International Journal of Science Engineering and Advance Technology, ISSN 2321-6905 IJSEAT, Vol. 3, Issue 12

December-2015



International Journal of Science Engineering and Advance Technology

Privacy Preservation and traceability support using Public Auditing Mechanism

JayanthiAnusha¹, K.LakshmiPriya²

¹PG Scholar, Pydah College of Engineering, Kakinada, AP, India, ²Assistant Professor, Pydah College of Engineering, Kakinada, AP, India. E-mail: anusha.jayanthi24@gmail.com.

Abstract— as future enhancement, we enhance the Oruta system in two interesting problems we will continue the study for our future work. One of them is traceability, which means the ability for the group manager (i.e., the original user) to reveal the identity of the signer based on verification metadata in some special situations. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information to identity the privacy to public verifiers. Since Oruta is based on the ring signatures, where the identity of the signer is unconditionally protected, the current design of ours does not support traceability. To the best of our knowledge, designing an efficient public auditing mechanism with the capabilities of preserving identity privacy and supporting traceability is still open. Another problem for our future work is how to prove data freshness (prove the cloud possesses the latest version of shared data) while still preserving identity privacy. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

Key words: Public auditing, privacy-preserving, cloud computing, shared data, TPA (third party auditor).

I. Introduction

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. Many mechanisms have been proposed to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing. In these mechanisms, data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking. A public verifier

could be a data user (e.g., researcher) who would like to utilize the owner's data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking services. Moving a step forward, Wang et al. designed an advanced auditing mechanism .so that during public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers. Unfortunately, current public auditing solutions mentioned above only focus on personal data in the cloud.

Protect these confidential information is essential and critical to preserve identity privacy from public verifiers during public auditing. In this paper, to solve the above privacy issue on shared data, we propose Oruta, a novel privacy-preserving public auditing mechanism. More specifically, we utilize ring signatures to construct homomorphism authenticators in Oruta, so that a public verifier is able to verify the integrity of shared data without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier. In addition, we further extend our mechanism to support batch auditing, which can perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks. Meanwhile, Oruta is compatible with random masking, which has been utilized in WWRL and can preserve data privacy from public verifiers. Moreover, we also leverage index hash tables from a previous public auditing solution to support dynamic data. A high-level comparison among Oruta and existing mechanisms is presented.

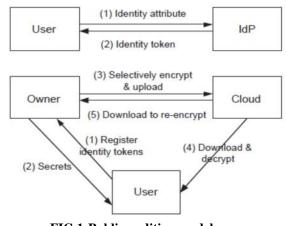


FIG 1:Public auditing model

II. RELATED WORK

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. We exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity. In this talk, I will first discuss a number of pressing security challenges in Cloud Computing, including data service outsourcing security and secure computation outsourcing. Then, I will focus on data storage security in Cloud Computing. As one of the primitive services, cloud storage allows data owners to outsource their data to cloud for its appealing benefits. However, the fact that owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging. In this talk, I will present our recent research efforts towards storage outsourcing security in cloud computing and describe both our technical approaches and security & performance evaluations. Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the ondemand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed.

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphism authenticator with random masking to

achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

III.DESIGN OBJECTIVES

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2.It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

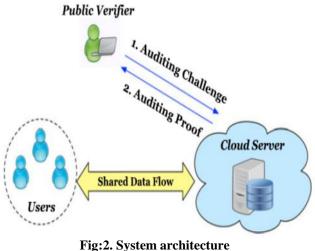


Fig:2. System architecture SYSTEM PREMERILIERS

Cloud server

- ✓ In the first module, we design our system with Cloud Server, where the datas are stored globally. Our mechanism, Oruta, should be designed to achieve following properties:
- ✓ (1) Public Auditing: A public verifier is able to publicly verify the integrity of shared data without retrieving the entire data from the cloud.
- (2) Correctness: A public verifier is able to correctly verify shared data integrity.

- ✓ (3) Unforgeability: Only a user in the group can generate valid verification metadata (i.e., signatures) on shared data.
- ✓ (4) Identity Privacy: A public verifier cannot distinguish the identity of the signer on each block in shared data during the process of auditing.

Group of users

- ✓ There are two types of users in a group: the original user and a number of group users. The original user initially creates shared data in the cloud, and shares it with group users. Both the original user and group users are members of the group. Every member of the group is allowed to access and modify shared data. Shared data and its verification metadata (i.e., signatures) are both stored in the cloud server. A public verifier, such as a thirdparty auditor providing expert data auditing services or a data user outside the group intending to utilize shared data stored in the cloud server.
- ✓ Owner Registration: In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database.
- ✓ Owner Login: In this module, owner have to login, they should login by giving their email id and password.
- ✓ User Registration: In this module if a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.
- ✓ User Login: If the user is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading.

Public verifier

- ✓ When a public verifier wishes to check the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the Cloud server responds to the public verifier with an auditing proof of the possession of shared data.
- ✓ Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof. Essentially, the process of public auditing is a challenge and- response protocol between a public verifier and the cloud server

Auditing Module

✓ In this module, if a third party auditor TPA (maintainer of clouds) should register first. This system allows only cloud service providers. After third party auditor gets logged in, He/ She can see how many data owners have uploaded their files into the cloud. Here we are providing TPA for maintaining clouds.

- ✓ We only consider how to audit the integrity of shared data in the cloud with *static groups*. It means the group is pre-defined before shared data is created in the cloud and the membership of users in the group is not changed during data sharing.
- ✓ The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud. Another interesting problem is how to audit the integrity of shared data in the cloud with *dynamic groups* — a new user can be added into the group and an existing group member can be revoked during data sharing — while still preserving identity privacy.

IV.PROPOSED SYSTEM

- In this paper, to solve the above privacy issue on shared data, we propose Oruta, a novel privacypreserving public auditing mechanism.
- More specifically, we utilize ring signatures to construct homomorphic authenticators in Oruta, so that a public verifier is able to verify the integrity of shared data without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier.
- In addition, we further extend our mechanism to support batch auditing, which can perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks.
- Meanwhile, Oruta is compatible with random masking, which has been utilized in WWRL and can preserve data privacy from public verifiers. Moreover, we also leverage index hash tables from a previous public auditing solution to support dynamic data. A high-level comparison among Oruta and existing mechanisms is presented.

USER REGISTRATION

If a user wants to access the data which isstored in a cloud, he/she should register theirfirst. These details are maintained in a Database.

USER LOGIN

If the user is an authorized user, he/she candownload the file which has been stored by dataowner. The user can modify the data by threedifferent types of operations they are i. insert

- ii. Delete
- iii. update

1. INSERT

The user m joins to theshared data. He/she inserts a new block computes the new cloudserver. For the rest of the block, the identifiers of these blocks are not changed.

Identifier of the inserted block m j and then uploads to the total number of the block in the shared data increases to n+1.

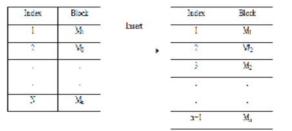


Table 1 inserting a new data block

2. DELETE

The user deletes block mj, its identifier idjfrom the cloud server. The identifier and content of other blocks in shared data are remaining the same. The total number of blocks in the shared datadecreases to n-1. For deletion operation the user don'twant to compute new identifier.

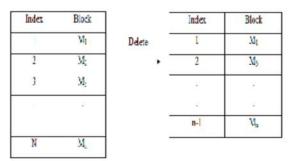


 Table 2 deleting a data block

3. UPDATE

The user updates the j-th block in the shareddata with the new block m j. The new identifier of this block is updated and the identifier of the othershared data is not updated. The total number of blocks in shared data id still n.

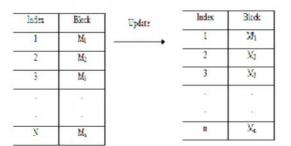


Table 3 updating a data block

PARTY AUDITOR THIRD PARTY AUDITOR REGISTRATION

The third party auditor (maintainer of clouds)wants to do some cloud offer; they should registerfirst, to do auditing on the cloud data.

THIRD PARTY AUDITOR LOGIN

After third party auditor gets logged in, He/she can see how many data owners have uploaded their files into the cloud and who are the user send anauditing request. The third party auditor the audit the data if any modifications are made then the public verifier send a report to the data owner with theoriginal data and the modified data.

RESULTS

SCREEN SHOTS

Member Registration	Image: Description I	etherer 🔒	egant Tank 🖗 ng 🖞 pap	• { • 5 • 6 • 0 • 1	II talent SR Bernel	erono devento	Latwis 🗌 de 🖬 de cannag		
	Image: Description I								
	Image: Description I								
	Image: Description I								
	Image: Description I								
Province - Province - Scraft BUGARGY TO ANT Crancella McCrifet. Traine Prodomer Province	Province Pro			Me	mber Regis	stration			
Province - Province - Scraft BUGARGY TO ANT Crancella McCrifet. Traine Prodomer Province	Province Pro			1000	1				
V Data-Habitani (Per di paro il 20 di 100 CM C) Mala di India. C'anteri A dendo (Per di paro il 20 di 100 CM C) Mala di India.	V Dane de po Dane : Pour de pour de pour de la se de la contra de la			LEMIN	NE 12				
V Excel De land Version Versio	V Dane-Hankvela: "There winneder:, "Constitutions." (Constitutions of the second states of th			Passia					
V Excel De land Version Versio	Canada Maria				0	2			
Creace Re: MAZINGA. Code Company Creace Re: MAZINGA. Code Code Code Code Code Code Code Code	V Danselskavels Dien effender, Diefertinger, Tenel Dansel in Australian (Die effender, Diefertinger, Tenel Deren in + basis kongestant, Diefertinger, Diefertinger, Diefertinger, Bistering Deren in + basis kongestant, Diefertinger, Die im Bistering Biste			(root)	-2:4(1)	-			
There Paradonery There Parado	Huma Pordstrate Huma Pordstrate Providence Providen			5.0	pletergana	.0017			
There Paradonery There Parado	Huma Pordstrate Huma Pordstrate Providence Providen			1.000	an anna anna				
2/1 Disputed Text 2/1 Disputed Disputed Text 2/1 Disputed Disputed Disputed 2/1 Disputed Disputed Disputed 2/1 Disputed Disputed Disputed 2/1 Disputed Disputed Disputed 2/2 Disputed Disputed Disputed 2/2 Disputed Disputed Disputed 2/2 Disputed Disputed Disputed Disputed 2/2 Disputed Disputed Disputed Disputed 2/2 Disputed Disputed Disputed Disputed	Propriet Frant Propriet Provide Propriet Provide Propriet Provide Provide			1.00					
2 ² ¹ ² Standbollow ² The Mindee ² CONSTRUCT. ² Distant Andres ¹ ² Status of the ² 1 States for the ² 2 States for the ² 2 States for the ² 2 States ² Stat	Image: State State State Image: State State State Image: State State State Image: State State Image: State State Image: State Image			3	Hare: Pondcherry				
2 ² ¹ ² Standbollow ² The Mindee ² CONSTRUCT. ² Distant Andres ¹ ² Status of the ² 1 States for the ² 2 States for the ² 2 States for the ² 2 States ² Stat	Image: State State State Image: State State State Image: State State State Image: State State Image: State State Image: State Image				5h5				
2 ² ¹ ² Standbollow ² The Mindee ² CONSTRUCT. ² Distant Andres ¹ ² Status of the ² 1 States for the ² 2 States for the ² 2 States for the ² 2 States ² Stat	Image: State State State Image: State State State Image: State State State Image: State State Image: State State Image: State Image			1		-			
n (Sound (ad (a) antices = a facto Sound states)	or jonno (ak pa jonno, z = 2 kasta Sangarban) @One 4 ↓ Onzola za 1 (ak pa 5 zen 2 ze 2 ze 0 (f 0 m) hang 17 kang Strang, 17 data) to 0 2 zen de Done. 0 m				Distance .	Peest			
n (Sound (ad (a) antices = a facto Sound states)	or jonno (ak pa jonno, z = 2 kasta Sangarban) @One 4 ↓ Onzola za 1 (ak pa 5 zen 2 ze 2 ze 0 (f 0 m) hang 17 kang Strang, 17 data) to 0 2 zen de Done. 0 m								
n (Sound (ad (a) antices = a facto Sound states)	or jonno (ak pa jonno, z = 2 kasta Sangarban) @One 4 ↓ Onzola za 1 (ak pa 5 zen 2 ze 2 ze 0 (f 0 m) hang 17 kang Strang, 17 data) to 0 2 zen de Done. 0 m								
n (Sound (ad (a) antices = a facto Sound states)	or jonno (ak pa jonno, z = 2 kasta Sangarban) @One 4 ↓ Onzola za 1 (ak pa 5 zen 2 ze 2 ze 0 (f 0 m) hang 17 kang Strang, 17 data) to 0 2 zen de Done. 0 m								
n (Sound (ad (a) antices = a facto Sound states)	or jonno (ak pa jonno, z = 2 kasta Sangarban) @One 4 ↓ Onzola za 1 (ak pa 5 zen 2 ze 2 ze 0 (f 0 m) hang 17 kang Strang, 17 data) to 0 2 zen de Done. 0 m								
prezen a a destri stangaristan V Com Allingen merer, David mei Ren 5 gen 2 st. 8 st. 0 st. 0 st. 1 stang 20 stang dirente, St. André Ten () standardate. () st.	(paran =) =) had to damp arten i se generation i se genera	06	gaantakaa 👔	bloc principe. 🍅 CPV	11100.00 - 180	LW Notice 1.	NATION PICTS - Nat.		R.ØS
prezen a a destri stangaristan V Com Allingen merer, David mei Ren 5 gen 2 st. 8 st. 0 st. 0 st. 1 stang 20 stang dirente, St. André Ten () standardate. () st.	(paran =) =) had to damp arten i se generation i se genera	07.1	8 czastowa 👔	No. prizozac. 🌘 CP	ettocat 🌒 o	Lin Meneri 🖓	NUBLACTS No.		1.05
NATING TO COMPANY AND A DESCRIPTION OF A	contraus C () - con P () () = C () P () () P () () () P () () () P () () P () () P () () P () () () P () () () P () () P () () () P () () () () () () () () () () () () ()			Her arfantast. Distan	ertocat 🌾	Link forderer 1	20120-005-40-		Rø2
nenze, 📴 ha bil 🗌 nen 🛱 po 🖏 sente 🖏 sta 🛱 so 🛛 ne 🔘 so 🦉 kalans 🗟 nakons Sil landas, 🚅 dandi 🗛 densta 🗌 tra 📑 sol 🗃 sol hake Battare . 🗐 n	Lonester, 🗋 ho M 🦳 and 🛱 par 🖞 searer 🎗 sto 🖨 sto 🖉 at 🔕 sto G at 🔕 sto Lanes Sciences, 🥔 danad Sciences, 🥥 danad A Alexate 🗌 bat 🔂 Sciences Decision, 🗒 K	gan guinais	Del 195		erreocae 🛛 🌒 o	LN Neter 1 2	50150 PC15 - %0		t e s
		gan guinais	Del 195		1710-04. (Ø0	La retor () 2	59.50(9C15-%).		1.02
Lagrad Brick	Cogne Bird	gar Bórais Garaica A	Del 195		итгосак. (9 о к 4	LN Neberl 2			
Logout Back	Cogue and	par (póraio Spraices - 4 408-09/14 pr	Dok tels I Rech Fie Rompord Bar	E X E Oda	× +		- C 💽 - Gauge	P	
		par (póraio Spraices - 4 408-09/14 pr	Dok tels I Rech Fie Rompord Bar	E X E Oda	× +		- C 💽 - Gauge	P	
		orr Dorato Opration 4 (OR.D) Lagan Oberaty .	Del 1951 A Sect Pa Barry or Da No Of Cont Plans (Came	E X E Oda	× +		- C 💽 - Gauge	P	
		ina (Lokario Constanti I Constanti I Colemati I - 🖓	Del 1951 A Sect Pa Barry or Da No Of Cont Plans (Came	E X E Oda	× +		- C 💽 - Gauge	P	
	User Id File Name Group Status Date	ina (Lokario Constanti I Constanti I Colemati I - 🖓	Del 1951 A Sect Pa Barry or Da No Of Cont Pages (1 per	E X E Oda	× +		- C 💽 - Gauge	P	
User Id Ele Name Group Status Date		or Johann Grai cai i Geologiag ar	Deb tens a Deces Te Deces you have Te child new (P are 12 source and Back	n 2 x 5 0 m 6 x	x 👌	ddDenis. 🕫 denil a	= C Coope A debata - Tan - C 334-Galee Diroc	P	
User Id File Name Group Status Date		or policie or to ing at conto ing at	Dek ten a Des Fielden gesta seut on Par Saun at Brits User Id	n 2 m ∎ ns Ont Om File Name	× to the second	dioreis. Ødrei 1	= c)	P	
wan get tut Ginge Underse 2014-01-12-12-2017		or policies of the policies of the policies	Del gas a Dechra Borg of Le Not of Mark Place 15 seen of Back User Id 150	n 1 geona n 1 ge ∎ ne One One File Name gentar	K Landons 22 naturel Group Doug	ddonnis, Ørtendt a Status Wristed	n o i i - case A teres i i se i se ote doc Date 20(+-2)-11 12 2019	P	
Value Optimal Optimal 2014-03-01 of 2018 instampathy material Social Upmat 2016-03-01 of 2018	matanapatry material brook to the second tot	or policies of the policies of the policies	Lok yes a best for Sound the total own Plane Sound of Back User Id sale materiapitity	n 2 oc a oc Orr O oc File Name gatar nesse in	x y Il Indexes 22 national Group Group Group Stronge	ddonnis, et senda , Status Uptariad Ignad	n C - Comp A cardon - Tor C - State Andrea Data State - State - State State - State - State State - State - State	P	
Name Spit.ht Only: Underset Spit.ht Diright indexquery maximum lint Singlitz Uptimal Spit.ht Spit.ht indexquery maximum lint Singlitz Uptimal Spit.ht Spit.ht indexquery maximum lint Singlitz Uptimal Spit.ht Spit.ht	Specific	or policies of the policies of the policies	Det tots Post tots tots Post Post Post of Low tots Post User Id user Id user Id user Id	File Name gata	K L I industry 52 naturel Group Distas Stroig2 Distas	Status Status Voisier Ligned	n co i an composition de la co	P	
same -get tot Owage ingeneration instanceship masses int Google Upper States int is 13 0001 instanceship masses int Google Upper States int is 13 0001 instanceship masses int Google Upper States int is 13 0001 instanceship States int is 10 001 States int is 13 001 States int is 13 001 instanceship States int is 10 001 States int is 13 001 States int is 13 001 instanceship States int is 10 001 States int is 13 001 States int is 13 001	Instançary Instant Doug2 Lightst 2000 12 K 15 0013 Instançary micro (r) Doug2 Iprat 30702 (r) 30702 (r) Instançary micro (r) Doug2 Iprat 30702 (r) 30702 (r) Instançary micro (r) Doug2 Doug2 Doug2 3010-12 (r) 31118	or policies of the policies of the policies	D4 gas a bash a Borg of La Net Tree Prov 5 part Net Tree Prov	File Name	Group Group Group Group Group Group	Status Status water lanal Sovercal	Date	P	
Name Statistic Oraștic Undersite Statistici Statistici nataregadary nasarea înt Statistic Statistici <	instançalory material in Souge Lignal Effect 12 Bits instructivy meterial Gen42 Supral Strik-12-01 11 Dits instructivy meterial Voyal Devendor Strik-12-01 11 Dits	er johene pelon i Okolinger beerete - 😰	Deb tes + Post his Bory of be tout - mil (Pare 5 and tout - mil (Pare 5 and	File Name gt to name in mane in mane in	Group Ones Single Single Ones Single Ones Single	dowe. Reeds Status warns upped upped bywnod bywnod bywnod	2 0 () - Soup Loose Tief () an George Date RE-2-2-2 at 250 RE-2-2 at 250 RE-2-2 at 120 RE-2-2 at 120 RE-2-2 RE-2-	P	
Non Statut Oragi Underset 2014-01-01.02 (2015) instrugativy mases int Sougi2 Uptual 2014-01-01.02 (2015) instrugativy mases int Sougi2 Uptual 2014-01-01.02 (2015) instrugativy mases int Sougi2 Uptual 2014-01-01.01 (2015) instrugativy mases int Sougi2 Upward 2014-01-01.01 (2014) instrugativy mases int Uptual 2014-01-01.01 (2014) 2014-01-01.01 (2014) instrugativy mases int Uptual Downald 2014-01-01.01 (2014) 2014-01-01.01 (2014) instrugativy mases int Uptual Downald 2014-01-01.01 (2014) 2014-01-01.01 (2014) instrugativy mases int Sougi2 Ownald 2014-01-01.01 (2014) 2014-01-01.01 (2014)	Instançaby Instanç	er johene pelon i Okolinger beerete - 😰	Det es • Des fois de que de se reur l'est Place d'anne • Back User Id • Stanpathy • Astronomy • Astronomy • Astronomy • Astronomy • Astronomy	File Name gt.tat rest are one ora gt.tat restriction restriction restriction	Group Ones Sixe Sixe Sixe Sixe Sixe Sixe Sixe Sixe	Status Status water uposi u u u u u u u u u u u u u u u u u u u	Date Date Date mercedu arrow ac	P	
Name Optimiz O	instruction Sought Lighted Effect of 64: 63 MBB instruction memory in Develop Lighted Effect of 64: 63 MBB instruction memory in Develop Lighted Effect of 64: 63 MBB instruction memory in Develop Develop Effect of 64: 63 MBB instruction memory in Develop Develop Effect of 64: 63 MBB instruction Develop Develop Develop Effect of 64: 63 MBB instruction Develop Develop Develop Effect of 64: 63 MBB instruction Develop Develop Develop Effect of 64: 63 MBB instruction Develop Develop Develop Effect of 64: 63 MBB instruction Develop Develop Develop Effect of 64: 63 MBB instruction Develop Develop Effect of 64: 63 MBB Effect of 64: 64: 64: 64: 64: 64: 64: 64: 64: 64:	er johene pelon i Okolinger beerete - 😰	tet so * Board Board Same we not the first Same User Id was missipary missipary missipary missipary missipary	File Name 2 to 2 no 0 n 0 to 20104 ream in ream in ream in ream in	Group Ones Ones Ones Ones Ones Ones Ones Ones	dórete. Revel a Status outrad uposi bornod ouers uponi bornod ouers uponi	Collectory Control Cont	P	
Name Statistic Oraștic Understat Zalendi - Cale da Statistic Instanțative Instanțative Statistic Statistic Statistic Statistic Instanțative Instanțative Statistic Statistic Statistic Statistic Statistic Instanțative Instanțative Statistic	extension masses int Sought Lighted 2004 bit 10 800 bit extractivey memory in Sought State 4 State 40 bit State 40 bit extractivey memory in Sought State 40 bit State 40 bit State 40 bit extractivey memory in State 40 bit State 40 bit State 40 bit State 40 bit extractivey memory in State 40 bit State 40 bit State 40 bit State 40 bit extractivey memory in State 40 bit State 40 bit State 40 bit State 40 bit extractivey memory in State 40 bit State 40 bit State 40 bit State 40 bit extractivey memory in State 40 bit State 40 bit State 40 bit State 40 bit extractivey memory in State 40 bit State 40 bit State 40 bit State 40 bit extractive memory in State 40 bit	or Johnson Generation I Generation I	Let us The Dark Story of the set of the Story of the User Id user story of the story of the s	File Name grifer south of the second of the second file research research research research	Coup Group Orac Orac Orac Orac Orac Orac Orac Orac	Status Status ustina ustina ustina ustina tourna tourna tourna ustina ustina ustina ustina	Date Date Date Re-production Re- Re- Re- Re- Re- Re- Re- Re- Re- Re-	P	
each gift M Grapp (spland) 22(1)-(1)-(1) (2) (2) (3) indiangulary income Int Grapp (spland) 22(1)-(1)-(1) (2) (3) indiangulary income Int Grapp (spland) 22(1)-(1)-(1) (2) (3) indiangulary income Int Grapp (spland) 22(1)-(1)-(1) (2) (3) indiangulary income Int Grapp (spland) (spland) (spland) indiangulary income Int Grapp (spland) (spland) (spland) (spland) indiangulary income Int Grapp (spland) 22(in-(1)-(1) (2) (3) (spland) indiangulary income Int Grapp (spland) 22(in-(1)-(1) (2) (3) (spland) indiangulary income Int Grapp (spland) 22(in-(1)-(1) (2) (3) (spland) indiangulary income Int Grapp (spland) 22(in-(1)-(1) (2) (3) (spland) indiangulary income Int Grapp (spland) (spland) 22(in-(1)-(1) (2) (3) indidre memme Int	instangatory masses int Doug2 Lightal 2004 12 66 12 5015 instrugently messes int Grad 2 Signal 4 2014-12 66 12 5015 instrugently messes int Grad 2 Signal 4 2014-12 66 12 5015 instrugently messes int Grad 2 Signal 4 2014-12 66 12 5015 instrugently messes int Grad 2 Signal 4 2014-12 66 12 5015 instrugently messes int Grad 2 Signal 4 2014-12 66 12 6015 instrugently messes int Grad 2 Signal 4 2014-12 66 12 6017 instrugently messes int Grad 2 Signal 4 2014-12 66 12 6017 instrugently messes int Grad 2 Signal 4 2014-12 66 12 6017 instrugently messes int Grad 2 Signal 4 2014-12 66 12 6017 instrugently messes int Grad 2 Signal 4 2014-12 66 12 6017 instrugently messes int Grad 2 Signal 4 2014-12 66 12 6017 instrugently messes int Grad 2	er johene pelon i Okolinger beerete - 😰	Let us The Exist Status and a The Exist Status and a The Exist Status and a User Id Status Statu	File Name Stars in concernation	Croup Croup Dass Singe Singe Sin Sin Sin Singe Singe Singe Sin Singe S	Status Status Ustina Ismai Dovical Coarsi Island Ustina Dovical	Date Date Date Merch Date Merch Date Merch Date Merch Date Merch Date Merch Date Merch Date Merch Date Merch Date Merch Date	P	
Name Capital Only: Values 2214-0-1-312.20.3% Instanceshy Names in Social Update 2214-0-1-312.20.3% Instanceshy Names in Social Update 2214-0-1-312.20.3% Instanceshy Social Social 2014-0-1-0-312.20.3% Instanceshy Social Social 2014-0-1-0-312.20.3% Instanceshy Instanceshi Social 2014-0-1-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-1-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-0-312.20.3% Instanceshi Social Social-0-0-0-312.20.3% 2014-0-0-0-312.2	exclusion/party masses int Sought Lighted Effect bit 64:10 mith instructions memory in Sought Statute Statute Statute instructions memory in Statute Statute Statute Statute Statute instructions memory in Statute Statute Statute Statute Statute instructions memory in Statute Statute Statute Statute instructions memory in Statute Statute Statute Statute instructions memory in Statute Statute Statute Statute instructions Statute	or Johnson Generation I Generation I	Let us The Data Science of the Science of the Science of the Science of the Science of the Science of the Science of the Science of the Science of the Scie	File Name	Group Group Cost Cost Cost Cost Cost Cost Cost Cost	Status Status outros operat operat operat operat operat operat operat operat operat operat	• • • ■ • • • • • • • • • • • • • • • •	P	
each gift M Grapp (spland) 22(1)-(1)-(1) (2) (2) (3) indiangulary income Int Grapp (spland) 22(1)-(1)-(1) (2) (3) indiangulary income Int Grapp (spland) 22(1)-(1)-(1) (2) (3) indiangulary income Int Grapp (spland) 22(1)-(1)-(1) (2) (3) indiangulary income Int Grapp (spland) (spland) (spland) indiangulary income Int Grapp (spland) (spland) (spland) (spland) indiangulary income Int Grapp (spland) 22(in-(1)-(1) (2) (3) (spland) indiangulary income Int Grapp (spland) 22(in-(1)-(1) (2) (3) (spland) indiangulary income Int Grapp (spland) 22(in-(1)-(1) (2) (3) (spland) indiangulary income Int Grapp (spland) 22(in-(1)-(1) (2) (3) (spland) indiangulary income Int Grapp (spland) (spland) 22(in-(1)-(1) (2) (3) indidre memme Int	inducipative masses int Sought Light all Effect 15 861 1985 instructive memory in Sought Light all Statuta 26 41 1985 instructive memory in Sought Light all Statuta 26 41 1985 instructive memory in Sought Light all Statuta 26 41 1985 instructive memory in Sought Descend Statuta 26 41 1987 instructive memory in Sought Descend Statuta 26 41 1987 instructive memory in Sought Descend Statuta 26 41 1987 instructive memory in Sought Descend Statuta 26 41 1987 instructive memory in Sought Descend Statuta 26 41 1987 instructive memory in Sought Descend Statuta 26 41 1987 instructive memory in Sought Descend Statuta 26 41 1981 instructive Sought Sought Descend Statuta 26 41 1981 instructive Sought Descend Statuta 26 41 1981	ina (Lokario Constanti I Constanti I Colemati I - 🖓	Let us The Data Science of the Science of the Science of the Science of the Science of the Science of the Science of the Science of the Science of the Scie	File Name	Group Group Cost Cost Cost Cost Cost Cost Cost Cost	Status Status outros operat operat operat operat operat operat operat operat operat operat	• 0 () • • • • • • • • • • • • • • • • • • •	P	
		or policies on the part of the state of the	Dek ten a Des Fielden gesta seut on Par Saun at Brits User Id	n 2 m ∎ ns Ont Om File Name	× to the second	dioreis. Ødrei 1	= c)	P	
wan get.tut Goupt Wetster 2014-04-18-18-26-28		n Directo Al Contactor Al Conta	Del gas a Dechra Borg of Le Not of Mark Place 15 seen of Back User Id 150	n s €oos n £oos ∎oo Ore Oos File Name gatar	K Landons 22 naturel Group Doug	ddonnis, Ørtendt a Status Wristed	n o i i - case A teres i i se i se ote doc Date 20(+-2)-11 12 2019	P	
Value QULLINI QULLINI QULLINI 2014-03-03 all 20-09 materiaphity materiaphity Society Society Society	matempathy meanwrith finolog lighted 2014-12-56-12-5612	r Lokais A.Diagan Hentr - Q	Lok yes a best for Sound the total own Providence of Back User Id sale materiapitity	n 2 oc a oc Orr O oc File Name gatar nesse in	x y Il Indexes 22 national Group Group Group Stronge	ddonnis, et senda , Status Uptariad Ignad	n C - Comp A cardan - Ton C - San raine Stock Dather Ann-24-19 at A carda attent to 11 anna	P	
Name Spit.ht Only: Underset Spit.ht Diright indexquery maximum lint Singlitz Uptimal Spit.ht Spit.ht indexquery maximum lint Singlitz Uptimal Spit.ht Spit.ht indexquery maximum lint Singlitz Uptimal Spit.ht Spit.ht	Instangety neutre ht Doug2 lipited 2004-10-06-10-0616 Instangety meaner.ht Dos40 lipited 2004-10-06-11-1200	or policies on the part of the state of the	Det tots Post tots tots Post Post Post of Low tots Post User Id user Id user Id user Id	File Name gitte north	K L I industry 52 naturel Group Distas Stroig2 Distas	Status Status Voisier Ligned	n co i an composition de la co	P	
same -get tot Owage ingeneration instanceship masses int Google Upper States int is 13 0001 instanceship masses int Google Upper States int is 13 0001 instanceship masses int Google Upper States int is 13 0001 instanceship States int is 10 001 States int is 13 001 States int is 13 001 instanceship States int is 10 001 States int is 13 001 States int is 13 001 instanceship States int is 10 001 States int is 13 001 States int is 13 001	Instançariy Instançariy Instançariy Dougl Lignal 200-11 6 (1) 0113 Instançariy memori // 20-42 3geal 337/12-03 (1) 13/2 Instançariy Homan // 20-42 3geal 337/12-03 (1) 13/2 Instançariy Homan // Voq2 Downood 20/12-16 (1) 11/2	or polyans or the polyans of the polyans of the polyans	D4 gas a bash a Borg of La Net Tree Prov 5 part Net Tree Prov	File Name	Group Group Group Group Group Group	Status Status water lanal Sovercal	Date	P	
Non- Statut Oragin Underside 2214-03-03.03 (20.05) instancystry Instance for instruction Social Spinal 2214-03-03.03 (20.05) instruction Instruction Social Spinal 2214-03-03.03 (20.05) instruction Instruction Spinal Spinal 2214-03-03.03 (20.05) instruction Instruction Spinal Spinal 2214-03-03.03 (20.05) instruction Spinal Spinal Spinal Spinal	Instance Social Lighted 2014-12-06-12-061 Instance Health Million Social 3001-06-06-12-061 Social Instance Health Million Social Social Social Social Social Instance Health Million Social	r Lokais A.Diagan Hentr - Q	Deb tes + Post his Bory of be tout - mil (Pare 5 and tout - mil (Pare 5 and	File Name gt to name in mane in mane in	Group Ones Single Single Ones Single Ones Single	dowe. Reeds Status warns upon upon upon upon upon upon upon upon	2 0 () - Soup Loose Tief () an George Date RE-2-2-2 at 250 RE-2-2 at 250 RE-2-2 at 120 RE-2-2 at 120 RE-2-2 RE-2-	P	
Non- Statistic Grapping Underside Statistical (Statistic)	Instançariy Instanci în Dougă Optimal Dăroși Optimal Instançariy Instançariy Instançariy Sanad Sanad Sanad Sanad Instançariy Instançariy Instançariy Sanad	r Lokais A.Diagan Hentr - Q	Det es • Des fois de que de se reur l'est Place d'anne • Back User Id • Stanpathy • Astronomy • Astronomy • Astronomy • Astronomy • Astronomy	File Name gt.tat rest are one ora gt.tat restriction restriction restriction	Group Ones Sixe Sixe Sixe Sixe Sixe Sixe Sixe Sixe	Status Status water uposi u u u u u u u u u u u u u u u u u u u	Date Date Date mercedu arrow ac	P	
Non- 201.01 On-N2 Varbanist 2214-01-01.02.00.00 Instancy.org/m Instance.org/m Group2 Uptowed 2214-01-01.02.00.00 Instancy.org/m Instance.org/m Group2 Uptowed 2214-01-01.02.00.00 Instancy.org/m Instance.org/m Group2 Uptowed 2214-01-01.02.00 Instancy.org/m Instance.org/m Group2 Uptowed 2214-01-01.02.00 Instancy.org/m Instance.org/m Group2 Uptowed 2214-01-01.02.00 Instancy.org/m Instance.org/m Group2 Uptowed 2214-01.01.02.00 Instancy.org/m Instance.org/m Group2 Uptowed 2214-01.01.02.00 Instancy.org/m Instance.org/m Group2 Uptowed 2214-01.01.02.00 Instance.org/m Instance.org/m Group2 Uptowed 2214-01.01.01.01	extension Sought Lighted Effect in 64.12 Million instruction Hearter Fri Dove12 Lighted Effect in 64.12 Million instruction Hearter Fri Dove12 Lighted Effect in 64.12 Million instruction Hearter Fri Dove12 Lighted Effect in 64.12 Million instruction Hearter Fri Dove12 Dove100 Effect in 64.12 Million instruction Hearter Fri Dove12 Dove100 Effect in 64.12 Million instruction Hearter Fri Dove12 Dove100 Effect in 64.12 Million instruction Hearter Fri Dove12 Uptimed Effect in 64.12 Million	r Lokais A.Diagan Hentr - Q	tet so * Board Board Source Source *** The The Source Source *** User 1d *** *** *** *** *** *** *** *	File Name 2 to 2 no 0 n 0 to 20104 ream in ream in ream in ream in	Group Ones Ones Ones Ones Ones Ones Ones Ones	Status Status outrad uposi bornod owns uponi bornod owns uponi	Collectory Control Cont	P	
Name Statistic Oracity Understand Statistic Instancestry Instance Social Understand Social Understand Instancestry Instance Social Understand Social Understand Instancestry Instance Social Understand Social Understand Instancestry Instance Social Understand Social	Audiospany Audiosp	r Lokais A.Diagan Hentr - Q	Let us The Dark Story of the set of the Story of the User Id user story of the story of the s	File Name grifer south of the second of the second file research research research research	Coup Group Orac Orac Orac Orac Orac Orac Orac Orac	Status Status ustina ustina ustina ustina tourna tourna tourna ustina ustina ustina ustina	Date Date Date Re-production Re- Re- Re- Re- Re- Re- Re- Re- Re- Re-	P	
each pit hit On-site instance instances instances Social Lipscal 2214-02-03 LB 20.05 instances Oracle Lipscal 2214-02-03 LB 20.07 instances memo	Instançariy	r Lokado escala 9.09 jung an aratiy - 💽	Let us Let us to a fact to any other to a fact the first to any us of the first to any other to	File Name Stars in concernation	Croup Croup Dass Singe Singe Sin Sin Sin Singe Singe Singe Sin Singe S	Status Status Ustina Ismai Dovical Coarsi Island Ustina Dovical	Date Date Date Merch Date Merch Date Merch Date Merch Date Merch Date Merch Date Merch Date Merch Date Merch Date Merch Date	P	
Name Capital Only: Values 2214-0-1-312.20.3% Instanceshy Names in Social Update 2214-0-1-312.20.3% Instanceshy Names in Social Update 2214-0-1-312.20.3% Instanceshy Social Social 2014-0-1-0-312.20.3% Instanceshy Social Social 2014-0-1-0-312.20.3% Instanceshy Instanceshi Social 2014-0-1-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-1-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-0-312.20.3% Instanceshi Social Social-0-0-0-312.20.3% 2014-0-0-0-312.2	instruction insure bit Soug2 Lighted Effect 12 66 12 0626 instruction instruction Soug2 Lighted 1010-12 66 12 0626 instruction instruction Soug2 Lighted 1010-12 66 12 0626 instruction instruction Soug2 Source 1010-12 66 12 0626 instruction instruction Source Source 1010-12 66 12 0627 instruction instruction Source Source 1010-12 66 12 0627 instruction instruction Source 1010-12 66 12 0627 1010-12 66 instruction instruction Source 1010-12 66 12 0627 1010-12 66 instruction instruction Source Lighted 1010-12 66 12 0627 instruction instruction Source Source 1010-12 66 12 0621 instruction instruction Source Source 1010-12 66 12 0621 instruction instruction Source Source 1010-12 66 12 0612 instruction instruction Source	or polyans or the polyans of the polyans of the polyans	Let us Construction of the second se	File Name	Group Group Cost Cost Cost Cost Cost Cost Cost Cost	Status Status outros operat operat operat operat operat operat operat operat operat operat operat	• • • ■ • • • • • • • • • • • • • • • •	P	
Name Capital Only: Values 2214-0-1-312.20.3% Instanceshy Names in Social Update 2214-0-1-312.20.3% Instanceshy Names in Social Update 2214-0-1-312.20.3% Instanceshy Social Social 2014-0-1-0-312.20.3% Instanceshy Social Social 2014-0-1-0-312.20.3% Instanceshy Instanceshi Social 2014-0-1-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-1-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-0-312.20.3% Instanceshi Social Social-1-0-0-312.20.3% 2014-0-0-0-312.20.3% Instanceshi Social Social-0-0-0-312.20.3% 2014-0-0-0-312.2	instruction Sought Uption Editer 12 & 612 (2015) instruction instruction Sought Uption Editer 12 & 612 (2015) instruction instruction Sought Uption Editer 12 & 612 (2015) instruction instruction Sought Uption Editer 12 & 612 (2015) instruction instruction Sought Developed Editer 12 & 612 (2015) instruction instruction Sought Editer 12 & 612 (2015) Editer 12 & 612 (2015) instruction instruction Sought Editer 12 & 612 (2015) Editer 12 & 612 (2015) instruction instruction Sought Editer 12 & 612 (2015) Editer 12 & 612 (2015) instruction instruction Sought Editer 12 & 612 (2015) Editer 12 & 612 (2015) instruction instruction Sought Editer 12 & 612 (2015) Editer 12 & 612 (2015) instruction instruction Sought Editer 12 & 612 (2015) Editer 12 & 612 (2015) instruction instruction Sought Editer 12 & 612 (2015) Editer 12 & 612	or policie or to ing at conto ing at	Let us Construction of the second se	File Name	Group Group Cost Cost Cost Cost Cost Cost Cost Cost	Status Status outros operat operat operat operat operat operat operat operat operat operat operat	• • • ■ • • • • • • • • • • • • • • • •	P	

VII. CONCLUSION

We utilize ring signatures to construct homomorphic authenticators, study for our future so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish block. To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism who is the signer on each to support batch auditing. There are two interesting problems we will continue to work. One of them is traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations. Since Oruta is based on ring signatures, where the identity of the signer is unconditionally protected, the current design of ours does not support traceability.

VIII. REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[4] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[6] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[7] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126,1978.

[8] The MD5 Message-Digest Algorithm (RFC1321). https://tools.ietf.org/html/rfc1321, 2014.

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-610, 2007.

[10] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.