PRO-SMS USING CLOUD: A PROTOCOL FOR END-END PRIVATE MESSAGING

N. Mohamed Azharudeen, P. Saravanan M. E. and Melvin Abraham
Department of IT, Sathyabama University, Chennai, India
E-Mail: Azharudeen051294@gmail.com

ABSTRACT

Privacy has been a major concern with respect to messaging now a day. In the traditional SMS system, the messages have the danger of being observed due to the presence of the SMS center in between the users who help to transfer of messages. A concern when confidential data needs to be shared through an SMS. These messages are transmitted as plaintext from the mobile user (MS) to the SMS center (SMSC) across a wireless net. The contents of these messages are stored in the systems of the network operators and can well be read by their personnel during the whole transmission process. And then the traditional SMS service offered by several mobile operators does not assure privacy of messages being transmitted over the net. To overwhelm, a protocol provides end-to-end privacy during the transmission of SMS over the mesh. This is accomplished by integrating Google's GCM service with information hiding techniques incorporated using cryptographic algorithms of AES.

Keywords: SMS, GCM, AES.

INTRODUCTION

Content Messaging is a striking constituent of cellular phone systems that permits customers to post and receive short, literary messages to and from other cell phones. Content informs, referred to all the more formally as the Short Message Service (SMS), has become an exponentially worldwide since 1995 with more than 6.1 trillion messages being sent every year in 2010. Even for all its ubiquity, a rule for the secure and productive conveyance of instant messages utilizing a shared topology has not been given out. Past work in SMS key administration has included customer server innovations for use in portable managing an account; personality based encryption, which requires a private key creating power; and adjustments of the costly Off-the-Record Messaging convention. PKI and shared secret key based key administrative arrangements have likewise been discharged industrially. As of now, however, there is no shared based key assention convention for SMS other than Moxie Marlinspike's adjustment of OTR. This undertaking is added to a second, more productive plan for key understanding and message security utilizing the Short Message Service Two separate conventions for secure content informing are created in this proposal.

The main set up a safe session on top of the Short Message Service using a common mystery. The second convention is utilized to set up that mutual mystery. The Secure SMS convention (SSMS) is motivated by the Secure Real-time Transport Protocol (SRTP) for secure Voice over IP (VoIP). SSMS sets up a protected session over SMS like SRTP sets up a safe session over RTP. SSMS encodes and verifies every message with a grouping number to avoid replay assaults. SSMS likewise has forward mystery properties that shield already transmitted messages on account of an endpoint bargain. The Key Agreement Protocol for SMS (KAPS) is roused by ZRTP. It utilizes the Elliptic Curve Differ-Hellman key consent to set up a common mystery without conjuring a trusted outsider. Credibility is given by key congruity (like SSH), and a verbal type of client verification. Together, key progression and client confirmation forestall man-in-the-center assaults from going unnoticed. KAPS is additionally strong to endpoint trade off as it restores crisp mystery when the aggressor is missing.

Related work

Sahai and Waters [3] presented the primary quality based encryption (ABE) where both the ciphertext and the mystery key are named with an arrangement of properties. A client can decode a ciphertext if and just if there is a match between the traits recorded in the ciphertext and the properties held by him. ABE plans can be arranged into two sorts: key-approach ABE (KPABE) and ciphertext-strategy ABE (CP-ABE). KP-ABE. In a KP-ABE plan, the ciphertext is connected with an arrangement of traits, while an entrance structure is inserted in the mystery keys [3], [10], [12], [6], [7], [13]. CP-ABE. In a CP-ABE plan, an entrance structure is embedded in the ciphertext, while the mystery keys are connected with an arrangement of qualities [4], [5], [16].

In the fundamental work [3], Sahai and Waters left an open issue, specifically how to develop an ABE plan where the mystery keys can be removed from different powers with the goal that clients can diminish the thrust on the focal power. Pursue [10] addressed this inquiry positively by proposing a MAABE plan. As said in [10], the specialized obstacle in building an MA-ABE plan is to oppose the agreement assaults. To beat this obstacle, every single mystery key of a client is attached to his GID. In [10], numerous powers must interface to instate the framework, and a focal power is required. Lin *et al.* [17] proposed an MA-ABE plan where the central power is not required. This plan was gotten from the appropriated key era (DKG) convention [18] and the joint zero mystery sharing (JZSS) convention [19]. To instate the framework, the numerous powers should cooperatively execute the DKG convention and the JZSS convention twice and k times, individually, where k is the level of the polynomial chose by every power. Every power must keep k+2 mystery keys.

Besides, this plan is ok-strong, to be specific the plan is secure if and just if the quantity of the traded off clients is close to k, and k must be settled in the setup stage. M¨uller et al. [20] proposed a conveyed CP-ABE plan. This plan was ended up being secure in the bland gathering [4], rather than diminishing to a many-sided quality suspicion. In this plan, a focal power is required to produce the worldwide key and issue mystery keys to clients. A completely secure multi-power CP-ABE (MACP-ABE) plan in the standard model was proposed by Liu et al. [21]. This plan depended on the past CP-ABE plan [8]. In this plan, there are various focal powers and quality pavers. The focal powers circulate identity related keys to clients, while the quality powers disseminate credit related keys to clients. Before having property keys from the trait powers, the client must acquire mystery keys from the different focal powers. This plan was developed in the bilinear gathering with the composite request (N = p1p2p3). Liquor and Waters [11] proposed another MA-ABE plan called decentralizing CP-ABE (DCP-ABE) plan. This plan enhanced the past MA-ABE plans that require joint efforts among numerous powers to starting the framework. In this plan, no participation between the numerous powers is required in the setup stage and the key era stage, and a focal power is not required. Strikingly, a dominant presence in this plan can join or leave the framework progressively without the need to reinitialize the framework. The plan was built in the bilinear gathering with the composite request (N = p1p2p3), and accomplished full (versatile) security in the arbitrary prophetic model. Besides, they additionally proposed two strategies to make a prime request bunch variation of their plan. All things considered, the powers can gather a client's quality by following his GID. Chase and Chow initially proposed [12] a security, protecting MA-ABE (PPMA-ABE) plan which enhanced the best plan [10] and uprooted the need of a focal power.

In past MA-ABE plans [10], [17], to acquire the Relating mystery keys, a client must present his GID to Every power. Subsequently, numerous powers can team up to gather the client's qualities by his GID. In [12], Chase and Chow gave a mysterious key using so as to issuing convention for the GID the 2-party secure figuring strategy. Accordingly, a gathering of powers can't work together to gather the clients qualities by following his GID. By and by, the different powers must collaborate to starting the framework. In the meantime, every pair of powers must execute the 2-party key trade convention to share the seeds of the chose pseudorandom capacities (PRFs) [22]. This plan is N -2 most tolerant, in particular the plan is secure if and just if the quantity of the traded off powers is close to N - 2, where N is the quantity of the dominant voices in the framework. The powers can't know any data about the client's GID, yet they can know the client's properties. Pursue and Chow [12] additionally left an open testing, research issue of the most proficient method to develop a PPMA-ABE plan without the need of participation among Powers. Li [15] proposed an MACP-ABE plan with responsibility.

In this plan, the unknown key issuing convention [12] was utilized. In particular, a client can be distinguished when he shared his mystery keys with others. In like manner, the various powers must coordinate to instate the framework. As of late, a protection safeguarding decentralized KP-ABE (PPDKP-ABE) plan was proposed by Han et al. [13]. In this plan, various powers can work autonomously with no joint effort. Particularly, a client can acquire mystery keys from various powers without discharging anything about his GID to them, and the focal power is not required. Interesting al. [14] proposed a protection saving decentralized CPABE (PPDCP-ABE) plan where straightforward access structures can be actualized. In any case, like that in [12], the compelling voices in these plans can likewise gather the client's properties. Unknown Credential.

In an unknown accreditation framework [23], a client can get a qualification from a guarantor, which incorporates the client's nom de plume traits. By utilizing it, the client can persuade an outsider that he gets a qualification containing the given nom de plume properties without discharging whatever other data. In a different show accreditation framework [24], a certification can be Evil presence began a subjective number of times, and can't be connected to each other. In this way, while developing our PPDCP-ABE, we accept that every client has gotten an unknown qualification including his GID and traits. At that point, he can persuade the numerous powers that he has a GID and holds the using so as to compare qualities the unknown accreditation system

PROPOSED SYSTEM

The Cipher-SMS gives a conclusion to-end security amid the transmission of SMS over the system. The Cipher-SMS convention is accomplished by utilizing cryptographic calculations of AES and MD5. The Cipher-SMS convention keeps the SMS data from different assaults, including SMS revelation, over the air (OTA) change, replay assault, man-in-the-center assault, and mimic assault. The proposed SMS based structure gives a low-transfer speed, solid, proficient and financially savvy answer for SMS Transmission. Figure SMS is the primary convention that is totally taking into account the symmetric key cryptography of AES and hash cryptography of MD5 for cell system. This Cipher-SMS sends lesser number of transmitting bits, creates less calculation overhead, and lessens transmission capacity utilization and message traded as contrast with existing conventions.

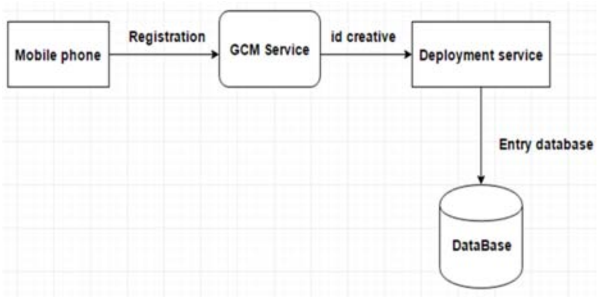
MODULES

- User Authentication Module
- Connecting to The AS
- Sending a message

- Message Sending Options and Their Working

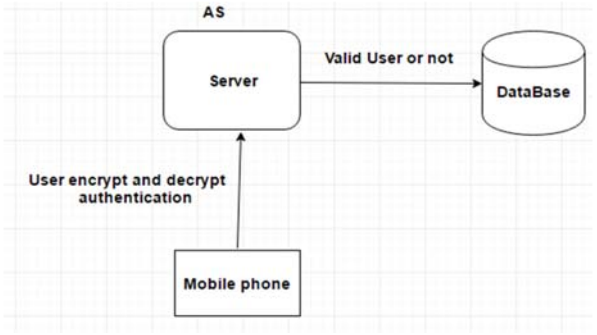
User authentication module

Alludes to every gadget enrolling itself with the GCM Server and being designated an enlistment ID. A GCM server application which will go about as a transfer between the Android gadgets. Gadget one will make an impression on the GCM server by summoning a callback URL gave by the server. Utilizing the beneficiary name GCM applications disjoin will pick the individual RegId from its store and send the message alongside RegId to the Google Cloud Messaging server.



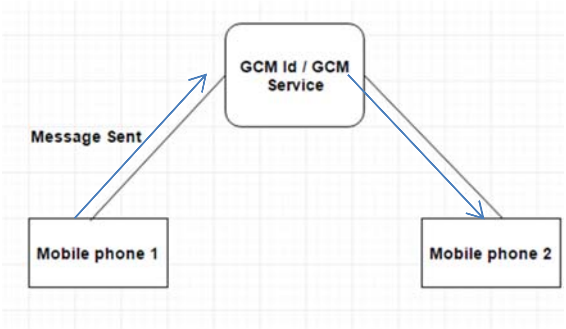
CONNECTING TO THE AS (Authentication Server)

The term remains for International Mobile Equipment Identity which is one of a kind to every cellular telephone permitting every client to be distinguished by his gadget. This is open on the portable phone. In every gadget it sends its IMEI number and enlistment ID to the AS which stores in the database. AS then sends the whole database list comprising of every associated client to every gadget.



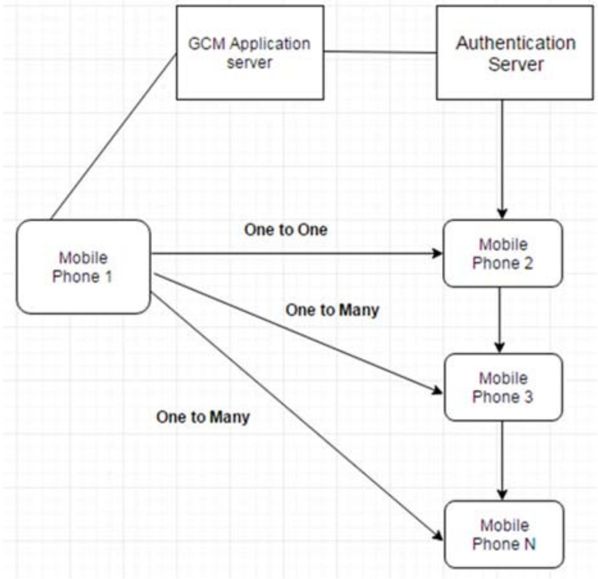
Sending a message

To make an impact on some other related users, sender scrambles and sends message close by recipient's name to AS. AS will rotate toward the sky contrasting recipient information and forward mixed message and beneficiary enrollment ID to GCM server. GCM server will send mixed message to the different customers who will then disentangle.

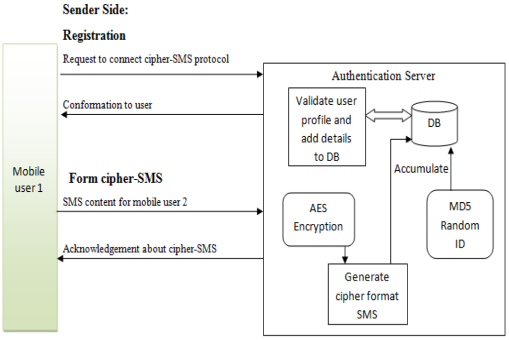


Message sending options and their working

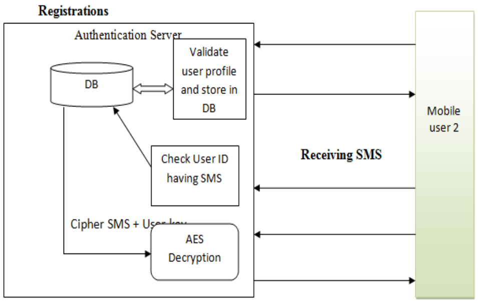
Making an impression on a solitary client (one-one) our numerous clients (one-numerous) through AES encryption with the establishment of the application, every cell phone is apportioned a gadget ID. The procedure starts by the separate cell phones naturally sending their gadget IDs to the GCM server. The GCM stores the gadget IDs of those clients and computes and gives back a special identifier, i.e., A Registration ID to each device. These enlistment IDs are then sent from the gadgets to the AS.



ARCHITECTURE


Sender Side:
Registration
Request to connect cipher-SMS protocol
Confomation to user
Mobile user 1
Form cipher-SMS
SMS content for mobile user 2
Acknowledgement about cipher-SMS
Authentication Server
Validate user profile and add details to DB
DB
Accumulate
AES Encryption
MD5 Random ID
Generate cipher format SMS

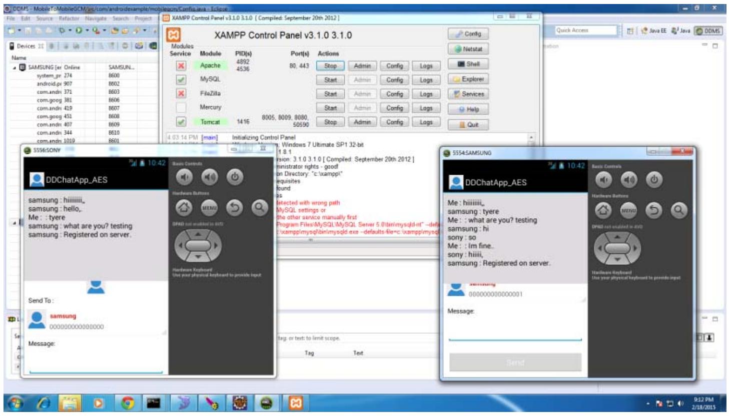
Receiver Side:



In this design, first the client registers in the application that is put away in the database. MD5 is utilized to accept the enlistment. On the off chance that enlistment is affirmed the client gets the affirmation to chip away at the application. This procedure ought to be finished by the other client too, so as to pass the correspondence. Two gadgets are required to keep in mind the end goal to convey the message. Initial, one client sends the message to another client over the system which will be continued by figure content. Figure content uses AES calculation which scrambles the test keeping in mind the end goal to change it into figure content. This procedure is finished by the sender.

At that point the beneficiary first checks whether this sender is enrolled in the database. In the event that it is enrolled, the messages are unscrambled and sent to the next client. This procedure will be done again from the recipient side of the sender, however the main change is there will be no acceptance part. The message will be straightforwardly passed.

SNAPSHOT

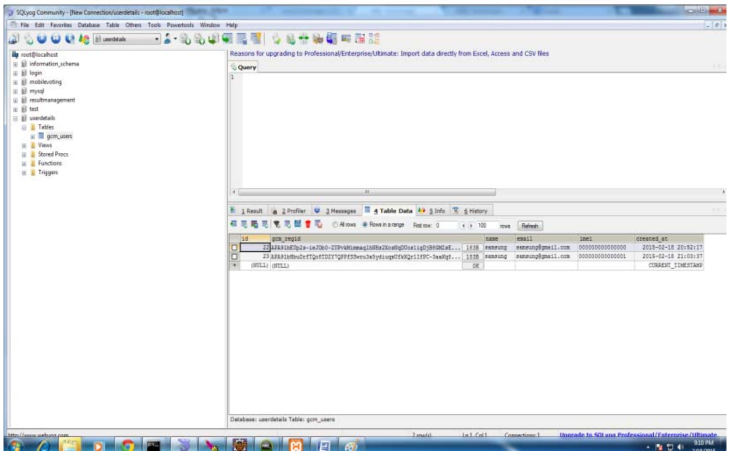


samsung : hiiiiiiii,,
samsung : hello,.
Me : : tyere
samsung : what are you? testing
samsung : Registered on server.

samsung
000000000000000

Me : hiiiiiiii,,
samsung : tyere
Me : : what are you? testing
samsung : hi
sony : so
Me : : Im fine..
sony : hiiiii,
samsung : Registered on server.

000000000000001



Reasons for upgrading to Professional/Enterprise/Ultimate: Import data directly from Excel, Access and CSV files

id	gcm_regid		name	email	imei	created_at
22	APA91bEDp2s-ieJOb0-ZUPvkMimmaqlhNHa2KoaNqDUoa1igDjB6GMZaE...	183B	samsung	samsung@gmail.com	000000000000000	2015-02-18 20:52:17
23	APA91bMbuDrfTQo8TDZY7QPPfS3wru3m5ydiuqxUfkXQr1IfPC-3aaKq6...	183B	samsung	samsung@gmail.com	000000000000001	2015-02-18 21:03:37
(NULL)	(NULL)	0K				CURRENT_TIMESTAMP

Database: userdetails Table: gcm_users

CONCLUSIONS

There is dependably a space for changes in any product bundle, however great and effective it might be finished. Be that as it may, the most imperative thing ought to be adaptable to acknowledge further change. At this moment we are simply managing content correspondence. In future this product might be reached out to incorporate components such as File exchange: this will empower the client to send documents to various arrangements to others by means of the talk application. Voice visit: this will be upgrade the application to larger amount where correspondence will be conceivable by means of voice calling us in telephone. Video visit: this will promote improved the element of calling into video correspondence.

REFERENCES

[1] J. Han, W. Susilo, Y. Mu, J. Zhou and M. H. Au. 2014. PPDCP-ABE: Privacy-preserving decentralized cipher-policy attribute-based encryption. in Proc. ESORICS'14, vol. 8713 of Lecture Notes in Computer Science, pp. 73-90, Springer, Switzerland.

[2] P. Bichsel, J. Camenisch, T. Groβ, and V. Shoup. 2009. Anonymous credentials on a standard java card. In Proc. CCS'09, pp. 600–610, ACM.

[3] A. Sahai and B. Waters. 2005. Fuzzy identity-based encryption. in Proc. EUROCRYPT'05, vol. 3494 of Lecture Notes in Computer Science, pp. 457-473, Springer, Heidelberg.

[4] J. Bethencourt, A. Sahai, and B. Waters. 2007. Ciphertext-policy attributebased encryption. In Proc. S& P'07, pp. 321-334, IEEE.

[5] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. CCS'07, pp. 456-465, ACM, 2007.

[6] V. Goyal, O. Pandey, A. Sahai and B. Waters. 2006. Attribute-based encryption for fine-grained access control of encrypted data. In Proc. CCS'06, pp. 89-98, ACM.

[7] R. Ostrovsky, A. Sahai, and B. Waters. 2007. Attribute-based encryption with non-monotonic access structures. In Proc. CCS'07, pp. 195-203, ACM.

[8] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. 2010. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Proc. EUROCRYPT'10, vol. 6110 of Lecture Notes in Computer Science, pp. 62-91, Springer, Heidelberg.

[9] B. Waters. 2011. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Proc. PKC'11, vol. 6571 of Lecture Notes in Computer Science, pp. 53–70, Springer, Heidelberg.

[10] M. Chase. 2007. Multi-authority attribute based encryption. In Proc. TCC'07, Vol. 4392 of Lecture Notes in Computer Science, pp. 515–534, Springer,Heidelberg.

[11] A. Lewko and B. Waters. 2011. Decentralizing attribute-based encryption. In Proc. EUROCRYPT'11, vol. 6632 of Lecture Notes in Computer Science, pp. 568-588, Springer, Heidelberg.

[12] M. Chase and S. S. Chow. 2009. Improving privacy and security in multiauthority attribute-based encryption. in Proc. CCS'09, pp. 121-130, ACM.

[13] J. Han, W. Susilo, Y. Mu and J. Yan. 2012. Privacy-preserving decentralized key-policy attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems. 23(11): 2150-2162.

[14] H. Qian, J. Li and Y. Zhang. 2013. Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure. in Proc. ICICS'13, vol. 8233 of Lecture Notes in Computer Science. pp. 363-372, Springer, Heidelberg.

[15] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong and D. Xie. 2011. Multi-authority ciphertext-policy attribute-based encryption with accountability. in Proc. ASIACCS'11, pp. 386-390, ACM.

[16] J. Herranz, F. Laguillaumie, and C. R_afols. 2010. Constant size ciphertexts in threshold attribute-based encryption. In Proc. PKC'10, vol. 6056 of Lecture Notes in Computer Science, pp. 19-34, Springer, Heidelberg.

[17] H. Lin, Z. Cao, X. Liang and J. Shao. 2008. Secure threshold multi authority attribute based encryption without a central authority. In Proc. DOCRYPT'08, vol. 5365 of Lecture Notes in Computer Science, pp. 426-436, Springer, Heidelberg.

[18] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin. 1999. Secure distributedkey generation for discrete-log based cryptosystems. In Proc. EUROCRYPT'99, vol. 1592 of Lecture Notes in Computer Science, pp. 295-310, Springer, Heidelberg.

[19] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin. 1996. Robust threshold dss signatures. In Proc. EUROCRYPT'96, vol. 1070 of Lecture Notes in Computer Science, pp. 354-371, Springer, Heidelberg.

[20] S. M uller, S. Katzenbeisser and C. Eckert. 2008. Distributed attribute-based encryption. In Proc. ICISC'08, vol. 5461 of Lecture Notes in Computer Science, pp. 20-36, Springer, Heidelberg.

[21] Z. Liu, Z. Cao, Q. Huang, D. S. Wong and T. H. Yuen. 2011. Fully secure multi-authority ciphertext-policy attribute-based encryption without random

oracles. In Proc. ESORICS'11, vol. 6879 of Lecture Notes in Computer Science, pp. 278-297, Springer, Heidelberg.

[22] M. Naor, B. Pinkas, and O. Reingold. 1999. Distributed pseudo-random functions and KDCs. In Proc. EUROCRYPT'99, vol. 1592 of Lecture Notes in Computer Science, pp. 327-346, Springer, Heidelberg.

[23] J. Camenisch and A. Lysyanskaya. 2011. An efficient system for nontransferable anonymous credentials with optional anonymity revocation. In Proc. EUROCRYPT'01, vol. 2045 of Lecture Notes in Computer Science, pp. 93-118, Springer, Heidelberg.

[24] G. Persiano and I. Visconti. 2004. An efficient and usable multi-show nontransferable anonymous credential system. In Proc. FC'04, vol. 3110 of Lecture Notes in Computer Science, pp. 196-211, Springer, Heidelberg.

[25] D. Boneh and X. Boyen. 2004. Short signatures without random oracles. In Proc. EUROCRYPT'04, vol. 3027 of Lecture Notes in Computer Science, pp. 56-73, Springer, Heidelberg.

[26] A. Beime. 1996. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel.