Secure Computations in Minimal Model Using Simple ESCT Decomposition. PRELIMINARY VERSION

M. Sampson, D. Voudouris, G. Papakonstantinou
Dept of Electrical and Computer Engineering
Division of Computer Science
Computing Systems Laboratory
National Technical University of Athens
157 80, Zografou Campus, Greece

Abstract

This paper deals with the use of a minimal model for performing secure computations. The communication is based on a protocol which makes use of minimal ESCT (Exclusive-or Sum of Complex Terms) expressions in order to perform a secure computation. The complexity of this protocol is directly proportional to the size of the ESCT expression in use, which is much smaller in comparison to other proposed minimal models (e.g. ESOP). Hence, this paper provides a very usefully application of the ESCT expressions in the field of cryptographic protocols.

I. Introduction

The secure computations in a minimal model problem was initially introduced by Feige, Kilian and Naor in [1]. In particular, the problem is as follows. Alice and Bob are two players who hold n-bit private input strings $a \in \{0,1\}^n$ and $b \in \{0,1\}^n$ respectively, and share a random string. Both want a third player, Carol, to learn the output $f(a,b)$ of a predetermined function $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ without revealing any unnecessary information bout their inputs. Alice and Bob are allowed to send a single message through a private channel and are considered to be computationally unbounded. The following example should further clarify the basic idea behind this model.

Consider the simple case where Alice and Bob hold one-bit input string $a \in \{0,1\}$ and $b \in \{0,1\}$ respectively. They want Carol to compute the exclusive-or function (EXOR) $f(a,b) = a \oplus b$ without revealing any unnecessary information. Both share a random key $k \in \{0,1\}$. At first, Alice sends the one bit message $a \oplus k$ to Carol through a private channel. Bob does the same with the message $b \oplus k$. Carol receives both messages and computes $(a \oplus k) \oplus (b \oplus k) = a \oplus b$ which the desired output. It is obvious that the messages of Alice and Bob remain private through the whole procedure, because they are transmitted through private channels and Carol acquires just the result of f, not the input strings, since k is random.

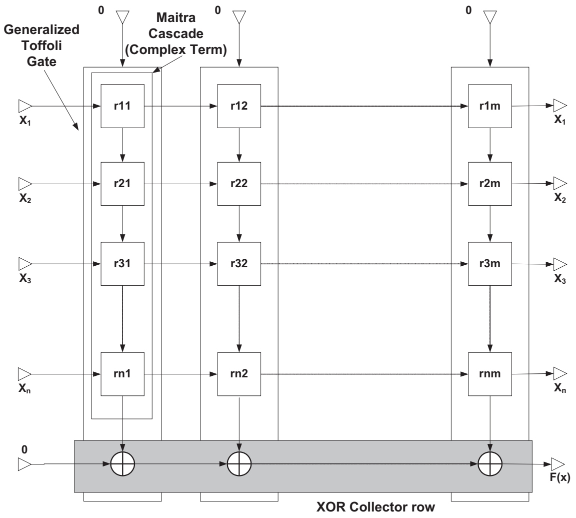

Fig. 1. Reversible wave cascade CA

From the above, we can easily find the communication and randomness complexity of this protocol. If each of Alice and Bob send n_a and n_b bits and the random string is n_k bits long, then we have a $(n_a, n_b; n_k)$-protocol. Accordingly, the previous protocol which securely computes the EXOR functions is a $(1,1;1)$-protocol.

In [1], a protocol for secure computations was presented. For a arbitrary function $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$, the message exchange goes as follows. Alice sends a 2^n-bit message, while Bob an $(n+1)$-bit message to

Carol. Furthermore, a common $2^n + n$ random string is used. In this case, the protocol is $(2^n, n+1; 2^n+n)$-protocol.

The protocol used in this paper has been initially presented in [2]. The problem has been addressed using ESOP (Exclusive-or Sum of Products) expression as a minimal model. It is a $(2t, t{+}1; 3t)$-protocol, where t is the number of product terms in a minimal ESOP expression of the function $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$. That paper proposes a communication protocol based on the fact that any function can be expressed using an ESOP expression. The complexity of the protocol is directly analog to the number of product terms of the minimal ESOP expression. The protocol will be further analyzed in the following sections.

In this paper, a better and more general minimal model is used in order to achieve better complexity in communication. In particular, we examine the "exclusive-or" sum of simple disjoint decomposition expressions, in order to achieve better minimality. This general formalism includes as a special case the ESOP expressions used in [2]. Furthermore, ESCT (Exclusive-or Sum of Complex Terms) expressions are adopted as a special case of the general case because by definition they can be directly mapped to a simple disjoint decomposition. These ESCT expressions also include ESOPs as special case. Moreover, efficient algorithms exist for mapping an arbitrary function to such optimal [3], [4], [5], [6], [7], [8], [9] or near optimal [10], [11], [12], [8], [9], [13] ESCT expressions. The proposed ESCT formalism, improves the one of [2] using ESOPs, by about 40%, as will be shown the following sections.

II. Theoretical Background

In this section we provide some theoretical background for the simple disjoint decomposition as well as the ESCT expressions.

The disjoint decomposition of a Boolean function is a representation of type $f(X) = h(Z, g(Y))$ with Y and Z being sets of variables partitioning the set X. Disjoint decomposition has many applications in computer science and discrete mathematics, including logic synthesis [14], combinatorial optimization problems over graphs and networks [15], reliability theory [16] and game theory [17]. It is very important to have efficient algorithms that find all the decompositions for a given function. For Boolean functions, however, the existing methods either involve the solution of an NP-complete problem or have exponential running time making them inefficient to use.

Let x_i be binary variable literals, y a binary value (constant input) and G_i arbitrary 2-input 1-output boolean functions ($1 \leq i \leq n$). Then $U = G_n(x_n, G_{n-1}(x_{n-1}, G_{n-2}(x_{n-2}, \ldots, G_1(x_1, y))))$ is an n-variable complex term (or Maitra term) that depends on variables $x_1, \ldots, x_n$. Functions G_i will be called the **cell functions** of the term.

The G_i cell function can be any single-output two-input function. It has been proved in [18] that it is sufficient for G_i to be any of the six functions $x+y$ (cell 1), $\overline{x}+y$ (cell 2), $\overline{x}y$ (cell 3), xy (cell 4), $x \oplus y$ (cell 5), y (cell 6) which we will call **cell set** for the rest of the paper.

A product term is a special case of a complex term where the $G_i(x,y)$ function may be of the form: $xy, \bar{x}y, x\bar{y}, \bar{x}\bar{y}, x, y, 0, 1$. If the last four cases are not allowed then the product term is actually a minterm.

An ESCT (Exclusive-or Sum of Complex Terms) expression (some times also called reversible wave cascade or Maitra expression) for a switching function is an exlusive-OR sum of complex terms:

$$Q = \sum_{i=1}^{m} \oplus M_i,$$

where M_i are complex terms and m is their number in the expression. The same variable ordering is used for every M_i. The size, $s(Q)$, of the expression Q is defined as the number of complex terms inside the expression. The corresponding architecture is shown in Figure 1. If we only allow cells of type 3,4 and 6 the ESCT expressions are reduced to ESOP expressions.

It is obvious that using ESCT instead of ESOP expressions can lead to expressions with significantly less number of terms. Generally an ESCT expression has about 40% less terms compared to the ESOP counterpart.

Furthermore, there is significant research activity in the field of ESCT minimization and several efficient algorithms (both exact or heuristic) have been proposed. Some algorithms for finding minimal ESOP or ESCT expressions for an arbitrary completely specified switching function, but with limitations on its number of input variables or the number of terms in its minimal forms, have been presented in the past [3], [4], [5], [6], [7], [8], [9]. Others have been designed in order to detect almost minimal ESOP or ESCT expressions but for more input variables [10], [11], [12], [8], [9], [13].

It is obvious that ESCT expressions is a special case of expressions of "exclusive-or sum" of simple disjoint decomposition expressions. Indeed, $G_n(x_n, G_{n-1}(x_{n-1}, G_{n-2}(x_{n-2}, \ldots, G_1(x_1, y)) \ldots))$ can be written as $G_n(x_n, G_{n-1}(x_{n-1}, G_{n-2}(x_{n-2}, \ldots, G_k(x_k, G')) \ldots))$, where $G' = (x_{k-1}, G_{k-1}(\ldots, G_1(x_1, y)))$ or $G_n(x_n, G_{n-1}(x_{n-1}, \ldots, x_k, G'(x_{k-1}, \ldots, x_1)) \ldots))$.

III. Protocol using an esct expression

In this section, the communication protocol is presented. This protocol is the one proposed in [2] with the difference that it is modified to handle ESCT expressions. For clarity reasons, it will be redescribed.

Suppose Alice and Bob want Carol to securely compute function f such that $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ without any unnecessary information to be revealed. Both hold private input strings $a \in \{0,1\}^n$ and $b \in \{0,1\}^n$. The basic outline of the communication is as follows.

1) Obtain a minimal (or near minimal) ESCT expression for f like the following
$f(a,b) = A_1(a, B_1(b)) \oplus A_2(a, B_2(b)) \oplus \ldots \oplus A_t(a, B_t(b))$
where A_i and $B_i, i \leq i \leq t$ are complex terms such that $A_i : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and $B_i : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.
2) For each complex term $A_i(a, B_i(b))$, Alice and Bob make Carol learn the value $A_i(a, B_i(b)) \oplus K^i$ where $K^i \in \{0,1\}$ is a random key known only to Bob.
3) Carol has obtained t one-bit messages $A_i(a, B_i(b)) \oplus K^i, i \leq i \leq t$ and Bob transmits the one-bit message $K^1 \oplus K^2 \oplus \ldots \oplus K^t$. Now Carol only has to add this message to the previously received messages $\bigoplus_{i=1}^{t} A_i(a, B_i(b)) \oplus K^i$ in order to obtain the value of f.

A. Detailed Protocol

Adapting the analysis from [2] to the current scheme one can obtain the following protocol. Let A and B be functions such that $A : \{0,1\}^n \to \{0,1\}$ and $B : \{0,1\}^n \to \{0,1\}$. Let also $a \in \{0,1\}^n$ and $b \in \{0,1\}^n$ be the input strings held by Alice and Bob respectively. The goal is Carol to obtain the value of $A(a, B(b)) \oplus k$ where k is a random key known only Bob.

In order for the protocol to be further analyzed, some special operations need to be defined adopted from [2]. Given a 2-bit message (x, y) the operations **shift** and **get** are defined as follows.

- $\textbf{shift}^0(x,y) = (x,y)$
- $\textbf{shift}^1(x,y) = (y,x)$
- $\textbf{get}^0(x,y) = x$
- $\textbf{get}^1(x,y) = y$

In other words, $\textbf{shift}^0$ returns the inputs unchanged, $\textbf{shift}^1$ swaps the inputs, $\textbf{get}^0$ returns the first input bit and $\textbf{get}^1$ returns the second one.

Alice and Bob share a 3-bit random string $((K^0, K^1), s)$. The first 2 bits are used for encryption of the message to Carol, while the third is used for shuffling the message. Alice and Bob perform the following.

- $B(b)$ can be either 0 or 1. Taking under consideration both possibilities, Alice creates a two-bit message $(A(a,0), A(a,1)$, encrypting it using the (K^0, K^1) keys. So the message becomes $(A(a,0) \oplus K^0, A(a,1) \oplus K^1$. Furthermore, Alice shuffles the message using the s random bit. Now the message is $\textbf{shift}^s((A(a,0) \oplus K^0, A(a,1) \oplus K^1)$ which is sent to Carol. Depending on the value of s the message can take the following two forms.

$$\begin{cases} (A(a,0) \oplus K^0, A(a,1) \oplus K^1) \; if \text{ s=0} \\ (A(a,1) \oplus K^1, A(a,0) \oplus K^0) \; if \text{ s=1} \end{cases}$$

- On the other hand Bob knows that if $B(b) = s$ then the first bit of the message received by Carol is the correct one. Otherwise the correct bit is the second one. So Bob sends the one-bit value $B(b) \oplus s$ to Carol.
- Carol obtains the one-bit value $\textbf{get}^{B(b)\oplus s}\textbf{shift}^s((A(a,0) \oplus K^0, A(a,1) \oplus K^1)$ which is equal to $A(a, B(b)) \oplus K^{B(b)}$ as can be easily verified by examining every possible combination concerning the value of $B(b)$.

The above protocol which is a $(2,1;3)$-protocol achieves secure computation since only Bob knows the random key $K^{B(b)}$.

B. Generalization of the Protocol

Considering the above analysis, a generalized formulation of the protocol can be easily derived.

Let f be a function such that $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and let
$f(a,b) = A_1(a, B_1(b)) \oplus A_2(a, B_2(b)) \oplus \ldots \oplus A_t(a, B_t(b))$
be an ESCT expression of the the function f. Alice and Bob share a $3t$-bit random string
$(((K_1^0, K_1^1), s_1), ((K_2^0, K_2^1), s_2) \ldots ((K_t^0, K_t^1), s_t)$.

Alice and Bob hold private input strings $a \in \{0,1\}^n$ and $b \in \{0,1\}^n$ respectively. The communication is as follows:

- Alice sends $2t$-bit message to Carol such that
$(\textbf{shift}^{s_1}(A_1(a,0) \oplus K_1^0, A_1(a,1) \oplus K_1^1)$, $\textbf{shift}^{s_2}(A_2(a,0) \oplus K_2^0, A_2(a,1) \oplus K_2^1)$,..., $\textbf{shift}^{s_t}(A_t(a,0) \oplus K_t^0, A_t(a,1) \oplus K_t^1))$
- Bob then sends two distinct messages. The first is a t-bit message
$(B_1(b) \oplus s_1, B_2(b) \oplus s_2, \ldots, B_t(b) \oplus s_t)$,
while the second is the one-bit message
$\bigoplus_{i=1}^{t} K_i^{B_i(b)} = K_1^{B_1(b)} \oplus K_2^{B_2(b)} \ldots K_t^{B_t(b)}$
- Finally Carol Computes the value
$\bigoplus_{i=1}^{t} \textbf{get}^{B_i(b)\oplus s_i} (\textbf{shift}^{s_i} (K_i^0, A_i(a, B_i(b)) \oplus K_i^1)) \oplus \bigoplus_{i=1}^{t} K_i^{B_i(b)}$

It is obvious from the above analysis that the proposed protocol is a $(2t, t+1; 3t)$-protocol.

This protocol holds the same privacy and uniformity properties as the one proposed in [2]. The main difference is that the use of ESCT instead of ESOP expressions for the representation of the function leads to significantly less number of terms that define the complexity of the protocol.

Using already published experimental results [8], [19], [20], [11], [21], [10], [6], [22] we can form the following Table I. We have taken into account the best solutions (so far), for ESOP and ESCT expressions, for functions of the MCNC benchmark library [23]. Hence, we can conclude that using ESCT expressions instead of ESOP as in [2] we have a substantial reduction (39%)in the number of terms in the exclusive-or sum and consequently in the communication cost of the proposed protocol.

TABLE I. Benchmark functions.

Name	ESOP Terms	ESCT Terms
5xp1	31	20
9sym	51	34
com1	9	6
inc	31	15
f51m	31	19
misex1	12	11
rd53	14	7
rd73	35	19
rd84	57	30
t481	13	10
Total	**280**	**171**
Average Terms	**28**	**17.1**
Reduction	**39%**	

IV. Conclusions and future work

In this paper, an enhanced model for the minimization of the communication costs for a secure computation protocol presented in [2] is presented. The new model results to almost 40% less communication cost. Future work may deal with the development of more fast and efficient algorithm for ESCT expression minimization as well as finding more general "exclusive-or" sum of simple disjoint decomposition than the ones of ESCTs.

Acknowledgment

This work has been funded by the project PENED 2003. This project is part of the OPERATIONAL PROGRAMME "COMPETITIVENESS" and is co-funded by the European Social Fund (80%) and National Resources (20%).

References

[1] U. Feige, J. Kilian, and M. Naor, "A minimal model for secure computation," in *Proceedings of the 26th ACM Symposium on Theory of Computing (STOC 94),pp. 554563*. ACM, 1994.

[2] T. Mizuki, T. Otagiri, and H. Sone, "Secure computations in a minimal model using multiple-valued esop expressions," in *Theory and Applications of Models of Computation, Third International Conference, TAMC 2006, Beijing, China, May 15-20, 2006*. SpringerLink, 2006.

[3] G. Papakonstantinou, "Synthesis of cutpoint cellular arrays with exclusive-or collector row," in *Electronic Letters 13(1977)*, 1977.

[4] D. Voudouris, S. Stergiou, and G. Papakonstantinou, "Minimization of reversible wave cascades," in *IEICE Trans. on Fund., Vol E88-A, No. 4, pp. 1015-1023, 2005/04*. IEICE, 2005.

[5] D. Voudouris and G. Papakonstantinou, "Maitra cascade minimization," in *6th IWSBP, 2005, Freiberg (Sachsen), Germany.*, 2005.

[6] D. Voudouris, M. Sampson, and G. Papakonstantinou, "Exact esct minimization for functions of up to six input variables," in *Elsevier Integr. VLSI J. 41, 1 (Jan. 2008), 87-105*. Elsevier, 2008.

[7] T. Hirayama and T. S. Y. Nishitani, "A faster algorithm of minimizing and-exor expressions," in *IEICE Trans. on Fund., Vol E85-A, No. 12, pp. 2708-2714, 2002/12*. IEICE, 2002.

[8] S. Stergiou, D. Voudouris, and G. Papakonstantinou, "Multiple-valued exclusive-or sum-of-products minimization algorithms," in *IEICE Trans. on Fundamentals. vol. E87-A, NO. 5, May 2004*. IEICE, 2004.

[9] A. Gaidukov, "Algorithm to derive minimum esop for 6-variable function," in *5th IWSBP, September 2002*, 2002.

[10] A. Mishchenko and M. Perkowski, "Logic synthesis of reversible wave cascades," in *International Workshop on Logic And Synthesis 2002, New Orleans, Louisiana, June 4-7*. International Workshop on Logic And Synthesis 2002, 2002.

[11] D. Voudouris, M. Kalathas, and G. Papakonstantinou, "Decomposition of multi-output boolean functions," in *HERCMA 2005, Athens, Hellas*. HERCMA, 2005.

[12] G. Lee, "Logic synthesis for celullar architecture fpga using bdd," in *ASP-DAC 97, pp 253-258 Jan 1997*, 1997.

[13] A. Mishchenko and M. Perkowski, "Fast heuristic minimization of exclusive-sums-of-products," in *5th International Reed-Muller Workshop, Starkville, Mississippi, August, 2001*, 2001.

[14] S. Hassoun and T. Sasao, *Logic Syrithesis arid Verification*, 1st ed. Kluwer Academic Publishers, 101 Philip Drive, Norwell, MA 02061, USA: Kluwer Academic Publishers, 2002.

[15] R. H. Mohring and E. J. Radermacher, "Substitution decomposition of discrete structures and connections to combinatorial optimization," in *Ann. Discrete Math, vol. 19. pp. 251-264*. Elsevier, 1984.

[16] W. Bimbdum and J. D. Esary, "Modules of coherent binary systems," in *SIAM Journal of Applied Math., vol. 13, pp. 444-451*. SIAM, 1965.

[17] L. S. Shapley, "Solutions of compound simple games," in *Advances in Game Theory, no. 52 in Ann. of Math. Study, pp. 267-280*. Princeton University Press, 1964.

[18] R. C. Minnick, "Cutpoint cellular logic," in *IEEE Trans. Electron. Comput., vol. EC-13, Dec, 1964, pp. 685-698.*, 1964.

[19] D. Voudouris, S. Stergiou, and G. Papakonstantinou, "Minimization of reversible wave cascades," in *IEICE Trans. on Fundamentals, Vol E88-A, No. 4, pp. 1015-1023, 2005/04*. IEICE, 2005.

[20] D. Voudouris and G. Papakonstantinou, "Maitra cascade minimization," in *6th IWSBP, 2004, Freiberg (Sachsen), Germany*. IWSBP, 2004.

[21] D. Voudouris, M. Sampson, and G. Papakonstantinou, "Variable reordering for reversible wave cascades," in *HERCMA 2007, Athens, Hellas*. HERCMA, 2007.

[22] ——, "Finding minimal esct expressions for boolean functions with weight of up to 7," in *International Conference on Computer Design, CDES08, Las Vegas, 2008*. CDES08, 2008.

[23] S. Yang, "Logic synthesis and optimization benchmarks user guide version 3.0," in *Tech. rep., Microelectronics Center of North Carolina, Jan. 1991.*, 1991.