XTR Cryptosystem for SMS Security

Ashok Kumar Nanda, *Member, IACSIT* and Lalit Kumar Awasthi, *Member, IACSIT*

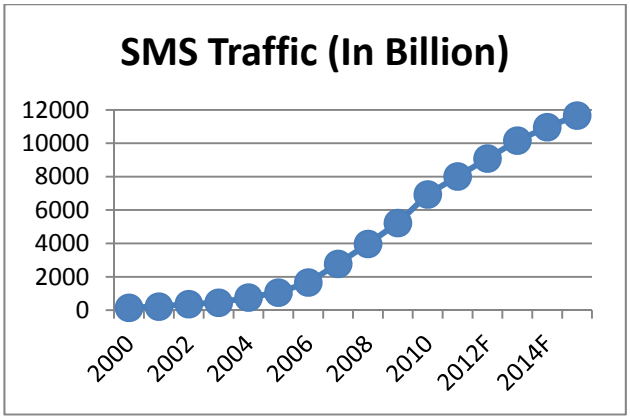
***Abstract*—Short message service (SMS) is getting more popular now-a-days. It will play a very important role in the future business areas which will be based on mobile commerce (M-Commerce). Presently, many business organizations use SMS for their business purposes. SMS's security has become a major concern for business organizations and customers. There is a need for an end to end SMS Encryption in order to provide a secure medium for communication. Security is main concern for any business company such as banks who will provide these mobile banking services. Till now there is no such scheme that provides complete SMSs security. The transmission of an SMS in GSM network is not secure at all. Therefore, it is desirable to secure SMS for business purposes by additional encryption. In this paper, we have analyzed different cryptosystems for implementing security for SMS's. Here, we have given a proposal to incorporate XTR cryptosystem and XTR – NR message recovery signature scheme into existing SEESMS frames. We have plan to implement XTR cryptosystem with XTR – NR message recovery signature scheme. So this enhanced scheme will increase the current security level and fastest speed with respect to key generation, encryption decryption with small key size.**

***Index Terms*—Performance analysis, SMS security, XTR cryptosystem, XTR – NR message recovery signature scheme.**

I. Introduction

SMS stands for Short Message Service. In 1992, the first SMS technology enables the sending and receiving of messages between mobile phones. SMS message contains at most 140 bytes (1120 bits) of data, so one SMS message can contain up to 160 characters (if 7-bit character encoding is used) and 70 characters (if 16-bit Unicode UCS2 character encoding is used). SMS provides a convenient means for people to communicate with each other using text messages via mobile devices or Internet connected computers. It is possible to send ringtones, pictures, operator logos, wallpapers, animations, business cards and WAP configurations to a mobile phone with SMS messages. One major advantage of SMS is that it is supported by 100% GSM mobile phones. Almost all subscription plans provided by wireless carriers include inexpensive SMS messaging service. The mobile messaging market is growing rapidly and is a very profitable business for mobile operators. It can be seen from Figure I that the total number of SMS sent globally as exponential curve during 2000 to 2015F.

As per Table I, Many people of United States, EU5 (UK, Germany, France, Spain and Italy) and Japan prefer information exchange as text message (SMS) as compared to instant message by mobiles. The major advantages of SMS are: i) SMS is a personal like phone call but a person can read at any time without any disturbance to the work ii) Messages are instantly recorded so that one can refer at any time iii) It is relatively less SPAM free iv) SMS is discreet in nature v) SMS bills are considered as negligible vi) SMS is more convenient for deaf and hearing-impaired people to communicate vii) SMS is a store-and-forward service viii) SMS doesn't overload the network as much as phone calls ix) It is possible to send SMS many people at a time x) easy to use xi) common messaging tool among consumers xii) works across all wireless operators xiii) no specific software required to installation. The disadvantages of SMS are: i) Consumes more time to type as compared to phone call ii) No proper authentication of SMS sender iii) Length of SMS is maximum 140 - 160 characters iv) Reliability and versatility can be compromised when using SMS v) does not support sending media, including videos, pictures, melodies or animations vi) does not offer a secure environment for confidential data during transmission. The same table indicates that few people of United States, EU5 (UK, Germany, France, Spain and Italy) and Japan access financial services such as bank account information and financial news or stock quotes using SMS because SMS are not fully secure in wireless environment due to its broadcast nature.



Source: Portio Research Ltd.

Fig. 1. Growth of SMS – world from 2000 to 2015F (F stands for forecast).

TABLE I: Mobile behavior in United States, EU5 (UK, Germany, France, Spain and Italy) and Japan – October, November, December 2010 Percent of Total Mobile Audience (Age 13+)

	US	Europe	Japan
Used Messaging			
Sent Text Message	68%	82.7%	41.6%
Instant Messaging	17.2%	14.2%	3.6%
Accessed Financial Services			
Bank Accounts	11.4%	8%	7%
Financial news or stock quotes	10.2%	8%	16.5%

Source: comScore MobiLens (Feb 2011)

SMS is getting more popular now-a-days. It will play a very important role in the future business areas of mobile commerce (M - Commerce) and mobile banking (M -

Manuscript received June 26, 2012; revised July 20, 2012.

The authors are with the Computer Science and Engineering Department at National Institute of Technology, Hamirpur, Himachal Pradesh, India (e-mail: ashokkumarnanda@yahoo.com, lalit@nith.ac.in).

DOI: 10.7763/IJET.2012.V4.495

Banking). Up to now many business organizations use SMS for their business purposes. SMS's security has become a major concern for business organizations and customers. There is a need for an end to end SMS Encryption in order to provide a secure medium for communication. Security is main concern for any business company such as banks who will provide these mobile banking services. Currently there is no such scheme that provides complete SMSs security.

Presently researchers proposed some security concepts regarding SMS security. Most of the proposals are software frames to be installed on mobile device and /or on the SIM cards to implement security.

This paper proposed some idea regarding to exchange SMS in secure manner at peers' level. It requires a software framework to certify the signature of mobile of both sender & receiver. Here users are allowed to choose cryptosystems and security parameters for transmitting secure message to achieve better cost and efficiency of the operation with low memory space and energy consumption.

Rest of paper is organized as follows. Section II provides about related work of SEESMS. Section III describes about SMS Security. Section IV presents regarding SMS encryption. Section V discuss XTR algorithm. Section VI is discussed the comparison of different traditional cryptosystem with XTR. Section VII represents XTR-NYBERG-RUEPPEL (XTR – NR) message recovery SIGNATURE scheme and followed by discussion with future work.

II. Related Work

Particularly about Secure Extensible and Efficient SMS (SEESMS), the proposal presented by Alfredo De Santis and his team members [1] which designed a Java based framework for exchanging secure SMS. They considered RSA, DSA and ECDSA algorithms. Here we have considered the same SEESMS frame with Elgamal and XTR cryptosystems for SMS security purpose.

III. SMS Security

Now-a-days, SMS is used for M-Commerce purpose. SMS will play a very vital role in the future banking or commercial purpose because of its simplicity and cheapness. Upcoming payment system will be based on the mobile device by using SMS. Money can be debited or credited from the bank through the SMS by using the GSM network. But some security related services of SMS should be available when we go for such M-Commerce or M-Banking.

Network operators are demanding spam control and anti-spoofing capabilities to protect their SMS network and subscribers. When customers have complaints regarding SMS, operators do have not any other options to block such types of SMS rather than blocking such SMS subscribers.

There are some security gaps for SMS. Such as Snooping, SMS Interception, Spoofing, Modification, Faking, Flooding, Spam and other SMS-related scams are a global problem. There are many security threats to mobile subscribers and operators. It is easy to sneak a virus as a Trojan attachment in an SMS message.

There are many incidents of rogue operators gaining unauthorized access to the SS7 networks of major service providers and routing millions of text messages into those networks. Therefore it does congestion and blocking other genuine SMSs. So it may delay or may not reach to recipients. Quite often they are attempts at delivering massive volumes of spam into the network. Service providers often end up building new facilities to deal with the increase in messaging traffic - with no corresponding increase in revenue. Spoofing is great opportunity for fraud - coaxing users into providing sensitive personal data, which results in a financial windfall for the bad guy. In fact, there have been reports of spoofing cases where messages are sent disguised as official government announcements for emergencies.

Current trends in mobile devices are raising the probability of attack. Devices have much more functionality than they used to – they have become small computers.

Currently users expect high level of security while doing mobile transactions. Some familiar problems are mentioned here for popular M-Commerce: data confidentiality while transmitting, data and application access must be controlled, data integrity, loss of device must have limited impact, and non repudiations. When SMS used for M-Commerce the following services are required [2]: Confidentiality: only the valid communicating users can view the SMS. Integrity: the SMS can't be tampered by the intruders. The system should be able to find out such alteration. Non-repudiation: no party can deny the receiving or transmitting the data communicating between them. Authentication: each party has to have the ability to authenticate the other party. Authorization: it has to be ensured that, a party performing the transaction is entitled to perform that transaction or not.

We realized that security is most essential for mobile users and network operators to avoid different threats at different levels. The transmission of an SMS in GSM network is not secure at all. Therefore it is desirable to secure SMS for business purposes by additional encryption.

IV. SMS Encryption

SMS encryption is the process of transforming SMS information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information. Encryption is also used to protect data in transit, for example data being transferred via networks mobile telephones Encrypting data in transit also helps to secure it as it is often difficult to physically secure all access to networks. Encryption can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message. Successfully using encryption to ensure security may be a challenging problem [3]. There are so many algorithms are available for SMS encryption. The application of SMS encryption algorithms is dependent upon operating system of the types of mobile device. The other factors like energy consumption, speed, security and others are to be considered while choosing the encryption techniques.

V. XTR ALGORITHM [4]

XTR is an algorithm for public-key encryption. XTR stands for 'ECSTR'. It stands for Efficient and Compact Subgroup Trace Representation. From a security point of view, XTR is a traditional discrete logarithm system: For its security it relies on the difficulty of solving discrete logarithm related problems in the multiplicative group of a finite field. Some advantages of XTR are its fast key generation (much faster than RSA), small key sizes (much smaller than RSA, comparable with ECC for current security settings), and speed (overall comparable with ECC for current security settings) [5].

The XTR cryptosystem [5] was originally proposed in the context of using the trace representation of finite field elements to represent them efficiently and compactly. However, the representation and formulae given in the original paper are essentially the same as those of third-order characteristic sequences. XTR was specifically presented using the field GF ($p2$) and the polynomial $f(x) = x^3 - ax^2 + a^p x - 1$. This was done to optimize the efficiency of calculation and representation.

Let us first note that if we choose $q = p^2$, then a third-order characteristic sequence has order Q dividing $q^2 + q + 1 = p^4 + p^2 + 1 = (p^2 + p + 1)(p^2 - p + 1)$. Note that the subgroup of order $p^2 - p + 1$ within GF (p^6) is not contained in any proper subfield. To avoid an index calculus attack, we prefer choosing sequences corresponding to this subgroup. Thus, Q should divide $p^2 - p + 1$. If α is a root of the polynomial $f(x) = x^3 - ax^2 + bx - 1$, then $a = \alpha + \alpha^{p^2} + \alpha^{p^4}$ and $b = \alpha^{-1} + \alpha^{-p^2} + \alpha^{-p^4}$. But, using the relation $\alpha^{p^2 - p + 1} = 1$, we get $b = \alpha^{-1} + \alpha^{-p^2} + \alpha^{-p^4} = \alpha^p + \alpha^{p^3} + \alpha^{p^5} = a^p$

Let $\{s_k\}$ be the sequence generated from this polynomial. Using this same relation, we see that

$$s_{-k} = \alpha^{-k} + \alpha^{-kp^2} + \alpha^{-kp^4} = (\alpha^k)^p + (\alpha^{kp^2})^p + (\alpha^{kp^4})^p = s_k^p$$

Hence, we can restrict the public key to s_m and need not calculate the negative terms s_{-k} when performing calculations.

Finally, we shall note that, in the original paper, Lenstra and Verheul present a method for choosing p and a representation of GF (p^2) so that all computation takes place over GF (p).

VI. COMPARISON OF DIFFERENT ALGORITHMS

This section presents the strength, key generation time, encryption time, decryption time and security strength of different encryption algorithms.

There are so many cryptosystems are available in market to implement. Some of traditional crypto algorithms are compared in below mentioned Table II with respect to security level, implementation of number of bits and their encryption speed. We can choose the suitable algorithms depends on our predefined parameter like mobile device, importance of security requirements, key generation time, encryption/decryption speed, energy consumption and space size. Here we have plan to improve the performance of different parameters of the article [6] by using latest light weight cryptosystem.

TABLE II: RELATIVE STRENGTH COMPARISON OF ENCRYPTION ALGORITHMS [7]

Algorithms	Security Level	Speed	Implementation	Remarks
XTR	-	Fastest	-	Small key size
IDEA	Very High	Fast	Upto 128 bit Shared Secret	-
Blowfish	Military Grade	Fastest	256 to 448 bits Shared Secret	Stronger Than DES
DES	Low	Fast	40 to 56 bit Shared Secret	Most Widely Used. Avoid to use when possible
RSA	Military Grade	Very Slow	2048 bit Public Key	-
MD5	High	Slow	128 bit Message Digest	Messages haven't been altered.
SHA	High	Slow	160 bit Message Digest	Messages haven't been altered.

VII. XTR-NYBERG-RUEPPEL (XTR – NR) MESSAGE RECOVERY SIGNATURE SCHEME

From a security point of view, XTR is a traditional discrete logarithmic system. For its security it relies on the difficulty of solving discrete logarithm related problems in the multiplicative group of a finite field. Some advantages of XTR are its fast key generation (much faster than RSA), small key sizes (much smaller than RSA, comparable with ECC for current security settings), and speed (overall comparable with ECC for current security settings) [5]. In 1996, the Nyberg-Rueppel signature scheme was improved as ElGamal version. In 2000, the XTR-Nyberg-Rueppel version was presented. Then, the XTR – Blind – Nyberg – Rueppel version and the verifiable encryption of XTR-Nyberg-Rueppel version were presented in 2003 and 2007, respectively. We are considering XTR version of the Nyberg-Rueppel (NR) message recovery signature scheme. XTR can in a similar way be used in other 'ElGamal-like signature schemes.

A. XTR-NR Signature Generation [5]

It is stated that to sign a message M containing an agreed upon type of redundancy using the XTR version of the NR protocol, Alice does the following:

Let *P, q & Tr(g)* be shared XTR public key data.

1) Alice selects a random integer $u \in [2, q-3]$, and $n = u$ and $c = T_r(g)$ in $S_n(c) = (c^{n-1}, c^n, c^{n+1}) \in GF(P^2)^3$ so $S_u(T_r(g)) = (T_r(g^{u-1}), T_r(g^u), T_r(g^{u+1})) \in GF(p^2)^3$ where q is prime number
2) Alice determines a symmetric encryption key K based on $T_r(g^u) \in GF(p^2)$.
3) Alice uses an agreed upon symmetric encryption method with key K to encrypt M, resulting in the encryption E.
4) Alice computes the (integer valued) hash h of E.
5) Alice computes $s = (k \cdot h + u) \bmod q \in \{0, 1 \ldots q-1\}$.
6) Alice's resulting signature on M is (E, s).

B. XTR-NR Signature Verification [5]

It is assumed that Alice's XTR public key data for digital signatures consist of p, q, $T_r(g)$, and $T_r(g^k)$ for a secret integer k that is known only to Alice. However, in addition it is assumed that not only $T_r(g^k)$ but also $T_r(g^{k-1})$ and $T_r(g^{k+1})$ (and thus $S_k(T_r(g))$) are available to the verifier. These additional GF(p^2) elements are either part of the public key or they are reconstructed by the verifier. $T_r(g^{k-1})$ (or $T_r(g^{k+1})$) can be reconstructed from p, q, $T_r(g)$, $T_r(g^k)$, and $T_r(g^{k+1})$ (or $T_r(g^{k-1})$) using an explicit and easily computed formula. Reconstruction of $T_r(g^{k+1})$ (or $T_r(g^{k-1})$) given just (p, q, $T_r(g)$, $T_r(g^k)$) requires additional assumptions and a slightly more involved computation. To verify Alice's signature (E, s) and to recover the signed message M, verifier Bob does the following.

1) Bob checks that $0 \le s < q$; if not failure.
2) Bob computes the hash h of E.
3) Bob replaces h by $-h \bmod q \in \{0, 1 \ldots q - 1\}$.
4) Bob applies Algorithm 5.27 *stated in [5] to Tr(g), $S_k(T_r(g))$ (*with k unknown to Bob*), $a = s$, and $b = h$ to compute $T_r(g^s \cdot g^{hk})$ (*which equals $T_r(g^u)$*)*.
5) Bob determines a symmetric encryption key K based on $T_r(g^s \cdot g^{hk}) \in GF(p^2)$.
6) Bob uses the agreed upon symmetric encryption method with key K to decrypt E resulting in M.
7) The signature is accepted if and only if M contains the agreed upon redundancy.

XTR – NR signature generation is faster 3 times than traditional NR signature generation and verification are faster than XTR – NR signature verification is faster 1.75 times than traditional methods. For both signature generation & verification, with considering identical equal length of other variants of the hybrid of NR scheme, the overhead part of length depending on the desired security (i.e. group size) and the length of message part is dependent on message itself the agreed upon redundancy and symmetric encryption.

VIII. Discussion and Future Work

The importance of SMS will increase because many financial Institutes and business organizations will use then if they are secured. We need to provide proper security to SMSs which will carry business transactions with confidential and valuable data. We have to improve design of security level for SMS, mobile device and wireless networks. From Table II, we conclude that XTR cryptosystem provides more security and is faster in speed with respect to key generation, encryption and decryption with small key size.

Our future work is to implement XTR cryptosystem with XTR – NR message recovery signature scheme for mobile phones for SMS security.

Acknowledgements

This research work is supported by ministry of human resource development (MHRD), Government of India. The authors would like to thank the anonymous reviewers for their insightful comments.

References

[1] D. Santis, A. Castiglione, A. Cattaneo, G. Cembalo, M. Petagna, F. Petrillo, U. F, "An Extensible Framework for Efficient Secure SMS," in *Proc. 4th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)* - 2010, pp. 843 – 850.

[2] A. Hossain, S. Jahan, M. M. Hussain, M. R. Amin, and S. H. Shah Newaz, "A proposal for enhancing the security system of short message service in GSM," in *Proc. International Conference on Anti-counterfeiting, Security, and Identification (ASID)* - 2008, pp: 235 – 240.

[3] Encryption - Wikipedia, the free encyclopedia. [Online]. Available: http://en.wikipedia.org/wiki/Encryption

[4] K. Giuliani and G. Gong, Analogues to the Gong-Harn and XTR Cryptosystems. [Online]. Available: http://comsec.uwaterloo.ca/~ggong/publication/CACR03-Analogue.pdf

[5] A. K. Lenstra and E. R. Veheul, An Overview of the XTR Public Key System. [Online]. Available: http://www.win.tue.nl/~klenstra/xtrsurvey.ps

[6] A. Mary and S. Devrim, "SMS Security: An Asymmetric Encryption Approach," in *Proc. Sixth International Conference on Wireless and Mobile Communications (ICWMC)* - 2010, pp. 448-452.

[7] This site has some good info for those concerned. [Online]. Available: http://security.resist.ca/crypt.shtml

Mr. Ashok Kumar Nanda passed M.Tech in Computer Science & Engineering (CSE) from Guru Jambheswar University (GJU), Hissar, Haryana, India. He has around 8yrs teaching experience for both UG & PG courses. He was Associate Professor during Dec'06 to Jun'09. After that, he joined as full time research scholar in Cosmputer Science & Engineering (CSE) Department at National Institute of Technology (NIT), Hamirpur, Himachal Pradesh, India. His research area is light weight cryptography on Mobile devices. He has published 2 International Journal papers and 8 International Conferences papers. He is life member of Cryptography Research Society of India (CRSI), Computer Society of India (CSI), Indian Society for Technical Education (ISTE), graduate student member of IEEE and associate member of The Institution of Engineers (India) and member of International Association of Computer Science and Information Technology (IACSIT), International Association of Engineers (IAENG), Internet Society.

Prof. Lalit Kumar Awasthi was born on 19 May 1966. He is a senior most Professor in Computer Science & Engineering (CSE) Department at National Institute of Technology, Hamirpur, Himachal Pradesh, India. He has completed M. Tech. CSE from Indian Institute of Technology (IIT), Delhi in 1993 and Ph. D. from Institute of Technology (IIT), Roorkee, India in 2003. He holds *First position* in Merit List of Shivaji University, India for B. Tech. In Computer Science & Engineering. He joined CSE Department at NIT, Hamirpur, Himachal Pradesh, India in August 1988 as lecturer. He has more than 23yrs teaching experience. Recently he has joined as Director of Atal Bihari Govt. Engineering College Pragati Nagar, Himachal Pradesh, India. He is member of many National bodies as expert, such as National Board of Accreditation (NBA), All India Council of Technical Education (AICTE), India. His research area includes Checkpointing, Grid Computing, Mobile Computing and cloud computing. Under his guidance, five students have completed their PhD degree, and other five are pursuing their Ph. D. He has guided many M. Tech and B. Tech students for their dissertation/projects. He has published and presented more than 154 papers in National /International Journals/Conferences and book chapters. He is reviewer of many reputed International journals like IEEE, Taylor and Frances, Inderscience etc. He is Life Member of Computer Society of India (CSI), Indian Society for Technical Education (ISTE), Fellow Member of The Institution of Engineers (India) and Senior Member of IEEE and member of International Association of Computer Science and Information Technology (IACSIT), International Association of Engineers (IAENG), Internet Society.