SAX: A Privacy Preserving General Purpose Method applied to Detection of Intrusions
François Trouset, Pascal Poncelet, Florent Masseglia

To cite this version:

HAL Id: lirmm-00430646
https://hal-lirmm.ccsd.cnrs.fr/lirmm-00430646
Submitted on 9 Nov 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
SAX: A Privacy Preserving General Purpose Method applied to Detection of Intrusions

François Troussel  
LGII2P - Ecole des Mines d’Alès, Parc Scientifique G. Besse, 30035 Nîmes, France  
francois.troussel@ema.fr

Pascal Poncelet  
LIRMM UMR CNRS 5506, 161 Rue Ada, 34392 Montpellier Cedex 5, France  
poncelet@lirmm.fr

Florent Masseglia  
INRIA Sophia Antipolis, route des Lucioles - BP 93, 06902 Sophia Antipolis, France  
florent.masseglia@inria.fr

ABSTRACT
To overcome the problem of attacks on networks, new Intrusion Detection System (IDS) approaches have been proposed in recent years. They consist in identifying signatures of known attacks to compare them to each request and determine whether it is an attack or not. However, these methods are set to default when the attack is unknown. However, it is frequent that an attack has already been detected by another organization and it would be useful to be able to benefit from this knowledge to enrich the database of signatures. Unfortunately, this information is not so easy to obtain. In fact, organizations do not necessarily want to spread the information that they have already faced this type of attack. In this paper, we propose a new approach to intrusion detection in a collaborative environment but by preserving the privacy of the collaborative organizations. Our approach works for any signature even if it needs a complex program to be detected and ensures that private data and programs will not be disclosed. Via our approach, any program from the various collaborative sites can be executed without disclosing any information on attacks between distributed IDS from one organization approach, called Secure Algorithm eXecution (SAX) which allows to compute any algorithm while preserving privacy of data and also of the program code which is computed.

Categories and Subject Descriptors
D.4.6 [Security and Protection]: Algorithms, Privacy

General Terms
Algorithms, Security

Keywords
Intrusion Detection, Attacks, Collaborative Organizations, Privacy

1. INTRODUCTION
The fast growing computational Grid environments has increased risk of attack and intrusion. Thus misuse detection has become a real concern for companies and organizations. Whereas earlier attacks focused on Web servers (often misconfigured or poorly maintained), the most recent ones take advantage of Security service and Web applications weaknesses which become more vulnerable [4, 2]. To overcome this problem, new approaches called Intrusion Detection Systems (IDS) have been developed. Installed on networks, they aim to analyze traffic requests and detect malicious behavior (e.g., Prelude-IDS, Snort). They can be classified into two broad categories (e.g., [8, 9]): the Anomaly Detection Systems which attempt to detect attacks and the Abuse Detection Systems which detects unknown comportment so called abuse from a specification of allowed ones. Recently, approaches called Collaborative Intrusion Detection Systems (CIDS) (e.g., [1, 12, 5, 7, 11]) have been proposed. In comparison with isolated IDS, CIDS significantly improve time and efficiency of misuse detections by sharing information on attacks between distributed IDS from one or more organizations. The main principle of these approaches is to exchange information using peer-to-peer links. However, the exchanged information are mostly limited to IP addresses of requests (e.g., [1, 5, 7]) and consider that data can be freely exchanged among the peers. The last constraint is very strong: companies, for reasons of confidentiality, do not want to spread out that they were attacked and therefore are unwilling to give any information on it.

In this article, we propose a secure collaborative detection approach, called SAX (Secure Algorithm eXecution), which ensures that private data and programs will not be disclosed. Via our approach, any program from the various collaborative sites can be executed without disclosing any information from the local IDS to the outside. Collaborative Sites are free to work with signatures of attacks or non-attacks and may give information on the type of intrusion detected. Thus, when new request is checked, the response will be one of: it is an attack (with its type if available), it is a non-attack, or unknown (if none of the IDS data leads to a positive or negative conclusion). To our knowledge, very little studies are concerned with this topic of security in such collaborative environment. The only works [10, 7] consider both collaborative and security aspects. In its context, security mainly concerns information on IP addresses and ports. It uses Bloom’s filters to manage data exchanges. Our problem is different in that, we want to exchange data, i.e., more complex than IP addresses and ports. In fact, we want to be able to exchange and execute any algorithm of anomaly detection on the full request.

In previous studies, we focused on those anomalies whose...
signature detection may be expressed as a regular expressions. But there is still a lot of cases that cannot be expressed like that and which need specific programs to be detected. Instead of handling them one by one, we decided to study a general-purpose method able to execute any program while preserving privacy of data and also of the program code (once it has been translated into the adequate formalism). This method is described in this article.

The article is organized as follows. In section 2, we present the problem. An overview of our approach is given in section 3 and 4. The various algorithms are described in section 5. Finally section 6 concludes and presents various perspectives.

2. PROBLEM STATEMENT

$DB$ is a database such as $DB = DB_1 \cup DB_2 ... \cup DB_D$. Each database $DB_i$ is equivalent to a tuple $<id, S_{Alg}>$ where $id$ is the identifier of the database and $S_{Alg}$ is a set of anomaly detection programs expressed as a finite state automaton and initial program data. The details are described in section 3. The other part of input data of the program is the request string $R$ owned by the client site $S$. Each program will provide two kinds of value: a three states flag ($\text{True}$/\text{False}$/\text{Unknown}$) specifying whether the request is an attack or not or has not been identified at all and an integer (the type of the attack) when the request is effectively identified as an attack ($\text{True}$ state).

Definition 1. Given a database $DB = DB_1 \cup DB_2 ... \cup DB_D$ and a request string $R$, the secure approach in such a collaborative environment consists in finding a program $Alg$ from $DB$ such that execution of $Alg$ upon $R$ gives a False or True result (identify an attack or a non-attack) while ensuring that the client site does not provide the request string $R$ to anyone and that none of the databases $DB_i$ provided any information from its content to anyone (programs and data).

3. THE SAX APPROACH

This section will provide an overview of the secure architecture SAX (Secure Algorithm eXecution). It is designed to answer the problem of privacy preserving in a collaborative environment. Inspired by the work of [6], this architecture offers the advantage of achieving the various operations while ensuring that neither party may have access to private data contained in the initial databases. In addition to the client site $S$ which is responsible to provide the request to be tested, the architecture requires four non-collaborative and semi honest sites [3]: they follow the protocol correctly, but are free to use the information they have collected during the execution of the protocol. These independent sites collect, store and evaluate information in a secure way. The different functions provided by these sites are:

- **The Control Site CTRL**: $CTRL$ is used to rule the various operations needed to execute the program. To do this, it interacts with the two non colluding sites $NC_1$ and $NC_2$.
- **Non Colluding Sites $NC_1$ and $NC_2$**: These two symmetric sites collect garbled data from all databases as well as the garbled request to be tested from $S$.

Under the control of $CTRL$ and by interaction with $PS$, they perform several secure operations in order to insure that none of them will be able to infer any of the intermediate results or the final result which is returned to site $S$.

- **The Processing Site PS**: This site is used both by $NC_1$ and $NC_2$ to process, in a secure way, the various needed operations. Like $NC_1$ and $NC_2$, $PS$ also cannot deduce any pertinent value of intermediate or final result from the data it processes.

Remark: The data kept by $NC_1$ ($\hat{a}$) and $NC_2$ ($\bar{a}$) are random data such that $\hat{a} \oplus \bar{a} = V$ where $V$ is the real value. But as $NC_1$ and $NC_2$ are non-colluding, the value of $V$ will never be known by any of the sites. (Details will be explained in the following sections).

3.1 Encoding of the program

To perform a secure computation of client site $S$ data by a program coming from an external site $DB_i$ (which may be anonymized), we consider the program as a deterministic automaton $<\text{State}, \text{Trans}, \text{Init}, \text{Final}>$ where $\text{State}$ is the set of states of the automaton, $\text{Init}$ is the initial state, $\text{Final}$ is the set of final states and $\text{Trans}$ is the set of transitions. Each transition is a quadruplet $(\text{State}_{initial}, \text{Action}, \text{State}_{final}, \text{Final}_{final})$ meaning that if the automaton is in state $\text{State}_{initial}$ and that $\text{Action}$ is performed and returns a boolean value then the automaton’s current state changes to $\text{State}_{final}$ if the boolean value is false or to $\text{Final}_{final}$ if it is true. The automaton starts with state $\text{Init}$ and ends when reaching any of the final states from $\text{Final}$.

Remark: To ensure that computation is secure, none of the performed action shall return any data to the site $DB_i$ which gave the program to be computed. This means that only the client site $S$ gets results.

This encoding implies that all of the states (but final ones) are connected to two other states in the graph of the automaton (in fact $\text{State}_{final}$ and $\text{State}_{final}$). These links are designated by $\oplus$ leading to $\text{State}_{final}$ and $\ominus$ leading to $\text{State}_{final}$.

Each action is in fact a list of 3-uptets $(\text{OpNum}, \text{Aff}_1, \text{Aff}_2)$ where $\text{OpNum}$ is the number of the operation to be processed, and $\text{Aff}_1$ and $\text{Aff}_2$ are two random sequences of bits of of same length. Each 3-uptet of the list performs the same action by using different operators which will be effectively executed by $NC_1$ and $NC_2$. There is a list to avoid $NC_1$ and $NC_2$ from deducing any link between the value of $\text{OpNum}$ and a “corresponding state” in $CTRL$.

The automaton is managed by $CTRL$ while $NC_1$, $NC_2$ maintain the memory and performs the operations on the values through $PS$. If $CTRL$ maintains the list of operation numbers to be performed for each node, the protocol to be performed when executing this operation is aimed by $NC_1$ and $NC_2$ and data used as input and output of this operation will only be kept (garbled) in $NC_1$ and $NC_2$. Thus $CTRL$ will know nothing about the real operation that is performed and no more on the values used and produced by the operation. $NC_1$ and $NC_2$ also owns a list of Registers which contains address in the memory. These register will be used to perform indirect and based memory access. Instead of the data kept in their memory which are garbled, the real values of registers are known by both $NC_1$ and $NC_2$. 


After Performing the Action associated to a state, CTRL receives two bits (one from NC1 and one from NC2). If these two bits are identical then CTRL follows the link ⊕ otherwise it follows the link ⊙.

For each operation OpNum of CTRL, NC1 and NC2 have a corresponding 5-uptlet (Protos, NCA, Arg1, Arg2, Res, Incr) where Protos is a list of binary operations (p elements), NCA is a random number (1+m+n+p+q bits), Arg1 is the list of values from the memory that may potentially be used as first argument of operation (n elements), Arg2 is similar to Arg1 but for the second argument (m elements), Res is the list of potential storages for the result in memory or a a register number, Incr is the list of potential storages for the result in memory or a a register number, and a register number Reg and an Offset to perform indirect or based memory addressing.

Remark: there is several ways to implement an action that does only register increments, but it also exists a non operation prototype named NOP designed for this purpose.

Remark: If \( Aff1, Aff2 \) are such that \( Aff = Aff1 \oplus Aff2 \oplus NCA \oplus NCA \) where NCA is the part of NCA owned by NC1 and NCA is the part owned by NC2. \( Aff \) is a list of boolean flags (true/false) that are used to specify which affection shall be effectively done (see section 3.3). We will use the notations \( \hat{Aff} = Aff1 \oplus NCA \) owned by NC1 and \( \hat{Aff} = Aff2 \oplus NCA \) owned by NC2.

In fact \( Aff1 = \hat{Aff} \oplus RND1 \), \( Aff2 = \hat{Aff} \oplus RND2 \), \( NCA = RND1 \oplus RND3 \) is owned by NC1 and \( NCA = RND2 \oplus RND3 \) is owned by NC2 where \( RND1 \), \( RND2 \) and \( RND3 \) are generated by DB, and \( Aff = \hat{Aff} \oplus \hat{Aff} \).

3.2 Initialization of the processus and global processing

The exchange of data between the different sites is done by using the secure method \( SEND^S(\vec{v} | \vec{v}') \) which sends the vector of bits \( V = \vec{v} \oplus \vec{v}' \) to NC1 and NC2. It is defined in order to send \( \vec{v} \) to NC1 and \( \vec{v}' \) to NC2 (or vice versa). A random vector \( R \) is used to garble transmitted data such that \( \vec{v} = R \) and \( \vec{v}' = V \oplus R \) or vice versa. This method is used in particular to send the data from the databases DB, and to send the request from site S. Thus, the process described in figure 1 starts in the following way:

* First, the site S sends its request to NC1 and NC2 using the SEND S method (See arrow number 1 in figure 1).

More precisely, the request \( R \) taken in its boolean form: a vector of bits.

* A random vector of bits \( A \) is then generated with the same size as the request \( R \) to compute the new vector \( Z = A \oplus R \). \( Z \) is sent to NC1 and NC2 (or vice versa).

* Each database DB, sends the transition matrix of its automaton to CTRL (See arrows number 2) The size of the needed memory, the number of needed adress registers and their initial value are naturally sent to NC1 and NC2 as their real values are known by both sites. The initial value of the memory is sent to NC1 and NC2 by using SEND S. DB, also sends the list of actions to be performed (5-uplets) to NC1 and NC2.

From this point, the computation of the request is done under the control of CTRL. It will ask NC1 and NC2 execute action (See arrow number 3).

* The action is effectively performed securely by NC1 and NC2 through PS (See arrow number 4 and 5).

* The result of the action is a boolean divided in two parts, one is owned by NC1 and the other by NC2 such that none are able to infer its real value. Both parts are then securely returned to CTRL (see arrows 5 and 6).

* While NC1 and NC2 are updating the value of the different registers as needed by the action, CTRL compares the two values he received and updates the current state of the automate in consequence.

* The process is repeated under control of CTRL unless the automaton moves into a final state.

* When entering a Final state, the result value previously stored by the program by executing the secure action AFFEC T S is aggregated or sent to the client site S by NC1 and NC2 (See arrow number 7) under the control of CTRL.
This choice depends of the configuration of the anonymity behaviour (See section 4).

3.3 Execution of action

When CTRL enter a non final state, he starts by randomly selecting one of the 3-uplets (OpNum, A\textsubscript{f1}, A\textsubscript{f2}) from the list associated to this state. It then generates a random number R\textsubscript{OP} of same length than A\textsubscript{f1} and A\textsubscript{f2}. Then CTRL sends A\textsubscript{q} = A\textsubscript{f1} \oplus R\textsubscript{OP} to NC\textsubscript{1} and A\textsubscript{q} = A\textsubscript{f2} \oplus R\textsubscript{OP} to NC\textsubscript{2}.

NC\textsubscript{1} (respectively NC\textsubscript{2}) computes the vectors of bits \( \vec{a} = \vec{a}_\oplus \oplus \vec{a}_\text{NC} \) (respectively \( \vec{a} = \vec{a}_\oplus \oplus \vec{a}_\text{NC} \)) and extract \( \vec{b}_n = \vec{a}[0] \), \( \vec{b}_r = \vec{a}[n + 1 \ldots n + m] \), and \( \vec{b}_q = \vec{a}[n + m + 1 \ldots n + m + p + q] \) (and respectively NC\textsubscript{2} extract then \( \vec{a}_n \) parts from \( \vec{a} \)). We will use the notation \( \vec{a}_n \) for which is the \( j \)th bit of the vector of bits \( \vec{b}_n \) and similarly for the \( \vec{b}_r \) form.

Now let \( \vec{v}_1 \) and \( \vec{v}_2 \) (respectively \( \vec{v}_3 \) and \( \vec{v}_4 \)) be two distinct vectors of bits of length greater or equal to the lengths on any of the values in \( \vec{a}_\text{NC} \) for \( \vec{v}_1 \) and \( \vec{a}_\text{NC} \) for \( \vec{v}_4 \) used to store the actual arguments of operations. We shall also use \( \vec{a}_n \) and \( \vec{a}_r \) (respectively \( \vec{a}_n \) and \( \vec{a}_r \)) to store the computed results of the operation.

Now NC\textsubscript{1} (respectively NC\textsubscript{2}) computes the following secure instructions (See notations in section 5):

\begin{equation*}
\text{for each} \ i \in [1..n] \ \text{do} \ \text{AFFECT}^i(\vec{v}_1, \vec{b}_i, \vec{a}_\text{NC}; \vec{v}_1, \vec{b}_i, \vec{a}_\text{NC});
\end{equation*}

\begin{equation*}
(\vec{a}[i]) \leftarrow (\vec{b}_n)[i];
\end{equation*}

\begin{equation*}
\text{for each} \ i \in [1..n] \ \text{do} \ \text{PROTOCOL}(\vec{v}_1, \vec{v}_2) ;
\end{equation*}

\begin{equation*}
\text{AFFECT}^i(\vec{b}_n, \vec{a}_n, \vec{v}_2) ;
\end{equation*}

Remark: There exists more complex operators on indexes but incrementation is sufficient for our purpose as we shall care that operations on indexes are not private: NC\textsubscript{1} and NC\textsubscript{2} knows their real value. We shall also notice that operations on indexes shall never combine data stored in the memory otherwise NC\textsubscript{1} and NC\textsubscript{2} will gain access to the real values of data stored in their memory.

3.4 Proof of privacy

\begin{property}
The implementation allows to compute securely any program while encoded in the correct form.
\end{property}

\begin{proof}
The secure operations computed may be any boolean operation. We have encoded the operation and \( \land \) \( \land \) and not \( \neg \) \( \neg \) that form a generator system of the booleans. That means that any other boolean operation may be encoded securely. If in theory, we consider the memory maintained by NC\textsubscript{1} and NC\textsubscript{2} to be infinite it is easy to encode any Turing Machine using CTRL, NC\textsubscript{1}, NC\textsubscript{2} and PS. To do that we only need one Register, and to decompose each transaction of the Turing Machine in three single transactions of our automaton, the first consists in testing the value at the current (Register) position by using COMPARE\textsuperscript{S}, the second stores new data at the current position using AFFECT\textsuperscript{S} and the third increments the Register with value 1 or -1 using operator NOP\textsuperscript{S}.

\begin{property}
This secure execution of a program prohibits DB to know any of the client’s data.
\end{property}

\begin{proof}
The proof is evident as no data is returned to DB. On the client side, it may not be true but it depends on the program which is computed by the system which is of the responsibility of DB. Thus if the program deliver data comming from DB to the client, that means that DB (who writes the program) has decided that it shall be so and thus it is a normal result approved by DB.

\begin{property}
CTRL does not know any of the incoming and outgoing data and does not even know what processing has been performed on the data.
\end{property}

\begin{proof}
CTRL does not have access to any of the data managed by NC\textsubscript{1} and NC\textsubscript{2}. It also has only access to operation numbers and does not know to which protocols it corresponds. Further more the values of A\textsubscript{f1} and A\textsubscript{f2} are pure random values from which it cannot infer anything, even the length of those may be greater that the one really needed by NC\textsubscript{1} or NC\textsubscript{2}. The only thing that CTRL may infer is the sequence of states encoutered during a run.

\begin{property}
None of NC\textsubscript{1}, NC\textsubscript{2} or PS can infer what processing has been performed.
\end{property}

\begin{proof}
At each step, when executing an action, NC\textsubscript{1} and NC\textsubscript{2} perform several operation using various values from the memory and it does not know which of the values will be used as inputs of the operator, nor which result is stored in the memory no more than where it is effectively stored. This is due to the usage of the secure conditional assignment operator AFFECT\textsuperscript{S}.

Secondly when NC\textsubscript{1} is performing any boolean operation it does not know if NC\textsubscript{1} negates or not any of the value or the result (because to implement the negation, only one from NC\textsubscript{1} and NC\textsubscript{2} has to negate the value which is a property of \( \oplus \) : if \( A = X \oplus Y \) then \( \neg A = \neg X \oplus Y = X \oplus \neg Y \).

\begin{property}
None of NC\textsubscript{1}, NC\textsubscript{2} or PS can deduce any real value of the incoming or produced data.
\end{property}

\begin{proof}
NC\textsubscript{1} and NC\textsubscript{2} own only garbled data at the beginning of the process. During the processing the usage of secure operators insures that they get only garbled data from which they cannot infer any information on the real values. In the case of PS it does not owns any data and gets pure random data from NC\textsubscript{1} and NC\textsubscript{2} and returns random values. (See proof of operators for more details).

Remark: The values of m, n, p, q and r are choosen by DB\textsubscript{2} when producing the automata. The cost in time is linearly increasing with the value of \( m + n + p + q + r \). At the same time, the “randomness” of the resulting program increases by \( m \times n \times p \times q \times r \). When encoding program DB\textsubscript{3} must choose values such that time cost is bearable and garbling of the algorithm is the highest one.

4. ANONYMISATION

There is two main ways to do anonymization: in buffering inputs programs issued by databases DB\textsubscript{1} and execute them randomy or in buffering results before sending them
randomly to the client. The first one essentially introduce costs in term of space (we need to store the automata in CTRL and associated data in NC1 and NC2). The second one essentially introduce time costs (we may process other DBs’s programs while the desired result has already been obtained. And we will do that until the client gets this result). A third way is to mix the two approaches and adapt parameters (size of both buffers) to adjust anonymization process according to the needs and bearable costs.

As we are dealing with anomaly detection, the result is not so complex: an algorithm may detect an attack and then give the type of the detected attack, or identify a non attack request or may not be able to identify the request. In fact only the first positive or negative result has to be kept. In this section, we present the various algorithms used in SAX approach. In order to simplify writing, we consider the following way:

\[ \text{AFFECT}^S (\var{x} | \var{y}, \var{z}, \var{v}| \var{w}) \]

where \( \var{x}, \var{y}, \var{z}, \var{v}, \var{w} \) are random values whatever the affectation has been effective or not. That means that no one can predict the value stored in \( \var{V a}r \) unless it already know the value of \( \var{Cond} \) (but NC1 and NC2 only knows random values).

The secure operator \( \text{AFFECT}^S \) shall be used in the following way:

\[ \text{AFFECT}^S (\var{x}, \var{y}| \var{V a}lue, \var{Cond}, \var{Value}| \var{w}, \var{V a}lue) \]

where \( \var{x}, \var{y} \) are owned by NC1 and \( \var{w} \) is owned by NC2.

The implementation of \( \text{AFFECT}^S \) require the secure operators \( \text{COMPARE}^S \) and \( \text{AFFECT}^S \). At the origin, the accumulator is set securely with the value “unknown”. Thus, when anonymization is done by buffering results, we only get time costs, and the parameter is the number of aggregations to be performed before sending an aggregated result to the client.

5. THE SECURE ALGORITHMS

In this section, we present the various algorithms used in SAX approach. In order to simplify writing, we consider the following notations:

Let \( (\var{x} | \var{y}, \var{z}) \) be a tripartite computation of any function \( h^S \) between NC1, NC2 and PS where NC1 owns some of the entries \( \var{x}, \var{y}, \var{z} \) and gets part of the result \( \var{x} \) and similarly NC2 owns some of the entries \( \var{y}, \var{z} \) and gets part of the result \( \var{z} \).

The final result is obtained by applying the binary operator XOR \( (\oplus) \) between \( \var{x} \) and \( \var{z} \). However, this does not mean that NC1 sends exactly \( \var{y}, \var{z} \) to PS an receives the result \( \var{z} \) from PS. In fact, NC1 garbles its inputs \( \var{y}, \var{z} \) by adding random noise and gets \( \var{y}^{\oplus}, \var{z}^{\oplus} \) which are securely sent to PS. Similarly, NC2 sends its garbled inputs to PS.

At the end of the process, both sites receives a part of garbled result from PS (respectively \( \var{x}^{\oplus} \) and \( \var{z}^{\oplus} \)). This intermediate result may now be used as input of further computation.

We will also use the following simplifications:

1. \( g^S (\var{x}, \var{y}) \Leftrightarrow g^S (\var{x} | \var{y}) \)
2. \( h^S () \) is a 2 argument function then \( h^S (\var{x}_1, \cdots, \var{x}_n | \var{y}_1, \cdots, \var{y}_n) \) will correspond to \( h^S (h^S (\cdots | \var{x}_3 | \var{y}_3); \var{x}_3 | \var{y}_3); \cdots; \var{x}_n | \var{y}_n) \)

5.1 The algorithm \( \text{AFFECT}^S \)

The operator \( \text{AFFECT}^S \) implements a conditional affection of value to a variable. The non secure equivalent operator \( \text{AFFECT} \) could be sepçified as follows:

\[
\text{AFFECT} (\var{V a}r, \var{Cond}, \var{Value}) \Leftrightarrow \text{if} \ (\var{cond}) \ \text{then} \var{V a}r \rightarrow \var{Value}; \\
\text{else} \var{V a}r \rightarrow \var{V a}r;
\]

\[
\text{fi}
\]

The secure implementation of this operation (which is shown in algorithm 1 ensure that no one can infer whether the affection has effectively been done or not. That means that no one can predict the value stored in \( \var{V a}r \) unless it already know the value of \( \var{Cond} \) (but NC1 and NC2 only knows random values). The secure operator \( \text{AFFECT}^S \) shall be used in the following way:

\[ \text{AFFECT}^S (\var{V a}r, \var{Cond}, \var{V a}lue| \var{w}, \var{V a}lue) \]

The implementation of \( \text{AFFECT}^S \) require the secure operators \( \text{COMPARE}^S \) and \( \text{AFFECT}^S \), which implements respectively a secure computation of bitwise operators OR and AND on vectors of bits of same length \( (\var{S}_1 \text{ and } \var{S}_2) \) and returns the sequence \( \var{V a}lue \). At the end of the process of \( \text{AFFECT}^S \), the new value computed will be stored in the original variables \( \var{v}_a \) for NC1 and \( \var{v}_a \) for NC2.

Algorithm 1: Algorithm \( \text{AFFECT}^S \)

**Data:** \( \var{V a}r = \var{v}_a \oplus \var{v}_{\text{ar}} \) of length \( n \) is the value of the variable.

// Value = \( \var{v}_a \oplus \var{v}_{\text{ar}} \) is the value to be conditionally affected (of length \( n \)).

// \( \var{Cond} = \var{c}_{\text{ond}} \oplus \var{v}_{\text{ar}} \) is the 1 bit condition true if the affection shall be done and false otherwise.

1. \( \forall k \in 1..n \), NC1 and NC2 and PS compute
\[
\var{v}_{\text{ar}} | \var{w}_k = h^S (\var{v}_{\text{ar}} | \var{w}_k) \]

\[ \var{V a}lue = \var{v}_a \oplus \var{v}_{\text{ar}} \]

\[ \var{w}_{\text{ar}} = \var{w} \]

**Property 6.** \( \text{AFFECT}^S \) prohibits NC1 and NC2 to access the value stored in the variable \( \var{V a}r \). They even do not know if the value stored in \( \var{V a}r \) has changed or not.

**Proof:** All the values stored in NC1 and NC2 are randomized. This count also for \( \var{V a}r, \var{Cond} \) and \( \var{V a}lue \). That means that none knows the real value stored in \( \var{V a}r \) and \( \var{V a}lue \). To know whether \( \var{V a}lue \) is affected to \( \var{V a}r \) or not they shall know the real value of \( \var{Cond} \) but as it is also randomized they cannot infer whether the value of \( \var{V a}r \) has been changed or not. In any case, the new value of \( \var{v}_a \) and \( \var{v}_{\text{ar}} \) are new random values whatever the affection has been effective or not.

**Complexity:** The methods \( \text{COMPARE}^S \) and \( \text{AFFECT}^S \) require 34n binary operations, generate 6n aleatory bits, send 12n bits and receive 10n bits (including parameters). PS performs 12n binary operations, generates 3n + 1 aleatory bits, receives 12n bits (6n from NC1 and NC2 each) and sends 6n bits (3n to NC1 and NC2 each). Obviously this has to be compared with the length of inputs (n bits).
Algorithm 2: The Algorithm $\land^S$

**Data:** $(\hat{x}, \hat{y}|\tilde{x}, \tilde{y})$ vector of bit/s are such that $\hat{x}$ and $\hat{y}$ are in $NC_1$, and $\tilde{x}$ and $\tilde{y}$ are in $NC_2$

**Result:** $(A^R \oplus B^R) = \{\hat{x} \oplus \hat{y}\}$ such that

1. $NC_1$ and $NC_2$ mutually generate and exchange four random vector of bit/s $R_A$, $R'_A$, $R_B$, and $R'_B$ such that: $\hat{x} = \hat{x} \oplus R_A$, $\hat{y} = \hat{y} \oplus R'_A$,
   \[\hat{x}' = \hat{x} \oplus R_B\] and $\hat{y}' = \hat{y} \oplus R'_B$.

2. $NC_1$ sends $\hat{x}'$ and $\hat{y}'$ to $PS$.

3. $NC_2$ sends $\tilde{x}'$ and $\tilde{y}'$ to $PS$.

4. $PS$ computes $\hat{c} = \hat{x}' \land \tilde{y}'$ and $\hat{c} = \hat{y}' \land \tilde{x}'$ and generates a random vector of bit/s $R_{PS}$.

5. $PS$ sends $A'_{PS} = \hat{c} \oplus R_{PS}$ to $NC_1$ and $B'_{PS} = \hat{c} \oplus R_{PS}$ to $NC_2$.

6. $NC_1$ computes $A^R = A'_{PS} \oplus (\hat{x} \land R'_B) \oplus (\hat{y} \land R_B) \oplus (\tilde{x} \land \tilde{y}) \oplus (R_B \land R'_A) \oplus (\tilde{x} \land \tilde{y}) \oplus (\hat{y} \land R_A) \oplus (\tilde{x} \land \tilde{y}) \oplus \hat{x} \land \tilde{y} \oplus (R_A \land R'_B)$.

7. $NC_2$ computes $B^R = B'_{PS} \oplus (\tilde{x} \land R'_A) \oplus (\tilde{y} \land R_A) \oplus (\tilde{y} \land \tilde{x}) \oplus (R_A \land R'_B) \oplus \hat{x} \land \tilde{y} \oplus (\tilde{x} \land \tilde{y}) \oplus (\tilde{x} \land \tilde{y}) \oplus (\hat{x} \land \tilde{x}) \oplus (\hat{y} \land \tilde{y}) \oplus (R_A \land R'_B)$.

$\oplus \tilde{x} \land \tilde{y}$. Which is a re-written form of $(\hat{x} \oplus \hat{y}) \land (\tilde{x} \oplus \tilde{y})$. However, this operation is never performed by the non-collaborative sites and the final result is kept shared between $NC_1$ and $NC_2$.

The $\lor^S$ protocol is identical to the $\land^S$ protocol except for the last two steps (steps 6 and 7) performed by $NC_1$ and $NC_2$. Thus we get the final result:

$A^R \oplus B^R = \hat{x} \oplus \hat{y} \oplus (\tilde{x} \land \tilde{y}) \oplus (\tilde{x} \land \tilde{y}) \oplus (\tilde{x} \land \tilde{y}) \oplus (\hat{x} \land \hat{y}) \oplus (\hat{x} \land \hat{y}) \oplus \hat{x} \land \tilde{y} \oplus \tilde{x} \land \tilde{y} \oplus (\hat{x} \land \tilde{y}) \oplus (\hat{x} \land \tilde{y})$.

This reduces to the desired result: $A^R \oplus B^R = \hat{x} \oplus \hat{y} \oplus (\tilde{x} \land \tilde{y}) \oplus (\tilde{x} \land \tilde{y}) \oplus (\tilde{x} \land \tilde{y}) \oplus (\hat{x} \land \hat{y}) \oplus (\hat{x} \land \hat{y}) \oplus \hat{x} \land \tilde{y} \oplus \tilde{x} \land \tilde{y}$ which is a re-written form of $(\hat{x} \oplus \hat{y}) \lor (\tilde{x} \oplus \tilde{y})$.

Algorithm 3: The algorithm $\lor^S$

**Data:** $(\hat{x}, \hat{y}|\tilde{x}, \tilde{y})$ vector of bit/s such that $\hat{x} \lor \tilde{y}$ belongs to $NC_1$, and $\hat{y} \lor \tilde{x}$ belongs to $NC_2$.

**Result:** $(A^R \oplus B^R) = \{\hat{x} \lor \hat{y}\}$ such that

1.5. These steps are same as initial 5 steps of $\land^S$ function.

6. $NC_1$ computes $A^R = A_{PS} \oplus (\hat{x} \land R'_B) \oplus (\hat{y} \land R_B) \oplus (\tilde{x} \land \tilde{y}) \oplus (R_B \land R'_A) \oplus (\tilde{x} \land \tilde{y}) \oplus (\hat{y} \land R_A) \oplus (\tilde{x} \land \tilde{y}) \oplus \hat{x} \land \tilde{y} \oplus (R_A \land R'_B)$.

7. $NC_2$ computes $B^R = B'_{PS} \oplus (\tilde{x} \land R'_A) \oplus (\tilde{y} \land R_A) \oplus (\tilde{x} \land \tilde{y}) \oplus (R_A \land R'_B) \oplus \hat{x} \land \tilde{y} \oplus (\tilde{x} \land \tilde{y}) \oplus (\hat{x} \land \tilde{x}) \oplus (\hat{y} \land \tilde{y}) \oplus (R_A \land R'_B)$.

**Property 7.** $\land^S$ and $\lor^S$ forbid $NC_1$ to gain any information of private data of $NC_2$ (and vice versa). Moreover, the PS learns none of their private inputs.

**Proof:** From the protocol, $B_{PS}$ is the only value that $NC_2$ can learn from the private data of $NC_1$. Due to the noise, $R_{PS}$, added by $PS$, $NC_2$ is still not able to deduce the values of $\hat{x}$ or $\hat{y}$. As the roles of $NC_1$ and $NC_2$ are interchangeable, the same argument holds for $NC_1$, not able to learn the private inputs $\tilde{x}$ or $\tilde{y}$ of $NC_2$. However, one key security aspect of not leaking any information to $PS$ is achieved by randomizing the inputs before transmitting them to the Processing Site. Due to the randomization performed during the initial step, it just infers a stream of uniformly distributed values, and cannot distinguish between a genuine and a random value.

**Complexity:** Length of bit vector is 1: For the operator $\land^S$, $NC_1$ and $NC_2$ each performs 10 binary operations (0 $\oplus$ and 4 $\land$). $\lor^S$ does two more $\oplus$ that means 12 binary operations. For both operators $NC_1$ and $NC_2$ generate 2 random bits, exchange 2 $\times$ 2 random bits and send 2 $\times$ 1 bits to $PS$. $PS$ generates 1 random bit and performs 4 binary operation ($2 \oplus$ and 2 $\land$) and returns 2 bits to $NC_1$ and $NC_2$ each.
5.3 The Algorithm $\text{COMPARE}^S$

Algorithm 4: The Algorithm $\text{COMPARE}^S$

Data: Half part of $V$ and $W$ is owned by $NC_1$ and the other part is owned by $NC_2$

Result: $(\bar{i}|\bar{n})$ is such that $\bar{n} \oplus \bar{r} = 1$ if $V = W$ else 0

1. $NC_1$ computes $X \leftarrow \bar{\bar{v}} \oplus \bar{w}$ where $X = (X_1, X_2, \cdots, X_l)$ and $l$ is the length of the vector $V$ and $W$.

2. $NC_2$ computes $Y \leftarrow \bar{\bar{v}} \oplus \bar{w}$ where $Y = (Y_1, Y_2, \cdots, Y_l)$.

3. $(\bar{\mu}|\bar{n}) \leftarrow OR^S(X_1, X_2, \cdots, X_l|Y_1, Y_2, \cdots, Y_l)$

4. There is two ways to gets the result either $NC_1$, $NC_2$ perform $(\bar{i}|\bar{n}) = (\neg\bar{n}|\bar{n})$ or $(\bar{i}|\bar{n}) = (\bar{i}|\neg\bar{n})$.

7. REFERENCES