Applied Mathematics & Information Sciences
An International Journal

An Undetachable Threshold Digital Signature Scheme Based on Conic Curves

Yang Shi[1] *and Guoyue Xiong*[2]

[1]School of Software Engineering, Tongji University, Shanghai 200092, China
[2]School of Economics and Management, Tongji University, Shanghai 200092, China

Received: 8 Jul, 2012; Revised 4 Oct., 2012; Accepted 6 Jan., 2012;
Published online: 1 Mar. 2013

Abstract: Based on analysis of security problems from malicious hosts, a special undetachable threshold digital signature scheme is proposed. This scheme uses a cryptosystem based on conic curves and achieves the most important security characteristic of protecting mobile agents against malicious hosts, that is, undetachability. Furthermore, this scheme solves the case where a host can force an agent to commit to a sub-optimal transaction. Computational studies show that this scheme is superior to the RSA-based undetachable threshold digital signature scheme.

Keywords: Conic curves, undetachable threshold digital signatures, mobile agents

1. Introduction

1.1 Mobile agents

Mobile agents [1-2] are programs bundled with data and execution states, typically written in platform independent languages, that can suspend execution, migrate to other computers connected over a network, and resume execution there enabled with certain properties that work on behalf of users in a distributed heterogeneous environment. They have two distinguishing characteristics: mobility and autonomy.

Mobile agent technology brings significant benefits to many areas such as electronic commerce because of its advantages [3]. However, security is one of the main problems with this technology.

1.2 Security issues of Mobile Agents

Threats to the security of mobile agents generally fall into four comprehensive categories [4]:

1. agent against agent platform
2. agent platform against agent
3. agent against other agents
4. other entities against agent system

Hohl [5] identified several attacks from malicious hosts on mobile agents such as 1) spying on code, data, control flow and interactions with other agents, 2)illegal manipulation of code, data, control flow and interactions with other agents, 3) incorrect execution of code, masquerading as another host, denial of execution, and 4) returning wrong results for system calls issued by the agent.

Thus security issues, especially threats from potentially malicious hosts, become a great obstacle to widespread deployment of applications in electronic commerce based on mobile agent technology.

2. Previous works on undetachable digital signatures

2.1 The preliminary idea

Obviously, the signing key is easily compromised when mobile agents migrate from one host to another or are run on a malicious host. Suppose that we have a way to conceal a function that produces a digital signature; the problem then is that even if the real signature routine can be kept secret, the whole routine could still be abused to sign arbitrary documents, which makes the signing process worthless. We therefore need a way to glue the signature routine to the function f that produces the output that is to be signed. The output producing routine f could, for example, add to each document a prefix saying that the following digitally signed order form is valid only for

[*] Corresponding author: e-mail:xiongguoyue@tongji.edu.cn

a single train ticket issued for a specific date and costing less than a certain price. Thus, the purpose of this paper is to include in the general purpose signature routine some task specific information which is forced to be part of the signed file. This is the reason that Sander and Tschudin [6] proposed the idea of undetachable digital signatures which allow mobile agents to effectively produce a digital signature inside a remote and possibly malicious host without the host being able to deduce the agents secret or to reuse the signature routine for arbitrary documents. By binding usage restrictions to a signature key given to the agent, the damage a malicious host can do is potentially limited. The approach is to encode constraints into the signature key. A constraint is a restriction or a limitation such as a new iPad costing no more than 300 USD. If the constraints are not met a valid signature is not produced, preventing arbitrary messages from being signed. Their main idea is as follows:

First, let Sig be a rational function used by C (a customer) to produce the digital signature $Sig(m)$ for an arbitrary message m. Next, suppose the message m is the result of a rational function f applied to some input data x. Finally, the function v that C publishes to let others check the validity of the digital signature z is regarded to be a valid signature of m if and only if $z = Sig(m)$ To create "undetachable" signatures from the customer's mobile agent, $f_{Signed} = Sig \circ f$ is computed, and f_{Signed} and f are both sent to S (a shop). S then evaluates both $m = f(x)$ and $z = f_{Signed}(x)$. Although the signature function Sig is not known by others, every one can verify the validity of message m by testing $Ver(z) =^{?} m$, where $Ver(z)$ is a verification algorithm.

2.2 Some implementations

Kotzanikolaou et al. [7] presented an RSA implementation of undetachable digital signatures. However, this scheme does not provide server non-repudiation because it does not contain the server's signature [8]. Lee et al.[8] proposed an RSA based construction of undetachable digital signatures called "strong non-designated proxy signature". Their scheme is more secure than the scheme proposed by Kotzanikolaou et al. [7] and often abbreviated to "LKK-SPS". In 2002, a strong proxy signature scheme with proxy signer privacy protection was published [9]and a pragmatic alternative to undetachable signatures [10] was also proposed.

2.3 Undetachable threshold digital signatures

To solve the problem that a host can force an agent to commit to a sub-optimal transaction, Borselius, Mitchell and Wilson [11] introduced the notion of undetachable threshold signatures and proposed an RSA-based implementation. Suppose a user has a private signature key and a public verification key. Suppose also that the user has a 'constraint string' R, which defines what types of signature that can be created. Then, an undetachable threshold signature scheme enables the user to provide n entities with 'shares' of the private signature key (where the shares are a function of R).

3. Cryptosystems based on conic curves

3.1 Conic-based cryptography

Besides RSA, there are some other encryption schemes such as the encryption scheme using Plotkin arrays[12], the encryption scheme from lattice assumptions [13] and the encryption scheme based on conic curves. In 1999, Cao [14-15] gave some feasible cryptosystems based on conic curves. In 2001, Dai et al. [16-17] proved that some of Cao's schemes were no stronger than corresponding systems based on the multiplicative group. However, this does not mean that cryptosystems based on conic curve are insecure. In fact, no effective attack has been found.

In recent years, some progress on conic-based cryptosystems has also been achieved. Long, Cao and Chen [18] proposed a new dynamic threshold commercial key escrow (DTCKE) scheme based on conics. Yang and Liu [19] proposed a protocol for zero-knowledge proof of identity based on ElGamal using conics. Motivated by the KMOV scheme on elliptic curves, a public key cryptosystem scheme was proposed by Chen, Song and Li [20] that was based on conic curves over the ring Z_n. Lin, Wang and Li[21] proposed a digital multi-signature scheme on the generalized conic curve over Z_n. Furthermore, Lu, Cao and Zhou [22] presented a threshold undeniable signature scheme based on conics.

3.2 Conic curves over F_p

Let p be an odd prime number and F_p be a finite field of order $p$and let $F_p^\star$ be the multiplicative group of F_p .

The conic curve $C(a,b)$ over F_p is the solution set in the affine space $GC(P^2)$ of the equation $y^2 = ax^2 - bx$, where a and b are elements in F_p.

Let $H = \{t \in F_p : t^2 \neq a\} \bigcup \{\infty\}$. We can define a bijection $P : H \to C(a,b)$where $\infty \to (0,0), t \to (x_t, y_t), t \neq \infty$, and $x_t = b(a-t^2)^{-1}, y_t = bt(a-t^2)^{-1}$.

A conic $\langle C(a,b), \oplus, P(\infty) \rangle$ becomes an abelian group under the operation $\oplus$ as shown below:

(1) for every $P(t) \in C(a,b), P(t) \oplus P(\infty) = P(\infty) \oplus P(t) = P(t)$

(2) for any $P(t_1), P(t_2) \in C(a,b)$ where $t_1, t_2 \neq \infty, P(t_1) \oplus P(t_2) = P(t_3)$ with

$$t_3 = \begin{cases} (t_1 t_2 + a)(t_1 + t_2)^{-1}, t_1 + t_2 \neq 0 \\ \infty, t_1 + t_2 = 0, \end{cases}$$

The cardinality of $C(a,b)$ is given by

$$|C(a,b)| = \begin{cases} p-1, (\frac{a}{p}) = 1 \\ p+1, (\frac{a}{p}) \neq 1, \end{cases}$$

where $(\frac{a}{p})$ denotes the Legendre symbol.

3.3 Cryptosystem based on conic curves over Z_N

Let p and q be prime numbers and let $N = pq$.

In the same way as above, the conic curve $C_N(a,b)$ is defined as the set of pairs $(x,y) \in Z_N^2$ satisfying $y^2 \equiv$

$ax^2 - bx(modN)$. Cao [15] studied the case where $p \equiv q \equiv 1(mod6)$.

Suppose that

$$(a,N) = 1$$

and

$$(\frac{a}{p}) = (\frac{a}{q}) = -1$$

It is clear that $3|(2(p-1)(q-1)+1)$ since $2(p-1)(q-1) \equiv -1mod3$. Thus, we have the pair of numbers 3 and $\frac{2(p-1)(q-1)+1}{3}$.The product of these two numbers is 1 modulo $\phi(N) = (p-1)(q-1)$, and the pair can be used as the decryption key and the encryption key respectively.

Scalar multiplication is used to denote a repeat of $\oplus$ and the conic curve discrete logarithm problem (CCDLP) is the following. Given a conic curve $C_N(a,b)$ defined over Z_N , a point $P \in C_N(a,b)$of order n, and a point $Q = lp$ where $0 < l \leq n-1$, determine l.

The security of this cryptosystem relies upon the difficulty of factoring the integer N into its two prime factors and the computational intractability of CCDLP [14].

4. Undetachable digital signatures based on conic curves

Our scheme offers bilateral security for both customers and shops inspired by the LKK-SPS scheme, and provides more security than the LKK-SPS scheme. For instance, our scheme is resistant to low exponent attacks and replay attacks. The application scenario of the scheme is the typical one used in papers on undetachable signatures such as [6-8] and [11] . The cryptosystem used in the scheme relies on conic curves over Z_N [14-15]. A secret sharing solution based on Vandermonde matrices [23] proposed in [24] is used in the Sign algorithm.

4.1 Settings

Settings for the customer:

- C is the identity of the Customer;
- N_C is the modulus of C's conic curve(N_C is public);
- d_C is the decryption key (i.e. the signature key) for C's cryptosystem(d_C is private);
- $e_C = 3$ is the encryption key (i.e. the verification key) for C's cryptosystem(req_C is public);
- req_C indicates the requirements of the customer;
- T_C is the timestamp of req_C .

Settings for shops:

- S is the identity of a shop;
- N_S is the modulus of S's conic curve(N_S is public);
- d_S is the decryption key (i.e. the signature key) for S's cryptosystem(d_S is private);
- $e_S = 3$ is the encryption key (i.e. the verification key) of C's cryptosystem($e_S = 3$ is public);
- bid_S is the bid information for S ;
- T_S is the timestamp of bid_S.

4.2 The operator $\otimes$

To construct undetachable digital signatures with bilateral security, we propose a new operator:

First, the mapping Q is defined as

$$Q : C(Z_N) \to H, \langle x,y \rangle \to \frac{y}{x}$$

where $H = \{T \in Z_N : t^2 \neq a\} \bigcup \{\infty\}$. In effect, Q is the inverse mapping of P. Then the operator $\oplus$ is defined as

$$\otimes : C(Z_N) \times C(Z_N) \to C(Z_N)$$

$$\langle x_1,y_1 \rangle \times \langle x_2,y_2 \rangle \to Q(\langle x_1,y_1 \rangle) \cdot P(Q(\langle x_2,y_2 \rangle))$$

Proposition 1.$\otimes$ satisfies the left distributive law with respect to $\oplus$.

Proof. Let $t_i = Q(\langle x_i,y_i \rangle)$,$i = 1,2,3$. then

$$\begin{aligned}
&\langle x_1,y_1 \rangle \otimes \langle x_2,y_2 \rangle \oplus \langle x_3,y_3 \rangle \\
&= Q(\langle x_1,y_1 \rangle) \cdot P(Q(\langle x_2,y_2 \rangle \oplus \langle x_3,y_3 \rangle)) \\
&= t_1 P(Q(P(t_2) \oplus P(t_3))) = t_1(P(t_2) \oplus P(t_3)) \\
&= \underbrace{(P(t_2) \oplus P(t_3)) \oplus \cdots \oplus (P(t_2) \oplus P(t_3))}_{t_1} \\
&= \underbrace{P(t_2 \oplus \cdots \oplus P(t_2)}_{t_1} \oplus \underbrace{P(t_3 \oplus \cdots \oplus P(t_3)}_{t_1} \\
&= (t_1 P(t_2) \oplus (t_1 P(t_2)) \\
&= (\langle x_1,y_1 \rangle \otimes \langle x_2,y_2 \rangle) \oplus (\langle x_1,y_1 \rangle \otimes \langle x_3,y_3 \rangle).
\end{aligned}$$

4.3 Security scheme

The security scheme is composed of four algorithms.

[1] SetupAgents

The customer C runs the following algorithm:

$$\{a_0, a_1, ..., a_{t-2}\} \xleftarrow{\$} Z_{\phi_{N_C}}$$

$$a_{t-1} \xleftarrow{\$} \{1, 2, ..., \phi_{(N_C)} - 1\}$$

Generate the polynomial $g = \sum_{i=0}^{t-1} a_i x^i$,$d_C \leftarrow g(0)$ For each $j = 1,2,...,n$, computes $d_C \leftarrow g(j)$,$h_C \leftarrow hash(C||reg\_C||T_C)$,$0 \leq h < N_C$ and $K_j \leftarrow d_C \cdot P(h_C)$

Give (C, reg_C, T_C) and h_C to the $j-th$ agent A_j.

Give the following undetachable threshold signature function pair to the $j-th$ agent A_j as part of the executable code:

$$f(x) = x \cdot P(h_C) \tag{1}$$

and

$$f_{Signed,j}(x) = x \cdot K_j \tag{2}$$

For each $j = 1,2,...,n$, let $Str_j = K_j||h_C||...$ be the string of key parameters for A_j, generate the signature of Str_j as $\sigma_{Str_j} = d_C \cdot P(hash(Str_j))$: and give σ_{Str_j} to the $j-th$ agent.

[2] VerifyAgent

After the $j-th$ agent A_j migrats to the host of S , the following equation should be verified first:

$$P(hash(Str_j)) \equiv^? e_C \cdot \sigma_{Str_j}$$

If this is a valid signature generated by C, then S believes that the key information C gives to A_j is not modified by any malicious host.

[3] Sign

Suppose that the shop S gets t or more valid agents and S is willing to deal with S. Then S can generates an undetachable signature ζ and a signature ζ_S on behalf of himself. To simplify the description, we suppose that these t agents are $A_{x_1}, A_{x_2}, ...A_{x_t}$.

Suppose that

$$X = \begin{pmatrix} 1 \; x_1^1 \cdots x_1^{t-1} \\ 1 \; x_2^1 \cdots x_2^{t-1} \\ \vdots \; \vdots \; \ddots \; \vdots \\ 1 \; x_t^1 \cdots x_t^{t-1} \end{pmatrix}$$

The adjoint matrix of X is

$$X^* = \begin{pmatrix} x_{11}^* \; x_{12}^* \cdots x_{1t}^* \\ x_{21}^* \; x_{22}^* \cdots x_{2t}^* \\ \vdots \; \vdots \; \ddots \; \vdots \\ x_{t1}^* \; x_{t2}^* \cdots x_{tt}^* \end{pmatrix}$$

Compute

$$h_S \leftarrow hash(C||reg\_C||T_C||S||bid\_S||T_S), 0 \le h_S < N_S$$

$$\zeta \leftarrow \sum_{i=1}^{t} \sum_{j=1}^{t} (x_{j,i}^* \cdot f_{Signed,x_i}(h_S))$$

$$\zeta_S \leftarrow d_S \cdot P(h_S)$$

The shop gives $S, bid\_S, T_S, \zeta, \zeta_S, h_S$ to the agent.

The agent then migrates to next host of another shop and repeats the operations above. After the mobile agent has travelled around all the shops, it goes back to customer C. If there is at least one shop bid satisfying the requirements of C, then the transaction can be completed.

[4] Verify

Whether the transaction is valid or not can be checked using the following two equations.

$$\pi P(h_S) \otimes P(h_C) =^? e_C \zeta \tag{3}$$

$$P(h_S) =^? e_S \zeta_S \tag{4}$$

If C worries that a malicious host has deleted some bid information of other shops, cryptographic tracing [25] can be introduced to protect the computational results of the roaming agent. Heavy penalties should be imposed on the owners of malicious hosts to prevent their attempts to obtain dishonest profits in this way again.

5. Analyze of the scheme

5.1 Correctness and security

Proposition 2. Suppose that $Sig(x) = d_C x$ and $f_{Signed}(x) = d_C x \cdot P(h_S)$. Suppose that f is defined as in equation(1) and that $f_{Signed,x}$ is defined as in equation(2). Then the proposed scheme is an undetachable threshold digital signature scheme.

Proof.

$$(Sig \circ f)(x) = Sig(f(x))$$

$$= Sig(x \cdot P(h_C)) = d_C x \cdot P(h_C) \equiv f_{Signed}(x).$$

Suppose that the determinant of X is $\pi = det(X) = \prod_{t \ge i > j \ge 1} (x_i - x_j)$ and that π is an invertible element on $Z_{\phi(N_C)}$.

$$\pi^{-1} \sum_{i=1}^{t} \sum_{j=1}^{t} (x_{ji}^* \cdot f_{Signed,x_i}(\bullet)) = \pi^{-1} \sum_{i=1}^{t} \sum_{j=1}^{t} (x_{ji}^* \cdot K_{x_i})$$

$$= \pi^{-1} \sum_{i=1}^{t} \sum_{j=1}^{t} (x_{ji}^* \cdot d_{C_{x_i}} \cdot P(h_C))$$

$$= \pi^{-1} [\sum_{i=1}^{t} \sum_{j=1}^{t} (x_{ji}^* \cdot d_{C_{x_i}}] \cdot P(h_C))$$

$$= (\pi^{-1} \pi)(d_C P(h_C)) = Sig \circ f.$$

If π is not invertible on $Z_{\phi(N_C)}$, then the above equation does not hold. However, a similar process works without π^{-1} . In effect, the correctness and security of the scheme are not affected by π^{-1}.

Proposition 3. A transaction is valid if and only if equations (3) and (4) are true and all timestamps are valid.

Proof. If the mobile agent is not detached, then:

$$e_c \zeta = e_c \sum_{i=1}^{t} \sum_{j=1}^{t} (x_{ji}^* \cdot f_{Signed,x_i}(h_S))$$

$$= e_c \sum_{i=1}^{t} \sum_{j=1}^{t} (x_{ji}^* \cdot (h_S) K_{x_i})$$

$$= e_c \sum_{i=1}^{t} \sum_{j=1}^{t} (x_{ji}^* \cdot h_S d_{C_{x_i}} \cdot P(h_C))$$

$$= e_c \sum_{i=1}^{t} \sum_{j=1}^{t} (x_{ji}^* \cdot d_{C_{x_i}}) h_S P(h_C)$$

$$= e_c \pi d_C h_S (mod \phi(N_C)) \cdot P(h_C)$$

$$= \pi h_C P(h_C)$$

$$= \pi P(h_S) \otimes P(h_C).$$

$$e_S \zeta_S = e_S d_S (mod \phi(N_S)) \cdot P(h_S) = P(h_S)$$

The security of the equations above relies upon the difficulty of CCDLP [14].

5.2 Computational advantage

RSA is vulnerable under the low exponent attack found by Coppersmith [26] but cryptosystems based on conic curves are not [15]. This scheme offers security relying on the difficulty of the factoring problem, which is the same as the RSA implementation of undetachable signatures, but the verification key, 3, is far shorter than that for the RSA implementation [11]. Thus, the speed of the most frequent operation, verification, is very fast.

An experiment to compare the speed of verification is performed using Java with JDK 1.4 on an IBM ThinkPad T43 with Intel CPU 797 MHz running Microsoft Windows XP. 1024-bit modules are used for both cryptosystems. The public keys for RSA are chosen randomly. 256-bit randomly generated binary strings are used instead of the output of secure hash functions for convenience. The mean verification time for 1000 trials of the RSA cryptosystem is 38ms, whereas only 1ms is needed for the scheme using conic curves.

6. Conclusion

In this paper, we present a novel implementation of undetachable threshold digital signatures and a correspondent security scheme. Compared to [11], our scheme uses a different cryptosystem to construct undetachable signatures. This scheme can control the risk of signature key compromise as well as the risk that the signature routine may be abused to sign arbitrary information. It also solves the problem of a host forcing an agent to commit to a sub-optimal transaction. Since our scheme can resist reply attacks and protect integration of a shops bid information, it is more secure than the signature scheme in [11]. In addition, our scheme has the computational advantage mentioned above. Further adaptation of our scheme and algorithms may be useful in various contexts such as ad hoc networks [27] and wireless sensor networks [28].

Acknowledgement

This work is supported by the National Natural Science Foundation of China (No. 61202382, 71071114)

References

[1] A. Puliafito, S. Riccobene and M. Scarpa, An analytical comparison of the client-server, remote evaluation and mobile agents paradigms, Proc. First International Symposium on Agent Systems and Applications, (1999) 278-292.

[2] C. Busch, V. Roth and R. Meister, Perspectives on Electronic Commerce with Mobile Agents, Proc. XI Amaldi Conference On Problems of Global Security, (1998)1-13.

[3] D.B. Lange and M. Oshima, Seven good reasons for mobile agents, ACM Commun. 42 (1999) 88-89.

[4] W. Jansen, Countermeasures for mobile agent security, Comp. Commun. **13** (2000) 1667-1676

[5] Fritz Hohl, Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts, Mobile Agents and Security, Lecture Notes in Computer Science, Springer-Verlag, 1419 (1998) 92-113.

[6] T. Sander and C. Tschudin, Protecting Mobile Agents Against Malicious Hosts, Mobile Agents and Security, Lecture Notes in Computer Science, Springer-Verlag, 1419 (1998) 44-60.

[7] P.Kotzanikolaous, M. Burmester and V. Chrissikopoulos, Secure Transactions with Mobile Agents in Hostile Environments, ACISP 2000, Lecture Notes in Computer Science, Springer-Verlag, 1841 (2000) 289-297.

[8] B. Lee, H. Kim and K. Kim, Secure mobile agent using strong non-designated proxy signature, ACISP 2001, Lecture Notes in Computer Science, Springer-Verlag, 2119 (2001) 474-486.

[9] K. Shum and V. Wei, A strong proxy signature scheme with proxy signer privacy protection, Eleventh IEEE International Workshop on Enabling Technologies: Infrastucture for Collaborative Enterprises (WETICE'02). IEEE, (2002) 55-56.

[10] N. Borselius, C. Mitchell and A. Wilson, A pragmatic alternative to undetachable signatures. ACM SIGOPS Oper. Sys. Rev., **2** (2002) 6-11.

[11] N. Borselius, J. Mitchell and A. Wilson, Undetachable threshold signatures, Proc. 8th IMA International Conference, Lecture Notes on Computer Science, Springer-Verlag, 2260 (2001) 239-244.

[12] C. Koukouvinos and D. E. Simos, Encryption schemes using Plotkin arrays, Appl. Math. Inf. Sci. **5** (2011) 547-557.

[13] F. Wang, Y. Hu and C. Wang, Post-Quantum Secure Hybrid Signcryption from Lattice Assumption, Appl. Math. Inf. Sci. **6** (2012) 23-28.

[14] Z. Cao, A Public Key Cryptosystem Based on a Conic Over Finite Fields Fp, CHINACRYPT' **98**, (1998) 45-49. (In Chinese)

[15] Z. Cao, Conic analog of RSA cryptosystem and some improved RSA cryptosystems, J. Sci. Heilongjiang Univ., **4**(1999) 15-18. (In Chinese)

[16] Z. Dai, D. Pei, J. Yang and D. Ye, Cryptanalysis of a Public Key Cryptosyasem based on Conic Curves, Proc. International Workshop on Cryptographic Techniques and E-Commerce, Hong Kong: City University of Hong Kong Press, (1999) 259-261.

[17] Z. Dai, D. Ye and D. Pei, Cryptanalysis of EIGamal type encryption schemes based on conic curves, Electron. Lett, 7(2001) 426.

[18] Y. Long, Z. Cao and K. Chen, A dynamic threshold commercial key escrow scheme based on conic, Appl. Math. Comp. **171**(2) (2005) 972-982.

[19] Z. Yang and M. Liu, ZKp based identification protocol on conic curve in distributed environment, The Fifth International Conference on Computer and Information Technology, (2005) 690-694.

[20] Z. Chen, X. Song and J. Li, A public-key cryptosystem scheme on conic curves over the ring Zn, Proc. 5th WSEAS International Conference on Information Security and Privacy table, (2006) 156-160.

[21] S. Lin, B. Wang and Z. Li, Digital multisignature on the generalized conic curve over Zn, Comp. Secu. 1-2 (2009) 100-104.

[22] R. Lu, Z. Cao and Yuan Zhou, Threshold undeniable signature scheme based on conic, App. Math. Comp. 1,4 (2005) 165-177.

[23] F. Soto-Eguibar and H. Moya-Cessa, Inverse of the Vandermonde and Vandermonde confluent matrices, Appl. Math. Inf. Sci. **5** (2011) 361-366.

[24] W. Zhang, D. He, X. Wang and Y. Zheng, A New RSA Threshold Group Signature Scheme Based on Modified Shamir's Secret Sharing Solution, J. Elec. Info. Tech. 11 (2005)1745-1749 (In Chinese).

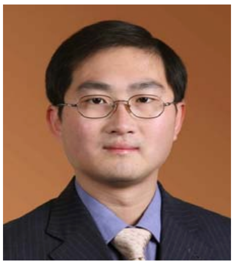
[25] G. Vigna, Cryptographic Traces for Mobile Agents, Mobile Agents and Security, Lecture Notes in Computer Science, Springer-Verlag, 1419 (1998) 137-153.

[26] D. Coppersmith, Small Solutions to polynomial equations, and low exponent RSA vulnerabilities, J. Crypt. **10** (1997) 233-260.

[27] W. Wu and Y. Chen, Cryptanalysis of A PAACP: A Portable Privacy-Preserving Authentication and Access Control Protocol in Vehicular Ad Hoc Networks, Appl. Math. Inf. Sci. (2012) 463S-469S.

[28] J.Ho, H. Shih, B. Liao and J. Pan, A Reduce Identical Composite Event Transmission Algorithm for Wireless Sensor Networks, Appl. Math. Inf. Sci. (2012) 713S-719S. J.R Banavar, A. Maritan, A. Rinaldo, Nature **399**, 130-132 (1999).

Yang Shi is currently a faculty of the School of Software Engineering, Tongji University, China. His research interests are information security and Software engineering. He received his PhD degree in 2005. He was a postdoctoral researcher of Tongji University from 2007 to 2010. He has published more than 20 research articles in reputed journals and international conferences.



Guoyue Xiong works as a member of the School of Economics and Management, Tongji University, China. He has an interdisciplinary education background, bachelor degree of computer science and PhD degree of management. Now he is interested in the research field of electronic commerce, information system and marketing engineering.