ISSN 2047-3338

Hierarchical Threshold Outsource Secret Sharing and Interactive Proof Scheme for Land Conflicts

Ngye Antoinette Agwa[1], Takumi Kobayashi[2], Chika Sugimoto[3], Ryuji Kohno[4]

[1,2,3]Graduate School of Engineering Science, Yokohama National University, Japan

[4]University of Oulu Research Institute Japan

Abstract— **A land dispute involves conflicting claims to the ownership right of landed property by two or more parties that can be addressed within a legal framework. The advancements in networking and computing technologies have opened a gateway for the landowners to make any legal transaction on their landed properties, such as selling and conveniently transferring ownership through the internet. Despite all the advantages of digital technology advancement and the global use of the internet, the fraudulent act of manipulating digital content to compromised ownership rights is a common phenomenon in land conflicts. In this study, a scheme of multi-prover zero-knowledge arguments and outsourcing secret sharing has been proposed to solve land disputes. In this proof, participants only have to run a small amount of competition on their devices. Simultaneously, complex computation is sent to the cloud service provider for verification and construction.**

Index Terms— **Outsource Secret Sharing, Homomorphism Encryption, Ownership Proof, Zero-Knowledge Interactive Proof, Land Dispute and Cloud Service Provider**

I. INTRODUCTION

CONSIDER an application where digital certificate content is stored in the cloud. It becomes necessary to prevent the digital certificate from being falsified. Therefore, the most promising measure for ownership protection is to discourage people from forging ownership rights. One way to deter falsification is to make it detectable and highly punishable by law. If a person is accused of falsification by the owner, then the problem of ownership dispute arises. Considering such scenarios, previous proposals to resolve ownership right focus on resolving disputes using the watermark buyer-seller protocol [1]-[6]. Another way is to use the deduplication protocol proposed in the literature of [7]-[11]. The decision is made by a verifier (a judge, for example) after comparing numerous claims of ownership results from an ownership dispute. Generally, this result may not determine the rightful owner in a situation where the rightful owner is not participating in the argument. Besides, only a single claim of ownership is often faced by one and adapts to its rightfulness. Suppose a Fraudster obtains a digital copy, claims to be the rightful owner, and starts selling the land to another person without proof of ownership. An honest buyer purchasing the land will get into trouble when the rightful owner later detects the (Unpremeditated) used. In such a condition, proof of ownership is required. On the other hand, it guarantees the buyer that he obtains the right of possession of the land parcel. On the one hand, it makes the unauthorized selling or ownership transfer right (inheritance) complicated since honest buyers request ownership proof from the seller. In such a situation, the ownership proof should be transferable. For example, the new buyer (Lala) can show to another buyer (Titi) how Lala took good care of acquiring the property. All landowners are required to register with the appropriate authority who will issue a land certificate in return. One might think that it is insignificant to achieve proof of ownership when a registration center is involved.

Nevertheless, the critical point is that ownership refers not only to a registered land but also to all related lands that are still to be registered. Generally, during the sale or inheritance of a land parcel, the following two primary conditions should be considered by the person in question: First, a rightful owner of a land certificate should perform ownership proof on the land parcel. Secondly, multiple registrations of the same land parcel have to be avoided by the appropriate authority. Otherwise, a falsifier may gradually modify a land certificate and register it under another name and hence be able to perform a fake ownership proof.

In this paper, we present a model for ownership proof of digital land certificates as follows: we start by proposing an innovative secret sharing scheme, as shown in Fig. 1. During ownership transfer of a plot (selling or inheritance, for example), the land certificate is verified to convince the buyer that the land certificate presented is from a Bonafide certificate. In our proposer, secret shares are distributed to dissimilar shareholders (state authorities, landowners, and neighbors). The shareholders can get the secret justly with a small number of operations. While Costly computations are outsourced to a cloud service provider (CSP), and the CSP can gain no information about the secret. Besides, the reputation system can successfully prevent shareholders from colluding with the server. *A* zero-knowledge interactive proof scheme is performed during the resolution of a land dispute.

When compared with earlier schemes, our proposed method has the following advantages:

1) The scheme can accurately check the malevolent behavior of shareholders or the server.

2) Costly computations are outsourced to a CSP. With the CSP's computational power, it can execute complex verification and homomorphic encryption operations, and the CSP will obtain no information about the secret.

3) Through a combination with the zero-knowledge protocol (ZKP), a proposed interactive proof scheme using HTSS (hierarchical secret sharing scheme) can Counter-attack collusion between the shareholders and the server. Besides, ZKP proof of ownership competes with the act's state regarding security guarantees and performance. That is, our approach demonstrates proof of ownership without revealing any information about the secret.

4) Shareholders can be added and remove from the scheme. We present preliminaries in section II. In section III, we construct a zero-knowledge interactive proof scheme base on outsourcing HTSS. In section IV, we indicate our proposed scheme's security, and in section V, we compare our method with conventional schemes. Finally, in section VI, we present the conclusion of our proposed scheme.

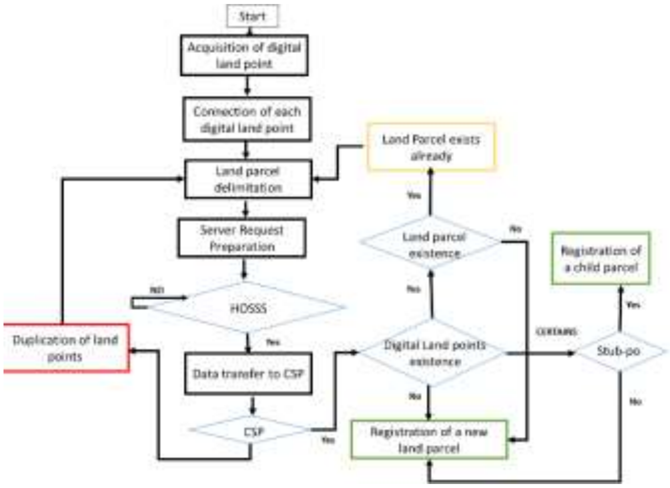
Start
Acquisition of digital land point
Connection of each digital land point
Land parcel delimitation
Server Request Preparation
HOSSS
NO
Yes
Data transfer to CSP
CSP
Yes
Duplication of land points
Land Parcel exists already
Yes
Land parcel existence
No
Yes
Digital Land points existence
No
Registration of a new land parcel
CONTAINS
Stub-po
Yes
No
Registration of a child parcel

Fig. 1. Flow chart of Land Parcel Registration

II. LITERATURE REVIEW

A. Homomorphism Secret Sharing

Homomorphism secret sharing propose in [12] described the property of homomorphism secret sharing. There is a great need to securely store land data information to prevent theft of information and leakage. Secret sharing is an essential tool with many applications. [13], [14] proposed general ideas of secret sharing. Hierarchical secret sharing is the problem in which a secret is shared among groups of participants partition into levels depending on their authority. [15]-[17] presents important notions on (t, n) threshold secret sharing. Unfortunately, these schemes cannot prevent malicious behaviors. Also, only a single secret can be share at a time. In [18], the author introduced the notion of multistage secret sharing base on Lattice that can counter attack resistance. Participants' malicious behavior can be prevented by the CSP using the concept proposed in [19]-[21]. However, in the proposal, new participants cannot be added to the scheme. [22], [23] suggested the possibility of adding new participants into the scheme without changing the secret. Take for example two secrets B_1 and B_2, shared by polynomials $p(x)$ and $p'(x)$. If we add the shares each $f(i) = p(i) + p'(i), i = 1 \leq i \leq n$, $f(i)$ can be viewed as a sub-share of secret $B_1 + B_2$. Suppose that we define B as the secret domain and φ as the shared domain. A set of functions $F_1 : \sum^t \rightarrow B$ can be calculated, where $I = \subseteq \{1,2,..,n\}$ and $|I| = t$. Given a random set of t values $B_{i_i},..,B_{i_i}$, we can define the following equation for the secret k:

$$B = F_I\left(B_{i_1},..,B_{i_t}\right) \tag{1}$$

for $I = \{i_i,..,i_t\}$

Definition 1: Suppose that they are two operations ⊕ and ⊗ on the secret domain B and share domain Σ, respectively. That is;

$$B = F_I\left(B_{i_1},..,B_{i_t}\right), B' = F_I\left(B'_{i_1},..,B'_{i_t}\right) \tag{2}$$

Then,

$$B \otimes B' = f_I\left(B_{i_1} \otimes B'_{i_1},...,B_{i_t} \otimes B'_{i_t}\right) \tag{3}$$

From definition 1, Shamir's polynomial is $(+,+)$ homomorphic, which indicates that the sum of the secret shares is equivalent to shares of the sum.

B. Hierarchical Threshold Scheme (t, n)

Definition 2: Let A be a set of n participants and assume that A is composed of levels $\mathrm{A} = \bigcup^m{}_{i=o} \mathrm{A}_i$ where $\mathrm{A}_i \cap \mathrm{A}_j = \Theta$ and A_0 is the highest level for all $0 \leq i < j \leq m$. Let n_l be the number of shareholders associated with level A_l, we can obtain $n = |\mathrm{A}| = \sum_{l=0}^{m} n_l$. Then, we can define a threshold u_l for $l = 0,..,m$, which satisfies $0 < k_0 < \cdots < k_m$. In addition, we set $\mathrm{K} = \{k_i\}^m{}_{l=0}, k = k_m$, and $k_1 = 0$. Then the $(\mathbf{K}, n)$ -hierarchical threshold access structure is;

$$\Gamma\left\{ v \subset \mathrm{A} : \left| v \cap \left(\bigcup_{j=0}^{i} \mathrm{A}_i \right) \right| \geq k_{i,} \ \forall \in \{0,1,..,m\} \right\} \tag{4}$$

A corresponding (k, n)-hierarchical threshold secret sharing scheme, is a scheme that realizes this access structure. Which is a method of assigning each participant $u \in \mathrm{A}$ secret share $\sigma(u)$ of a given secret S such that authorized subsets $\mathrm{V} \in \Gamma$ may recover the secret from the shares possessed by their participants, $\sigma(\mathrm{V}) = \{\sigma(\mathrm{A}) : u \in \mathrm{V}\}$, while the shares of unauthorized subsets $\mathrm{V} \notin \Gamma$ do not reveal any information about the value of the secret.

Next, we describe the procedure for Birkhoff interpolation use to reconstructs the secret. The elements of $e_{i,j}$ are 0 or 1 and $\sum e_{i,j} = N+1$. Not that there should be no empty row or namely an i for which $e_{i,j} = 0$ for $i, j = 0,1,..,n$. Supposed that, $\chi = [x_1,..,x_l]$ be a given set of l distinct points where $x_1 < \ldots < x_l$. Then, the Birkhoff interpolation problem of Tassa that corresponds to the triplet E, χ, U_c and given data $c_{i,j}$ one must find a polynomial f of degree $t - 1$, that satisfies the conditions:

$$f^{(i)}(x_i) = c_{i,j},\ e_{i,j=1} \tag{5}$$

For each given set of the triplet (E, χ, U_c) there is a unique solution for each given set of $c_{i,j}$ if and only if the determinant of $D(E,\chi,U_c)$ is different from zero. Let $U_c = \{u_0,..,u_{t-1}\} = \{1, x, x^2, ..., x^t\}$ where $u_k{}^j$ is the j -th derivative of u_k for $k = 0,..,t-1$. Then the matrix $\mathrm{A}(E,\chi,U_c)$ is define as follows:

$$\mathrm{A}(E,\chi,U_c) = \begin{bmatrix} u_0{}^{j1}\ u_1{}^{j_1}\ u_2{}^{j_1}\ ..\ u^{j_1}{}_{t-1} \\ u_0{}^{j2}\ u_1{}^{j2}\ u_2{}^{j2}\ ..\ u^{j2}{}_{t-1} \\ . \\ . \\ u_0{}^{jc}\ u_1{}^{jc}\ u_2{}^{jc}\ ..\ u^{jc}{}_{t-1} \end{bmatrix}$$

Such that, the polynomial f(x) ∈ $R_{t-1}[x]$ can be constructed as:

$$f(x) = \sum_{k=0}^{t=1} \frac{\det(\mathrm{A}(E,\chi,U_{ck}))}{\det(\mathrm{A}(E,\chi,U_c))} x^k \tag{6}$$

where $\mathrm{A}(E,\chi,U_{ck})$ is obtained from (E,χ,U_c) by replacing its $(k + 1)$ -th column with the shares $c_{i,j}$.

C. Multi-Prover Zero-Knowledge Argument (MPZKA)

MPZKA is an interactive proof that permits a group of shareholders or provers (P) to synchronously prove to a verifier (v) many times that they share a secret in such a way that V will not obtain any information about the secret. This group proves is either accepted or rejected by the verifier. MPZKA was equally studied in [24]. The zero-knowledge protocol has recently gained significant acceptance in [25]-[27]. In [28], secret shares were chosen from the finite filed and distributed to roadside units (RSU) and on-board units (OBU). In this protocol, a duplicate of each of the secret chosen from FG (q) was distributed to a group of RSUs (prover). The problem with this protocol is that a malicious RSU can decide to share the secret with another RSU, not in the group. In [29], the secure multiparty computation was used to solve the duplication problem. Unconditionally secure multiparty computation (MPC) was equally introduced in [30] and was subsequently studied in the literature of [31]-[33]. Our scheme assumes the presence of a trusted center that is involved in distributing secret shares to shareholders, as presented in Fig. 2. After distributing secret shares, the center becomes inactive or closed. The MPZKA scheme relay that a group of provers synchronously prove to a verifier V that they share a secret or that they do not share any secret without revealing any information about the secret.

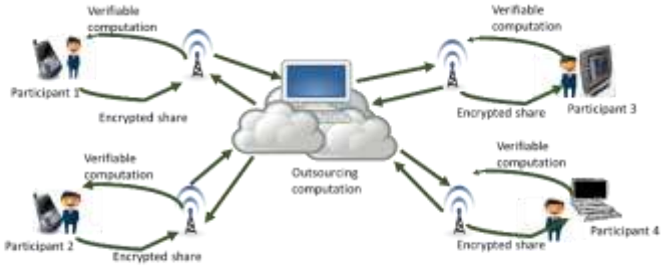

Fig. 2. Outsource Secret Shearing

III. ZERO-KNOWLEDGE INTERACTIVE PROOF SCHEME BASE ON OUTSOURCING HTSS

In this section, combining ZKP and outsourcing computation, we propose a novel outsourcing ZKP interactive proof scheme base on HTSS for land dispute resolution. In the outsourcing HTSS protocol, t or more participants from different levels can reconstruct the secret. The zero-knowledge proof is performed later on during a dispute about the legitimacy of a land certificate. Our proposed scheme consists of six-phases, namely; an initialization phase, secret sharing phase, outsourcing phase, reconstruction phase, add and removed phase, and ZKP proof phase. In the initialization phase, we define some useful parameters. Thereafter, in the secret-sharing phase, the CSP distributes secret share to each participant, follows by verification information that is then broadcasted to the participant, and shareholders receive a random value to encrypt secret shares. Then shareholders send shares to the CSP, and after computation, the CSP returns the results to the Shareholders, where the CSP obtains no valuable information concerning the secret. Next, shareholders can receive the secret fairly during reconstruction. In the "Add" and "Remove" phase, shareholders can be added into the scheme (in a situation where landowners split the land and sell it to another person, for example), and a shareholder can be removed during the transfer of ownership right. Finally, the secret shares are used during the proof of ownership right.

A. Initialization Phase

A dealer randomly chooses two large primes p and q, such that $q(/\ p-1)$ and g is a generator of the $p-th$ order subgroup from $(FG(q))$ and H(X) is a one-way hash function. A secret S is shared among n participants $p_i,...,p_n$ split into different levels $\mathrm{A}_0,...,\mathrm{A}_m$. Considering that n_l is the number of shareholders associated with level A_l and t_l is the threshold associated with level A_l for $l = o,i,...,m$. The identity of participant $p_{i,j} \in \mathrm{A}_l$ is the pair (i, j) for $i = 1,\ldots,n_l$, $j = t_{l-1}$ and $t_1 = 0$.

B. Distribution of Secret to Each Participants

A trustable dealer takes the following steps to distribute shares among all participants:

1) The dealer selects random elements $b_1,\ldots,b_{t-1}$ from the finite filed FG(q) to constitute a polynomial with t-1 degree polynomial

$$f(x) = \sum_{v}^{t=1} b_i x^v \bmod q \tag{7}$$

where $b_0 = S$ is the secret value. The corresponding shares are $w_i = f^j(i)$, where $f^j(i)$ is the $j-th$ derivative of the polynomial f(x).

2) The dealer randomly chooses $t-1$ coefficients $b'_0,\ldots,b'_t$ from $FG(q)$, and generate a polynomial with t-1 degree.

$$f'(x) = \sum_{v}^{t=1} b'_i x^v \bmod q \tag{8}$$

where b_0' distributed to all participants is a random value from $FG(q)$) and the corresponding shares are $w'_i = f'^j(i)$,

3) According to the property of homomorphism secret sharing [34],[35] the share of each shareholder is

$$\gamma_{i,j} = w_{i,j} \otimes w'_{i,j} = f^j(i) \otimes f'^j(i) \tag{9}$$

4) The dealer distribute $(\gamma_{i,j} H(b_0))$ to the shareholders $p_{i,\ j}$, for $i = 1,..,n_l$, $j = t_{l-1}$ and $l = 1,0,\ldots,m.$ where $H(b_0)$ is a one way hash function.

5) The dealer broadcast verification information

$$\psi_v = g^{b_v \otimes b'_v} \bmod p,\ v = 0,\ldots,t-1 \tag{10}$$

C. Outsourcing Phase

To manipulate digital land data, an authorized group of participants must agree by providing their shares to the CSP as follows:

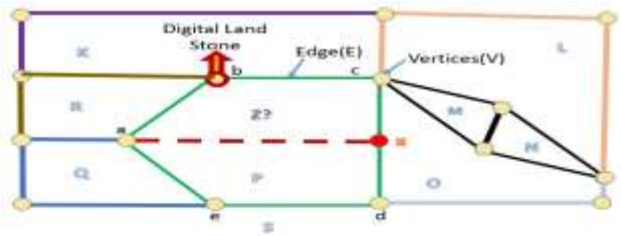

Fig. 3. An Example of a Digital Land Map

1) An authorized subset of t participants sends $\gamma_{i,j}, \psi_v$ to the CSP.

2) CSP runs a verification algorithm to check whether equation (11) is correct.

$$g^{\gamma_{i,j}} = \prod_{v}^{t=1} \psi_v^{\left(\frac{v!}{(v-j)!}\right) i^{v-j}} = g^{f^i(x)} \bmod p \tag{11}$$

where $v = 0,\ldots,t-1$.

3) If equation (11) holds then, CSP performs step (2) otherwise, the protocol is aborted, and the decryption behavior of p_i is broadcasted.

*4) CSP use Birkhoff interpolation to reconstruct the secret s'_0 with any **k** points $E,\ \chi, U_c$ such that*

$$f(x) = s'_0 \sum_{k=0}^{t=1} \frac{\det(\mathrm{A}(E,\chi,U_{ck}))}{\det(\mathrm{A}(E,\chi,U_c))} x^k \tag{12}$$

from equation (12), the CSP can learn $s'_0 = F(0) = b_0 \otimes b'_0$ and returns s'_0 to t active participants.

D. Decryption and Verification of Phase

To achieve decryption and verification, each participant can obtain the secret by running a small amount of computation using the following steps:

1) The shareholders can obtain secrets by computing $s = b_0 \otimes b'_0$

2) Each participant then verifies the correctness of its share by checking if $h(b_0) = h(s)$. If it is correct, then the computation of CSP is correct. Otherwise, the result is wrong.

a) Example 1:

We start by defining a neighbor, in a cadastral survey, a neighbor is a person that shares an edge or vertices of a land parcel with another person. Fig. 3. shows the demarcated land parcel (a, b, c, d, e), This example assumed that there are two landowners, three state authorities and 7 neighbor (K, L, M, O, S, Q, R) defined as $[k_0, k_1, k_2] = [2, 3, 7]$, where $k_m = k_2 = 7$.

1) The dealer selects random values (a_0, a_1..., a_6) from finite filed to construct a polynomial of degree 6 such that

$$f(x) = a_0 + \sum_{v}^{6} a_i x^i \bmod q \tag{13}$$

where a_0 is the secret.

2) The dealer then distributes shares $\gamma_{i,j}$ to all participants as presented in table I with g_0 belonging to landowners of the land parcel (a, b, c, d, e), g_1 belonging to state authorities, and g_0 to neighbors. These neighbors are determining from Fig. 3.

3) The secret b_0 is computed using H (E, X, U$_c$) and H (E, X, U$_0$).

$$H=(E,\chi,U_c)=\begin{bmatrix} 1 & \mathrm{p}_1 & p_1{}^2 & p_1{}^3 & p_1{}^4 & p_1{}^5 & p_1{}^6 \\ 1 & p_2 & p^2{}_2 & p_2{}^3 & p_2{}^4 & p_2{}^5 & p_2{}^6 \\ 0 & 0 & 1 & p_3 & p_3{}^2 & p_3{}^3 & p_3{}^4 \\ 0 & 0 & 0 & 1 & p_4 & p_4{}^2 & p_4{}^3 \\ 0 & 0 & 0 & 0 & 1 & p_5 & p_5 \\ 0 & 0 & 0 & 0 & 1 & p_6 & p_6{}^2 \\ 0 & 0 & 0 & 0 & 1 & p_7 & p_7{}^2 \end{bmatrix} \quad (14)$$

TABLE I
SECRET SHARE DISTRIBUTION

Participants	Shares u_a	Share u_b	shares (U_c)
$p1 \in g_0$	F(p_1)	G(p_1)	F(p_1)⊕G(p_1)
$p2 \in g_0$	F(p_2)	G(p_2)	F(p_2)⊕G(p_2)
$p3 \in g_1$	$F^2(p_3)$	$G^2(p_3)$	F(p_3)⊕ $G(p_3)$
$p4 \in g_1$	$F^2(4)$	$G^2(4)$	F(p_4)⊕ $G(p_4)$
$p5 \in g_2$	$F^3(p_5)$	$G^3(p_5)$	F(p_5)⊕ $G(p_5)$
$p6 \in g_2$	$F^3(p_6)$	$G^3(p_6)$	F(p_6)⊕ $G(p_6)$
$p7 \in g_2$	$F^3(p_7)$	$G^3(p_7)$	F(p_7)⊕ $G(p_7)$

$$H=(E,\chi,U_0)=\begin{bmatrix} u_1 & \mathrm{p}_1 & p_1{}^2 & p_1{}^3 & p_1{}^4 & p_1{}^5 & p_1{}^6 \\ u_2 & p_2 & p^2{}_2 & p_2{}^3 & p_2{}^4 & p_2{}^5 & p_2{}^6 \\ u_3 & 0 & 1 & p_3 & p_3{}^2 & p_3{}^3 & p_3{}^4 \\ u_4 & 0 & 0 & 1 & p_4 & p_4{}^2 & p_4{}^3 \\ u_5 & 0 & 0 & 0 & 1 & p_5 & p_5 \\ u_6 & 0 & 0 & 0 & 1 & p_6 & p_6{}^2 \\ u_7 & 0 & 0 & 0 & 1 & p_7 & p_7{}^2 \end{bmatrix} \quad (15)$$

E. Adding a New Participant

Here we consider a situation where a landowner wants to split a piece of land and sell or give it to another person, thereby introducing a new neighbor. New neighbor (s) can be added using the add algorithm, as presented below.

Definition 2; let Γ be an access structure arranged in different groups $(G_0,\ldots,G_i)$ and t_h the threshold of group G_h for $h=0,\ldots,l$. Consider a secret *S,* a group of shares Ω*,* and a set of participants *P* where the pair $(i,\, j \in \mathrm{I}\times\mathrm{I})$ is the unique ID of participant $p_{i,j} \in \rho$, such that $j=t_{h-1}(j=t_l-t_h)$ and $W=\subset\rho$ $t_{-1}=0$. Therefore, we can define the algorithms add, reset, reconstruct as follows:

a) Add algorithm

It takes as input a set of shares $\gamma_1,\ldots,\gamma_w$ held by a subset $W=\subset\rho$ of participants, and the $ID(i^{'},j^{'})$ of the new participant. If *W* is unauthorized, that is *W* /∈ Γ it outputs *φ* otherwise, *W* ∈ Γ and participants compute $\gamma_{i^{'},j^{'}} := f^{\,j^{'}}(i^{'})$ in a distributed manner. That is, each participant $\rho_l \in W$ performs the following steps: for $l=1,\ldots,w.$

1) The derivative of each participant's partial Birkhoff interpolation polynomial at $x=i^{'}$ is computes as

$$y_j=\gamma_l\sum_{v=j^{'}}^{t-1}\frac{v!}{(v-j^{'})!}(-1)^{l-1+v\frac{\det(\mathrm{A}_{l-1,v}(E,\chi,U_{ck})}{\det(\mathrm{A}_{l-1,v}(E,\chi,U_c)}}\,i^{'v-j^{'}} \quad (16)$$

where $i^{'}=j^{'}-th$ is the derivative of its partial Birkhoff interpolation polynomial.

2) Each p_i randomly splits the result into w values such that; $y_l=\beta_{1,l}+\ldots+\beta_{w,l}$ and sends $\beta_{w,l}$ to the CSP. For $p_{m,j}\in W$, for $m=1,\ldots,w$ and $m\neq l$ using a secure network.

3) CSP collects all values $\beta_{w,l}$ received and computes

$$\beta_l := \sum_{m=1}^{w}\beta_{l,m} \quad (17)$$

4) CSP sends β_l to the new participants $p_{\,i^{'},j^{'}}$ through a secure network and broadcasts $c_0,\ldots,c_{t-1}$ that was receive from the sharing algorithm.

5) The new participants $p_{\,i^{'},j^{'}}$ computes it shares $\gamma^{'}{}_{i^{'}j^{'}}$ by adding all values β_l such that;

$$\Gamma_{ii^{'},j^{'}} = \sum_{l=1}^{f}\beta_l \quad (18)$$

6) The correctness of share is verify using the following equation:

$$g^{\gamma^{'}{}_{i^{'},j^{'}}} \equiv \prod_{v=j^{'}}^{t-1} d_v{}^{\frac{v!}{(v-j^{'})!}\,i^{'v-j^{'}}} = g^{\,f^{j^{'}}(x)} \quad (19)$$

a) Example 2

In land registration we consider three groups of participants namely, landowner, state authorities and neighbors. Share of each participant can be generated by the dealer as follows; Consider that participant form each authorized group (G$_1$, G$_2$ and G$_3$) provide their secret share to the CSP and CSP generate $f(x)=11+5x+8x^2 \bmod 7$ *that is,* $\varphi_1=3,\ \varphi_2=7,\ \varphi_3=8$

The add algorithm can create a share for a newcomer (P$_4$) as follows:

1) Each participant P_i privately computes $\varphi_i \times \gamma_i = \varphi_1, \gamma_1 = 7 \times (4-2)(4-3)(1-3) = 4$ $\varphi_2 \times \gamma_2 = 4 \times (4-1)(4-4)(2-1)(2-3) = 6$ $\varphi_3 \times \gamma_3 = 13 \times (4-1)(4-2)(3-1)(3-2) = 7$

2) Each p_i randomly split the results and exchange them, as shown in the share-exchange matrix $\varepsilon_{t \times t*}$..

3) Participants then compute and send $\sigma_1 = 5, \sigma_2 = 3, \sigma_3 = 8$ to P_4.

4) P_4 adds up these values to compute p'_4 share $\varphi_4 = 16$

$$\varepsilon_{t \times t^* =} \begin{pmatrix} \sigma_{11} = 2 & \sigma 21 = 1 & \sigma_{31} = 1 \\ \sigma_{12} = 1 & \sigma_{22} = 1 & \sigma_{32} = 4 \\ \sigma_{13} = 2 & \sigma_{23} = 2 & \sigma_{33} = 3 \end{pmatrix}$$

F. Remover of a Participant

Here we consider a situation where a landowner wants to transfer ownership of the plot to another person. Now, the old landowner (Titi) is removed from the scheme and replaced with the new owner (Lala), or during plot fusion, a neighbor can be removed. In other to remove a participant, we use the reset algorithm. This algorithm takes as input a set of shares $P' = \{p'_1, \ldots, p'_n\}$ belonging to V ⊂ P of the participant, with their respective unique $ID(i', j')$. That is, each old participant $\rho_l \in \nu$ performs the following steps: for $l = 1, \ldots, \nu$.

1) Each participant p_i computes its partial Birkhoff interpolation coefficient.

$$b_{l,0} = \omega_l (-1)^{l-1 \frac{d(\mathrm{A}_{l-1,0}(E, \chi, U_{ck}))}{d(\mathrm{A}(E, \chi, ULc))}} \left(b_{l,t-1} = \gamma_l (-1)^{i+t \frac{-2d(\mathrm{A}_{l-1,t-1}(E, \chi, u_{ck}))}{d(\mathrm{A}(E, \chi, U_c))}} \right) \quad (20)$$

2) Each participant constructs a polynomial $f_l'(x) = a'_{l,0} + a'_{l,1}x + a'_{l,2}x^2 +, \ldots, a'_{l,t'-1}x^{t'-1}$ of degree t′ – 1, where $a'_{l,0} = a_{l,0}(a'_{l,t-1} = a_{l,t-1})$ is the partial Birkhoff interpolation coefficient and $a'_{l,1}, \ldots, a'_{l,t'-1} \in FG(q)$ is randomly selected.

3) Each participant computes $f\alpha = a_{l,0} + a_{l,t-1}$

4) Each participant then computes sub-share $\gamma_{l,i'l'}$ for such that

$$\gamma_{l,i',j^;} = f\alpha^{j'}(i') \quad (21)$$

5) Next, each participant *sends sub-share $\gamma_{l,i',j'}$ to participant $p'_{i',j'} \in P$ using a secure network and broadcasts the audit data, composed of commitments to each coefficient of polynomial $f'_l(x) = \gamma_l, k' := g^{a_{l,k}}$, for $k = 0, \ldots, t' - 1$ and commitment $\gamma_0 = g^m(\omega_{t-1} = g^m)$ of the old polynomial f(x).*

6) Each participant erases it shares from the previous time period and compute it final new share form the secret b_0 as $p_{i',j'} \in P'$ and computes its share $\gamma_{l,i',j'}$ by adding all sub-shares $\omega_{l,i',j'}$ ωl,i0,j0 received as;

$$\gamma'_{i',j'} := \sum_{l=1}^{\nu} \beta_{l,i'',j'} \quad (22)$$

7) Each participant can verify the correctness of it share as follows:

1) Each new participant $p_{i',j'} \in P'$ checks the function value of each polynomial

$$g^{\gamma_{i',j'}} \equiv \prod_{k=j}^{t-1} \gamma_k^{\frac{k'}{(k-j')!} i^{k-j}} = g^{f(j')}(i') \quad (23)$$

for $l = 1, \ldots, r$

2) Each participant checks whether the free coefficient (last coefficient) of all polynomials $f'_l(i')$ leads to the original secret $s \in S$

$$\gamma_0 \equiv \sum_{l=1}^{\nu} \gamma'_{l,0}, \quad \left(\gamma_{t-1} \equiv \sum_{l=1}^{\nu} \gamma_{l,t'-1} \right) \quad (24)$$

3) If equations (23) and (24) are satisfied, it accepts $\gamma_{l,i',j'}$ as its valid share otherwise it rejects the response.

G. Reconstruct Phase

It takes as input shares held by a subset V ⊂ P of the participant. If V ∈ Γ, it outputs m ∈ M and reconstructs the secret using Birkhoff interpolation it outputs φ otherwise. Having access to the original audit data, it is possible to verify whether the reconstruction of the secret s ∈ S is a correct opening value for commitment $\omega_0 = g^{a_0}(\gamma_{t-1} = g^{a_{1t-1}})$, if it is possible to verify whether the reconstruction of the secret $s \in S$ is a correct opening value for commitment $\gamma_0(\gamma_{t-1})$ that is $g^s \equiv \gamma_0(g^s \equiv \gamma_{t-1})$.

H. Multi-Prover Zero-Knowledge Argument.

In this section, we consider the falsification of a land title of a particular piece of land. Each of the claimers has to prove in a law court which one of them is the rightful owner of that land parcel. Using multi-prover zero-knowledge argument in such a way that the Lawyers (Verifier) do not learn anything about the secret as follows:

1) The dealer use secret b_0 to calculate $h = g^{b_0} \bmod p$ such that the verifier who gets p, q, g, h can verify that p, q are prime and that g, h are of other q.

2) Supposed that a group of participants has come to present themselves as witnesses by pooling their shares $y_{i,j}$, such that every shareholder has a secret input $Y_{si} = y_{i,j}$. Then, the t active participants have to run the secure multi-party computation (SMC) for a function $y_{si} = y_{st}$, where $y = f(0)$ and $c_i = b_{l,0} = w_l(-1)^{l-1\frac{(d(A_{l-1,0}(E,X,U_{ck}))}{d(A(E,X\ U_c))}}$ as in equation (20)

3) After running the SMC protocol, ever shareholder has a secret H_i such that $Y = \sum_{r=0}^{t} b_i H_i \bmod p$ where $b_i \le i \le n$ can publicly be computed [40].

4) One or more attackers may randomly choose $t-1(c_i,\ldots,c_{t-1})$ from GF(q) and generate a polynomial with t-1 degree

$$g(x) = \sum_{r=0}^{t-1} c_i x^r \bmod q \tag{25}$$

where $S^* = c_0$ is the secret.

5) The attacker then repeats section III B above and distribute secret shares to participant p'_i.

Next, the attacker repeats section III C and obtain $S' = S^* \otimes c_0$.

6) Finally, the attacker repeats step a-b in section II G and obtain a secret h_i for every p'_i.

7) During the resolution of a dispute, every p'_i , p_i chooses randomly a number s_i and $u_i \in Z_p$ and compute $t_{i,j} = g^{s_i} \bmod p$ where p'_i , p_i are participants from the malicious landowner and the rightful landowner respectively *and send $t_{i,j}$ to v , for $i = 1,2,\ldots,n.$*

8) V chooses a random number using nonlinear feedback shift register (NLFSR) [35] in $m \in [1,0]^*$ and sends it to every p_i respectively.

9) p_i computes $d_i = s_i - m(y_i - b'_0) \bmod q$ .and sends d_i to v , for $i = 1,2,\ldots,n$.

10) v accepts that p_i share a secret Y such that $g^Y = h$ else, v rejects the response. Note that the verifier can only be convinced that p_i share s_0 after a certain number of rounds and step 8), 9) and 10) is repeated forever p'_i .

IV. SECURITY ANALYSIS

In this section, we analyze the security performance of our proposed scheme as follows:

Theorem 1. In our proposed scheme, any $t-1$ or fewer participants get nothing about the secret.

Proof: in our scheme, any $t - 1$ or fewer participants from different levels can cooperate by providing their share $\gamma_{i,j}$ for $i = 1,\ldots,n_h,\ j = t_{h-1}$ where $h = o,\ldots,m$ but, they cannot obtain the secret b_0 because the Birkhoff interpolation requires t values to determine the unique solution. In addition, The CSP does not know any valuable information about b_0. The scheme protects the participant's privacy since the CSP knows nothing about the input and output of p_i . The share sent by an authorized set of p_i to the CSP is encrypted; thus, the CSP cannot obtain any valuable information about b_0. In [13], it was proven that perfect security of hierarchical secret sharing holds for the (K, n) where $K = k^m{}_{i,j} = 0$ and that $k = k_m$. To add a new participant, $\rho_{i',j'}$, each existing participant $\rho_l \in W$ of an authorized subset $W \in \rho$ computes $f_l^{j'}(i')$. During this operation, this sub-share of participants leaks no information about their own share as they randomly split and distributes secret share to the other participants. But confidentiality is preserved as a participant only forwards the sum of all values received while hiding the individual sub-shares. The additive property of homomorphic used during distribution of sub shares and the polynomials use in secret sharing guarantees accessibility.

Theorem 2: Participants and CSP use public verification information to verify the correctness of shares, and the malicious behavior of participants can be noticed in time.

Proof: the correctness of shares γ_l can be verified by using public verification information of each participant $\rho_{i,j}$ and the commitment c_r to its share $\gamma_{i,j}$ using the commitments received as follows: $\rho_r = \prod_{k=j}^{t-1} d_k^{(k-j)!} = g^{f(j)}(i)$ where d_k is the commitment to coefficient d_k for $k = 0,1,\ldots,t-1$. Thus, by verifying $p_r \equiv g^{c_{i,j}}$ the correctness of its share can be checked.

In our proposed approach for zero-knowledge proof, shareholders' secret value cannot be revealed to any other shareholder or verifier even if shareholders exchange their secret shares as shareholders use SMC protocol in the interactive poof to jointly compute the secret over their inputs (secret shares) while keeping their secret shares private to them. Therefore, the privacy of all shareholders is maintained.

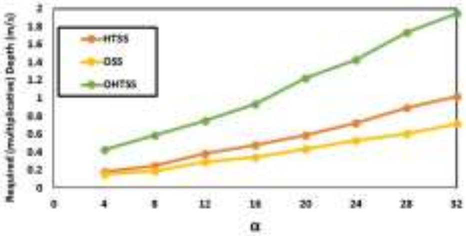

Fig. 3. Outsource Secret Sharing, Hierarchical Threshold Secret Sharing and Outsource Hierarchical Threshold Secret Sharing on various values for α with $\mu = 2^{-\alpha}$ in a plain state.

A. Security Complexity Analysis

In other to compare the quality of our proposed algorithm, we select two parameters α and μ and set $\mu = 2^{\alpha}$. At the same time, we consider that the algorithms' input/output has the same precision bits. Next, the dimension is fixed at $N = 217$, and the initial cipher text is set to modulus q_h up to 2^{2250} in other to achieve 128-bits according to Albrecht's LWE estimator [36]. In all the experiments, the initial modulus is set such that $\log\Delta + 10$ According to [37], the scaling factor bit-length (Δ) can be set to about 40. The most important factor affecting the running time is the depth because the computational cost of a homomorphism differs for each level. Next, we analyzed the encryption security performance matrices base on its throughput. Knowing that the higher the throughput of an algorithm, the better it is secured.

Encryption: for the encryption matrix, throughput is the average of total plain text divided by the average encryption time. In general, secret sharing schemes use a random variable measure in bits. To distribute a secret of one-bit, one polynomial (κ) with a threshold t participants, it requires $\kappa(t-1)$ random bits. To distribute a secret of length n bits, the entropy of $(t-1)n\kappa$ bits is required. Therefore, the throughput can be deduced as:

$$Throughput = \frac{Entropy}{computational_{time}} \tag{26}$$

V. PERFORMANCE EVALUATION

The performance evaluated was on an Intel(R) Core(TM) i5-3337U CPU @ 1.80GHz 1.80 GHz, 10 GB RAM, 64-bit, the server, and all hosts were running on the same computer in other to ignored network latency. Table II shows the time verification and time reconstruction of the secret. Table III shows our proposed schemes compared with conventional schemes. [34] proposed an outsourcing secret sharing scheme, but this scheme cannot be used in the hierarchical model. Homomorphism encryption and outsource secret sharing equally proposed in [35] with the additional ability to add and remove participants. Tassa [16] proposes a hierarchical secret sharing scheme, but the scheme requires that shareholders have a device with high computational power. Traverso [22] proposed a hierarchical verifiable and dynamic scheme that adds, removes, and renew secret shares, which can detect invalid secret shares, but it does not guarantee fairness; besides, the communication cost is high. [38] proposed a secret sharing scheme that guarantees fairness. In our proposed method, the protocol is executed only once; shareholders only have to run a small amount of decryption and verification with 0(1) communication cost. Fig. 5 shows that HTSS requires much less depth and complexity than OSS, and those of OHTSS are even smaller. The difference between the algorithms in terms of depth is that depth grows up as α increases. Fig. 6 shows the runtime of secret verification. It is visible that as the number of participants increase, the runtime grows exponentially. This time varies from 291.52 to 9576.24 according to the test results. Fig. 7 shows the reconstruction time complexity between our proposed and conventional schemes with the different file sizes. Fig. 8 shows the time to reconstruct the secret and return the result to the participants and the time taken to distribute the secret to each participant. It shows that the run time grows linearly as the number of participants increases with variable file size. It can be seen that the time increases as the size of the file increases. The fair secret sharing scheme proposed in [38] requires multiple rounds and cannot operate effectively on low computational complexity devices. However, [34] proposed an outsourcing secret sharing scheme that permits participants to perform the decryption operation only with O(1) computational cost. In contrast, the complex computation operation is sent to the CSP. It equally requires a dealer (trusted third party). But the outsourcing scheme was limited to only one level. In [16], the author presented a hierarchical secret sharing scheme with the flexibility to divide participants into groups depending on their authority with a high computational cost. In Fig. 9, we explained the difference between our proposed OHSSS and the conventional OSSS in terms of throughput. We can see that our proposed scheme is better to secure compared to the traditional method.

On the contrary, in our proposed scheme, the protocol needs to be executed only once. The complex operations are sent to CSP, and the participant only has to run a small amount of verification and decryption. We can also use the add and delete algorithm proposed in [22] to add new participants to our scheme without changing the original secret. Furthermore, participants can be removed from the scheme in a case of transfer of land ownership right. Our scheme equally provides an interactive proof system for any verifier to verify that an authorized set of participant shares the secret without getting any information about the secret b_0.

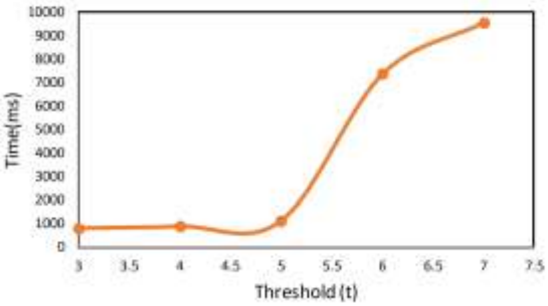

Fig. 4. Time taking by participant to Verify the Secret

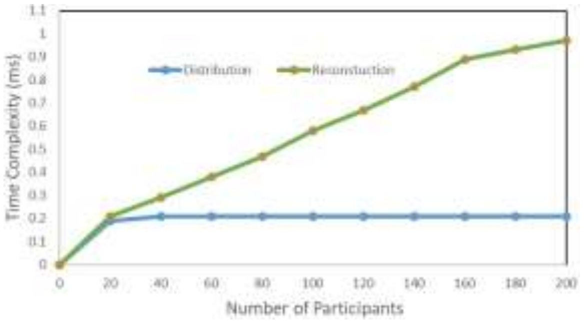

Fig. 5. Reconstruction Time Complexity Between our Proposed and Conventional Scheme with different file size.

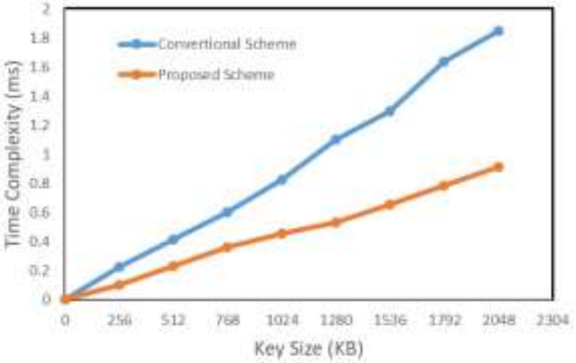

Fig. 6. Reconstruction and Distribution Time Complexity with Variable File Size.

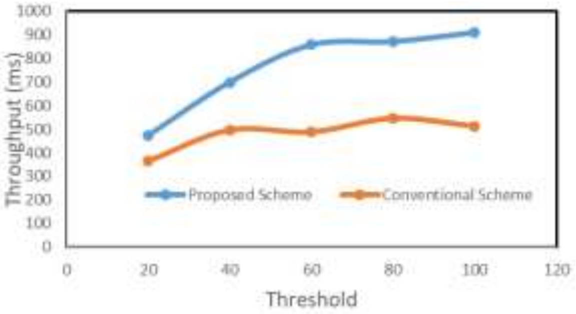

Fig. 7. Comparing Security level of OSSS and OHSSS

VI. CONCLUSION

Combining hierarchical threshold and outsourcing computation property, we propose an OHTSSS protocol base on homomorphism. This permits computationally weak participants to obtain the secret with only a small amount of operations. Simultaneously, expensive reconstruction and verification computation is outsourced to a CSP, and the CSP cannot learn anything about the secret. Participants can also be added or removed from the scheme using the add and delete algorithm without changing the original secret. Moreover, CSP and participants' malicious behavior can be accurately checked on time, and no multiple interactions are required between CSP and participants. In the second phase of this paper, a secure multi-Prover zero-knowledge argument was used to prove that all active participants actually shared the secret. Although our scheme has been proven to be more performant than the conventional method, the calculation investigated an increase of time complexity as the number of participants increases compared to the conventional method. The theoretical analysis of our proposed scheme demonstrated that Security requirements are satisfied. Also, our computer simulation results demonstrated that our scheme is more secure compare to the conventional scheme.

REFERENCES

[1] Kwon, Seong-Geun and Lee, Suk-Hwan and Kwon, Ki-Ryong and Lee, Eung-Joo and Ok, Soo-Yol and Bae, Sung-Ho, “Mobile 3D game contents watermarking based on buyer-seller” IEICE transactions on information and systems, Vol. 91, Number 7, pp. 2018–2026, 2008, The Institute of Electronics, Information and Communication Engineers.

[2] Gopalakrishnan, K and Memon, Nosir and Vora, Poorvi L “Protocols for watermark verification”, IEEE Multimedia, Vol. 8, Number 4, pp. 66–70, 2001.

[3] Ramkumar, Mahalingam and Akansu, Ali N ramkumar2004robust, “A robust protocol for proving ownership of multimedia content”, IEEE Transactions on Multimedia, Vol. 6, Number 3, pp. 469–478, 2004.

[4] Rial, Alfredo and Balasch, Josep and Preneel, “A privacy-preserving buyer–seller watermarking protocol based on priced oblivious transfer”, IEEE Transactions on Information Forensics and Security, Vol. 6, Number 1, pp. 202–212, 2010.

[6] Rial, Alfredo and Deng, Mina and Bianchi, Tiziano and Piva, Alessandro and Preneel, Bart, “A provably secure anonymous buyer–seller water-marking protocol”, IEEE Transactions on Information Forensics and Security, Vol. 5, Number 4, pp. 920–931, 2010.

[7] Li, Jin and Chen, Xiaofeng and Huang, Xinyi and Tang, Shaohua and Xi-ang, Yang and Hassan, Mohammad Mehedi and Alelaiwi, Abdulhameed, ”Secure distributed deduplication systems with improved reliability”, IEEE Transactions on Computers, Vol. 64, Number 12, pp. 3569–3579, 2015.

[8] He, Kun and Chen, Jing and Du, Ruiying and Wu, Qianhong and Xue, Guoliang and Zhang, Xiang, “Deypos: Deduplicatable dynamic proof of storage for multi-user environments”, IEEE Transactions on Computers, Vol. 65, Number 12, pp. 3631–3645, 2016.

[9] Yu, Chia-Mu and Chen, Chi-Yuan and Chao, Han-Chieh, “Proof of ownership in deduplicated cloud storage with mobile device efficiency”, IEEE Network Journal, Vol. 29, Number 2, pp. 51–55, 2015.

[10] mishra2018mpows, Mishra, Shivansh and Singh, Surjit and Ali, Syed Taqi, “MPoWS: merged proof of ownership and storage for block level deduplication in cloud storage”, 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–7, 2018.

[11] Jin, Xuexue and Wei, Lingbo and Yu, Mengke and Yu, Nenghai and Sun, Jinyun, “Anonymous deduplication of encrypted data with proof of ownership in cloud storage”, 2013 IEEE/CIC International Conference on Communications in China (ICCC), pp. 224–229, 2013.

[12] Benaloh, Josh Cohen, “Secret sharing homomorphisms: Keeping shares of a secret”, Conference on the Theory and Application of Cryptographic Techniques, pp. 251–260, 1986, Springer.

[13] D. R. Stinson and R. Wei, - Unconditionally secure proactive secret sharing scheme with combinatorial structures,” in International Workshop on Selected Areas in Cryptography. Springer, 1999, pp. 200-214.

[14] A. Herzberg. S. Jareckl. H. Krawczyk, and M. Yung, “Proactive secret sharing or: How to cope with perpetual leakage”, in

Annual International Cryptology Conference. Springer, 1995; pp. 339 352.

[15] O. Farras and C. Padris, "Ideal hierarchical secret sharing schemes", IEEE transactions on information theory, Vol. 58, No. 5, pp. 3273 3286; 2012.

[16] T. Tassa, "Hierarchical threshold secret sharing", Journal of cryptology, Vol. 20, No. 2, pp. 237-264, 2007.

[17] N. Paknist, M. Noroazi. and Z Esiami, "Distributed key generation protocol with hierarchical threshold access structure", IET Information Security, Vol. 9, No. 4, pp. 248-255, 2015.

[18] Pilaram, Hossein and Eghlidos, Taraneh, "An efficient lattice based multi-stage secret sharing scheme", IEEE Transactions on Dependable and Secure Computing, Vol. 14, No.1, pp. 2-8, 2015.

[19] P. Feldman, "A practical scheme for non-interactive verifiable secret. sharing", 28th Annual Symposium on Foundations of Computer Science 19877. IEEE, 1987, pp. 427438.

[20] I. P. Pedersen, "Non-Interactive and information-Theoretic secure verifiable secret sharing." Annual international cryptology conference, Springer, 1991, pp. 129-140.

[21] J. Benaloh and I. Leichter, "Generalized secret sharing and monotons. functions", in Conference on the Theory and Application of Cnptogra. phy. Springer, 1988; pp. 27-35.

[22] G. Traverso, D. Demirel, and Buchmann, "Dynamic and verifiable hierarchical secret sharing", International Conference on Information Theoretic Security. Springer, 2016.

[23] M. Nojoumian and D. R. Stinson, "On dealer-free dynamic threshold schemes", Advances in Mathematics of Communications, Vol. 7, No. 1, 2013.

[24] C. Tang and Z.-a. Yao, "Definition and construction of multi-prover zero-knowledge argument", in 2009 WRI International Conference on Communications and Mobile Computing, Vol. 3, IEEE, 2009, pp. 375–379.

[25] L. Lu, J. Han, Y. Liu, L. Hu, J.-P. Huai, L. Ni, and J. Ma, "Pseudo trust: Zero-knowledge authentication in anonymous p2ps", IEEE Transactions on Parallel and Distributed Systems, Vol. 19, No. 10, pp. 1325–1337, 2008.

[26] M. Shoaran and A. Thomo, "Zero-knowledge-private counting of group triangles in social networks," The Computer Journal, Vol. 60, No. 1, pp. 126–134, 2017.

[27] D. Saha and S. Sur-Kolay, "Secure public verification of ip marks in fpga design through a zero-knowledge protocol", IEEE transactions on very large scale integration (VLSI) systems, Vol. 20, No. 10, pp. 1749–1757, 2011.

[28] Rasheed, Amar A and Mahapatra, Rabi N and Hamza-Lup, Felix G., "Adaptive group-based zero knowledge proof authentication protocol in vehicular ad hoc networks", IEEE Transactions on Intelligent Transportation Systems, 2019.

[29] Goldreich, Oded, "Foundations of cryptography: volume 2, basic appli-cations", 2009, Cambridge university press.

[30] Cramer, Ronald and Damgard, Ivan and Dziembowski, Stefan and Hirt, Martin and Rabin, Tal, "Efficient multiparty computations secure against an adaptive adversary", International Conference on the Theory and Applications of Cryptographic Techniques, pp. 311–326, 1999, Springer.

[31] Rabin, T, "Verifiable secret sharing and multiparty protocols with honest majority", J. ACM, Vol. 41, No. 6, pp. 1089–1109, 1994.

[32] Beerliova-Trubiniova, Zuzana and Hirt, Martin, "Efficient multi-party computation with dispute control", Theory of Cryptography Conference, p 305–328, 2006, Springer.

[33] Choudhury, Ashish and Patra, Arpita, "An efficient framework for unconditionally secure multiparty computation", IEEE Transactions on Information Theory, Vol. 63, No 1, p 428–468, 2016, IEEE.

[34] E. Zhang, I. Peng. and M. Li, "Outsourcing secret sharing scheme based on homomorphism encryption", IET Information Security, Vol. 12, No. 1, pp. 94-99, 2017.

[35] Agwa, Ngye Antoinette and Kobayashi, Takumi and Sugimoto, Chika and Kohno, Ryuji, "Security of Patient's Privacy in E-Health using Secret Sharing and Homomorphism Encryption Scheme", 35th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), pp 155–160, 2020, IEEE.

[36] Albrecht, Martin R and Player, Rachel and Scott, Sam, "On the concrete hardness of learning with errors", Journal of Mathematical Cryptology, Vol. 9, No. 3, pp 169–203, 2015, De Gruyter.

[37] Cheon, Jung Hee and Kim, Dongwoo and Kim, Duhyeong and Lee, Hun Hee and Lee, Keewoo, "Numerical method for comparison on homomorphically encrypted numbers", International Conference on the Theory and Application of Cryptology and Information Security, pp 415– 445, 2019, Springer.

[38] Harn, Lein and Lin, Changlu and Li, Yong, "Fair secret reconstruction in (t, n) secret sharing", Journal of Information Security and Applications, Vol. 23, pp 1–7, 2015, Elsevier.

Ngye Antoinette Agwa received a bachelor's and master's degree in Information and communication technology from the Department of Telecommunication, Information and Communication Technology (TICT), Faculty of Industrial Engineering, University of Douala, Cameroon, in 2012 and 2014 respectively. Since 2018, Antoinette has been a Ph.D. student in the Graduate School of Engineering Science, Yokohama National University, Japan. Since 2017, Antoinette has been an Assistant Lecturer with the Department of Computer Engineering, Faculty of Engineering and Technology, University of Buea, Cameroon. Her research areas of interest are cryptography, Geography information Security Ultra Wide Band, and Global Navigation Satellite System. Since 2020, she has been a student member of IEICE.

Takumi Kobayashi received the B.S. and M.S. degrees in Engineering from Musashi Institute of Technology in 2011 and Tokyo City University in 2013 respectively. Kobayashi received Ph.D degree in Engineering from Yokohama National University in 2016. Currently, Kobayashi is working with the Graduate School of Science and Engineering in Yokohama National University. His research interest includes UWB communications, medical information communication technology and human body communication. Dr. is a member of IEICE and IEEE EMBS, and a member of JSMBE.

Chika Sugimoto (M'11) received the B.S. degree in engineering the M.S. and Ph.D. degrees in environment from the University of Tokyo. From 2006 to 2010, Chika was an Assistant Professor with the Graduate School of Frontier Sciences, University of Tokyo. Since 2010, she has been an Associate Professor with the Faculty of Engineering, Yokohama National University. She is a member of IEICE and IEEE EMBS.

Ryuji Kohno Ryuji Kohno (F'12) received the Ph.D. degree from the Dept. Elec. Eng., University of Tokyo in 1984. Since 1998, he has been a Professor with Yokohama National Univ. From 1984 to 1985, he was a Visiting Scientist in the Dept. Elec. Eng., Univ. of Toronto. Since 2007, he has been a Finnish Distinguished Professor with the Univ. of Oulu, Finland. He was also a Director with Sony CSL/ATL during 1998- 2002, a Director with the UWB Technical Institute, and a program coordinator with the Medical ICT Institute of the NICT during 2002-2011. Since 2012, he has been the CEO with the Univ. of Oulu Research Institute Japan - CWC-Nippon Inc. Ltd. He was a Principal Leader of MEXT 21st century and Global COE programs during 2002-2007 and 2008-2013, respectively. Since 2003, he has been a Director with the Medical ICT Center, YNU. Since 2006, he has also been an Associate Member of the Science Council of Japan. He is IEICE and IEEE Fellows. He was elected a BoG Member of the IEEE Information Theory Society in 2000, 2002, and 2006. He received the IEICE Greatest Contribution Award and NTT DoCoMo Mobile Science Award in 1999 and 2002, respectively.