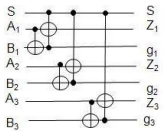

Fig. 6. Reversible multiplexer

TABLE III
COMPARISON OF DIFFERENT REVERSIBLE N BIT SISO REGISTER.

	Nayeem *et al.* [5]	Thapliyal [4]	Proposed
Quantum cost	12n	13n+1	10n
Garbage bits	2n+1	4n+1	2n+1
Gates	F and C	F and C	N, C and T

TABLE V
COMPARISON OF DIFFERENT REVERSIBLE N BIT MULTIPLEXER.

	Nayeem et al. [5]	Proposed
Quantum cost	5n	4n
Garbage bits	n	n
Gates	F and HNFG	N, C and T

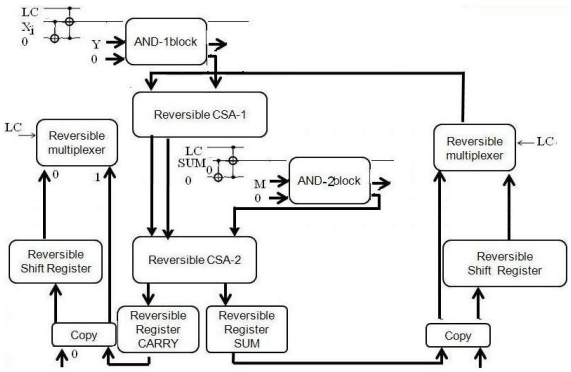

Fig. 7. Reversible Montgomery multiplier

The reversible Montgomery's multiplier is shown in Fig. 7 here the multiple bits are represented by broad lines and single bits are represented by thin lines. Reversible Montgomery Multiplier contains: Four-to-two n+1 CSAs, requiring 12(n+1) elementary gates and 4(n+1) garbage outputs; 2(n+1) Peres gates to compute AND-1 and AND-2 blocks requiring 8(n+1) elementary gates and 2(n+1) garbage outputs; two (n+1)-bit reversible multiplexors, requiring 8(n+1) elementary gates and 2(n+1) garbage outputs; two (n+1)-bit reversible PIPO shift registers, requiring 30(n+1) quantum cost and 2(3n+6) garbage outputs; two (n+1)-bit registers, requiring 2(5n+5) elementary gates and 2(n+2) garbage outputs; four gates for selections requiring 8 elementary gates and 4 garbage outputs; 2(n+1) Cnot gates to construct two COPY blocks, requiring 2(n+1) elementary gates; one Feynman gate to get another copy of SUM0 which requires one elementary gate. Therefore total quantum cost of reversible Montgomery multiplier is

12(n+1)+8(n+1)+8(n+1)+30(n+1)+2(5n+5)+8+2(n+1)+1 = 70n+79.

Modified Theorem 8:The present n bit reversible Montgomery multiplier can be realized by 16n+28 garbage bits and 70n+79 quantum cost.

IV. Conclusion

In this paper reversible logic is implemented in a cryptoprocessor. The proposed designs are implemented in a standard NCT gate library which can be experimentally realized. The proposed designs have better lower bound than [5] for quantum cost. Further in this paper we have introduced delay which is an important measure for evaluating logic design. The cost metrics which are quantum cost and delay are optimized by the quantum cost algorithm [15] and level compaction algorithm in [14] respectively. Therefore we conclude that present designs are more cost effective than the existing designs and also implementable since NCT gates are experimentally realized. Thus proposed work will engender a new thread of research in implementation of reversible hardware cryptography to thwart power analysis attack.

TABLE VI
Comparison of reversible Montgomery multiplier.

	Nayeem et al. [5]	Proposed
Quantum cost	80n+91	70n+79
Garbage bits	16n+28	16n+28
Delay	80n+91	65n+74
Gates	F, C, MTSG and HNFG	N, C and T

References

[1] S. Ravi, A. Raghunathan and S. Chakradhar, "Embedding Security in Wireless Embedded Systems," *in Proc. Int. Conf. VLSI Design*, pp. 269-270, Jan. 2003.

[2] O. K. Ommerling and M. G. Kuhn, "Design Princeples for Tamperresistant Smartcard Processors," *in Proc. USENIX Workshop on Smartcard Technology*, pp. 1-12, May 1999.

[3] J. J. Q. adn and D. Samyde, "Side-channel Cryptanalysis", *in Proc. SECI*, pp. 179-184, Sept. 2004.

[4] H. Thapliyal and M. Zwolinski, "Reversible logic to cryptographic hardware: a new paradigm," *in Proc. of the 49th IEEE International Midwest Symposium on Circuits and Systems*, Puerto Rico, vol. 1, pp. 342- 346, Aug. 2006.

[5] N. M. Nayeem, L. Jamal and H. M. H. Babu, "Efficient reversible Montgomery multiplier and its application to hardware cryptography," *Journal of computer science*, vol. 5, pp. 49-56, 2009.

[6] C. H. Bennett, "Logical reversibility of computation," *IBM J. Res. Dev.*, vol. 7, no. 6, pp. 525-532, 1973.

[7] P.L. Montgomer, "Modular Multiplication without Trial Division", *Math. Comput.*, vol. 44, no. 170, pp. 519-521, April 1985.

[8] G. W. Dueck and D. Maslov, "Reversible function synthesis with minimum garbage outputs," *in 6th International Symposium on Representations and Methodology of Future Computing Technologies*, pp 154-161, March 2003.

[9] D. Maslov, G. W. Dueck and N. Scott, "Reversible logic synthesis benchmark page," 2007 http://webhome.cs.uvic.ca/ dmaslov/.

[10] R. Wille, D. Groe, L. Teuber, G. W. Dueck and R. Drechsler , "RevLib: an online resource for reversible functions and reversible circuits," *38th International Symposium on Multiple-Valued Logic*, Dallas, Texas, pp. 220-225, May 2008.

[11] B. Desoete and A. De Vos, "A reversible carry-look-ahead adder using control gates," *Integration, the VLSI J.*, vol. 33, pp. 89-104, Dec. 2002.

[12] J. L. O. Brien, J. Pryde, A. G. White, T. C. Ralph and D. Branning, "Demonstration of an all-optical quantum controlled-NOT gate," *Nature*, vol. 426, pp. 264-267, Nov. 2003.

[13] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter, "Elementary Gates for Quantum Computation," *Phys. Rev. A*, vol. 52, pp.3457-3467, Nov. 1995.

[14] D. Maslov, G. W. Dueck, D. M. Miller and C. Negrevergne , "Quantum Circuit Simplification and Level Compaction," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 27, pp. 436-444, March 2008.

[15] A. Banerjee and A. Pathak, "An algorithm for minimization of quantum cost," *Appl. Math. Info. Sc.*, 2010 (in press).

[16] M. Mohammadi and M. Eshghi, "On figures of merit in reversible and quantum logic designs," *Quantum information Process*, vol. 8, no. 4, pp.297-318, Aug. 2009.

[17] H. Thapliyal and N. Ranganathan, "Design of reversible latches optimized for quantum cost, delay and garbage outputs," *23rd International Conference on VLSI Design*, Bangalore, India, Jan. 2010.

[18] P. Kaye, R. Laflamme and M. Mosca, "An introduction to quantum computing," *Oxford University Press*, New York, 2007.

[19] D. Groe, R. Wille , G. W. Dueck and R. Drechsler, "Exact multiple control Toffoli network synthesis with SAT techniques," *IEEE Trans. on CAD*, vol. 28, pp. 703-715, 2009.

[20] M. Soeken, S. Frehse, R. Wille, R. Drechsler, "RevKit: A Toolkit for Reversible Circuit Design," *Workshop on Reversible Computation*, 2010, http://www.revkit.org.

[21] A. Banerjee and A. Pathak, "Reversible Multiplier Design," *ICETET 2010*, Goa, India.