**KEY-POLICY ATTRIBUTE-BASED ENCRYPTION SCHEME FOR GENERAL CIRCUITS FROM BILINEAR MAPS**

Ferucio Laurențiu ȚIPLEA\*, Diana BOLOCAN\*\*

\* Department of Computer Science, “Al.I.Cuza” University of Iași 700506 Iași, Romania, e-mail: [fltiplea@info.uaic.ro](mailto:fltiplea@info.uaic.ro)

\*\* 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 from Bilinear Maps” 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 and ??. There are two forms of ABE scheme : chipertext-policy ABE (CP-ABE) [1] and key-policy ABE (KP-ABE) [2].

Previous works and why we need a better one

What do we compare

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.

*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: .

*Chinese Reminder Theorem.* Let be a natural number greater or equal to 1 and pairwise coprime integers. For any , the system of equations has a unique solution modulo :

The solution can be computed as follows:

- for every with , ;

- a integer value is computed for the equation ;

- the unique solution modulo of the system is .

*Mignotte sequences.* Let be a natural number greater or equal to 2 and . A Mignotte sequence is a sequence composed of pairwise coprime integers that satisfies .

*Mignotte’s scheme.* Mignotte’s scheme is a secret sharing scheme that uses Mignotte sequences. Given a Mignotte sequence, the scheme does the folowing:

- a random integer is chosen so that where and ;

- the shared secrets are computed as ;

- given shared secrets , the secret can be reconstructed using the Chinese reminder theorem for the system of equations modulo :

**3. BACKTRACKING ATTACK**

**4. NEW CONSTRUCTION**

**5. SECURITY SOUNDNESS**

**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