**KEY-POLICY ATTRIBUTE-BASED ENCRYPTION SCHEME FOR GENERAL CIRCUITS**

Diana BOLOCAN

Iași, Romania, e-mail: [dianabolocan.db@gmail.com](mailto:dianabolocan.db@gmail.com)

**Abstract.** Due to previous KP-ABE schemes being unviable when applied to complex circuits, a new efficient scheme is needed. Thus, the following contribution is presented. The paper “Key-Policy Attribute-Based Encryption Scheme for General Circuits” discusses about a new viable and secure cryptographic scheme based on attribute encryption for any given access structure represented through a circuit. The solution has two components: the physical transformation of the circuit and the modifications in the cryptographic algorithm. The new scheme keeps the size of the circuit unmodified, replacing the OR gates with NAND gates and adds additional functionalities in the algorithm for the new logical NAND gate. The solution uses the decisional bilinear Diffie-Hellman assumption to prove the security soundness of the new scheme and the proof of the AND gate functionality in backtracking attacks.

**Key Words.** *KP-ABE scheme, general circuit, decisional bilinear Diffie-Hellman assumption*

**1. INTRODUCTION**

Attribute-Based Encryption (ABE) is a cryptographic scheme in which the identity of the user is defined through a set of elements called attributes. The main purpose of ABE schemes is to establish simplified means of decryption by describing a group of authorized users. Each user is able to decrypt messages that were encrypted over the defined authorized sets of attributes, thus eliminating the need of user communication regarding the decryption key. There are two forms of ABE scheme : ciphertext-policy ABE (CP-ABE) [1] and key-policy ABE (KP-ABE) [2]. In the CP-ABE scheme, the data encrypted can be accessed only by the users whose attributes satisfy the security policy. The authorization is included in the encryption making the permission an implicit action. In the KP-ABE scheme, the access policy is written in the user’s key. Each key has an associated access structure which describes the type of ciphertext it can decrypt. The access structure is a tree whose leaves are all the elements from the attribute set and whose nodes are conjuctions and disjunctions.

In our paper we will discuss only about the KP-ABE for general circuits starting with describing previous works. Our construction appeared as a necessity for a new efficient scheme. In *Key-policy Attribute-based Encryption for Boolean Circuits from Bilinear Maps* [3] ??.

The paper is organized into eight sections. The next section contains theoretical notions which will be recalled throughout the presentation of the new KP-ABE scheme for general circuits and will provide a better understanding of the new construction. Before detailing the construction, we discuss about backtracking attack and why its existence is such an important problem that needs to be addressed and prevented in the general circuits extention of KP-ABE schemes. In the following four chapters the contribution is described alongside its security soundess, complexity and the new possible extention that can be applied over it. The eigth and the final chapter concludes our paper.

**2. PRELIMINARIES**

*Multiplicative cyclic group.* A *multiplicative group* is a set equipped with the binary operation which satisfies the following properties:

- ;

- so that;

- so that;

- .

A multiplicative group is called *cyclic* if there is an element which can generate all the elements of the group by repeatedly multiplying it with itself. Such elements are called *generators*.

*Bilinear maps.* Let there be , two multiplicative cyclic groups of the same order. A *bilinear map* from to it is a function where:

- , for ;

- is a generator of , for .

The *computational Diffie-Hellman problem* (CDH) states the fact that if and are given, looks like a random element of where is a generator of , a multiplicative cyclic group of order with randomly chosen elements from . The *decisional Diffie-Hellman problem* (DDH) is an indistinguishability problem in which there are two computational indistinguishable instances, and , where are elements defined as above and is a randomly chosen element of . The *decisional bilinear Diffie-Hellman problem* (DBDH) is the problem of distinguishing two elements and , where is a bilinear map defined from to , is a generator of and are randomly chosen elements of .

*Access structures.* Let be a set of elements called *attributes*. A set of nonempty subsets of is called *authorized access structure* if it is used to define the authorized user in a cryptographic system. Any other subset of that does not belong to is called *unauthorized* and it is an element of , the set of unauthorized users.

A *Boolean circuit* is a mathematical model for digital logic circuits composed of logic gates and wires. A Boolean circuit is called *monotone* if it contains only AND and OR gates. Depending on the structure of the circuit, the Boolean circuit can be restructured using the *De Morgan’s laws*. In propositional logic and Boolean algebra, De Morgan’s laws are a set of transformation rules which allow conjunctions and disjunctions to be rewritten using negation: and .

Thus, an AND gate can be replaced with an OR gate and vice versa. These laws will be later used in the physical transformation of the general circuit in the new construction.

A *general circuit* is a circuit composed of AND, OR and NOT gates each having their standard number of input wires, but whose output wires can vary in number.

*Shamir’s secret sharing scheme.* Shamir’s scheme is a scheme for sharing secrets that uses polynomial interpolation for reconstructing the secret. Given pair , where , there exists a unique polynomial function with the degree equal to so that . The shared secrets are chosen as where are pairwise distinct. Having the shares , for some group with , the secret can be obtained using Lagrange’s interpolation formula as:

KP-ABE has three probabilistic polynomial-time (PPT) algorithms and one deterministic polynomial-time (DPT) algorithm:

- is a PPT algorithm that takes as input the security parameter , outputing a set of public parameters and a master key ;

- is a PPT algorithm that encrypts the message according to the set of attributes and to the public parameters outputing the chipertext ;

- is a PPT algorithm that generates a decryption key for the access structure , given as a circuit, using the master key ;

- is a DPT algorithm that decrypts the ciphertext using the decryption key , returning the message or the special symbol .

**3. BACKTRACKING ATTACK**

For a better understanding of the backtracking attack in general circuits, a summary of the KP-ABE scheme will be presented:

- let there be a bilinear map with and two multiplicative cyclic groups of order and a generator of ;

- in order to encrypt a messsage , the value of is computed and multiplied with , where is a randomly chosen value from the setup phase and is a randomly chosen value from the encryption phase;

- each user that requests a decryption key triggers the key generation phase in which the value is shared from the top of the access structure to the bottom of it. The generated values outputed from the secret sharing are later used to compute the decryption key

- in order to decrypt a ciphertext the user gives the generated decryption key which is used to reconstruct bottom-up the value .

The share algorithm

The recons algorithm

The backtracking attack is an exploitation of information leakage present due to the functionality of OR gate that appears only when there is a fanout greater than one next to this logical gate. For example, given an access structure as in Fig. 1, the scheme is susceptible to the attack near the attribute 3 on level 0. When the decryption key is constructed, a pair of values will be generated by the OR gate from the output wire to the input wires. Let us suppose that the gate receives from the output wire the value . In the functionality of the OR gate is stated that for each element received, two new elements will be created with the property that the new elements are equal to the one currently received. Thus each wire obtains an identical element. In this case, the gate sends to each input wire the same value : . These values are exponents for the bilinear map and are used to generate and . Let there be a user with the set of attributes . The decryptor will learn the value , being able to find the value of just by noticing that .

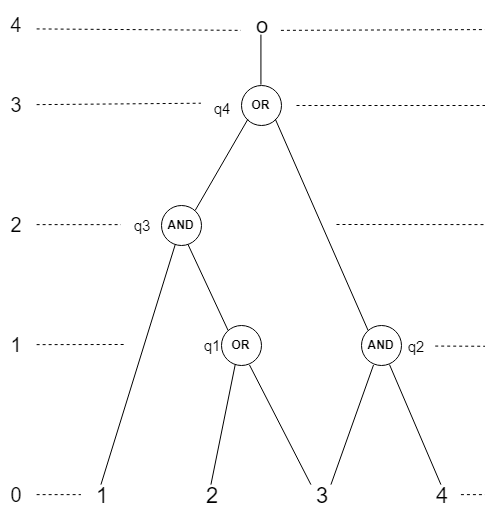


Fig. 1 General circuit susceptible to backtracking attack

Previous works that use bilinear maps in the cryptographic scheme have prevented the backtracking attack through different techniques such as placing an additional logical gate called FO (fanout) to share the OR gate’s secret [3] and expanding the general circuit in order to force the size of the fanout to one [4]. Both contributions are functioning solutions to the backtracking attack problem although they come up with disadvantages.

In the new logical gate’s case [3], the functionality of the FO gate requires random generation of two new values and so that ( is equal to , the value received from the output wires. This step is applied for every single element found in the output wires of the FO gate. All the values are further shared throughout the access structure whereas all the values are saved in a second storage and accessed only when the computation of the decryption key is needed. As it can be observed in the Fig. 2, the secret sharing algorithm outputs five main values and another two secondary values which are as important as the others in the construction of the decryption key. It is fairly easy to see that the scheme is rather costly when applied on complex general circuits. In the worst-case scenario the complexity of the decryption key can reach elements, where is the number of attributes, is the number of FO gates with a maximum fanout size of .

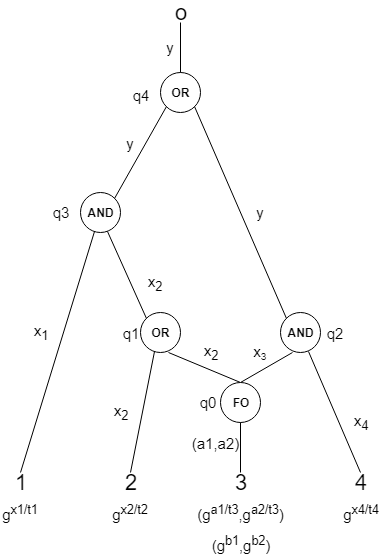


Fig. 2 Share algorithm applied on the general circuit

In the second contribution [4], the backtracking attack is prevented by expanding the general circuits so that the size of the fanout is forced to one. The expansion algorithm starts from the bottom and goes up to the output wire of the circuit multiplying attributes, wires and gates when there is a fanout greater than one. At first, this techniques seems to be an easy and well needed solution which proved to be less constly than the previous one due to the nonexistence of FO gates. Taking a better look at it, the scheme ignores the physical complexity of the new circuit. Thus, applying this solution over a complex general circuit will lead to a new massive access structure which is costly from a physical point of view. As it can be seen in the Fig. 3, the general circuit has been expanded from a 3-attributes, 4-gates and 9-wires structure to a 6-attributes, 5-gates and 11-wires structure. As for the complexity of the decryption key, the scheme output in the worst-case scenario elements, where is the number of attributes, is the number of FO gates with a maximum fanout size of .

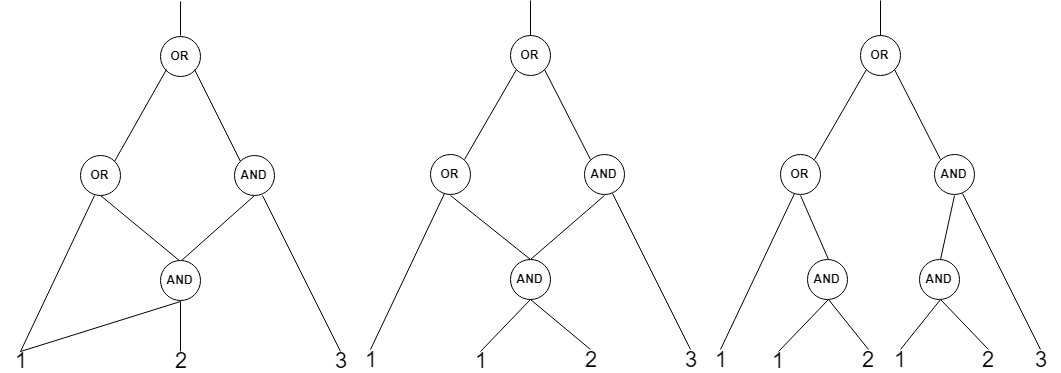


Fig. 3 Expansion of the general circuit

Thus, a new solution which can solve these disadvantages is more than welcomed. For these reasons, a new scheme has been defined so that it keep the number of shared secrets to a minimum and the size of the general circuit unmodified for an altogether better complexity.

**4. NEW CONSTRUCTION**

As is can be observed, the biggest difficulty encountered throughout in KP-ABE schemes for general circuits is the backtracking attack which apprears only in OR gates near a fanout greater than one. Furthermore, due to its secure functionality, the AND gate is the most stable gate that the circuit has and will always withstand information leakage. In both papers [3] and [4], the discussion about the problem of the backtracking attack in general circuits surrounds the idea that the OR gates connected to a fanout greater than one is predisposed to the attack and describes solutions that maintain the problematic gate. In article [3], the prevention is made by securing the fanout through the use of FO gates. In article [4] the fanout is forced into having its size equal to one by expanding the general circuit. In neither of these papers there are no modifications or improvements brought to the OR gate itself and no replacement with a more secure alternative is tried.

Thereby, a new construction is presented in which the OR gates are replaced with NAND gates whose functionality resembles the AND gate’s, preventing in this way the backtracking attack and maintaining the size of the general circuit.

**4.1 Physical alteration**

The access structure’s modification is quite simple: all the OR gates are replaced with NAND gates, as seen in Fig. 4. The idea of alterating the general circuit has sprung to mind after seeing the De Morgan’s laws of transformation. The functionality of the new gate is discussed in the next subsection.

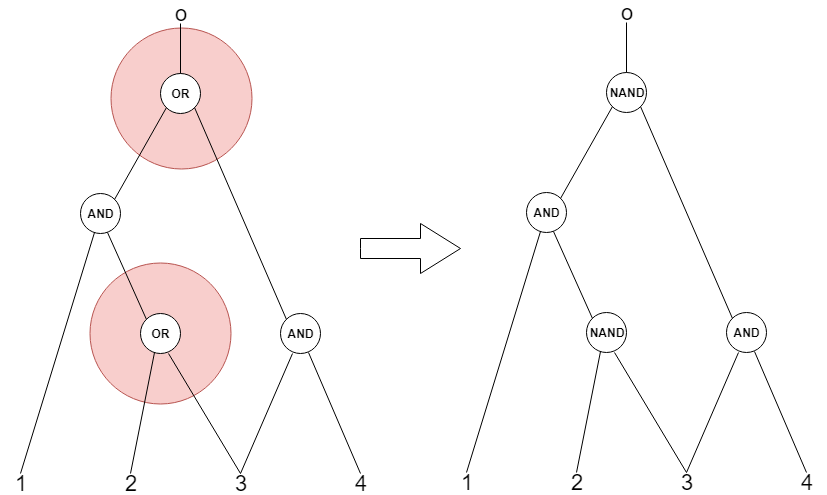


Fig. 4 Physical alterations in the general circuit

**4.2 The new cryptographic system**

The existance of a new logical gates brings alongside modifications in the KP-ABE scheme’s algorithms. As stated above, the functionality of the NAND gate resembles the AND gate’s. From all the existing algorithms, the secret sharing and the reconstruction algorithm are the most heavily modified. Therefore, the presentation will start with four main algorithms of the KP-ABE scheme continuing afterwards with the previous two.

:

- given the security parameter λ, a prime number is chosen alongside two multiplicative cyclic group and of the same order , a generator of and a bilinear map ;

- let be the set of attributes;

- the element is randomly chosen from ;

- for each , the element is randomly chosen from ;

- the algorithm outputs the public parameters (PP) and the master key (MSK) defined as below:

:

- the element is randomly chosen from ;

- the algorithm outputs the ciphertext :

:

- the algorithm is called saving the returned value in ;

- the algorithm outputs , where

for each .

:

-

**5. SECURITY**

**6. COMPLEXITY OF THE CONSTRUCTION**

**7. EXTENTIONS**

**8. CONCLUSIONS**

**REFERENCES**

1. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters, *Attribute-based encryption for fine-grained access control of encypted data*, in ACM Conference on Computer and Communications Security, pages 89–98. ACM, 2006. Preprint on IACR ePrint 2006/309

2. John Bethencourt, Amit Sahai, and Brent Waters, *Ciphertext-policy attribute based encryption*, in IEEE Symposium on Security and Privacy, S&P 2007, pages 321–334. IEEE Computer Society, 2007

3. Ferucio Laurențiu Țiplea and Constantin Cătălin Drăgan, *Key-policy Attribute-based Encryption for Boolean Circuits from Bilinear Maps*, in BalkanCryptSec 2014, Istanbul, Turkey, 16-17 October, 2014, pages 175-193, LNCS 9024

4. Peng Hu and Haiying Gao, *A Key-Policy Attribute-based Encryption Scheme for General Circuit from Bilinear Maps*, in International Journal of Network Security, **Vol. 19**, No. 5, pages 704-710, September 2017