



## **RANDOMIZE THE ENCODE COEFFICIENTS WITH A PSEUDO RANDOM FUNCTION PRESERVE DATA PRIVACY**

**S. Cathrin Pricilla Vahini\* & K. Adlin Suji\*\***

\* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

\*\* Associate Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

### **Abstract:**

*To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes critical. Recently, regenerating codes have gained popularity due to their lower repair bandwidth while providing fault tolerance. Existing remote checking methods for regenerating-coded data only provide private auditing, requiring data owners to always stay online and handle auditing, as well as repairing, which is sometimes impractical. In this paper, we propose a public auditing scheme for the regenerating-code-based cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, we introduce a proxy, which is privileged to regenerate the authenticators, into the traditional public auditing system model. Moreover, we design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely release data owners from online burden. In addition, we randomize the encode coefficients with a pseudorandom function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating code-based cloud storage.*

**Index Terms:** Cloud Storage, Regenerating Codes, Public Audit, Privacy Preserving, Authenticator Regeneration, Proxy, Privileged & Provable Secure

### **Introduction:**

To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes critical. Recently, regenerating codes have gained popularity due to their lower repair bandwidth while providing fault tolerance. Existing remote checking methods for regenerating-coded data only provide private auditing, requiring data owners to always stay online and handle auditing, as well as repairing, which is sometimes impractical. In this paper, we propose a public auditing scheme for the regenerating-code-based cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, the introduce a proxy, which is privileged to regenerate the authenticators, into the traditional public auditing system model. Moreover, the design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely release data owners from online burden. In addition, the randomize the encode coefficients with a pseudorandom function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating code based cloud storage. The focus on the integrity verification problem in regenerating-code-based cloud storage, especially with the functional repair strategy extended the single-server CPOR scheme (private version in) to the regenerating code-scenario designed and implemented a data integrity

protection (DIP) scheme for FMSR based cloud storage and the scheme is adapted to the thin-cloud setting<sup>1</sup>. However, both of them are designed for private audit, only the data owner is allowed to verify the integrity and repair the faulty servers. Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing and reparation in the cloud can be formidable and expensive for the users. The overhead of using cloud storage should be minimized as much as possible such that a user does not need to perform too many operations to their outsourced data (in addition to retrieving it). In particular, users may not want to go through the complexity in verifying and reparation. The auditing schemes in imply the problem that users need to always stay online, which may impede its adoption in practice, especially for long-term archival storage.

**Modules:**

- ✓ Data owner
- ✓ The Cloud
- ✓ Third party Auditor (TPA)
- ✓ Proxy Agent

**Data Owner:** Who owns large amounts of data files to be stored in the cloud.

**The Cloud:** Which are managed by the cloud service provider, provide storage service and have significant computational resources;

**The Third Party Auditor (TPA):** Who has expertise and capabilities to conduct public audits on the coded data in the cloud, the TPA is trusted and its audit result is unbiased for both data owners and cloud servers;

**Proxy Agent:** Who is semi-trusted and acts on behalf of the data owner to regenerate authenticators and data blocks on the failed servers during the repair procedure.

**Existing System:**

The focus on the integrity verification problem in regenerating-code-based cloud storage, especially with the functional repair strategy extended the single-server CPOR scheme (private version in) to the regenerating code-scenario designed and implemented a data integrity protection (DIP) scheme for FMSR based cloud storage and the scheme is adapted to the thin-cloud setting<sup>1</sup>. However, both of them are designed for private audit, only the data owner is allowed to verify the integrity and repair the faulty servers. Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing and reparation in the cloud can be formidable and expensive for the users. The overhead of using cloud storage should be minimized as much as possible such that a user does not need to perform too many operations to their outsourced data (in addition to retrieving it). In particular, users may not want to go through the complexity in verifying and reparation.

**Disadvantages:**

- ✓ Remote checking methods for regenerating-coded data only provide private auditing,
- ✓ Requiring data owners to always stay online and handle auditing, as well as repairing
- ✓ It is noted that data owners lose ultimate control over the fate of their outsourced data

**Proposed System:**

The focus on the integrity verification problem in regenerating-code-based cloud storage, especially with the functional repair strategy extended the single-server CPOR scheme (private version in) to the regenerating code-scenario designed and implemented a data integrity protection (DIP) scheme for FMSR based cloud storage

and the scheme is adapted to the thin-cloud setting<sup>1</sup>. However, both of them are designed for private audit, only the data owner is allowed to verify the integrity and repair the faulty servers. Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing and reparation in the cloud can be formidable and expensive for the users. The overhead of using cloud storage should be minimized as much as possible such that a user does not need to perform too many operations to their outsourced data (in addition to retrieving it). In particular, users may not want to go through the complexity in verifying and reparation. The auditing schemes in [7], [8] imply the problem that users need to always stay online, which may impede its adoption in practice, especially for long-term archival storage.

#### **Advantages:**

- ✓ The design a novel homomorphic authenticator based on BLS signature [17], which can be generated by a couple of secret keys and verified publicly.
- ✓ To allow privacy-preserving public auditing for regenerating code-based cloud storage. The coefficients are masked by a PRF (Pseudorandom Function) during the Setup phase to avoid leakage of the original data.
- ✓ Our scheme completely releases data owners from online burden for the regeneration of blocks and authenticators at faulty servers and it provides the privilege to a proxy for the reparation.
- ✓ Optimization measures are taken to improve the flexibility and efficiency of our auditing scheme; thus, the storage overhead of servers, the computational overhead of the data owner and communication overhead during the audit phase can be effectively reduced.

#### **Data Flow Diagrams:**

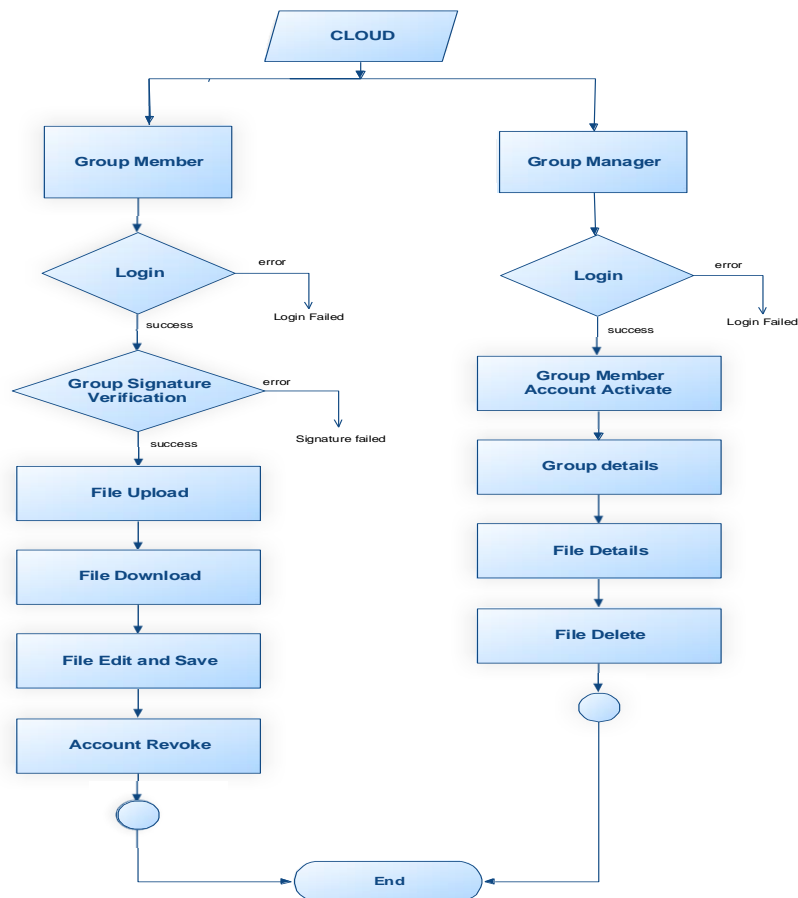


Figure 1: Data Flow Diagram

## System Architecture:

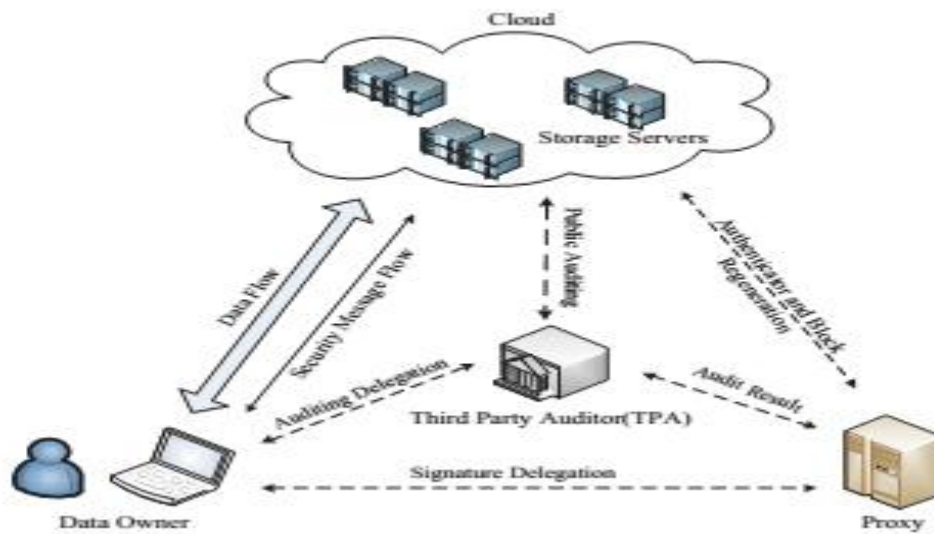


Figure 2: System Architecture

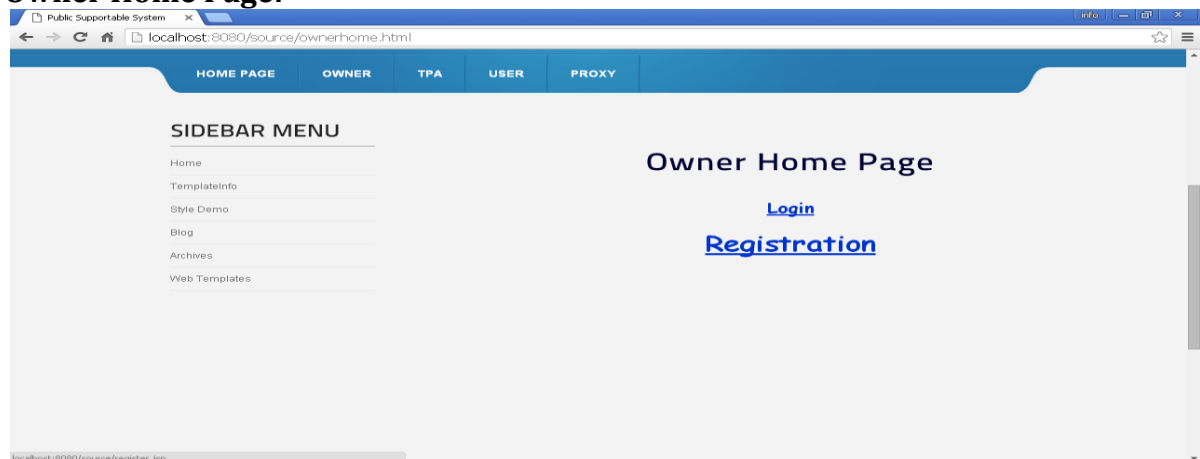
## Experimental Result:

**Test Results:** All the test cases mentioned above passed successfully. No defects encountered.

## Appendix 2-Screen Shots:



## Owner Home Page:



## Owner Registration:

Public Supportable System

localhost:8080/source/register.jsp

**SIDEBAR MENU**

- Home
- TemplateInfo
- Style Demo
- Blog
- Archives
- Web Templates

**Registration**

User ID:

Password:

ReType Password:

Gender: ☒ Male ☐ Female

Age:

Phone No:

Email ID:

Image Gallery Services Overview Contact Us

## Login:

Public Supportable System

localhost:8080/source/login.jsp

**SIDEBAR MENU**

- Home
- TemplateInfo
- Style Demo
- Blog
- Archives
- Web Templates

**Login Here**

User Name:

Password:

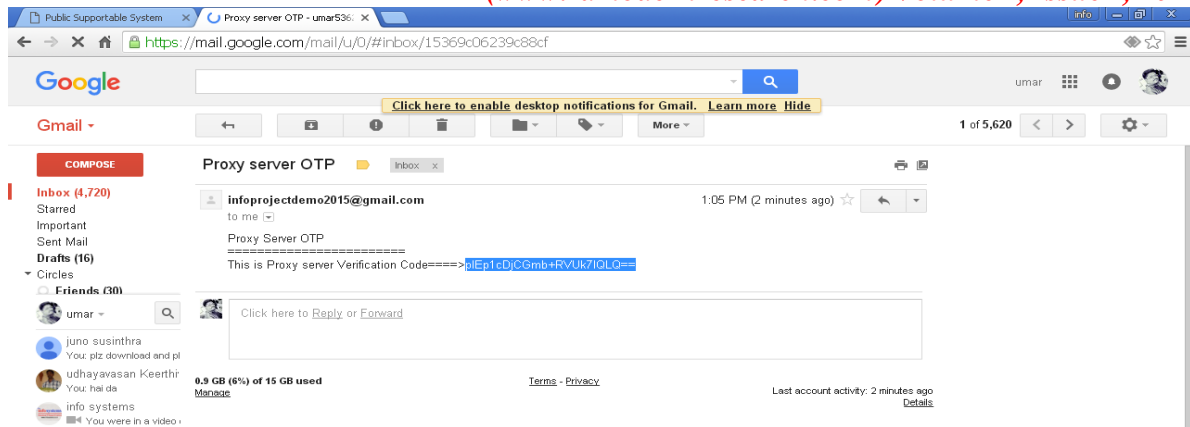
HOME PAGE OWNER TPA USER PROXY

**Your Login Success... !**

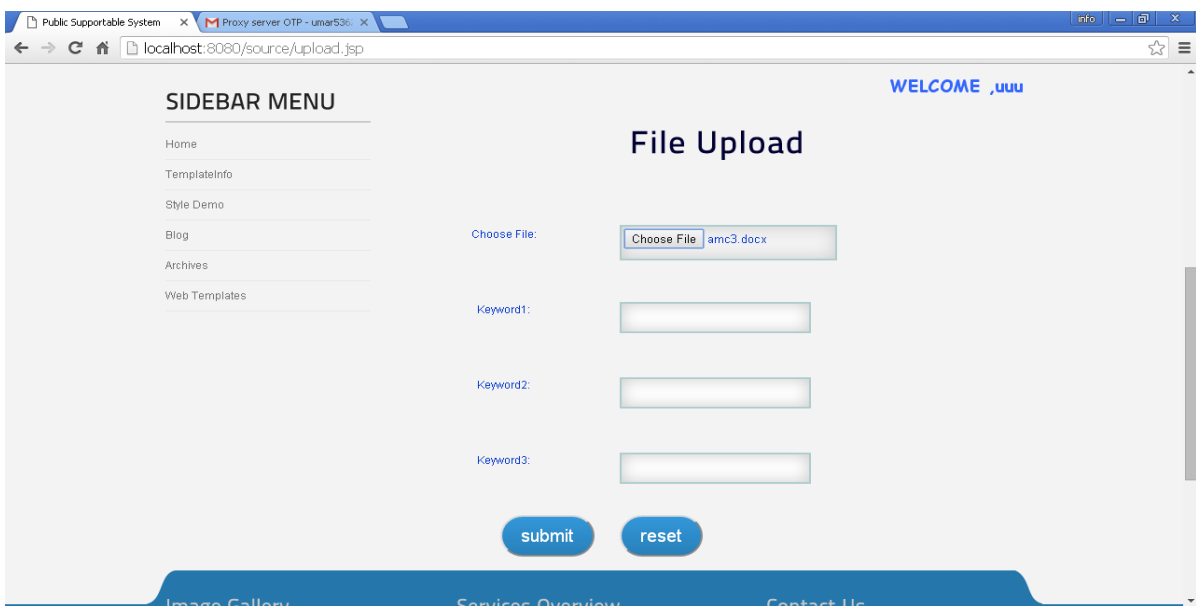
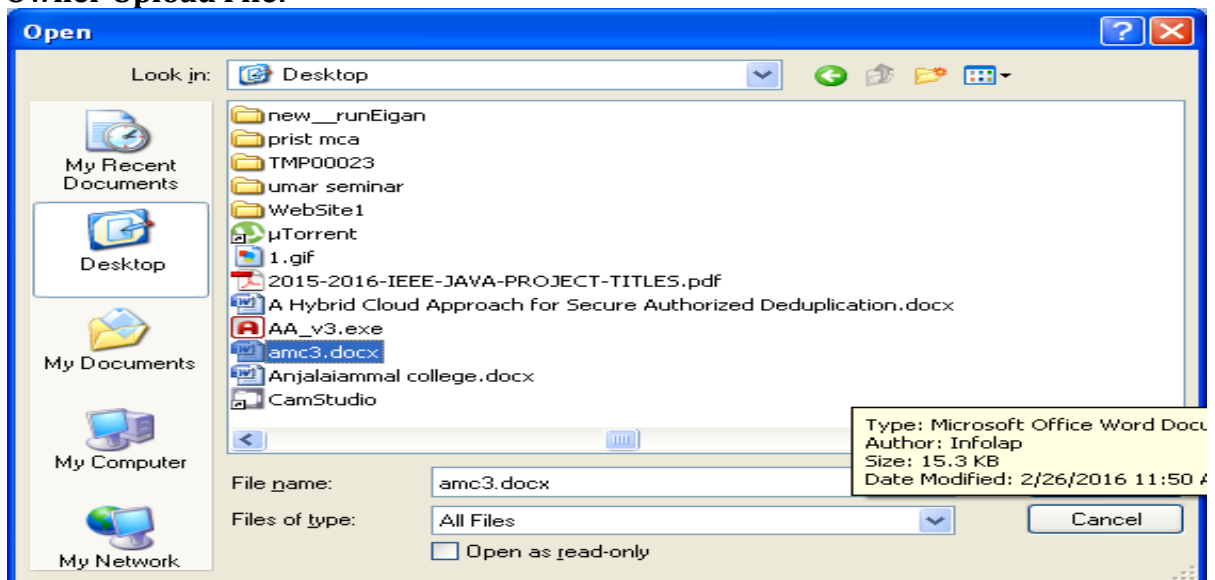
Hi uuu please go to Your Mail and Copy & Paste the Proxy Server OTP Code Here....

OTP Password:

Your computer might be at risk  
- avast! Antivirus is turned off  
- Automatic Updates is turned off  
- avast! Antivirus is turned off  
Click this balloon to fix this problem.



### Owner Upload File:





**SIDEBAR MENU**

- Home
- TemplateInfo
- Style Demo
- Blog
- Archives
- Web Templates

**File Upload**

WELCOME ,uuu

Choose File:

Keyword1:

Keyword2:

Keyword3:

### Upload:

**Host: 127.0.0.1 Database: protecting Table: filedetails**

uid	fileID	filename	filetype	filecluster
umar	5362	Abstract.doc	doc	CDC
umar	5363	umar1.txt	txt	CDC
umar	5364	umar1.txt	txt	CDC
umar	5365	umaraaa.txt	txt	CDC
umar	5366	Chest-x-ray.jpg	jpg	SC
umar	5367	Chest-x-ray.jpg	jpg	SC
umar	5368	New Text Document.txt	txt	CDC
viji	5369	sivaranjani.docx	docx	CDC
suji	5370	AA_v3.exe	exe	SC
suji	5371	AA_v3.exe	exe	SC
suji	5372	amc3.docx	docx	CDC
elaveini	5373	Text To Speech.sln	sln	SC
uuu	5374	amc3.docx	docx	CDC

**Query:**

```

3 SHOW /*!32352 FULL */ COLUMNS FROM `filedetails` ;
4 SHOW KEYS FROM `filedetails` ;
5 SELECT LEFT(`uid`, 256), `fileID`, LEFT(`filename`, 256), LEFT(`filetype`, 256), LEFT(`filecluster`, 256)

```

ected: 00:12:29 MySQL 5.0.27 Uptime: 0 days, 00:23:03 Ready.

### The Last Uploaded File Clustering:

**CDC**

File and Folder Tasks

Other Places

- source
- My Documents
- Shared Documents
- My Computer
- My Network Places

Details

File Name	Size
5362.p12	25 KB
5363.p12	1 KB
5364.p12	1 KB
5365.p12	1 KB
5366.p12	35 KB
5368.p12	1 KB
5370.p12	756 KB
5374.p12	19 KB
5363.p12	1 KB
5365.p12	1 KB
5367.p12	35 KB
5369.p12	14 KB
5372.p12	19 KB

### TPA Server Home Page:


### TPA Link:

### TPA Give or Block Permission of Owner:

USER ID	MAIL ID	CONTACT NO	STATUS
Elaveini	Elaveiniselvaraj@gmail.Com	9876543210	Active
Suji	Sujiedr@gmail.Com	90674325	Active
Umar	Umar5362@gmail.Com	7200732263	Block
Umar5362	Umar5362@gmail.Com	7200732263	Active
Uuu	Umar5362@gmail.Com	9876543210	Active
Viji	Knmviji@gmail.Com	9876543210	Block



### Owner File Details:



USER ID	FILE CLUSTER	FILE NAME	FILE TYPE	FILE ID
Umar	CDC	Abstract.Doc	Doc	5362
Umar	CDC	Umar1.Txt	Txt	5363
Umar	CDC	Umar1.Txt	Txt	5364
Umar	CDC	Umaraaa.Txt	Txt	5365
Umar	SC	Chest-X-Ray.Jpg	Jpg	5366
Umar	SC	Chest-X-Ray.Jpg	Jpg	5367
Umar	CDC	New Text Document.Txt	Txt	5368
Viji	CDC	Sivaranjani.Docx	Docx	5369
Suji	SC	AA_v3.Exe	Exe	5370
Suji	SC	AA_v3.Exe	Exe	5371
Suji	CDC	Amc3.Docx	Docx	5372
Eleveini	SC	Text To Speech.Sln	Sln	5373
Uuu	CDC	Amc3.Docx	Docx	5374

### Conclusion:

In this paper, we propose an open evaluating plan for the recovering code-based distributed storage framework, where the information proprietors are advantaged to assign TPA for their information legitimacy checking. To ensure the first information protection against the TPA, we randomize the coefficients in the first place rather than applying the visually impaired procedure amid the evaluating procedure. Considering that the information proprietor can't generally stay online in rehearse, so as to keep the capacity accessible and unquestionable after a noxious debasement, we present a semi-trusted intermediary into the framework display and give a benefit to the intermediary to handle the reparation of the coded pieces and authenticators. To better proper for the recovering code-situation, we plan our authenticator taking into account the BLS signature. This authenticator can be effectively produced by the information proprietor at the same time with the encoding method. Broad investigation demonstrates that our plan is provable secure, and the execution assessment demonstrates that our plan is exceedingly productive and can be plausibly incorporated into a recovering code-based cloud capacity framework.

### References:

1. Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, "Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 7, July 2015.
2. C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007, pp. 598–610.
3. G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319–333.
4. B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.
5. B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

6. K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.
7. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," J. Cryptol., vol. 17, no. 4, pp. 297–319, Sep. 2004.
8. S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., 2002, pp. 226–236.
9. L. Buttyan and J. P. Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks," ACM/Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.
10. J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," presented at the First Workshop Modeling Optimization Mobile, Ad Hoc Wireless Netw., Sophia Antipolis, France, 2003.