ISSN:0975-9646

ECC based Fault Tolerant and Secured E-Payment Protocol *

Aditya Bhattacharyya[#1], Sanjit Kumar Setua[*2]

[1,2] *Department of Comp. Sc, Vidyasagar University*
West Bengal, India

Abstract- A digital system is very vulnerable to the faults- may be natural or injected. Fault tolerance is a very important feature of a highly critical or secured system. Efficient detection of errors & verification of the correctness of computations may be a sufficient countermeasure for many security applications to provide a system which can resist fault based attacks. In this paper we consider hashed elliptic curve based payment protocol. Different error detection schemes & fault tolerant schemes have been considered in this paper. Point validation (PV) in elliptic curve cryptography is considered as a scheme against fault-analysis attack. Though, PV alone is not sufficient against all attacks, we consider recomputation along with PV. These structures provide a high probability of detecting errors due to faults. Additionally, we show that using N-modular redundancy, the fault –tolerability of the system can be increased.

***Keywords*: Elliptic curve cryptography, Fault Tolerance, Error detection, Recomputation.**

* This is an extended version of the awarded best paper [19] presented at the 3rd ICACNI, 2015, India.

I. INTRODUCTION

E-commerce has become a growing technology in the field of internet technology. The main concern is the customer's privacy. There are lots of works in maintaining customer's privacy on e-commerce. Blind signature schemes are one of them. They have been widely used to protect the right of a customer's privacy in the untraceable electronic cash systems [5]. A fraud customer can be identified by payment gateway which maintains tracing protocol. In order to prevent criminal

activities or to trace the fraud user we need some anonymity revocation mechanisms.

Based on the general payment model of Abad-Peiro et. al [10] ,we have used the following entities in our protocol

Customer (C): A user who wants to buy the products.

Merchant (M): An entity who sells the products.

Issuer (I) : Bank in which the customer having an account

Acquirer (A) : Bank in which the merchant having an account

Payment Gateway(PG) : Acts as an interface between the acquirer & issuer for the purpose of payment clearance.

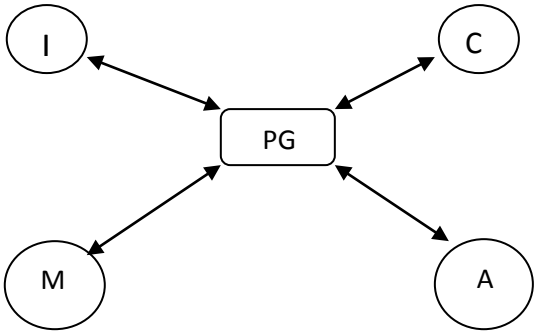


Fig 1 : Function of Payment Gateway

There is no direct interaction between client & merchant. All the correspondence & transactions should be sent through payment gateway. A payment gateway is connected to all customers, merchants and banks through Internet and responsible for the speed, reliability and security of all transactions.

There are lots of works in side channel analysis in ECC. But fault analysis attack in ECC contains a considerably few papers. [5] proposed an attack on RSA . They also proposed a countermeasure that makes the computation correct. [6] also proposed a fault-analysis attack on ECC. They suggest a countermeasure based on point validation(PV) . But the fact is that this method is not sufficient for all fault analysis attack. [4] presented a new fault based attack- Sign Change Fault attack (SCF) where change of sign in a point can change only the sign of y-coordinate.

To make e-commerce more secured and fast, numerous protocols have been proposed in this field. Chaum et.al proposed the first untraceable electronic system in the year 1982 [5]. After that, various technologies & protocols have been proposed. Bellare et.al [8] proposed iKP Secure electronic payment system. Here i=1,2,3 is a set of payment protocol based on public key cryptography. When the value of i increases from 1 to 3, the security requirements met by iKP increases. Kungspisdan's contribution in the area of mobile payment protocol revolutionizes the area [7]. They proposed a new secure lightweight mobile bill payment

protocol in simpler way satisfying necessary network security measures. Tellez contributed a client centric anonymous payment model PCMS which is combination of two sub protocols- Merchant registration protocol & Payment protocol [9] . They implemented their protocol on NOKIA N95 through PCMS wallet and they claimed that the mobile payment protocol preserves the security. Beside this Xing et.al. [4], Liu & Huang [1], Raulynaitis et. al [3] have enriched the research area.

Miller and Koblitz introduced the concept of Elliptic Curve Cryptography (ECC) which has attracted increasing attention in recent years due to its shorter key length and higher security in comparison with other public key cryptosystem like RSA. Such advantages make elliptic curve cryptography a better choice for public key cryptography. On-line e-cash systems require constant and real time involvement of the bank for every payment transaction, which demands excessive communication and computation costs.

Again a cryptographic hash function is a function which is considered practically impossible to invert. In security aspect, it supports digital signature , message authentication code (MAC) & different authentication. Beside this, the characteristics of hash (impossible to modify the message without changing the hash, infeasible to find two different messages with the same hash, infeasible to modify a message without changing the hash , etc) makes it popular among the cryptographers. It is very easy to hash deterministically and efficiently into an elliptic curve. With the hardness of discrete logarithm problem of elliptic curve and hash function, any system seems to be infeasible to attack. In this paper, we make extension of our previous work. We give emphasis to make our protocol fault tolerable, more reliable.

Rest of the paper is organized as follows . In the next section a brief introduction on the elliptic curve cryptography is given. Different error detection schemes in ECC has been described in the section 3. Section 4 represents our protocol graphically. Security measures and fault tolerance is described in section 5. In section 6 we conclude our paper.

II. ELLIPTIC CURVE CRYPTOGRAPHY PRELIMINARIES

An elliptic curve E over a field K is the set of solutions to the cubic equation

$E:F(x,y)= y^2+ a_1xy+ a_3y-x^3-a_2x^2-a_4x-a_6=0$ where $a_i \in k$ & the discriminant is given by

$\Delta = -d_2^2d_8 -8d^3_4-27d_6^2 +9d_2d_4d_6 \neq 0$

where $d_2= a_1^2+4a_2$,

$d_4 =2a_4 + a_1a_3$,

$d_6=a_3^2 + 4a_6$,

$d_8= a_1^2 + 4a_2a_6-a_1a_3a_4 + a_2a_3^2 – a_4^2$;

Now for the prime field, E can be rewritten as :

$$y^2 = x^3 + ax + b \bmod p.$$

together with the point at infinity O where

$$4a^3+27b^2\neq0$$

Again for the binary field E is transformed to :

$$y^2 + xy = x^3 + ax^2 + b$$

There are Point addition, Point doubling operation are performed on Elliptic curve. But the most effective and more secured operation is Elliptic Curve Scalar Multiplication (ECSM). If a point P(x,y) lies on the curve E and it is multiplied by a scalar k i.e., kP, then we can write Q=kP and Q lies on the curve E.

III. ERROR DETECTION SCHEMES IN ECC

The error detection schemes of ECC mainly in categories- Point Validation , Time redundant schemes & Hardware redundant schemes[18]. We give our emphasis on first two schemes. We will also consider three types of time redundant schemes. In the analysis part, we consider reliability of the schemes.

3.1 Point Validation (PV)

To resist fault attack Point validation can be used as the countermeasures [14][17]. For its simplicity (few finite operations are required) , its implementations in hardware module is relatively easy. A PV module is a computational module that takes a point Q as its input and checks whether the point is on the elliptic curve E – which is shown in the figure 2.

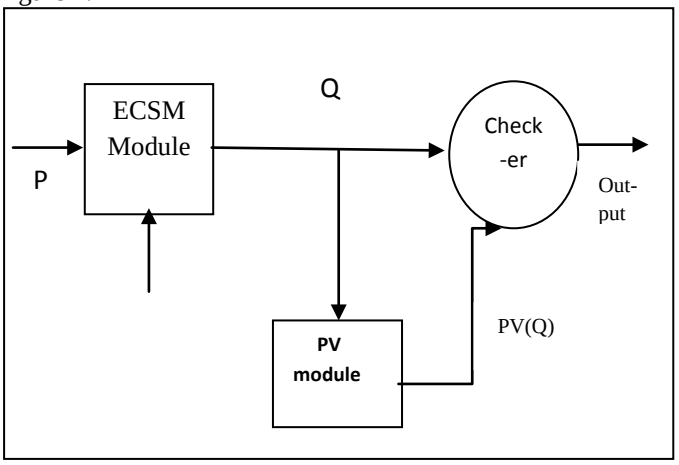


Fig 2: Elliptic curve PV module

If fault occurs , $Q_i \neq kP$. Let the number of elements be q & Q_i has (q-1) different representations. Then for $Q_0=Q_1$ & $Q_i \neq kP$ (undetected error). P_r (undetected error) $\approx (q-1)/q^3 \approx 1/q^2$,.

For sufficient large value of q, the probability factor for detecting undetected error become very small. But the fact is that alone PV is not sufficient to resist SCF attack[18]. Although its simplicity makes it acceptable to the cryptographic designer.

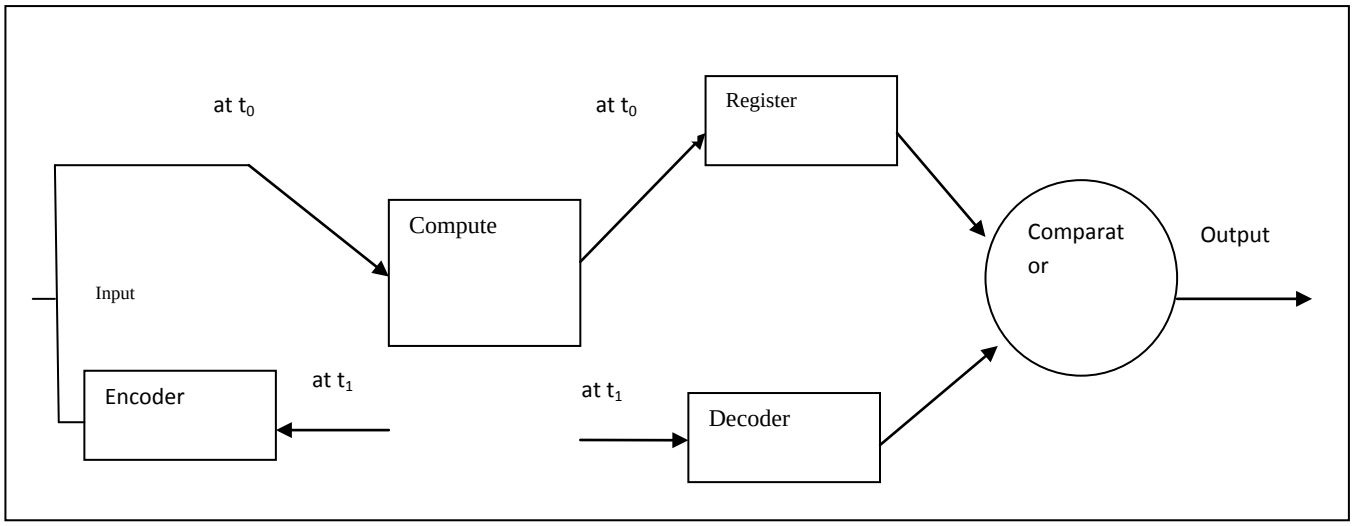


Fig 3: ECC based recomputation scheme

3.2 Time Redundant Schemes

In this scheme the time is a parameter to detect error. Here the result is computed twice.(one at time t_0 then at time t_1). Then the result is compared to measure. The re-computation and parallel computation based two schemes are used to detect the errors.

There are two data paths-lower and upper. The ECSM module is multiplexed at two different times t_0 and t_1 for upper and lower data path respectively. Here the register is kept for storing the result for upper data path. For lower data path , decoder transforms the result & send it to the comparator for comparing the result with previous one. Similarly for recomputation, the two ECSM modules perform parallel. Here the register or delay unit is used to synchronize the input.

IV. OUR PROTOCOL

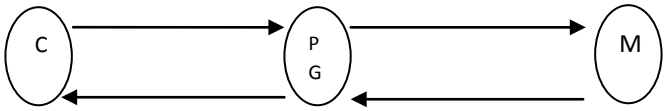
Notations: The following symbols are used to represent messages in our protocol :

As this is an extended version, we only introduce the steps through figure.

Notations	Description
P	Point on the curve
kP	Multiplication of point P with scalar k
P	A large prime number
Q	A large prime number such that $q\|\#E(Fp)$.
T_c	Temporary ID of Customer/ Client
TID	Identity of transaction that includes time & date of transaction
ID_x	Identity of X that contains the contact information of X
OD	Order description
N	Nonce/ Random number & timestamp generated to protect against replay attack
Price	Cost / Payment amount
h( )	One way hash function
OI	Order Information contain TID, OD, h(OD, Price)
K_{C-M}	Secret share between client & Merchant
r,s	Session keys used to encrypt the message
PRequest	Payment Request
E	Encrypted form of Message
Pack	Payment Acknowledge
ASrequest	Amount Subtraction Request
ASack	Amount Subtraction Acknowledge
ACresponse	Amount Claim Response
ACack	Amount Claim acknowledge
PG	Payment Gateway
TC	Type of card (Debit/Credit)
CKx	Time at the clock used by X
$KS_{A-B\,t}$	Shared the key between A to B for t bit shifting
TS	Transaction status (whether Accepted or Rejected)

I. Registration and Payment Initialization

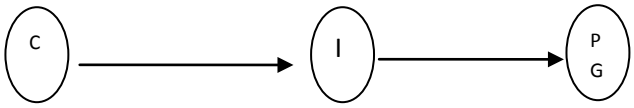
$(TID, n, IDReq_M, K_{C-M})_r$ $(TID, n, IDReq_M, K_{C-M})_s$



$\{ID_M, h((TID, n, ID_M, K_{C-M})_r\}$ $\{ID_M, h((TID, n, ID_M, K_{C-M})_s\}$

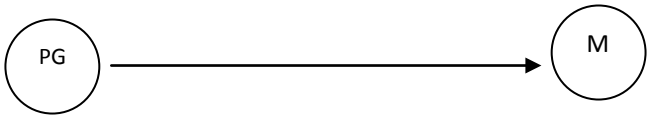
II. Payment Request & Amount Subtraction Request

ASrequest = PRequest =



$\{TID, ID_M, Price, n, h(OD, Price)\{(Price, h(OI), TC, ID_M), CK, KS_{C-Iz}\}$,

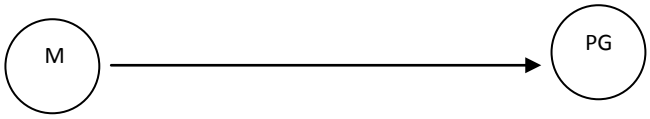
III. Payment Request Forwarding to Merchant



$E\{(T_c, TID, ID_M, n), Price, h(ID_M, OI), CK_C, KS_{PG-M}\}$

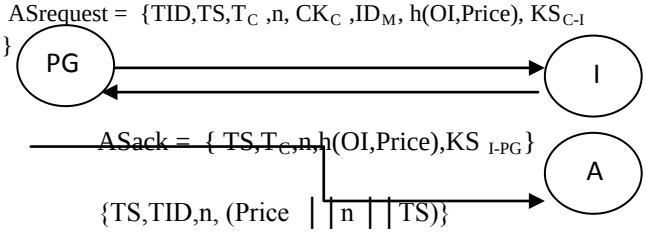
IV. Acknowledge the request

$ACrequest = E\{TS, T_C, n, CK_M, KS_{M-PG}, Price, h(OI)\}$



V. **Inter Banking Transfer**

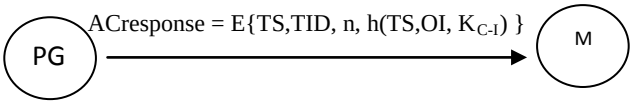
$ASrequest = \{TID, TS, T_C, n, CK_C, ID_M, h(OI, Price), KS_{C-I}\}$



$ASack = \{TS, T_C, n, h(OI, Price), KS_{I-PG}\}$

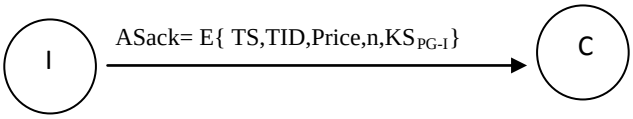
$\{TS, TID, n, (Price \,||\, n \,||\, TS)\}$

VI. **Payment response**



$ACresponse = E\{TS, TID, n, h(TS, OI, K_{C-I})\}$

VII. **Value Subtraction Response**



$ASack = E\{TS, TID, Price, n, KS_{PG-I}\}$

V. SECURITY AND FAULT-TOLERANCE

5.1 N-Modular Redundancy (NMR) based fault tolerant ECSM

In N-modular redundancy circuit a Boolean function is computed through odd number of identical logic circuits (i.e., N=2m+1 logic gates) and the output is processed through a voter [15].

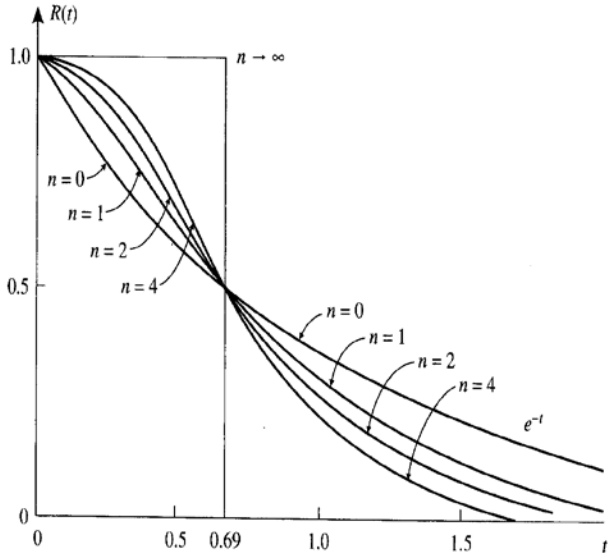


Fig 4 Showing reliability for 2n+1 circuits [15]. Graph is normalized for λ=1

This technique is very efficient in case of transient fault. A system's reliability R_i (t) within the time interval [0,t] can be defined by the Probability that it operates correctly (error free) in a time interval [0,t] i.e.,

R_i (t) = Pr {The fault f_i is inactive in [0,t]}

Similarly for the reliability of $R_{NMR}(t)$ is measured in time [0,t] by the probability that at most m modules are faulty.

$$R_{NMR}(t) = \sum_{k=0}^{m} \binom{N}{k} [1-R_m(t)]^k [R_m(t)]^{N-k}$$

Where R_m is the reliability of the module m .

The above equation can be of the form $R(t)= e^{-\lambda t}$, thus we get when $n\rightarrow\infty$, Mean Time To Failure

Mutual Authentication

The customer and the bank authenticate each other in the Interbank transfer phase. If an adversary wants to steal the information , he cannot compute *k* from the equation $Q = kPh(M)$, where M is the message, because he must solve the elliptic curve discrete logarithm problem

5.2 Anonymity

In our protocol , the client use a nickname i.e, temporary id Tc instead of his/her real identity. So neither PG nor M can map the true identity of client.

5.3 **Non-repudiation**

Non-repudiation of transaction is the property that the M can ensure that C can't deny the transaction, he/she has performed. In our protocol , since the session KS_{C-I} , KS_{C-M} is only generated by client or issuer , not by merchant , the merchant can provide a non-repudiable evidence that the client has requested the merchant to perform the transaction.

5.4 Replay Attack

The usage of different shared session key for every transaction prevents the replay attack. The attacker can't replay the messages without the shared key. Again, the timestamp which is generated in message ensures that replay attack is infeasible to it.

5.6 **Password Guessing Attack**

An attacker intercepts the payment request & amount claim response & tries to analyze it. He/ she may guess h(OI) . But the real problem is that the adversary can't compute k from the equation of the elliptic curve Q=kP h(OI), because he /she must solve the ECDLP which is impossible to guess.

5.7. Traceability/ Double spending

If any customer uses the same transaction twice illegally with the help of PG, this illegal transaction can be traced out by verifying T_c, TID.

Fault Tolerance

To ensure fault tolerance , we maintain possible measures-

- If in registration or initialization phase the link or request has lost, we use session key . The client can repeat the process using his/her transaction history.
- The client may not have sufficient money to buy the product in the step 2, I refuses the further process i.e., roll back the process & send a message to C.
- If the server of PG crashes in step 3, i.e., payment has been debited from Cbut not transferred to A, the log files are kept in database of I. PG then sends it to I & a message is forwarded to C.
- In step 5, if money transfer can't be operated may be due to for bank's server crash, the transaction can be repeated after server restarted by using the log file.
- If the acknowledgement of the payment has lost in both end due to link failures or server crash, the message is also send from the merchant's end to the client. Again, a periodic synchronization between the both end server and maintaining log files in the server can retrieve the message. Though the message from merchant doesn't matter as the transaction history which includes transaction time, reference number, payment details etc in the database of I.

VI. CONCLUSION

In this paper we proposed a secure and fault tolerable e-cash transfer system based on the elliptic curve discrete logarithm problem. The security features: mutual authentication, anonymity, non-repudiation, traceability are satisfied successfully by our system. The attacks – replay attack, password guessing attack can be prevented. Different fault tolerance issues have been considered. Different measures show that the system are fault tolerable. In addition to this, we showed that using N-modular redundancy, the fault –tolerability of the system can be increased.

REFERENCES

1. Liu,J., Huang, S. (2010). Identity-based threshold proxy signature from bilinear pairings. *Informatica*, 21(1), 41–56.
2. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48, 203–209.
3. Raulynaitis, A., Sakalauskas, E., Japertas, S. (2010). Security analysis of asymmetric cipher protocol based on
4. matrix decomposition problem. *Informatica*, 21(2), 215–228.
5. Xing, H., Li, F., Qin. Z. (2010). A provably secure proxy signature scheme in certificate less cryptography. *Informatica*, 21(2), 277–294.
6. Chaum, D. (1983). Blind signature for untraceable payments. In: *Proceedings of Eurocrypt'82*, Plenum, New York, pp. 199–203.
7. Au, M., Susilo, W., Mu, Y. (2008). Practical anonymous divisible e-cash from bounded accumulators. In: *Proceedings of Financial Cryptography and Data Security*, *LNCS*, Vol. 5143. Berlin. pp. 287–301, 2008.
8. Kungpisdan S (2005) Design and analysis of secure mobile payment systems. PhD thesis, Monash University
9. Bellare M, Garay JA, Hauser R, Herzberg A, Krawczyk H, Steiner M, Tsudik G, Herreweghen EV,Waidner M (2000) Design, implementation, and deployment of the ikp secure electronic payment system. IEEE J Select Areas Commun 18(4):611–627.
10. Tellez J. & Sierra J, "Anonymous Payment in a Client Centric Model for Digital Ecosystem", *IEEE DEST*, 2007, pp. 422-427.
11. A.Peiro J.L, Asokan N, Steiner M,Waidner M. "Designing a generic payment service ", IBM System Research Journal. Vol. 37(1), 1998, pp. 72-88.
12. Chou, J.S., Chen, Y.-L., Cho, M.-H., Sun, H.-M. (2009). A novel ID-based electronic cash system from pairings. In: *Cryptology ePrint Archive*, Report 2009/339. Available at http://eprint.iacr.org/.
13. Canard, S., Gouget, A. (2007). Divisible e-cash systems can be truly anonymous. In: *Proceedings of EUROCRYPT 2007*, *Lecture Notes in Computer Science*, Vol. 4515, Springer, Berlin, pp. 482–497.
14. Ciet, M., and Joye, M., "Elliptic Curve Cryptosystems in the Presence of Permanent and Transient Faults," Cryptology ePrint Archive, Report 2003/028, 2003.
15. Agustin Dom´nguez-Oviedo and M. Anwar Hasan. Algorithm-level error detection for ECSM. CACR 2009-05, University of Waterloo, 2009.
16. Adi Shamir. Method and apparatus for protecting public key schemes from timing and fault attacks. US Patent 5,991,415, November 1999.
17. Antipa, A., Brown, D., Menezes, A., Struik, R., and Vanstone, S., "Validation of elliptic curve public keys," Proceedings of PKC 2003, LNCS 2567, pp. 211-223,Springer-Verlag, 2003.
18. Sargunam B and Dhanasekaran R, "Error Detection Schemes for Finite Field Multipliers," *American Journal. Applied Sciences*,pp.137-144, Vol.11, No.1, 2014.
19. Aditya Bhattacharyya and S.K. Setua. Design of ECSEPP: Elliptic Curve Based Secure E-cash Payment Protocol. In: Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics,2015,Smart Innovation, Systems and Technologies 44, DOI 10.1007/978-81-322-2529-4_35..