Cost-Effective Authentic & Anonymous Data Sharing with Forward Security

[1]Prof. Ravi Nagar, [2]Devidas Mahadev Patil, [3]Dinesh Motiram Patil, [4]Chetan Dayaram Pagare

[1]Asst. Professor, [2,3,4]UG Student, [1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharshatra, India.

1ravinagar26@gmail.com, [2]devpatil789@gmail.com, [3]patildinesh646@gmail.com, [4]chetan.pagare10@gmail.com

Abstract: Data sharing has never been easier with the advances of cloud computing, and correct analysis on the shared knowledge offers an array of advantages to each the society and people. Knowledge sharing with an outsize sort of participants got to take into consideration many problems, what is more as potency, knowledge integrity and privacy of information owner. Ring signature may even be a promising applicant to build an anonymous and authentic knowledge sharing system. It permits a data owner to anonymously certify his info that might be place into the cloud for storage or analysis purpose. However the expensive certificate verification among the normal public key infrastructure (PKI) setting becomes a bottleneck for this resolution to be climbable. Identity-based (ID-based) ring signature, that eliminates the plan of action of certificate authentication, may even be used instead. Throughout this paper, a bent to any enhance the protection of ID-based ring signature by providing forward security: If a secret key of any user has been cooperated, all earlier generated signatures that embody this user still keep valid. This property is particularly necessary to any vast scale knowledge sharing system, as a results of it's unacceptable to spice up all knowledge house owners to re-authenticate their knowledge though a secret key of single user has been compromised. This offer a concrete and economical illustration of this theme, prove its security and supply an implementation to imply its utility.

Index Term — Authentication, data sharing, cloud computing, forward security, smart grid.

I. INTRODUCTION

The popularity and widespread use of “CLOUD” have brought nice convenience for knowledge sharing and assortment. Not solely will people acquire helpful knowledge additional simply, sharing knowledge with others will give variety of advantages to the society also. As square measure preventative example, customers in sensible Grid will get their energy usage knowledge in a very fine-grained manner and square measure inspired to share their personal energy usage knowledge with others, e.g., by uploading the knowledge to a 3rd party platform like Microsoft From the collected data a applied math report is formed, and one will compare their energy consumption with others .This ability to access, analyze, and answer far more accurate and careful knowledge from all levels of the electrical grid is vital to economical energy usage. Thanks to its openness knowledge sharing is usually deployed in a very hostile setting and susceptible to Variety of security threats. Taking energy usage knowledge sharing in sensible Grid as associate degree example, there square measure many security goals a sensible system should meet, including: knowledge legitimacy. Within the state of affairs of sensible grid, the data point energy usage knowledge would be dishonest if it's solid by adversaries. whereas this issue alone is resolved mistreatment well established cryptologic tools, one could encounter extra difficulties once alternative problems square measure taken under consideration, like namelessness and efficiency; namelessness.

Energy usage knowledge contains large info of customers, from that one will extract the quantity of persons within the home, the kinds of electrical utilities employed in a selected fundamental quantity, etc. Thus, it's vital to guard the namelessness of customers in such applications, and any failures to try to therefore could result in the reluctance from the customers to share knowledge with others; and a couple of potency. The number of users in a very knowledge sharing system may be vast and a sensible system should scale back the computation and communication value the maximum amount as attainable. Otherwise it might result in a waste of energy that contradicts the goal of sensible grid. This project is dedicated to work elementary security tools for realizing the 3 properties we tend to delineated. Note that there square measure alternative security problems in a very knowledge sharing system that square measure equally vital, like availableness and access management. However the study of these problems is out of the scope of this project.

II. LITERATURE SURVEY

There are some existing methods used which are as follows:

A. 1-Out-of-N Signature from a variety of Keys

This paper addresses how to use public-keys of a number of different signature schemes to generate 1-out-of-n signatures. Previously known constructions are for either RSA-keys only or DL (Discrete Logarithm)-type keys only. We present a widely applicable method to build a 1-out-of-n signature scheme that allows mixture use of different flavors of keys at the same time. The resulting scheme is more efficient than earlier schemes even if it is used only with a single type of keys. With all DL (Discrete Logarithm)-type keys, it yields shorter signatures than the ones of the previously known scheme based on the witness indistinguishable proofs by Cramer, et al. With all RSA-type keys, it reduces both computational and storage costs compared to that of the Ring signatures by Rivest, et al.

B. ID-Based Ring Signature and Proxy Ring Signature Schemes form bilinear pairing

In 2001, Rivest et al. firstly introduced the concept of ring signatures. A ring signature is a simplified group signature without any manager. It protects the anonymity of a signer. The first scheme suggested by Rivest et al. was based on RSA cryptosystem and certificate based public key setting. Their scheme is also based on the general certificate-based public key setting too. In 2002, Zhang and Kim proposed a new ID-based ring signature scheme using pairings. Later Lin and Wu suggested a more efficient ID-based ring signature scheme. Both these schemes have some inconsistency in computational aspect. In this paper a new ID-based ring signature scheme and a proxy ring signature scheme. Both the schemes are more efficient than current one. These schemes also take care of the inconsistencies in above two schemes.

The ring signature allows a user from set of possible signers to convince the verifier that the author of the signature belongs to the set but identity of the author is not disclosed. The ring signature may be considered to be a simplified group signature which consists of only users without the managers. It protects the anonymity of a signer since the verifier knows only that the signature comes from a member of a ring, but does not know exactly who the signer is. There is no approach to revoke the anonymity of the signer.

C. A Practical and provably Secure Coalition-resistant Group Signature Scheme

A group signature scheme allows a group member to sign messages anonymously on behalf of the group. Nevertheless, in the case of a dispute, the identity of a signature’s originator can be revealed (only) by a nominated entity. The interactive counter parts of group signatures are identity escrow schemes or group identification scheme with revocable anonymity. This work introduces a new provably secure group signature and a companion identity escrow scheme that are significantly more efficient than the state of the art. In its interactive, identity escrow form, this scheme is proven secure and coalition-resistant under the strong RSA and the decisional Diffie-Hellman assumptions. The security of the non-interactive variant, i.e., the group signature scheme, relies additionally on the Fiat-Shamir heuristic (also known as the random oracle model).

In contrast to ordinary signatures they provide anonymity to the signer that is a verifier can only tell that a member of some group signed. However, in special cases such as a legal dispute, any group signature can be “opened" by a designated group manager to reveal unambiguously the identity of the signature's originator. The main features of group signatures make them attractive for many specialized applications such as elective and bidding.

All companies submitting a tender form a group and each company signs its tender anonymously using the group signature. Once the chosen tender is selected, the winner can be traced while the other bidders remain anonymous. More generally, group signatures can be used to conceal organizational structures, e.g., when a company or a government agency issues a signed statement. Group signatures can also be integrated with an electronic cash system whereby several banks can securely distribute anonymous and untraceable e-cash.

D. ID-Based Ring Signature Scheme Secure in the Standard model

The only known building of ID-based ring signature schemes which maybe secure in the standard model is to attach certificates to non-ID-based ring signatures. This method leads to schemes that are somewhat inefficient and it is an open problem to find more efficient and direct structure. In this project, we suggest two such constructions. In this first scheme, with signature size linear in the cardinality of the ring, is secure in the standard model under the computational Diffie-Hellman assumption. The second scheme, achieving constant signature size, is secure in a weaker attack model (the selective ID and selective chosen message model), under the Diffie-Hellman Inversion assumption.

In an ID-based cryptosystem, public key of each user is easily computable from a string corresponding to this client’s identity (e.g. an email address, a telephone number, etc.). A private key generator (PKG) then computes the private keys from a master secret for the clients. This property avoids the necessity of certificates and associates an implicit public key (user identity) to each user within the system. Ring signature is a group-oriented signature with privacy concerns. A user can sign anonymously on behalf of a group on his own choice, while group members can be totally unaware of being conscripted in the group.

E. Foundation of group Signature: Formal Definition, Simplified Requirement and A Construction based on general assumption.

This paper provides theoretical foundations for the group signature primitive. We introduce strong, formal definitions for the core requirements of anonymity and traceability. We then show that these imply the large set of sometimes ambiguous existing informal requirements in the literature, thereby unifying and simplifying the requirements for this primitive. Finally we prove the existence of a build meeting on definitions based only on the sole assumption that trapdoor permutations exist.

A central line of work in theoretical cryptography is to provide formal (and strong) definitions of security for cryptographic primitives and then provide constructions based on general computational complexity assumptions (such as the existence of one-way or trapdoor functions), that satisfy the definitions in question. The value and difficulty of such “foundational" work is acknowledged and manifest. A classical example is public-key encryption.

The definitions and results of this paper are for the setting in which the group is static meaning the number and identities of members is decided at the time the group is set up and new members cannot be added later. We consider it important to begin with this setting because, even though dynamic groups have been considered proper definitions of security have not been provided even for the basic static-group case, and the important definitional issues arise already in the context.

Table 1: Comparative study

PAPER	AUTHOR	BASIC METHOD	MERIT	DE-MERIT
1-out-of-n Oblivious Signatures	†Raylin Tso, Takeshi Okamoto, and Eiji Okamoto	Oblivious Signature based method	**1**. Secure and quite efficient. **2**. Solution to the SFE problem	1. Traceability 2. Unforgeability 3. Exculpability
Foundations of Group Signatures: Formal Definition, Simplied Requirements, and a Construction Based on General Assumptions	Mihir Bellare* Daniele Micciancioy Bogdan Warinschiz	Group Signatures	1. Unforgeability. 2. Exculpability. 3. Traceability	1. Anonymity
A Practical and Provably Secure Coalition-Resistant Group Signature Scheme	Giuseppe Ateniese[1], Jan Camenisch[2], Marc Joye[3], and Gene Tsudik[4]	Coalition-Resistant Group Signature Scheme	1. Unforgeability. 2. Anonymity. 4. Exculpability. 4. Traceability.	1. Signature Verification 2. More Efficient for limited computing
ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings	Amit K Awasthi[1] and Sunder Lal[2]	Proxy Ring Signature Schemes	1. Provide anonymity. 2. Signature verification. 3. More efficient for limited computing.	1. Full Unforgeability.
ID-Based Ring Signature Scheme secure in the Standard Model	Man Ho Au[1], Joseph K. Liu[2], Y. H. Yuen[3], and Duncan S. Wong[4]	ID-Based Ring Signature Scheme	1. Anonymity 2. Full Unforgeability.	1. Correctness 2. Certificate Verification

III. AIMS & OBJECTIVES

Aims

The scalability and flexibility of cloud is attracted by everyone. Data sharing and storing are facilitated in cloud. Due to its directness, data sharing is always deployed in a private environment and vulnerable to security threats. So far the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. This project suggests a new idea called Forward Secure ID-Based Ring Signature. It allows an ID-Based ring signature to have forward security.

Identity-based (ID-based) cryptosystem removes the process of verifying and validating the public key certificates. Forward Secure ID-Based signature (IDFSRS) removes the costly verification. A private key generator (PKG) computes private keys from its master secret for users and associates an implicit public key to each user within the system. It does not need any pairing operations. The size of user secret key is just one integer.

Objective

1. Input Design is the process of transforming 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.

IV. PROPOSED SYSTEM

ID-Based Forward Secure Ring Signature Schemes:

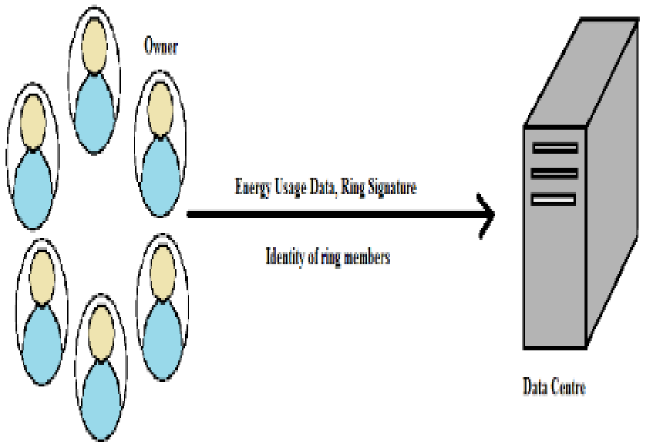
In this paper, a new notion called forward secure ID-based ring signature, which is an essential tool for building cost-effective authentic and anonymous data sharing system. For the first time, we deliver formal definitions on forward secure ID-based ring signatures; we present a concrete design of forward secure ID based ring signature. No previous ID-based ring signature schemes in the literature have the property of forward security, and we are the first to provide this feature we prove the security of the suggested scheme in the random oracle model, under the standard RSA assumption. Any verifier can be frustrated that a message has been signed by one of the members in this group also called the Rings but the actual identity of the user is hided from the originality. Ring signatures could be used for whistle blowing membership authentication for an ad hoc networks and many other applications which do not want complicated group formation stage but require signer anonymity.

V. ALGORITHMS

Step 1: The energy data owner who is present in the group sends his data with the signature which contains the public identity of any one member of the group. This phase only needs the public identity information of ring members, such as residential addresses, and does not need the collaboration from any ring members.

Step 2: Data owner uploads his personal data of electronic usage, together with a ring signature and the identity information of all ring members.

Step 3: By verifying the ring signature, one can be assured that the data is indeed given out by a valid resident (from the ring members) while cannot figure out who the resident is. Hence the anonymity of the data provider is ensured together with data authenticity. Meanwhile, the verification is efficient which does not involve any certificate verification



Working Flow

A. Setup:

On input of a security parameter λ, the private key generator generates two random k-bit prime numbers u and v such that u=2u'+1 and v=2v'+1 where u', v' are some prime numbers. It then computes N=uv. For a fixed parameter p, it chooses a random prime number e such that $2p<e<2p+1$ and gcd (e,Ø (N)) = 1. It chooses two hash functions H1 :{ 0, 1}*→ Z*N and H2 :{ 0, 1}*→ {0, 1}p .The public parameters are (k,p,e,N,H1,H2) and the master secret key msk is (u,v).

B. Extract:

For user i, where i ε Z, with identity IDi ε {0, 1}* requests for a secret key at time period which is denoted by an integer, where 0 ≤t < T, the PKG using its knowledge of the factorization of N computes the user secret key. sKi,t = [H1(IDi)] 1/e(T+1-t) mod N using its knowledge of the factorization of N.

C. Update:

When the secret key sk i,tis given as input for a time period t, if t < T the user updates the secret key as ski,t+1 = (ski,t)e mod N Otherwise the algorithm outputs "⊥" meaning that the secret key has expired.

D. Sign:

To sign a message m ε {0, 1}* in time period t, where 0 ≤t < T, on behalf of identities of the members L = {ID1,....,IDn}, a user with identity IDπε L and secret key skπ,t. This outputs the signature for the list of identities L, time period t and the message m as б = (R1,..., Rn,h1,....,hn,s).

E. Verify:

To verify a signature б for a message m, a list of identities L and the time period t, check whether hi= H2(L, m, t, Idi,Ri) for i = 1,...., n and e(T+t-1) = Πni=1 (Ri.H1(IDi)hi) mod N. Output valid if all equalities hold else produces the output as invalid. Thus the forward secure identity-based ring signature scheme is defined by the above five procedures or algorithms such as "Setup, Extract, Sign, Verify and Update".

VI. MATHEMATICAL MODEL

ID-Based Key Generation

Step 1:

1. For all $i \in \{1,\ldots,n\}$, $i \neq \pi$, choose random $A_i \in \mathbb{Z}^*_N$ and compute
   $R_i = A_i^{e^{(T+1-t)}}$ *mod N*
   and
   $h_i = H_2(L,m,t,ID_i,R_i)$.
2. *Choose random* $A_\pi \in \mathbb{Z}^*_N$ and compute
   $R_\pi = A_\pi^{e^{(T+1-t)}}$
   $$\cdot \prod_{i=1,i\neq\pi}^{n} H_1(ID_i)^{-h_i} \; mod\ N$$
   and
   $h_\pi = H_2(L,m,t,ID_\pi,R_\pi)$.
3. Compute
   $$S = (sk_{\pi,t})^{h_\pi} . \prod_{i=1}^{n} A_i \; mod\ N$$
4. Output the signature for the list of identifies L, the message m, and time period t as σ = $(R_1,\ldots,R_n,h_1,\ldots,h_n,s)$.

Verify: To Verify a signature σ for a message m, a list of identifies L and the time period t, check whether $h_i = H_2(L,m,t,ID_i,R_i)$ for i=1,….,n and

$$s^{e^{(T+1-t)}} = \prod_{i=1}^{n} (R_i \cdot H_1(ID_i)^{h_i}) \; mod\ N.$$

Output valid if all equalities hold. Otherwise output invalid.

CORRECTNESS

Step 2:

We shall show that signatures signed by honest signers are always verified to be valid. For the verification equation.

$$s^{e^{(T+1-t)}} = \prod_{i=1}^{n} (R_i \cdot H_1(ID_i)^{h_i}) mod\ N :$$

:

Left Hand Side:

$$= s^{e^{(T+1-t)}}$$

$$= ((sk_{\pi,t})^{h_\pi} \cdot \prod_{i=1}^{n} A_i \; mod\ N)^{e^{(T+1-t)}}$$

$$= \left((H_1(ID_\pi) \quad \frac{1}{e^{(T+1-t)}})^{h_\pi} \cdot \prod_{i=1}^{n} (A_i) \quad mod\ N \right) e^{(T+1-t)}$$

$$= H_1(ID_\pi)^{h_\pi} \cdot \prod_{i=1}^{n} (A_i)^{e^{(T+1-t)}} mod\ N.$$

Right Hand Side:

$$= \prod_{i=1}^{n} (R_i \cdot H_1(ID_i)^{h_i}) \; mod\ N$$

$$= \left(\prod_{i=1,i\neq\pi}^{n} \quad (R_i \cdot H_1(ID_i)^{h_i}) \right) \cdot (R_\pi \cdot H_1(ID_\pi)^{h_\pi}) \; mod\ N$$

$$= \left(\prod_{i=1,i\neq\pi}^{n} (A_i^{e^{(T+1-t)}} \cdot H_1(ID_i)^{h_i}) \right).$$

$$\left((A_\pi^{e^{(T+1-t)}} \quad \prod_{i=1,i\neq\pi}^{n} H_1(ID_i)^{-h_i}) \cdot H_1(ID_\pi)^{h_\pi}) \right) \; mod\ N$$

$$= (\prod_{i=1}^{n} A_i^{e^{(T+1-t)}}) \cdot H_1(ID_\pi)^{h_\pi} mod\ N$$

= Left Hand Side

VII. EXPECTED OUTPUT

The user must login the system and user must join the group for data sharing. By using forward ring signature algorithm the keys are distributed among the legitimate users through which they can access the data i.e shared in the group to access the data or share the user must have the public key shared among the group members.

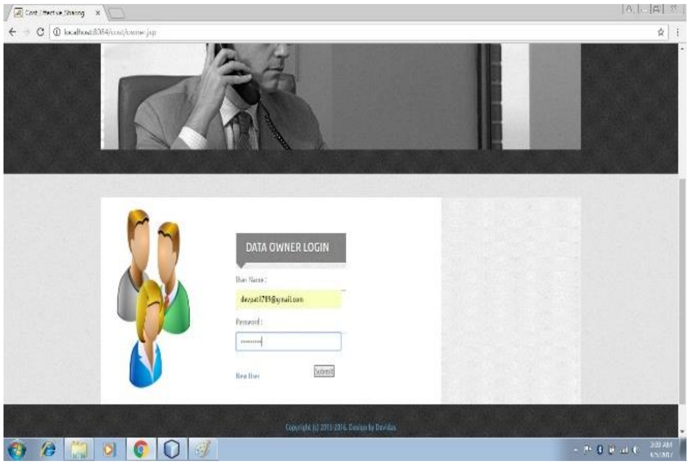
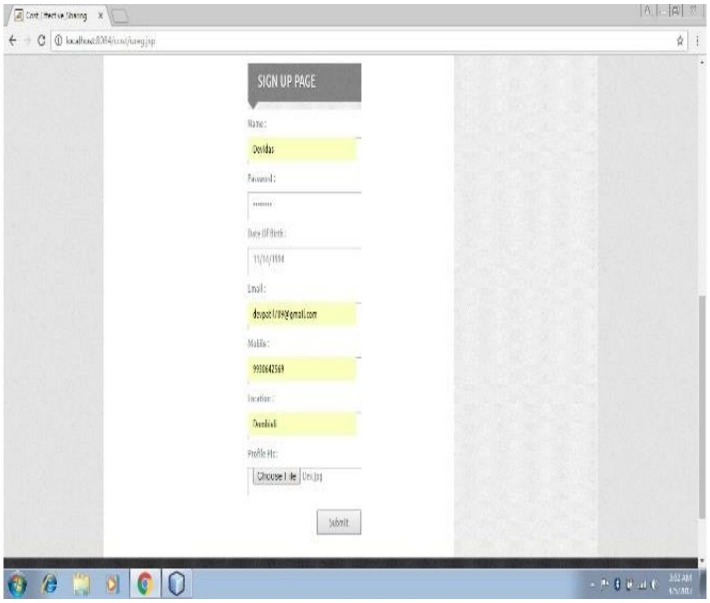


Fig 1. Data-Owner Login Page



SIGN UP PAGE

Name:
Devidas

Password:
****

Date Of Birth:
11/10/1994

Email:
devpatil789@gmail.com

Mobile:
9930642569

Location:
Dombivli

Profile Pic:
Choose File Dev.jpg

Submit

Fig 2. Data-Owner Register page

VIII. CONCLUSION

We have tried to implemented “Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou”,”Cost-Effective Authentic and Anonymous Data Sharing With Forward Security”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 64,NO. 4, APRIL 2015 and according to the implementation the conclusion is “Motivated by the practical needs in data sharing, we proposed a new notion called forward secure ID-based ring signature. It allows an ID-based ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-based setting. This scheme offers unconditional anonymity and can be proven forward- secure unforgetable in the random oracle model, assuming RSA problem is hard. This scheme is very efficient and does not require any pairing operations. The size of user secret key is just one integer, while the key update process only requires an exponentiation. We believe this scheme will be very useful in many other practical applications, especially to those require user privacy and authentication, such as ad-hoc network, e-commerce activities and smart grid. This current scheme relies on the random oracle assumption to prove its security. We consider a provably secure scheme with the same features in the standard model as an open problem and future research work.

REFERENCES

[1] M. Abe, M. Ohkubo, and K. Suzuki, “1-out-of-n signatures from a variety of keys,” in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inform. Security: Adv. Cryptol., 2002, vol. 2501, pp. 415–432.

[2] R. Anderson, “Two remarks on public-key cryptology,” Manuscript, Sep. 2000. (Relevant material presented by the author in an invited lecture at the Fourth ACM Conference on Computer and Communications Security, 1997.)

[3] (2014). [Online]. Available: http://en.wikipedia.org/wiki/ information retrieval

[4] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, “ID-based ring signature scheme secure in the standard model,” in Proc. 1st Int. Workshop Security Adv. Inform. Comput. Security, 2006, vol. 4266, pp. 1–16.

[5] A. K. Awasthi and S. Lal, “Id-based ring signature and proxy ring signature schemes from bilinear pairings,” CoRR, vol. abs/cs/ 0504097, 2005.

[6] M. Bellare, D. Micciancio, and B. Warinschi, “Foundations of group signatures: Formal definitions, simplified requirements and a construction based on general assumptions,” in Proc. 22nd Int. Conf. Theory Appl. Cryptographic Techn., 2003, vol. 2656, pp. 614–629.

[7] M. Bellare and S. Miner, “A forward-secure digital signature scheme,” in Proc. 19th Annu. Int. Cryptol. Conf., 1999, vol. 1666, pp. 431–448.

[8] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, “Security and privacy-enhancing multicloud architectures,” IEEE Trans. Dependable Sec. Comput., vol. 10, no. 4, pp. 212–224, Jul. \Aug. 2013.

[9] A. Boldyreva, “Efficient threshold signature, multisignature and blind signature schemes based on the gap Diffie-Hellman group signature scheme,” in Proc. 6th Int. Workshop Theory Practice PublicKey Cryptography: Public Key Cryptography, 2003, vol. 567, pp. 31–46.

[10] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Proc.Annu.Int. Cryptol. Conf. Adv. Cryptol., 2004, vol. 3152, pp. 41–55.

[11] E. Bresson, J. Stern, and M. Szydlo, “Threshold ring signatures and applications to ad-hoc groups,” in Proc. 22nd Annu. Int. Cryptol. Conf. Adv. Cryptol., 2002, vol. 2442, pp. 465–480.

[12] J. Camenisch, “Efficient and generalized group signatures,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 1997, vol. 1233, pp. 465–479.