Providing Hop-by-Hop Authentication and Source Privacy in Wireless Sensor Networks

Yun Li Jian Li Jian Ren
Department of Electrical & Computer Engineering
Michigan State University
East Lansing, MI 48824-1226
Email: {liyun1, lijian6, renjian}@egr.msu.edu

Jie Wu
Department of Computer & Information Sciences
Temple University
Philadelphia, PA 19122
Email: jiewu@temple.edu

***Abstract*—Message authentication is one of the most effective ways to thwart unauthorized and corrupted traffic from being forwarded in wireless sensor networks (WSNs). To provide this service, a polynomial-based scheme was recently introduced. However, this scheme and its extensions all have the weakness of a built-in threshold determined by the degree of the polynomial: when the number of messages transmitted is larger than this threshold, the adversary can fully recover the polynomial. In this paper, we propose a scalable authentication scheme based on elliptic curve cryptography (ECC). While enabling intermediate node authentication, our proposed scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. In addition, our scheme can also provide message source privacy. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the polynomial-based approach in terms of communication and computational overhead under comparable security levels while providing message source privacy.**

***Index Terms*—Hop-by-hop authentication, symmetric-key cryptosystem, public-key cryptosystem, source privacy**

I. Introduction

Message authentication plays a key role in thwarting unauthorized and corrupted packets from being circulated in networks to save precious sensor energy. For this reason, many schemes have been proposed in literature to provide message authenticity and integrity in network communications [1], [2]. These schemes can largely be divided into public-key-based and symmetric-key-based approaches.

A secret polynomial-based message authentication scheme was introduced in [1]. To thwart the intruder from recovering the polynomial by computing the coefficients of the polynomial, the idea of adding random noise, called a perturbation factor, to the polynomial was proposed [2]. However, a recent study shows that the random noise can be completely removed from the polynomial using error-correcting code techniques [3].

In this paper, we propose an unconditionally secure and efficient source anonymous message authentication (SAMA) scheme, based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This MES scheme is secure against no-message attacks and adaptive chosen-message attacks in the random oracle model [4]. Our scheme enables the intermediate nodes to authenticate the message so that all corrupted packets can be dropped to conserve sensor power. While achieving compromise-resiliency, flexible-time authentication and source identity protection, our scheme does not have the threshold problem. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the polynomial-based algorithms under comparable security levels. To the best of our knowledge, this is the first scheme that provides hop-by-hop node authentication without the threshold limitation, while having performance better than the symmetric-key based schemes. The distributed nature of our algorithms makes these schemes suitable for decentralized networks.

The major contributions of this paper include: (i) we develop a source anonymous message authentication (SAMA) scheme on elliptic curves that can provide unconditional source anonymity; (ii) we offer an efficient hop-by-hop message authentication mechanism without the threshold limitation; (iii) we devise network implementation criteria on source node privacy protection in WSNs; (iv) we provide extensive simulation results under ns-2 and TelosB on multiple security levels.

II. Terminology and Preliminary

In this section, we will briefly describe the terminology and the cryptographic tools that will be used in this paper.

A. Model and Assumptions

We assume that the wireless sensor network consists of a large number of sensor nodes. Each node can be a data source or a data sink, and is capable of communicating with its neighboring nodes directly. The whole network is fully connected through multi-hop communications. We assume that there is a security server (SS) that is responsible for generating, storing and distributing the security parameters among the network. This server will never be compromised. However, after deployment, the sensor nodes may be captured and compromised by attackers. Once compromised, all information stored in the sensor nodes can be accessed by the attackers. The compromised nodes can be reprogrammed and fully controlled by the attackers. However, the compromised nodes will not be able to create new public keys that can be accepted by the SS and other nodes.

Based on the above assumptions, this paper considers both passive attacks and active attacks. Our proposed authentication

978-1-4673-0775-8/12/$31.00 ©2012 IEEE

scheme aims at achieving hop-by-hop message authentication, compromised node resilience and efficiency.

B. Terminology

Privacy is sometimes referred to as anonymity. It generally refers to the state of being unidentifiable within the *ambiguity set* (AS). *Sender anonymity* means that a particular message is not linkable to any sender, and no message is linkable to a particular sender.

Definition 1 (SAMA)**.** *A* SAMA *consists of the following two algorithms:*

- Generate $(m, Q_1, Q_2, \cdots, Q_n)$*: Given a message* m *and the public keys* $Q_1, Q_2, \cdots, Q_n$ *of the AS* $\mathcal{S} = \{A_1, A_2, \cdots, A_n\}$*, the actual message sender* $A_t, 1 \leq t \leq n$*, produces an anonymous message* $\mathcal{S}(m)$ *using its own private key* d_t*.*
- Verify $\mathcal{S}(m)$*: Given a message* m *and an anonymous message* $\mathcal{S}(m)$*, which includes the public keys of all members in the AS, a verifier can determine whether* $\mathcal{S}(m)$ *is generated by a member in the AS.*

The security requirements for SAMA include:

- Sender ambiguity*: The probability that a verifier successfully determines the real sender of the anonymous message is exactly* $1/n$*, where* n *is the total number of members in the AS.*
- Unforgeability*: An anonymous message scheme is unforgeable if no adversary, given the public keys of all members of the AS and the anonymous messages* $m_1, m_2, \cdots, m_n$ *adaptively chosen by the adversary, can produce, in polynomial time, a new valid anonymous message with non-negligible probability.*

In this paper, the user ID and the user public key will be used interchangeably without making any distinctions.

C. Modified ElGamal Signature Scheme (MES)

Definition 2 (MES)**.** *The modified ElGamal signature scheme consists of the following three algorithms:*

Key generation algorithm*: Let* p *be a large prime and* g *be a generator of* $\mathbb{Z}_p^*$*. Both* p *and* g *are made public. For a random private key* $x \in \mathbb{Z}_p$*, the public key* y *is computed from* $y = g^x \bmod p$*.*

Signature algorithm*: The MES can also have many variants [5], [6]. For the purpose of efficiency, we will describe the variant, called the* optimal scheme*. To sign a message* m*, one chooses a random* $k \in \mathbb{Z}_{p-1}^*$*, then computes the exponentiation* $r = g^k \bmod p$ *and solves* s *from:*

$$s = rxh(m, r) + k \bmod (p - 1), \tag{1}$$

where h *is a one-way hash function. The signature of message* m *is defined as the pair* (r, s)*.*

Verification algorithm*: The verifier checks the signature equation* $g^s = ry^{rh(m,r)} \bmod p$*. If the equality holds true, then the verifier* Accepts *the signature and* Rejects *it otherwise.*

III. Related Work

A secret polynomial-based message authentication scheme was introduced in [1]. This scheme offers information theoretic security with ideas similar to a threshold secret sharing scheme, where the threshold is determined by the degree of the polynomial. When the number of messages transmitted is below the threshold, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation. However, when the number of messages transmitted is larger than the threshold, the polynomial can be fully recovered and the system becomes completely broken. To increase the threshold and the complexity for the intruder to break the secret polynomial, random noise, also called a perturbation factor, was added to the polynomial in [2]. The main idea is to thwart the adversary from computing the coefficient of the polynomial. However, the added perturbation factor can be completely removed using error-correcting code techniques [3].

The recent progress on elliptic curve cryptography (ECC) shows that the public-key schemes can be more advantageous in terms of memory usage, message complexity, and security resilience since public-key-based approaches have simple and clean key management [7].

The existing anonymous communication protocols are largely stemmed from mixnet [8]. A mixnet provides anonymity via packet re-shuffling through a set of mix servers (with at least one being trusted). Recently, message sender anonymity based on ring signatures was introduced [9]. This approach enables the message sender to generate a source-anonymous message signature with content authenticity assurance. The original scheme has very limited flexibility and very high complexity. Moreover, the original paper only focuses on the cryptographic algorithm, and the relevant network issues were left unaddressed.

IV. Proposed Source Anonymous Message Authentication (SAMA) Scheme

In this section, we propose an unconditionally secure and efficient source anonymous message authentication scheme (SAMA). Our design enables the SAMA to be verified through a single equation without individually verifying the signatures.

A. Proposed MES Scheme on Elliptic Curves

Let $p > 3$ be an odd prime. An elliptic curve E is defined by an equation of the form:

$$E: \ y^2 = x^3 + ax + b \bmod p,$$

where $a, b \in \mathbb{F}_p$, and $4a^3 + 27b^2 \not\equiv 0 \bmod p$. The set $E(\mathbb{F}_p)$ consists of all points $(x, y) \in \mathbb{F}_p$ on the curve, together with a special point $\mathcal{O}$, called the point at infinity.

Let $G = (x_G, y_G)$ be a base point on $E(\mathbb{F}_p)$ whose order is a very large value N. User A selects a random integer $d_A \in [1, N - 1]$ as his private key. Then, he can compute his public key Q_A from $Q_A = d_A \times G$.

Signature generation algorithm: For Alice to sign a message m, she follows these steps:

1) Select a random integer k_A, $1 \leq k_A \leq N-1$.
2) Calculate $r = x_A \bmod N$, where $(x_A, y_A) = k_A G$. If $r = 0$, go back to step 1.
3) Calculate $h_A \xleftarrow{l} h(m, r)$, where h is a cryptographic hash function, such as SHA-1, and $\xleftarrow{l}$ denotes the l leftmost bits of the hash.
4) Calculate $s = rd_A h_A + k_A \bmod N$. If $s = 0$, go back to step 2.
5) The signature is the pair (r, s).

When computing s, the string h_A that results from $h(m, r)$ shall be converted into an integer. Note that h_A can be greater than N, but not longer.

Signature verification algorithm: For Bob to authenticate Alice's signature, he must have a copy of her public key Q_A, then he:

1) Checks that $Q_A \neq \mathcal{O}$, otherwise it is invalid
2) Checks that Q_A lies on the curve
3) Checks that $nQ_A = \mathcal{O}$

After that, Bob follows these steps to verify the signature:

1) Verify that r and s are integers in $[1, N-1]$. If not, the signature is invalid.
2) Calculate $h_A \xleftarrow{l} h(m, r)$, where h is the same function used in the signature generation.
3) Calculate $(x_1, x_2) = sG - rh_A Q_A \bmod N$.
4) The signature is valid if $r = x_1 \bmod N$, it is invalid otherwise.

B. Proposed SAMA on Elliptic Curves

Suppose that the message sender (say Alice) wishes to transmit a message m anonymously from her network node to any other nodes. The AS includes n members, $A_1, A_2, \cdots, A_n$, e.g., $\mathcal{S} = \{A_1, A_2, \cdots, A_n\}$, where the actual message sender Alice is A_t, for some value $t, 1 \leq t \leq n$. In this paper, we will not distinguish between the node A_i and its public key Q_i. Therefore, we also have $\mathcal{S} = \{Q_1, Q_2, \cdots, Q_n\}$.

Authentication generation algorithm: Suppose that m is a message to be transmitted. The private key of the message sender Alice is $d_t, 1 \leq t \leq N$. To generate an efficient SAMA for message m, Alice performs the following three steps:

1) Select a random and pairwise different k_i for each $1 \leq i \leq n-1, i \neq t$, and compute r_i from $(r_i, y_i) = k_i G$.
2) Choose a random $k_i \in \mathbb{Z}_p$ and compute r_t from $(r_t, y_t) = k_t G - \sum_{i \neq t} r_i h_i Q_i$ such that $r_t \neq 0$ and $r_t \neq r_i$ for any $i \neq t$, where $h_i \xleftarrow{l} h(m, r_i)$.
3) Compute $s = k_t + \sum_{i \neq t} k_i + r_t d_t h_t \bmod N$.

The SAMA of the message m is defined as:

$$\mathcal{S}(m) = (m, \mathcal{S}, r_1, y_1, \cdots, r_n, y_n, s).$$

C. Verification of SAMA

Verification algorithm: For Bob to verify an alleged SAMA $(m, \mathcal{S}, r_1, y_1, \cdots, r_n, y_n, s)$, he must have a copy of the public keys $Q_1, \cdots, Q_n$. Then he:

1) Checks that $Q_i \neq \mathcal{O}, i = 1, \cdots, n$, otherwise it is invalid
2) Checks that $Q_i, i = 1, \cdots, n$ lies on the curve
3) Checks that $nQ_i = \mathcal{O}, i = 1, \cdots, n$

After that, Bob follows these steps:

1) Verify that $r_i, y_i, i = 1, \cdots, n$, and s are integers in $[1, N-1]$. If not, the signature is invalid.
2) Calculate $h_i \xleftarrow{l} h(m, r_i)$, where h is the same function used in the signature generation.
3) Calculate $(x_0, y_0) = sG - \sum_{i=1}^{n} r_i h_i Q_i$.
4) The signature is valid if the first coordinate of $\sum_i (r_i, y_i)$ equals x_0, invalid it is otherwise.

Remark 1. *It is apparent that when $n = 1$, SAMA becomes a simple signature algorithm.*

D. Security Analysis

Theorem 1. *The proposed source-anonymous message authentication scheme (SAMA) can provide unconditional message sender anonymity.*

Theorem 2. *The proposed SAMA is secure against adaptive chosen-message attacks in the random oracle model.*

V. AS Selection and Source Privacy

The appropriate selection of an AS plays a key role in message source privacy since the actual message source node will be hidden in the AS. In this section, we will discuss techniques that can prevent the adversaries from tracking the message source through the AS analysis in combination with the local traffic analysis.

Before a message is transmitted, the message source node selects an AS from the public key list in the SS as its choice. This set should include itself, together with some other nodes. When an adversary receives a message, he can possibly find the direction of the previous hop, or even the real node of the previous hop. However, if the adversary is unable to monitor the traffic of the previous hop, then he will be unable to distinguish whether the previous node is the actual source node or simply a forwarder node. Therefore, the selection of the AS should create sufficient diversity so that it is infeasible for the adversary to find the message source based on the selection of the AS itself.

VI. Performance Analysis

In this section, we will evaluate our proposed authentication scheme through both theoretical analysis and simulation demonstrations. We will compare our proposed scheme with the bivariate polynomial-based symmetric-key scheme described in [2]. *A fair comparison of our proposed scheme and the scheme proposed in [2] should be performed with $n = 1$.*

A. Theoretical Analysis

The secret bivariate polynomial is defined as [1]:

$$f(x,y) = \sum_{i=0}^{d_x} \sum_{j=0}^{d_y} A_{i,j} x^i y^j,$$

where each coefficient $A_{x,y}$ is an element of a finite field $\mathbb{F}_p$, and d_x and d_y are the degrees of this polynomial. d_x and d_y are also related to the message length and the computational complexity of this scheme. From the performance aspect, d_x and d_y should be as short as possible.

On the other hand, it is easy to see that the intruders can recover the polynomial $f(x,y)$ via Lagrange interpolation when either more than $d_y + 1$ messages transmitted from the base station are received and recorded by the intruders, or more than $d_x + 1$ sensor nodes have been compromised, In this case, the security of the system is totally broken and cannot be used anymore. This property requires both d_x and d_y to be very large for the scheme to be resilient to node compromising attack.

An alternative approach based on perturbation of the polynomial was also explored. The main idea is to add a small amount of random noise to the polynomial in the original scheme so that the adversaries will no longer be able to solve the coefficients using Lagrange interpolation. However, this technique is proven to be vulnerable to security attacks [3] since the random noise can be removed from the polynomial using error-correcting techniques.

While hop-by-hop authentication can be achieved through a public-key encryption system, the public-key-based schemes were generally considered as not preferred, mainly due to their high computational overhead. However, our research demonstrates that this is not always true, especially for elliptic curve public-key cryptosystems.

In our scheme, each SAMA contains an AS of n randomly selected nodes that dynamically changes for each message. For $n = 1$, our scheme can provide at least the same security as the bivariate polynomial-based scheme. For $n > 1$, we can provide extra source privacy benefits. Even if one message is corrupted, other messages in the network can still be secure. Therefore, n can be much smaller than the parameters d_x and d_y. In fact, even a small n may provide adequate source privacy while ensuring high system performance.

B. Experimental Results

In this section, we compare the bivariate polynomial-based scheme and our scheme based on comparable security levels.

1) Simulation parameter setup: The bivariate polynomial-based scheme is a symmetric-key-based implementation, while our scheme is based on ECC. This requires us to determine the comparable key sizes. If we choose the key size to be l for the symmetric-key cryptosystem, then the key size for our proposed ECC will be $2l$, which is much shorter than the traditional public-key cryptosystem. This progress facilitates the implementation of the authentication scheme using ECC.

In our simulation setting, we choose five security levels, which are indicated by the symmetric-key sizes l: 24bit, 32bit, 40bit, 64bit, and 80bit, respectively. The comparable key sizes of our scheme are 48bit, 64bit, 80bit, 128bit, and 160bit, respectively.

We also need to determine d_x and d_y for the bivariate polynomial-based scheme, and the n for our scheme. In our simulation, we select d_x equal d_y and choose three values for them: 80, 100, and 150. We assume that WSNs do not contain more than 2^{16} nodes in our simulation, which is reasonably large. For size n of the AS, we choose three values in the simulation: 10, 15, and 20.

2) Computational overhead: For a public-key based authentication scheme, computational overhead is one of the most important performance measurements. Thus we first conducted simulation to measure the process time. The simulations were carried out in 16-bit, 4 MHz TelosB mote.

Table I shows the process time of our scheme and the bivariate polynomial-based scheme for both authentication generation and verification. In the simulations, we assume that the key length of our scheme is $2l$.

3) Communication overhead and message transmission delay: The communication overhead is determined by the message length. For the bivariate polynomial-based scheme, each message is transmitted in the form of $< m, MAF_m(y) >$, where $MAF_m(y)$ is defined as: $MAF_m(y) = f(h(m), y) = \sum_{j=0}^{d_y} M_j y^j$. $MAF_m(y)$ is represented by its $d_y + 1$ coefficients, $M_i, \in \mathbb{Z}_p, 0 \leq i \leq d_y$, where $p \in (2^{l-1}, 2^l)$ is a large prime number. The total length of the message is $l(d_y + 1)$.

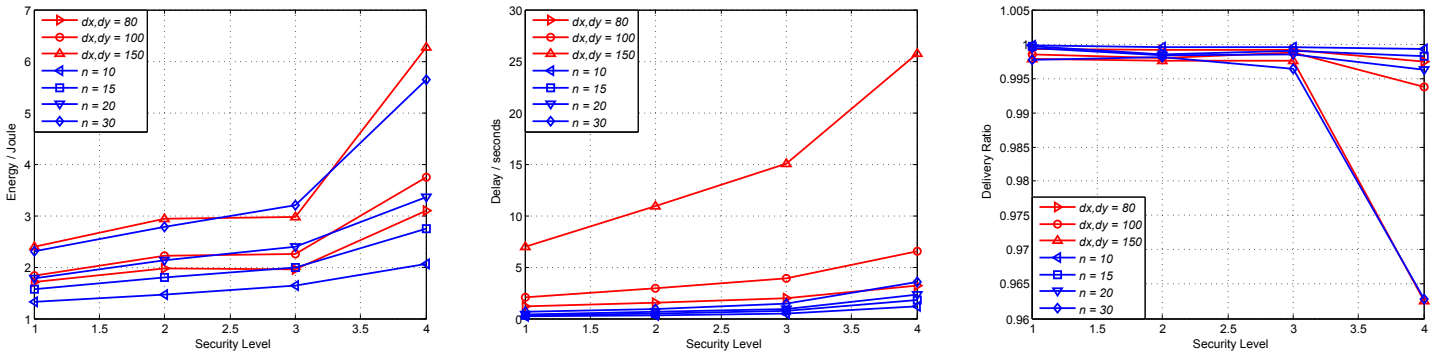
For our scheme, assuming that the network is composed of λ nodes in total, each ID will be of the length: $\lceil \log_2 \lambda \rceil$. When n nodes are included in the AS, the length of $\mathcal{S}$ is $n\lceil \log_2 \lambda \rceil$. Therefore, the total length of one message for our scheme is: $4l(n+1) + n\lceil \log_2 \lambda \rceil$.

4) Simulation results: The simulation results, carried out in ns-2 on a RedHat Linux system, demonstrate that our proposed scheme has a much lower energy consumption and message transmission delay; see Fig. 1(a)&(b). The security levels 1, 2, 3, 4 correspond to symmetric key sizes 24bit, 32bit, 40bit, 64bit, and elliptic curves key sizes 48bit, 64bit, 80bit, 128bit, respectively.

Our simulations also show that the delivery ratio of our scheme is slightly better than the bivariate polynomial-based scheme; see Fig. 1(c). Our simulation on memory consumption derived in TelosB, see Table II, shows that the overall memory consumption for the bivariate polynomial-based scheme is at least 5 times larger than our proposed scheme.

VII. Conclusion

In this paper, we first proposed a novel and efficient source anonymous message authentication scheme (SAMA) based on elliptic curve cryptography (ECC). While ensuring message sender privacy, SAMA can be applied to any messages to provide hop-by-hop message content authenticity without the weakness of the built-in threshold of the polynomial-based scheme. Both theoretical and simulation results, conducted using ns-2 and TelosB, show that, in comparable scenarios,



(a) (b) (c)

Fig. 1. Performance comparison of our proposed scheme and bivariate polynomial-based scheme: (a) energy consumption, (b) message delay, (c) delivery ratio

TABLE I. PROCESS TIME (S) FOR THE TWO SCHEMES (16-BIT, 4 MHZ TELOSB MOTE)

	POLYNOMIAL BASED APPROACH						PROPOSED APPROACH							
	$d_x, d_y = 80$		$d_x, d_y = 100$		$d_x, d_y = 150$		$n = 1$		$n = 10$		$n = 15$		$n = 20$	
	GEN	VERIFY	GEN	VERIFY	GEN	VERIFY	GEN	VERIFY	GEN	VERIFY	GEN	VERIFY	GEN	VERIFY
$l = 24$	9.31	0.25	14.45	0.31	31.95	0.46	0.24	0.53	4.24	2.39	6.16	3.51	8.38	4.44
$l = 32$	12.95	0.33	20.05	0.41	44.60	0.62	0.34	0.80	5.99	3.32	8.92	5.05	12.19	6.42
$l = 40$	13.32	0.35	20.57	0.44	45.73	0.65	0.46	1.05	8.03	4.44	11.94	6.71	16.18	8.50
$l = 64$	21.75	0.57	33.64	0.71	74.85	1.06	1.18	1.77	20.53	11.03	30.12	16.41	41.44	21.10
$l = 80$	26.40	0.70	41.03	0.88	90.86	1.30	1.46	2.22	25.58	13.90	37.66	20.96	50.96	26.18

TABLE II. MEMORY (KB) AND TIME (S) CONSUMPTION FOR THE TWO SCHEMES (TELOSB) (F STANDS FOR FLASH MEMORY)

	POLYNOMIAL BASED APPROACH									PROPOSED APPROACH												
	$d_x, d_y = 80$			$d_x, d_y = 100$			$d_x, d_y = 150$			$n = 1$			$n = 10$			$n = 15$			$n = 20$		
	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F	ROM	RAM	F
$l = 24$	21	3	26	21	4	40	26	4	90	21	1	0	21	2	0	21	2	0	21	2	0
$l = 32$	21	4	39	21	5	60	26	6	135	21	2	0	21	2	0	21	2	0	21	2	0
$l = 40$	21	4	39	21	5	60	26	6	135	21	2	0	21	2	0	21	2	0	21	3	0
$l = 64$	21	6	64	21	7	100	26	9	225	21	2	0	22	3	0	22	3	0	22	3	0
$l = 80$	21	7	77	21	8	120	26	10	270	20	2	0	21	3	0	21	3	0	21	4	0

our proposed scheme is more efficient than the bivariate polynomial-based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

ACKNOWLEDGEMENTS

This research was partially supported by the NSF under grants CNS-0845812, CNS-1050326 and CND-1117831.

REFERENCES

[1] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Advances in Cryptology - Crypto'92*, Lecture Notes in Computer Science Volume 740, pp. 471–486, 1992.

[2] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromise-resilient message authentication in sensor networks," in *IEEE INFOCOM*, (Phoenix, AZ.), April 15-17 2008.

[3] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on "perturbation polynomials"." Cryptology ePrint Archive, Report 2009/098, 2009. http://eprint.iacr.org/.

[4] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Advances in Cryptology - EUROCRYPT*, Lecture Notes in Computer Science Volume 1070, pp. 387–398, 1996.

[5] L. Harn and Y. Xu, "Design of generalized ElGamal type digital signature schemes based on discret logarithm," *Electronics Letters*, vol. 30, no. 24, pp. 2025–2026, 1994.

[6] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem," in *Advances in Cryptology - EUROCRYPT*, Lecture Notes in Computer Science Volume 950, pp. 182–193, 1995.

[7] H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control," in *IEEE ICDCS*, (Beijing, China), pp. 11–18, 2008.

[8] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, pp. 84–88, February 1981.

[9] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology–ASIACRYPT*, Lecture Notes in Computer Science, vol 2248/2001, Springer Berlin / Heidelberg, 2001.