Short Signcryption Scheme for the Internet of Things

Xuanwu Zhou[1,2], Zhigang Jin [1], Yan Fu[1,3], Huaiwei Zhou[3], Lianmin Qin[3]
[1] School of Electronics and Information Engineering, Tianjin University, Tianjin 300072, China
[2] Command College of the Chinese Armed Police Forces, Tianjin 300250, China
[3] Information Technology Research Center, Huarong Corporation, Yantai 265400, China
E-mail: schwoodchow@163.com

Keywords: internet of things, signcryption, provable security, distributed key management, system efficiency

Received: June 23, 2011

Signcryption is an effective cryptographic primitive, which simultaneously fulfils both the functions of encryption and signature with much lower cost than traditional schemes; it is an ideal method to provide confidentiality and unforgeability and ensure secure data storage and transmission in the IOT (Internet of things). In the paper, we propose a publicly verifiable short signcryption scheme S-ECSC for the Internet of things based on elliptic curves cryptosystem; and prove the provable security of S-ECSC under the Random Oracle model, including confidentiality in IND-CCA2 model, unforgeability in UF-CMA model and non-repudiation security. As per the efficiency analysis, S-ECSC achieves an average 80% reduction in computation cost compared with typical discrete logarithm, RSA based signcryption schemes, and has the lowest communication cost in Elgamal type signcryptions. With its superiority in efficiency and security, S-ECSC proves to be more suitable for resource-restricted environment in IOT and better satisfies the requirement of secure protocols in IOT, such as key management, secure routing, etc. At last, we take key generating and distributing protocol of distributed key management in IOT as an application example, and analyse the method and importance to apply S-ECSC into secure protocols in IOT.

Povzetek: Članek opisuje šifrirno shemo za internet stvari.

1 Introduction

The concept of IOT (Internet of Things) was first put forward by Ashton of the former MIT Auto-ID Center in 1999 when he was working on RFID (Radio Frequency Identification). Presently, the most widely-accepted definition of IOT is as follows [1, 2, 3, 4]. IOT is a self-configuring network in which things are connected with network according to certain protocols with RFID, ultra-red sensor, GPS(Global Positioning System), laser scanner, etc to interchange and transmit data, and ultimately achieve intelligent identification, positioning, tracing, supervision and management. IOT is the new direction of future computer and communication technology, and is regarded as the third landmark in the development of information technology after computer science and Internet.

According to the function classification, the hierarchical structure of IOT is composed of application layer, network layer and sensor layer. The basic function of network layer is secure and reliable interconnection between things via wire-based or wireless technology, in which the secure and dynamic interconnection via wireless network has been the overwhelming trend. In wireless network technology, many researchers have focused on IEEE802.11 WLAN (Wireless Local Area Network)， which is mainly composed of wireless Ad hoc network, WSN (Wireless Sensor Network) and WMN (Wireless Mesh Network). As a new wireless network, IEEE802.11 WLAN proves to be suitable for commercial, medical, domestic, military, and other applications with its superiority, such as inexpensiveness, adaptability and reliability, etc. In the Internet of things, IEEE802.11 WLAN has been playing an increasingly important role in secure and reliable connection between different objects. Whereas, the distributed network management and restricted network resources in IEEE802.11 WLAN have rendered many problems as to the security of confidentiality, integrity, non-repudiation and availability for data storage and transmission in IOT. Besides, security measures designed for traditional network, which has relatively abundant network resources, fixed connection, stable topology, special routing and comprehensive network service, are not completely applicable to wireless network environment in the Internet of thing. Therefore, it is of great necessity to design special security technology, protocols and corresponding algorithms for the secure and dynamic wireless communication in the Internet of things.

The confidentiality and integrity of message is the basic requirement for secure communication in IOT; in the symmetric setting, efforts focused on the composition of symmetric key encryption and message authentication code (MAC). In asymmetric settings, the composition method of “signature-then-encryption” has been employed. But these have all proved impractical not only for the insecurity in case of arbitrary schemes but also for the low efficiency regarding application into resource-restricted environment in IOT, which results from the sum cost of encryption and signature.

In 1997, Zheng proposed a cryptographic primitive “signcryption” [5], which simultaneously fulfils the integrated function of public encryption and digital signature with a computing and communication cost significantly smaller than that required by the “signature-then-encryption” method. Since then, signcryption has been a focus of cryptography as an ideal method to simultaneously provide confidentiality and unforgeability and many researchers have explored the application of signcryption in different security protocols [6, 7, 8, 9, 10, 11]. The study of signcryption algorithms suitable for IOT network environment and its application in IOT security schemes is an important direction in cryptography; it is more of a requirement from the rapid development of the Internet of things than just a requirement from the theoretical or applied cryptography research.

In order to improve the security and efficiency of communication in the Internet of things, we propose a publicly verifiable short signcryption scheme *S-ECSC* for the Internet of things based on elliptic curves cryptosystem; and prove the provable security of *S-ECSC* under the Random Oracle model, including confidentiality in *IND-CCA2* model, unforgeability in *UF-CMA* model and non-repudiation security. At last, we take key generating and distributing protocol for different terminals of distributed key management in IOT as an application example, and analyse the method and importance in the application of *S-ECSC* into secure protocols in IOT. Compared with other typical discrete logarithm, RSA and elliptic curves based signcryption schemes, *S-ECSC* is more suitable for resource-restricted environment in IOT communication with its superiority in computing and communication cost and can better satisfy the requirement of secure protocols in IOT, such as key management, secure routing, etc.

2 Short Signcryption Scheme on Elliptic Curves

First, we pin down the basic notions concerning signcryption which will facilitate the design and analysis of the short signcryption scheme.

2.1 Basic Notions in Signcryption

Definition 2.1.1 (Elliptic Curve) An elliptic curve $E(F_q)$ over finite field F_q is a sextuple: T = (q, a, b, P, l, h), where P=(x_P, y_P) is the base point of $E(F_q)$, prime l is the order of P. As to $t \in Z_l^*$, Q and $G \in E(F_q)$, $Q = tG$ denotes multiple double additions on elliptic curve. O is the point at infinity, satisfying $lP = O$ and $G + O = G$ for any point $G \in E(F_q)$.

Definition 2.1.2 (ECDLP, Elliptic Curve Discrete Logarithm Problem). ECDLP is the following computation:

$$x \leftarrow ECDLP(Q,P).$$

P is a base point and $Q \in \langle P \rangle$, $x \in Z_l^*$, $Q = xP$.

Definition 2.1.3 (Signcryption Scheme) A signcryption scheme Σ = (GC, GK, SC, USC) consists of the following algorithms:

1. Probabilistic common parameters generation algorithm GC (1^k) takes security parameter 1^k as input and returns a sequence of common parameters such as description of computational groups and hash functions.

2. Key generation algorithm GK (ID,1^k), which is also probabilistic, takes identity and security parameter as input and returns secret/public key-pair (sk_{ID}, PK_{ID}).

$$(sk_{ID}, PK_{ID}) \leftarrow GK\ (ID, 1^k).$$

3. Signcryption algorithm SC (sk_A, PK_B, m)that takes sender's secret key sk_A, receiver's public key pk_B and message $m \in SP_m$ (SP_m is the message space) as input and returns signcryption text C or $\perp$ (a reject symbol). It is also probabilistic algorithm.

$$C \bigcup \{\perp\} \leftarrow SC\ (sk_A, PK_B, m).$$

4. Deterministic unsigncryption algorithm USC (sk_B, PK_A, C)takes as input receiver's secret key sk_B, sender's public key PK_A and signcryption text C, and returns either message m or $\perp$.

$$m \bigcup \{\perp\} \leftarrow USC\ (sk_B, PK_A, C).$$

If the signcryption scheme is publicly verifiable, it is composed of an additional public verification algorithm PV.

5. Deterministic public verification algorithm PV (PK_A, PK_B, C, R) takes as input public key pair (PK_B, PK_A),signcryption text C and parameter R, and returns either “*true*” or $\perp$.

$$\text{“}True\text{”} \bigcup \{\perp\} \leftarrow PV\ (PK_A, PK_B, C, R).$$

2.2 *S-ECSC* Signcryption Algorithm

Short signcryption scheme $S-ECSC$ = (GC, GK, SC, USC, PV)

Common parameters generation

GC (1^k) =“On input (1^k) :

$K : E(F_q) \rightarrow \{0,1\}^{L_K(1^k)}$, $H : \{0,1\}^* \rightarrow Z_l^*$,

(K, H, T) $\leftarrow GC$ (1^k).”

T = (q , a , b , P , l , h),where P =(x_P , y_P) is the base point of $E(F_q)$, $ord(P) = l$ is a prime, O is the point at infinity.

Key pair generation

```
$GK$ ( $A, 1^k$ ) ="On input ( $A, 1^k$ ):
    $sk_A \xleftarrow{\$} Z_l^*$ , $PK_A = sk_A P \neq O$ ,
    ( $sk_A$ , $PK_A$ ) $\leftarrow$ ."
$GK$ ( $B, 1^k$ ) ="On input ( $B, 1^k$ ):
    $sk_B \xleftarrow{\$} Z_l^*$ , $PK_B = sk_B P \neq O$ ,
    ( $sk_B$ , $PK_B$ ) $\leftarrow$ ."
```

Signcryption

```
$SC$ ( $sk_A$ , $PK_B$ , $m$ )="On input ( $sk_A$ , $PK_B$ , $m$ ):
    If $sk_A \notin Z_l^*$ or $PK_B \notin < P >$ return $\perp$ ,
    $r \xleftarrow{\$} Z_l^*$ , $R$ =( $x_R$ , $y_R$ ) $\leftarrow rPK_B$ ,
    $\sigma \leftarrow K(R)$ , $c \leftarrow E_\sigma(m)$ ,
    $h \leftarrow H(\ m \parallel\ PK_A \parallel\ PK_B \parallel\ R)$ ,
    $s = (hsk_A + r) \bmod l$ ,
    $C$ =( $c$ , $h$ , $s$ )."
```

Symmetric encryption scheme Υ = (E , D) is an encryption scheme with passive indistinguishability defined in Definition 3. 2.8.

Unsigncryption

```
$USC$ ( $sk_B$ , $PK_A$ , $C$ )="On input ( $sk_B$ , $PK_A$ , $C$ ):
    If $sk_B \notin Z_l^*$ or $PK_A \notin < P >$ return $\perp$ ,
    Parse $C$ into ( $c$ , $h$ , $s$ ),
    If $h, s \notin Z_l^*$ or $c \notin SP_E$ return $\perp$ ,
    Else $I = sP - hPK_A$ , $R = sk_B I$ =( $x_R$ , $y_R$ ),
    $\sigma \leftarrow K(R)$ , $m \leftarrow D_\sigma(c)$ ,
    $h' \leftarrow H(\ m \parallel\ PK_A \parallel\ PK_B \parallel\ R)$ ,
    If $h = h'$ return $m$ , else return $\perp$ ."
```

Public Verification

If controversy arises between signcryption senders and receiver, a trusted third party can solve the repudiation. The third party evaluates the following formula after signcryption receiver publishing (R , C).

```
$PV$ ( $PK_A$ , $PK_B$ , $C$ , $R$ )=
    "On input $PK_A$ , $PK_B$ , $C$ , $R$ ):
    Parse $C$ into ( $c$ , $h$ , $s$ ),
    $\sigma \leftarrow K(R)$ , $m \leftarrow D_\sigma(c)$ ,
    $h' \leftarrow H(\ m \parallel\ PK_A \parallel\ PK_B \parallel\ R)$ ,
    If $h = h'$ return *true*, else return $\perp$ ."
```

3 Provable Security of *S-ECSC*

In this section, we will analyse the provable security of the signcryption in random oracle model, including confidentiality, unforgeability and non-repudiation.

3.1 Correctness of *S-ECSC*

Definition 3.1.1 Message space $Message(sk_A, PK_B)$ is the set of all m associated to each private/public key pair (sk_A , PK_B) output by GK ($ID, 1^k$) for which SC (sk_A , PK_B , m) never returns $\perp$.

Definition 3.1.2 A signcryption scheme Σ = (GC , GK , SC , USC) is correct if USC (sk_B , PK_A , C)= m for any private/public key pair (sk_A , PK_B) output by GK ($ID, 1^k$), any message $m \in Message(sk_A, PK_B)$, and any $C \neq \perp$ that might be output by SC (sk_A , PK_B , m).

Theorem 3.1.1 *S-ECSC* is correct for any private/public key pair (sk_A , PK_B) output by GK ($ID, 1^k$), any message $m \in Message(sk_A, PK_B)$ and any $C \neq \perp$ that might be output by SC (sk_A , PK_B , m).

Proof of correctness: Obviously, the signcryption scheme *S-ECSC* is correct if and only if

$$USC\ (SC\ (sk_A, PK_B, m)) = m\ .$$

As per the formula in the scheme,

$$sk_B I = sk_B (sP - hPK_A)$$
$$= sk_B (sP - hsk_A P\ ) = sk_B (s - hsk_A\ ) P$$
$$= sk_B rP = rPK_B = R = (x_R, y_R),$$
$$\sigma \leftarrow K(R).$$
$$\Rightarrow\ m \leftarrow D_\sigma(c),$$
$$h' \leftarrow H(\ m \parallel\ PK_A \parallel\ PK_B \parallel\ R),$$
$$\Rightarrow\ h = h',\ m \leftarrow USC\ (sk_B, PK_A, C).$$

Thus USC (SC (sk_A , PK_B , m))= m , the short signcryption *S-ECSC* is correct, as desired.

3.2 Confidentiality of *S-ECSC*

Definition 3.2.1 Computational Elliptic Curve Problem (CECP). Let T = (q , a , b , P , l , h) be an elliptic curve and *AC* an attacker on CECP , CECP is defined as the following:

```
Experiment $EXP_T^{CECP}(AC)$
    $d, e \xleftarrow{\$} Z_l^*$ ,
    $D = dP$ , $E = eP$ ,
    $F \in \langle P \rangle \leftarrow AC^T(D, E)$ ,
    If $F = deP$ return 1 else return 0.
```

Note that $F = deP = dE = eD$. (1)

Definition 3.2.2 Decisional Elliptic Curve Problem (DECP). Let $T = (q, a, b, P, l, h)$ be an elliptic curve and *AD* an attacker on DECP , DECP is defined as the following:

Experiment $EXP_T^{DECP}(AD)$

$b \xleftarrow{\$} \{0,1\}$,

If $b = 0$ $Sce_0 : d, e, f \xleftarrow{\$} Z_l^*$,

If $b = 1$ $Sce_1 : d, e \xleftarrow{\$} Z_l^*, f = de(\bmod l)$,

$D = dP, E = eP, F = fP$,

$b' \leftarrow AD^T(D, E, F)$,

If $b' = b$ return 1 else return 0.

Definition 3.2.3 DECP Oracle O_T^{DECP} . Let $T = (q, a, b, P, l, h)$ be an elliptic curve, DECP Oracle is defined as the following:

O_T^{DECP} =“on input (P, D, E, F)

If $D, E, F \notin < P >$ return $\perp$, else

If *DCEP* (D, E, F) =1 return 1,

If *DCEP* (D, E, F) =0 return 0.”

Definition 3.2.4 Elliptic Curve Gap Problem (ECGP). Let $T = (q, a, b, P, l, h)$ be an elliptic curve and *AECG* an attacker on ECGP , let’s consider the following experiment:

Experiment $EXP_T^{ECGP}(AECG)$

$d, e \xleftarrow{\$} Z_l^*$,

$F = fP \leftarrow AECG_T^{O_T^{DECP}(,,,)}(d, e)$,

If $f = de(\bmod l)$ return 1 else return 0.

The *ECGP advantage* of *AECG* is defined as

$$Adv_T^{ECGP}(AECG) = \Pr(EXP_T^{ECGP}(AECG) = 1). \quad (2)$$

Hypothesis 3.2.1 (ECGP is hard). Given elliptic curve T and secure parameter 1^k , the probability of solving ECGP in time t is $\xi(1^k, T)$ which is negligible, that is

$$\xi(1^k, T) = \Pr[1^k, d, e \xleftarrow{\$} Z_l^*, \\ Q \leftarrow xP : EXP_T^{ECGP}(AECG) = 1]. \quad (3)$$

Definition 3.2.5 Left-or-right signcryption oracle. Let $\Sigma = (GC, GK, SC, USC)$ be a signcryption scheme, a left-or-right signcryption oracle is defined as follows.

Oracle $SC_{sk_A, PK_B}(LR(m_0, m_1, b))$ =

“On input (m_0, m_1):

$b \in \{0,1\}, m_0, m_1 \in SP_m$,

$C \leftarrow SC(sk_A, PK_B, m_b)$,

Return C .”

Definition 3.2.6 Confidentiality of signcryption. Let *ASC* be an algorithm against the confidentiality of signcryption scheme Σ that has access to a left-or-right signcryption oracle and returns a bit. We consider the following experiment:

Experiment $EXP_{SGC}^{ind-cca2}(ASC)$

$(K, H, T) \leftarrow GC(1^k)$

,(sk_A, PK_A) $\leftarrow GK(A, 1^k)$,

$(sk_B, PK_B) \leftarrow GK(B, 1^k)$,

$C' \leftarrow SC_{sk_A, PK_B}(LR(m_0, m_1, b)), b \leftarrow \{0,1\}$,

$b' \leftarrow ASC^{SC_{sk_A, PK_B}(LR(,,b)), USC(sk_A, PK_B,)}$

If *ASC* queried $USC(sk_A, PK_B,)$ on a signcryption text previously returned by $SC_{sk_A, PK_B}(LR(m_0, m_1, b))$ then return 0,

If $b' = b$ return 1 else return 0.

The *IND-CCA2 advantage* of *ASC* is defined as

$$\delta(k) = Adv_{SGC}^{ind-cca2}(ASC) \\ = \Pr(EXP_{SGC}^{ind-cca2}(ASC) = 1). \quad (4)$$

A signcryption scheme is indistinguishable under adaptive chosen cipher-text attack if the *IND-CCA2 advantage* of any attacker *ASC* with reasonably restricted resources (time-complexity, frequency and length of queries) is negligible.

Definition 3.2.7 Left-or-right Encryption Oracle. Let $\Upsilon = (E, D)$ be the symmetric encryption algorithm in the signcryption scheme, a left-or-right encryption Oracle is defined as:

Oracle $E_\sigma(LR(m_0, m_1, b))$ =“On input (m_0, m_1):

$b \in \{0,1\}, m_0, m_1 \in SP_m$,

$C \leftarrow E_\sigma(m_b)$,

Return C .”

Definition 3.2.8 Passive Indistinguishability. Let *AI* be an algorithm against the passive indistinguishability of symmetric encryption scheme Υ, which has access to a left-or-right encryption oracle and returns a bit. We consider the following experiment:

Experiment $EXP_\Upsilon^{pi}(AI)$

$C' \leftarrow E_\sigma(LR(m_0, m_1, b))$,

$b \leftarrow \{0,1\}, b' \leftarrow AI^{E_\sigma(LR(,,b))}$,

If $b' = b$ return 1 else return 0.

The *pi advantage* of *AI* is defined as

$$\upsilon(k) = Adv_\Upsilon^{pi}(AI) = \Pr(EXP_\Upsilon^{pi}(AI) = 1). \quad (5)$$

An encryption scheme is passively indistinguishable if the *pi advantage* of any attacker *AI* with reasonably restricted resources (time-complexity, frequency and length of queries) is negligible.

Hypothesis 3.2.2 (Ideal Hash Function). Hash function has the property of Random Oracle. Namely, the outputs of hash function are randomly and uniformly distributed.

Theorem 3.2.1 If there exists an algorithm *ASC* against the *IND-CCA2* property of signcryption scheme Σ in time t with non-negligible advantage $\delta(k)$, using q_{SC}

queries to its signcryption oracle and (q_H , q_M) queries to its random oracles. Then we can thus formulate an *AECG* attacker on ECGP with non-negligible advantage ξ (1^k , T) in time t' , using q_{SC} queries to its signcryption oracle and $q_{SC}+q_H$ queries to its random oracles.

Proof of confidentiality: In our proof, the random oracles K and H are replace by the random oracle simulators with two types of "query-answer" lists. For example, Sim_K simulates random oracle K with two types of "query-answer" lists L_1^K and L_2^K . L_1^K consists of simple "query-answer" (R , σ) entries from K ,while L_2^K consists of special input-output entries ($PK_B \| \Omega_i \| (?,\sigma)$) which implies $\sigma = K(\Omega^{sk_B})$ with the implicit input Ω^{sk_B} stored and denoted as "?".

$\mathrm{Sim}\_K(L^K, R)$ ="on input (L^K , R):

If $1 \leftarrow DECP(D, PK_B, R)$ return $\perp$,

Else if $1 \leftarrow DECP(\Omega_i, PK_B, R)$ return σ_i ,

//there is an entry ($PK_B \| \Omega_i \| (?,\sigma_i)$) *in* L_2^K

Else if $R = R_i$, return σ_i *//there is an entry* (R_i, σ_i) *in* L_1^K

Else $\sigma_i \xleftarrow{\$} \{0,1\}^{L_K(1^k)}$, $R_i \leftarrow R$,

Add (R_i , σ_i) into L_1^K ."

If $EXP_{SGC}^{ind-cca2}(ASC)$ makes queries to random Oracle O^H , *AECG* will reply with simulator Sim_H .

$\mathrm{Sim}\_H(L^H, \hbar)$ ="on input (L^H , $\hbar$): // $\hbar$ =($m \| PK_A \| PK_B \| R$)

If $1 \leftarrow DECP(D, PK_B, R)$ return $\perp$,

Else if $1 \leftarrow DECP(\Omega_i, PK_B, R)$ and $m \| PK_A \| PK_B = m_i \| (PK_A)_i \| (PK_B)_i$

return σ_i *//there is an entry* ($\Omega_i \| (m_i \| (PK_A)_i \| (PK_B)_i \| ?$) *in* L_2^H

Else if $\hbar = \hbar_i$, return $\hbar_i$ *//there is an entry* $(\hbar_i, h_i)$ *in* L_1^H

Else $h_i \xleftarrow{\$} Z_l^*$, $\hbar_i \leftarrow \hbar$, Add ($\hbar_i$, h_i) into L_1^H ."

If $EXP_{SGC}^{ind-cca2}(ASC)$ makes queries to random Oracle O^{SC} , *AECG* will reply with simulator Sim_SC .

$\mathrm{Sim}\_SC(L_2^K, L_2^H, PK_A, PK_B, m)$ =

"On input ($L_2^K, L_2^H, PK_A, PK_B, m$): // $\hbar$ =($m \| PK_A \| PK_B \| R$)

$\sigma \xleftarrow{\$} \{0,1\}^{L^K(1^k)}$, $c \leftarrow E_\sigma(m)$,

$h \xleftarrow{\$} Z_l^*$, $s \xleftarrow{\$} Z_l^*$,

$\Omega \leftarrow sP - hPK_A$, $\Omega_i \leftarrow \Omega$,

$\sigma_i \leftarrow \sigma$, $m_i \leftarrow m$, $h_i \leftarrow h$,

Add entry $\Omega_i \| (?,\sigma_i)$ into L_2^K ,

Add entry ($m \| PK_A \| PK_B \| (?,h_i)$) into L_2^H , C = (c , h , s) and return C ."

If $EXP_{SGC}^{ind-cca2}(ASC)$ makes queries to O^{USC} , *AECG* will reply with simulator Sim_USC .

$\mathrm{Sim}\_USC(L^K, L^H, D, PK_A, PK_B, C)$ =

"On input ($L^K, L^H, D, PK_A, PK_B, C$):

Parse C into (c , h , s), $\Omega \leftarrow sP - hPK_A$,

If $\Omega = D$ return $\perp$,

If $\exists$ (R_i , σ_i) in L_1^K s.t. $1 \leftarrow DECP(\Omega_i, PK_B, R_i)$ or $\exists$ $\Omega_i \| (?,\sigma_i)$ in L_2^K s.t. $\Omega_i = \Omega$

Then $\sigma' \leftarrow \sigma_i$,

Else $\sigma' \xleftarrow{\$} \{0,1\}^{L_K(1^k)}$, $\Omega_i \leftarrow \Omega$, $\sigma_i \leftarrow \sigma'$,

Add entry $\Omega_i \| (?,\sigma_i)$ into L_2^K , $m \leftarrow D_{\sigma'}(c)$,

If $\exists$ ($\hbar_i$, h_i) in L_1^H s.t. $1 \leftarrow DECP(\Omega_i, PK_B, R_i)$

or $\exists$ ($\Omega_i \| (m_i \| (PK_A)_i \| (PK_B)_i \| ?), h_i$) *in* L_2^H s.t. $\Omega_i = \Omega$, $m_i = m$, $(PK_A)_i \| (PK_B)_i = (PK_A) \| (PK_B)$,

Then $h' \leftarrow h_i$,

Else $\Omega_i \leftarrow \Omega$, $(PK_A) \| (PK_B) \leftarrow (PK_A)_i \| (PK_B)_i$, $m_i \leftarrow m$, $h_i \xleftarrow{\$} Z_l^*$,

Add entry ($\Omega_i \| (m_i \| (PK_A \| PK_B)_i \| (?,h_i)$) into L_2^H ,

If $h = h_i$ return m , else return $\perp$."

Based on Theorem 3.2.1 we formulate an *AECG* attacker on ECGP; apparently contradicting Hypothesis 3.2.1, thus prove the confidentiality of the improved signcryption scheme.

The *AECG* attacker on ECGP is formulated as follows.

$AECG$ (T , D , E)=

"On input (T , $D = dP$, $E = eP$):

$h^*, s^* \xleftarrow{\$} Z_l^*$, $PK_A \leftarrow (h^*)^{-1}(s^*P + D)$,

$PK_B \leftarrow E$, $\sigma^* \xleftarrow{\$} Z_l^*$,

C^* = (c^* , h^* , s^*) $\leftarrow SC_{sk_A, PK_B}(LR(m_0, m_1, b))$,

// $c^{*} \leftarrow E_{\sigma^{*}}(m_b)$, and *the random oracle queries* O^{*} *are replaced with random oracle simulator* Sim_O^{*} .

If SC_{sk_A,PK_B} has ever queried $\mathrm{Sim\_}K(R)=\perp$,

Halt and return R ,

If SC_{sk_A,PK_B} has ever queried $\mathrm{Sim\_}H(\hbar)=\perp$,

Halt and return $\hbar$ (the rightmost $|R|$ bits of $\hbar$),

$EXP_{SGC}^{ind-cca2}(ASC)$ = "

// *random oracle queries* O^{*} *are also replaced with random oracle simulator* Sim_O^{*} .

If $EXP_{SGC}^{ind-cca2}(ASC)$ has ever queried $\mathrm{Sim\_}K(R)=\perp$,

Halt and return R ,

If $EXP_{SGC}^{ind-cca2}(ASC)$ has ever queried $\mathrm{Sim\_}H(\hbar)=\perp$,

Halt and return $\hbar$ (the rightmost $|R|$ bits of $\hbar$),

$b \leftarrow EXP_{SGC}^{ind-cca2}(ASC)$,

Return R ."

Let *ASC* be an attacker against *IND-CCA2* security of signcryption in time t , using q_{sc} queries to its signcryption oracle, q_{usc} queries to its unsigncryption oracle and (q_k , q_h) queries to its random oracles. *AECG* is an attacker against *ECGP* security of elliptic curve in time t' , using $q_{O^{DECP}}$ queries to its DECP Oracle O_T^{DECP} . *AI* is an attacker against *PI* security of the symmetric key encryption in time t'' . From the *AECG* algorithm formulated above, the following bound holds. More details about the probability proof of the theorem can be found in [5, 12, 13, 14].

$$Adv_{SGC}^{ind-cca2}(t\ ,q_{sc},q_{usc},q_k,q_h)\le 2\,Adv_T^{ECGP}(t'\ ,q_{O^{DECP}}) + 2\,Adv_{\Upsilon}^{pi}(t'') + q_{sc}\left(\frac{q_k+q_h+q_{sc}+q_{usc}+2}{2^{L^K(1^k)-1}}\right) + \frac{q_h+2q_{usc}}{2^{L^K(1^k)-1}}\ . \quad (6)$$

$$\Rightarrow\ Adv_{SGC}^{ind-cca2}(t\ ,q_{sc},q_{usc},q_k,q_h)/2 - q_{sc}\left(\frac{q_k+q_h+q_{sc}+q_{usc}+2}{2^{L^K(1^k)}}\right) - \frac{q_h+2q_{usc}}{2^{L^K(1^k)}} - Adv_{\Upsilon}^{pi}(t'') \le Adv_T^{ECGP}(t'\ ,q_{O^{DECP}}). \quad (7)$$

As *ASC* and *AECG* are reasonably resource bounded,

$$\Rightarrow\ q_{sc}\left(\frac{q_k+q_h+q_{sc}+q_{usc}+2}{2^{L^K(1^k)}}\right) - \frac{q_h+2q_{usc}}{2^{L^K(1^k)}}$$ is negligible.

And with the assumption Υ is passive indistinguishable, $Adv_{\Upsilon}^{pi}(t'')$ is negligible too.

$$\Rightarrow\ Adv_{SGC}^{ind-cca2}(t\ ,q_{sc},q_{usc},q_k,q_h)/2\le Adv_T^{ECGP}(t'\ ,q_{O^{DECP}}). \quad (8)$$

On account of all the above analyses, if the *IND-CCA2*security of signcryption will be broken by *ASC* with non-negligible advantage, so will the *ECGP* security of elliptic curve by *AECG* with non-negligible advantage. Therefore, *S-ECSC* achieves confidentiality in the *IND-CCA2* model, as desired.

3.3 Unforgeability of *S-ECSC*

Definition 3.3.1 Unforgeability of Signcryption. Let Σ = (GC , GK , SC , USC) be a signcryption scheme, and let *A* be an algorithm that has access to a signcryption oracle and returns a pair of strings. We consider the following experiment:

Experiment $EXP_{SGC}^{uf-cma}(A)$

$(sk_A, PK_A)\leftarrow GK(A,1^k)$,

$(sk_B, PK_B)\leftarrow GK(B,1^k)$,

$(m, C')\xleftarrow{\$} A^{SGC(sk_A,PK_B,)}(PK_A,PK_B)$.

If the following are true return 1 else return 0:

1. $m \leftarrow USC\ (sk_B, PK_A, C')$,
2. $m \in Message(sk_A, PK_B)$,
3. m is not a query of *A* to its signcryption oracle.

The *UF-CMA advantage* of A is defined as

$$Adv_{SGC}^{uf-cma}(A) = \Pr\ (EXP_{SGC}^{uf-cma}(A)=1). \quad (9)$$

To be specific, the *UF-CMA advantage* can be concluded as a function $\varepsilon(k)$ defined by

$$\varepsilon(k)=\Pr\,[\,(sk_A,PK_A)\leftarrow GK(A,1^k),\ (sk_B,PK_B)\leftarrow GK(B,1^k),\ (m,C')\xleftarrow{\$} A^{SGC(sk_A,PK_B,)}(PK_A,PK_B):\ m\leftarrow USC\ (sk_B,PK_A,C')]. \quad (10)$$

A signcryption is un-forgeable under chosen message attack if the *UF-CMA advantage* of any attacker *A* with reasonably restricted resources (time-complexity, frequency and length of queries) is negligible.

Hypothesis 3.3.1 (ECDLP is hard). Let T be an elliptic curve, and let *A* be an algorithm that has access to a elliptic curve oracle and returns a string. We consider the following experiment:

Experiment $EXP_T^{ECDLP}(A)$

$x \xleftarrow{\$} Z_l^{*}, Q \leftarrow xP$,

$x' \leftarrow A^T(P,Q)$.

If $x' = x$ return 1 and return 0 otherwise.
The *ECDLP advantage* of *A* is defined as

$$Adv_T^{ECDLP}(A) = \Pr\ (EXP_T^{ECDLP}(A) = 1). \quad (11)$$

Given elliptic curve T and secure parameter 1^k, the probability of solving ECDLP in time t is $\delta\,(1^k, T)$ which is negligible, that is

$$\delta\,(1^k, T) = \Pr\,[1^k, x \xleftarrow{\$} Z_l^*,$$
$$Q \leftarrow xP : EXP_T^{ECDLP}(A) = 1]. \quad (12)$$

Definition 3.3.2 Gap Elliptic Curve Discrete Logarithm (GECDL). Let $T = (q, a, b, P, l, h)$ be an elliptic curve and AGL an attacker on GECDL, O_T^{DECP} is DECP Oracle, let's consider the following experiment:

Experiment $EXP_T^{GECDL}(AGL)$

$d \xleftarrow{\$} Z_l^*, D \leftarrow dP$,

$d' \leftarrow AGL_T^{O_T^{DECP}(,,,)}(D)$,

If $d' = d$ return 1 else return 0.
The *GECDL advantage* of *AGL* is defined as

$$Adv_T^{GECDL}(AGL) = \Pr\ (EXP_T^{GECDL}(AGL) = 1). \quad (13)$$

Hypothesis 3.3.2 (GECDL is hard). Given elliptic curve T and secure parameter 1^k, the probability of solving GECDL in time t is negligible, that is

$$\delta\,(1^k, T) = \Pr\,[1^k, d \xleftarrow{\$} Z_l^*, d' \leftarrow$$
$$AGL_T^{O_T^{DECP}(,,,)}(D), EXP_T^{GECDL}(AGL) = 1]. \quad (14)$$

Proof of unforgeability: Let *ASC* be an attacker against *UF-CMA* security of signcryption executing in time t, using q_{sc} queries to its signcryption oracle, q_{usc} queries to its unsigncryption oracle and (q_k, q_h) queries to its random oracles. *AGL* is an attacker against *GECDL* security of elliptic curve executing in time t', using $q_{O^{DECP}}$ queries to its DECP Oracle O_T^{DECP}. From the algorithm formulated above, the following bound holds. Similarly, more details about the probability proof of the theorem can be found in [12, 13, 14].

$$Adv_{SGC}^{uf-cma}(t, q_{sc}, q_{usc}, q_k, q_h) \le$$
$$2\sqrt{Adv_T^{GECDL}(t', q_{O^{DECP}})} +$$
$$\left(\frac{q_{sc}(q_k + q_h + q_{sc}) + q_h + 1}{2^{L^K(1^k)-1}}\right). \quad (15)$$

As *ASC* is reasonably resource bounded,

$$\Rightarrow \frac{q_{sc}(q_k + q_h + q_{sc}) + q_h + 1}{2^{L^K(1^k)-1}} \text{ is negligible}$$

$$\Rightarrow Adv_{SGC}^{uf-cma}(t, q_{sc}, q_{usc}, q_k, q_h)$$
$$\le 2\sqrt{Adv_T^{GECDL}(t', q_{O^{DECP}})}. \quad (16)$$

If the *UF-CMA* security of signcryption will be broken by *ASC* with non-negligible advantage, so will the *GECDL* security of elliptic curve by *AGL* with non-negligible advantage. Therefore, *S-ECSC* achieves unforgeability in the *UF-CMA* model, as desired.

3.4 Nonrepudiation of *S-ECSC*

Definition 3.4.1 Non-repudiation of signcryption. It is computationally feasible for a third party to settle a dispute between signcryption sender and receiver in an event where sender denies the fact that he is the originator of signcryption.
Definition 3.4.2 Relation Map. A relation is a map defined as

$$\Re_{E,\pi}^H : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}. \quad (17)$$

For every string $x \in \{0,1\}^*$, random oracle $H \in 2^\infty$ and $E, \pi \in \{0,1\}^*$, it satisfies

$$\Re_{E,\pi}^H(x, x) = \Re_{E,\pi}^H(x, 0^*) = 0. \quad (18)$$

Besides, $\Re_{E,\pi}^H$ must be computable by a deterministic polynomial time algorithm $A^H(x, y, E, \pi)$. A malleability adversary s is a pair of probabilistic polynomial time algorithms (P, Q) with access to random oracle $H \in 2^\infty$.

The security notion of non-malleability for encryption scheme was introduced by Dolev, Dwork and Naor[15]. In this section, we generalize non-malleability into a more comprehensive security notion applicable to signcryption as well.
Definition 3.4.3 Non-malleability of Signcryption. A signcryption scheme $\Sigma = (GC, GK, SC, USC)$is non-malleable if any adversary can not by witnessing signcryption generating of a message m or querying a signcryption oracle, produce the signcryption text of a related message m'.

To be specific, a signcryption scheme is non-malleable if for every relation $\Re$ and every malleability adversary $s = (P, Q)$, there is a deterministic time algorithm Q' so that $|\tau(k) - \tau_*(k)|$ defined as follows is negligible.

$$\tau(k) = \Pr\,[H \leftarrow 2^\infty; (SC, USC) \leftarrow K(1^k);$$
$$\pi \leftarrow P^H(SC); x \leftarrow \pi^H(1^k); \beta \leftarrow SC^H(x); \beta' \leftarrow$$
$$Q^H(SC, \pi, \beta) : \Re_{E,\pi}^H(x, USC^H(\beta') = 1)], \quad (19)$$

$$\tau_*(k) = \Pr\,[H \leftarrow 2^\infty; (SC, USC) \leftarrow K(1^k);$$
$$\pi \leftarrow P^H(SC); x \leftarrow \pi^H(1^k); \beta'_* \leftarrow Q'^H$$
$$(SC, \pi) : \Re_{E,\pi}^H(x, USC^H(\beta'_*) = 1)]. \quad (20)$$

Theorem 3.4.1 The short signcryption scheme *S-ECSC* achieves non-repudiation security.

Proof of non-repudiation: In signcryption schemes, unforgeability implies non-repudiation if there is no duplication of the signcryption text. If the signcryption scheme is forgeable or malleable, the signcryption generator will have opportunity to repudiate.

In *S-ECSC,* the map $K : E(F_q) \to \{0,1\}^{L_K(1^k)}$ and $H : \{0,1\}^* \to Z_l^*$ are both unique, distinct (m_1 , r) and(m_2 , r) will generate different signcryption text C =(c , h , s). Furthermore, the scheme can be reinforced by state padding. The state padding not only ensures different signcryption text for distinct (m_1 , r) and (m_2 , r), but for the same original message (m , r) with different state information. Thus, the above signcryption scheme satisfies: as to $\left|\tau(k)-\tau_*(k)\right|$ for every c there is a k_c such that $\left|\tau(k)-\tau_*(k)\right| \le k^{-c}$ for every $k \ge k_c$. Thus the signcryption text C produced by SC (sk_A , PK_B , m) is not duplicable, and with the unforgeability proof of *S-ECSC* in *UF-CMA* model in section 3.3, we can come to the conclusion that *S-ECSC* achieves non-repudiation security, as desired.

4 Efficiency of *S-ECSC*

In this section, the short signcryption scheme *S-ECSC* will be compared with other typical schemes including discrete logarithm based signcryption *SCS* [5], *B&D* [16], *KCDSA*[17], *SC-DSA*[18] and RSA based signcryption *TBOS*[19] and elliptic curve based scheme *ECSCS*[20] and *ECGSC*[21].

In these schemes, such computing as modular exponential, modular inverse and elliptic curve addition ,elliptic curve scalar multiplication should be taken into comparison for computing complexity, while computing cost of modular addition, modular multiplication, hash, symmetric encryption/decryption are negligible. To ensure the security of the basic cryptographic primitives, the minimum security parameters of these cryptosystems recommended for the current practice are as follows: for DLP, $\left|p\right|$ =1024bits, $\left|q\right|$ =160bits. For RSA, $\left|N\right|$ =1024bits; for ECC, $\left|q\right|$ =131bits (79, 109 may also be chosen), $\left|l\right|$ =160bits. The block length of the block cipher is 64bits. The length of secure hash function is 128bits.

Schemes	*GC+GK*	*SC*	*USC*	*EC*	*PV*	*Length of C*
SCS	2*E*	1*E*+1 *I*	2*E*	/	/	$\vert D(\cdot)\vert+\vert KH(\cdot)\vert+\vert q\vert$
B&D	2*E*	2*E*+1 *I*	3*E*	0	2*E*	$\vert D(\cdot)\vert+\vert h\vert+\vert q\vert$
KCDSA	2*E*	2*E*	3*E*	Save *r,s* or 3*E*	2*E*	$\vert D(\cdot)\vert+\vert h\vert+\vert q\vert$
SC-DSA	2*E*	2*E*+2 *I*	3*E*+1 *I*	Save *r,s* or 2*E*+1 *I*	2*E*+1 *I*	$\vert D(\cdot)\vert+2\vert q\vert$
TBOS	2*E*+2*I*	2*E*	2*E*	0	2*E*	$\vert N\vert$
ECSCS	2*kP*	1 *kP* +1 *I*	2*kP*	/	/	$\vert D(\cdot)\vert+\vert h\vert+\vert n\vert$
ECGSC	2*kP*	2*kP*+1 *I*	3*kP*+1 *I*	0	2*kP*+1 *I*	$\vert l\vert+\vert LH(.)\vert+2\vert q\vert$
S-ECSC	2*kP*	1*kP*	2*kP*+1 *I*	0	2*kP*+1 *I*	$\vert D(\cdot)\vert+\vert h\vert+2\vert p\vert$

Table 1: Comparison of computing and communication cost

Notes of notations: 1. *GC* denotes the common parameters generation algorithm, *GK* denotes the keys generation algorithm; *SC* denotes the signcryption algorithm; *USC* denotes the unsigncryption algorithm; *EC* denotes the extra computation to accomplish public verifiability; *PV* denotes the public verification by a third party. *Length of C* denotes the length of signcryption text. 2. *E* denotes modular exponential; *I* denotes modular inverse; *KP* denotes scalar multiplication on elliptic curve. / denotes there is no relevant computation. 3. |*D* (·) |denotes the block length of block cipher, |*h*| denotes the outputs length of secure hash function, |*KH* (·)| denotes the length of key hash function in *SCS*, the same as |*h*|, |*LH* (.)| denotes the length of hash function with long message digest, much larger than |*h*|.

Remark 1. (Comparison with DLP based signcryption schemes). *SCS* is the fastest scheme in all of the four DLP based schemes (*SCS, B&D, KCDSA* and *SC-DSA*). Based on the result of Koblitz and Menezes [22], the computing cost in key generation in our scheme is 1/8 of that in *SCS*; signcryption operation in ours is about 1/8 of that in *SCS*, and unsigncrption is about 1/8 of that in *SCS*. To sum up, *S-ECSC* reduces about 87%computating cost compared with *SCS*.

Remark 2. (Comparison with RSA based signcryption scheme). As per the result of [22], the computing cost in key generation in our scheme is about 1/8 of that in *TBOS*; signcryption operation in ours is about 1/16 of that in *TBOS*, and unsigncrption is about 1/8 of that in TBOS, achieving a total 89%computating cost reduction over *TBOS*.

Remark 3. (Comparison with other ECC based schemes). The computing cost in key generation are the same; signcryption cost in ours is slightly lower than that in *ECSCS* while unsigncrption of *ECSCS* is slightly lower than ours, total resulting an equal computing cost, yet *ECSCS* proves to be unsuitable for public verifying. Although *ECGSC* is publicly verifiable, its computing cost in signcryption and unsigncryption is much larger than *S-ECSC*, resulting in a much higher total computing cost.

Remark 4. (Comparison of communication cost). As per the comparison of signcryption text length, except for RSA based *TBOS* signcryption, *S-ECSC* has the lowest communication cost in Elgamal type signcryption schemes.

Therefore, we may come to the conclusion that our short signcryption scheme *S-ECSC* has the highest efficiency and the lowest communication cost in all of the publicly verifiable schemes.

5 Application of *S-ECSC* in Secure Communication of IOT

In order to achieve confidentiality and integrity for secret key in the Internet of things, a secure channel should be established for the distribution and transmission in key management schemes. Meanwhile, the special network environment in IOT, such as wireless connection, micro-terminals and restricted resources, makes it necessary to design schemes of high efficiency which can fulfil the same function with much smaller computing and communication cost than traditional schemes. With its superiority in computing and communication, *S-ECSC* greatly improves the efficiency in key management in IOT in terms of key distributing time and bandwidth resources and better satisfies the requirement of secure protocols in key management. In this section, we will take the key management schemes in [23,24,25] as an example and propose a key applying and distributing scheme in key management of IOT based on *S-ECSC*. With this *S-ECSC* based scheme, we analyse the method and importance to apply *S-ECSC* in secure wireless communication for the Internet of things. The key applying and distributing protocol in key management of IOT based on *S-ECSC* is as follows.

(1)Initializing

PKG selects the system parameter, including the parameters in *S-ECSC*.

$sk_A \in Z_l^*$, $PK_A = sk_A P \neq O$, (sk_A, PK_A) is the private/public key pair for one of the distributed terminals *A*. $sk_B \in Z_l^*$, $PK_B = sk_B P \neq O$, (sk_B, PK_B)is the private / public key pair of PKG.

(2) Key applying

Step1: Terminal *A* encodes the applying request data {ID_A, Message} into plaintext $m \in Message$ (sk_A, PK_B), and applies the signcryption algorithm on m.

$$C \leftarrow SC\ (sk_A, PK_B, m).$$

Then signcryption text C will be transmitted to PKG.

Step2: PKG applies the unsigncryption algorithm on signcryption text C.

$$m \leftarrow USC\ (sk_B, PK_A, C).$$

Thus, PKG recovers plaintext m, and simultaneously fulfils authentication on identity of terminal *A* and examines the integrity of message m.

(3)Key generating and distributing

Step1: PKG generates secret key $k \in Message$ (sk_B, PK_A) with the key generating algorithm $KG(1^k)$, and applies the signcryption algorithm on k.

$$C' \leftarrow SC\ (sk_B, PK_A, k).$$

Then the signcryption text C' will be transmitted to terminal *A*.

Step2: Terminal *A* applies the unsigncryption algorithm on C'.

$$k \leftarrow USC\ (sk_A, PK_B, C').$$

Thus, *A* recovers secret key k, and fulfils authentication on identity of PKG and examines the integrity of secret key k.

With the application of *S-ECSC* in key applying and distributing, the above scheme achieves secure and efficient transmission of terminal secret key via the public channel of IOT. The scheme fulfils the integrated functions of encryption and digital signature in a single step and simultaneously achieves confidentiality, integrity and non-repudiation for the secret terminal key and other signcrypted message; whereas, the computing and communication cost is significantly smaller than traditional schemes.

6 Conclusions

The study of signcryption algorithms suitable for IOT network environment and its application in IOT security schemes is an important direction in cryptography; it is more of a requirement from the rapid development of the Internet of things than just a requirement from the theoretical or applied cryptography research. In the paper, we propose a publicly verifiable short signcryption scheme *S-ECSC* suitable for secure communication in the Internet of things; and prove the provable security of *S-ECSC* under the Random Oracle model, including confidentiality, unforgeability and non-repudiation security. At last, we take key generating and distributing protocol for different terminals of distributed key management in IOT as an example, and analyze the method and importance in the application of *S-ECSC* into secure protocols in IOT.

Compared with other typical discrete logarithm, RSA and elliptic curve based signcryption schemes; *S-ECSC* achieves about 87% reduction in computing cost than DLP signcryption schemes and about 89% reduction compared with RSA schemes. And it has the lowest communication cost in the Elgamal type schemes. Therefore, security schemes based on *S-ECSC* are most suitable for such circumstances as with restricted computation ability and integrated space, circumstances with limited bandwidth yet requiring for high-speed operation. Besides, the computational problems ECGP and GECDL in the paper can also be basis of security proof for other elliptic curve based schemes.

Acknowledgement

The authors should thank the anonymous reviewers for their constructive advice and comments to the paper, with which we can greatly improve our work.

References

[1] ITU(2005). ITU Internet Report 2005: The Internet of Things. ITU.

[2] Atzori L,Iera A,Giacomo M(2010). The Internet of Things : a survey. Computer Networks, pp.2787-2805.

[3] EpoSS (2010).Internet of Things in 2020:Roadmap for the Future.EpoSS.

[4] Zhu Hongbo,Yang Longxiang,Yu Quan(2010). Investigation of Technical Thought and Application Strategy for the Internet of Things . Journal of Communication, pp. 2-9.

[5] Zheng Y(1997). Digital signcryption or how to achieve cost (signature &encryption) << cost (signature) + cost(encryption). Advances in Cryptoloty-CRYPTO'97, Lecture Notes in Computer Science vol.1294,Springer-Verlag, Berlin ,pp.165-179.

[6] Zhang Chuanrong. Zhang Yuqing . Li Fageng and Xiao Hong(2010). New Signcryption Algorithm for Secure Communication of ad hoc Networks. Journal of Communications, pp.19-24.

[7] Luo Ming, Zuo Chunhua and Wen Yingyou (2010).Signcryption-based fair exchange protocol. Journal of Communications, pp.87-93.

[8] Kim H, Song J, Yoon H(2007). A practical approach of ID-based cryptosystem in ad hoc networks. Wireless Communications and Mobile Computing. pp.909-917.

[9] Li F G, Hu Y P, Zhang C R(2007). An identity-based signcryption scheme for multi-domain ad hoc networks. ACNS 2007, LNCS 4521, Springer-Verlag, Berlin , pp.373-384.

[10] Chen, Weidong. Feng Dengguo(2005). Some Apiplications of Signcryption to Distributed Protocols. Chinese Journal of Computers, pp.1421-1430.

[11] Kamat P, Baliga A, Trappe W(2006). An identity-based security framework for VANETs. VANET'06. Los Angeles, California, USA, pp.94-95.

[12] Baek J, Steinfeld R and Zheng, Y(2002). Formal Proofs for the Security of Signcryption. Public Key Cryptography'02, Lecture Notes in Computer Science vol.2274, Springer-Verlag,Berlin,pp.80-98.

[13] Shoup V (2004). Sequences of Games: A Tool for Taming Complexity in Security Proofs , International Association for Cryptographic Research (IACR) ePrint Archive: Report 2004/332.

[14] Bellare M and Rogaway P (2004).The Game-Playing Technique, International Association for Cryptographic Research (IACR) ePrint Archive: Report 2004/331.

[15] Dolev D, Dwork C and Naor M (1991).Non-malleable cryptography. 23rd ACM Symposium on Theory of Computing. IEEE ,New York.

[16] Bao, F and Deng R H(1998). A signcryption scheme with signature directly verifiable by public key. Public Key Cryptography'98, Lecture Notes in Computer Science vol.1431, Springer-Verlag, Berlin,pp.55-59

[17] Yum D H and Lee P J(2002). New Signcryption Schemes based on KCDSA. Proceedings of the 4thInternational Conference on Information Security and Cryptology, Seoul, South Korea, pp. 305-317.

[18] Shin J B, Lee Kand Shim K(2003). New DSA-Verifiable Signcryption Schemes. Proceedings of the 5th International Conference on Information Security and Cryptology, Seoul, South Korea, pp.35-47.

[19] Malone-Lee J and Mao W (2003). Two birds one stone: Signcryption using RSA. Topics in Cryptology – Cryptographers'Track, RSA Conference 2003, Lecture Notes in Computer Science vol.2612, Springer-Verlag, Berlin,pp.210-224.

[20] Zheng Y and Imai H(1998). How to construct efficient signcryption schemes on elliptic curves. Information Processing Letters, pp.227-233.

[21] Han Yiliang, Yang Xiaoyuan and etc(2006). ECGSC:Elliptic Curve Based Generalized Signcryption. Proceedings of The 3th International Conference on Ubiquitous Intelligence and Computing, Springer-Verlag, Berlin,pp.956-965.

[22] Koblitz N , Menezes A and Vanstone S(2000). The state of elliptic curve cryptography. Designs, Codes and Cryptography, pp.173-193.

[23] Li G S, Han W B(2005). A new scheme for key manegement in ad hoc networks. ICN2005, LNCS 3421,Springer-Verlag, Berlin,pp.242-249.

[24] Gu Jing-jing,Chen Song-Can,Zhuang Yi(2010). Wireless Sensor Networks-Based Topology Structure for the Internet of Things Location.Chinese Journal of Computer ,pp.1548-1556.

[25] Chen Juan,Fang Binxing,Yin Lihua(2010). A Source-Location Privacy Preservation Protocol in Wireless Sensor Networks Using Source-Based Restriced Flooding.Chinese Journal of Computer, pp.1736-1747.