International Journal of Pure and Applied Mathematics
Volume 100 No. 4 2015, 531-542
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v100i4.12

PRACTICAL DEPLOYMENT OF ONE-PASS KEY ESTABLISHMENT PROTOCOL ON WIRELESS SENSOR NETWORKS

Manoj Ranjan Mishra[1], Jayaprakash Kar[2] §, Banshidhar Majhi[3]

[1]School of Computer Application
KIIT University
Bhubaneswar, INDIA

[2]Information Security Research Group
Department of Information Systems
Faculty of Computing & Information Technology
King Abdulaziz University
KINGDOM OF SAUDI ARABIA

[3]Department of Computer Science & Engineering
National Institute of Technology
Rourkela, INDIA

Abstract: Implementation and viability of Pairing-based cryptographic protocol for wireless sensor network is a challenging task to research community. Recently we have proposed an efficient One-pass Key Authentication protocol for wireless sensor network in random oracle model where we have presented pairing algorithm which is suited to implement for our protocol. The main difficulty of pairing based protocol is the incredible hardware and software constraint. In this paper, we suggest practical deployments of pairing on sensor nodes of the proposed protocol. These include the hardware architecture and various micro pairing implementation issues on wireless sensor networks. In this paper, we present the practical deployment of Micro-pairings on sensor nodes and hardware architecture of our proposed protocol.

Key Words: micro-pairing, Montgomery, endomorphism

Received: February 29, 2015

§Correspondence author

1. Introduction

Pairing based cryptography is an promising area in modern cryptography which is firmly associated to Elliptic Curve Cryptography. It is a very challenging task to implement complex cryptographic operations like pairing on tiny and constrained devices. Pairing-based protocol is the emerging in Public Key Cryptography schemes but to perform the complex operations in a limited amount of time on sensor node is very important to research community. Computing the bilinear mapping Weil or Tate pairing on elliptic curve is very essential for cryptographic protocols. $e(P, Q)$ denotes the Tate pairing, where P and Q are any two points on elliptic curve $E(\mathbb{F}_{q^k})$. We briefs various algorithms for Tate pairing on embedded devices.

Many authors [12], [14] have presented implementations issues of pairing based protocols for WSNs. However, they do not specify the real practical deployment of pairings on sensor nodes. Oliveira et al. in [12] described the software implementation of pairings by TinyTate used TinyECC as the underlying library and targeted the MICAz mote. To improve the implementations of various pairing algorithms for wide range of sensor platforms micro-pairing is adopted. This results in the diversity in pairings types and to achieve high level of security. The key design for embedded systems is the optimization of operations of pairing, arithmetic routines and domain parameters.

2. Preliminaries

2.1. Pairing Types

The properties of pairing depends on the selected groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$. Generally pairings is of three types depending three basic groups.

- `Type-1`: Here $\mathbb{G}_1 = \mathbb{G}_2$.
- `Type-2`: Pairing where $\mathbb{G}_1 \neq \mathbb{G}_2$, $\exists$ homomorphism $\phi : \mathbb{G}_2 \to \mathbb{G}_1$ can computes efficiently.
- `Type-3`:Pairing where $\mathbb{G}_1 \neq \mathbb{G}_2$, $\not\exists$ an efficiently computable homomorphism $\phi : \mathbb{G}_2 \to \mathbb{G}_1$

2.2. Security Parameters

The protocol works on two adjacent nodes i and j. We consider pairing type-I, II and III. Level of security in pairing-based protocol depend on degree k, size of the underline finite field F_q and size of the group r.

The chosen security parameters k, r and q satisfy the following security requirements.

- Order of the group r should be very large. So that it is computationally infeasible to solve Elliptic Curve Discrete Logarithm Problem(ECDLP) in subgroup of order r of $E(F_q)$.
- k the embedding degree should be sufficiently large so that it is computationally infeasible to solve Discrete Logarithm Problem in $\mathbb{F}_{q^k}$.

In our proposed protocol, We consider pairing type-I, II and III. Level of security in pairing-based protocol depend on the value of the embedding degree k, size of the underline finite field F_q and size of the group r.

The chosen security parameters k, r and q satisfy the following security requirements.

- In order to make security strong using ECDLP, order of the group should be large enough. So solving ECDLP problem in an order r subgroup of $\mathbb{F}_{q^k}$ applying algorithm such as Pollard's ρ algorithm is computationally infeasible.
- The embedding degree k should be sufficiently large so that solving the DLP in $\mathbb{F}_{q^k}$ is computationally infeasible apply algorithm such as index-calculus method.

In cryptanalysis, if we take order $r =$ 160 bit prime, the number of steps need to solve ECDLP is 2^{80}. Over the extension field, it need 2^{80} steps for any DLP, if we select $k \cdot log_2 q \equiv 1024$. This values for the three parameters r, k and q is equivalent to 80-bit level of security in Symmetric Key cryptosystem like AES or DES. The following table summarizes the comparison of key sizes in pairing-based cryptography.

3. Our Proposed One-Pass Key Establishment Protocol

The following table we summarize our proposed protocol [3]. To generate the session key SK_{ij} in node i, we need to compute the following pairing operation.

Execution Time	Size of ROM(KB)	size of RAM(KB)
30.21s	18.384	1.831

Table 1: Performance evaluation of TinyTate on MICAz

$$SK_{ij} = \hat{e}((\lambda + h)S_i, Q_j)$$

Similarly the following three pairing operations are required to compute the session key SK_{ij} in node j.

- $\hat{e}(U, W)$
- $\hat{e}(S_i, V)$
- $\hat{e}(U + hQ_i, S_j)$

4. Practical Deployment

4.1. Tate Pairing on MICAz Sensor Node

To implement Tate pairing on MICAz sensor node that embeds ATmega 128 8-bit CPU, the following parameters are to be considered.

- `Finite Field`: In TinyTate, pairing is evaluated over prime field $\mathbb{F}_p$.
- `Selection of Curve`: Consider super singular curve $y^2 = x^2 + x$ over the prime field $\mathbb{F}_p$.
- `Parameters for Pairing operation`: The security parameters k, q and r to be chosen as $k = 2$, prime $q = 256$ bits and prime $r = 128$ bits. In order to simplify and easy to implement the arithmetic operations are to be performed on $\mathbb{F}_q^k$, value of $k = 2$ allows the elimination of denominator.
- `Projective co-ordinate system`: Since inverse operation is very costly in point addition and doubling operation, we consider projective co-ordinate system.

Following table summarizes the evaluation on performance of TinyTate.

1. **Setup** : Given security parameters k, the KGC chooses groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q.
   A generator P of $\mathbb{G}$, a bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ and collision resistant hash function
   $\mathcal{H}_1 : \{0,1\}^* \to \mathbb{G}$, $\mathcal{H}_2 : \mathbb{G} \times \{0,1,\}^* \to \mathbb{F}_q^*$, $\mathcal{H}_3 : \mathbb{G} \to \mathbb{F}_q^*$.
   It chooses a master-key $s \in \mathbb{F}_q^*$ and computes $P_{pub} = sP$.
   The KGC publishes the system public parameters $params = <\mathbb{G}, \mathbb{G}_T, \hat{e}, q, p, P_{pub}, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3>$.
2. **Extract** : KGC takes the input the identities ID_i and ID_j of node i and j respectively
   and runs the algorithm and Computes the private keys as $S_i = s \cdot Q_i$ and $S_j = s \cdot Q_j$
   of the node i and j respectively. $Q_i = \mathcal{H}_1(ID_i)$ and $Q_j = \mathcal{H}_1(ID_j)$.
   (Where Public key of node i and j are Q_i and Q_j respectively.
3. **Protocol**: The protocol involves by considering two arbitrary nodes i and j

Node i		**Node** j
Chooses randomly $\lambda \in \mathbb{Z}_q^*$ and computes $U = \lambda \cdot Q_i$.		
Computes $\mathcal{H}_2(U, ID_i \| ID_j) = \Gamma$ and $h = \mathcal{H}_3(\Gamma)$.		
$SK_{ij} = \hat{e}((\lambda + h)S_i, Q_j)$		
Computes $V = \lambda \cdot \Gamma$.		
	(U, V) $\longrightarrow$	
		Computes $\Gamma = \mathcal{H}_2(U, ID_i \| ID_j)$, $h = \mathcal{H}_3(Q)$
		Computes $W = s \cdot \Gamma$
		and Verify $\hat{e}(U, W) \stackrel{?}{=} \hat{(}S_i, V)$.
		Computes $SK_{ji} = \hat{e}(U + hQ_i, S_j)$

Figure 1: Proposed One-Pass Protocol

5. Overviews on Micro-Pairings

For low processor devices, implementation of pairing on sensor node is too heavy weights in pairing based cryptography. However the articles [12] [14] have proposed cryptographic protocols using pairing based cryptography for secure communication in sensor networks. It is an challenge to implements such protocols in low cost and faster processing time. Hence we briefs about Micro-pairings which is an powerful and efficient implementation of different pairing types on

Symmetric Key Size	Size of group(r)	$\mathbb{F}_{q^k}(k \cdot log_2 q)$ $\mathbb{F}_{q^k}(k \cdot log_2 q)$	Embedding degree(k)
80	160	$960 - 1280$	$2 - 8$
128	256	$3000 - 5000$	$12 - 18$
256	512	$12000 - 18000$	$24 - 36$

Table 2: Comparison of key-size in bit

a wide range of sensor platforms. Pairing based cryptographic protocol for embedded devices, micro-pairing has been designed to make practical for implementation. The software packages consists of sensor nodes MICA2/MICAz, Tmote Sky and Imote2. The evaluation of micro-pairings shows that, pairings having full-size security parameters are feasible on various hardware platforms. It has been examined that particular pairings can be computed faster and efficiently on tiny and constrained devices such as Tmote Sky or WICA2.

The objective of micro-pairing is to make high-speed implementations of various pairing algorithms for a wide range of sensor platforms. The prime design choices are to make the level of security high and faster in computation in low computational time. The following table shows 80-bit security level of implementation. It is important to find the optimal combination of domain parameters, pairing type and arithmetic routines which provides the efficient pairing performance on embedded device. The Efficient implementation of pairings algorithms and the arithmetics operation over prime field $\mathbb{F}_p$ and binary filed $\mathbb{F}(2^m$ provides high performance of Micro-pairings. We have followed the implementation of pairing presented in MIRACIL [15] library. This specifies all the prime tools to perform arithmetic operations on elliptic curve. The memory allocation in micro-pairing can be used from stack. Therefore entire memory of RAM can be re-utilized for multiple areas after the completion of the pairing operation. MIRACL library can be embedded on 8, 16 and 32-bit architectures.

5.1. Pairing Algorithms

The most efficiently computable pairings are Weil and Tate pairing on elliptic curve. Efficiency of Tate pairing is more Weil pairing. We consider `Type-1` pairing on super singular elliptic curve in our proposed protocol. Tate pairing is the bilinear mapping $\hat{e}(P, Q)$, where P and Q are two arbitrary linearly independent points on an elliptic curve $\mathbb{E}(\mathbb{F}_q^k)$, evaluates as an element of extension

field $\mathbb{F}_{q^k}$. If P is of prime order r, then the pairing is evaluated as an order of r. We can apply algorithm-1 to compute the Tate pairing for implementation in more efficient way in term of memory space, bandwidth and processing speed [13].

We consider the following elements for implementation of pairing

- As we have discussed `Type-1` pairings is more suitable on super singular curves, these curves can be divided into three sub-classes curves over binary fields as $q = 2^m$ with $k = 4$, curves over field of large prime characteristics 3 *i.e* $q = 3^m$ with $k = 6$ and curves over field of large prime characteristics $q = p, p > 3$ with $k = 2$. The most suitable curve for implementation on 8-bit processor is curves over filed of prime characteristics is $k = 4$.
- The binary field $\mathbb{F}_{2^{271}}$ can be chosen to achieve the security.
- Super singular curve is
$$y^2 + y = x^3 + x \tag{1}$$
The number of points on the curves is $2^{271} + 2^{136} + 1 = 487805.r$. Where r is a large prime.

The following table summarizes the cost of $\eta_T(P, Q)$ on $y^2 + y = x^3 + x$. For

Execution	$\|Mul\|$	$\|Sqrs\|$	$\|Sqrt\|$
Main loop	1904	544	544
Final loop	114	139	0

Table 3: cost of $\eta_T(P, Q)$ on $y^2 + y = x^3 + x$

MNT curve take $k = 4$ the algorithm to compute $e(P, Q)$ with Tate pairing is given below

6. Operation in Prime Field

While computing $e(P, Q)$, the most costly and the modular multiplication consumes more time as compare to modular addition and subtraction [9] [11]. Since modular inverse operation is most expensive, we can use projective co-ordinate system [10]. The improved hybrid method can be used for large integer multiplication and squaring. Stack is used for the memory for the variables that are used in the operations.

Algorithm 1: Computation of $\eta_T(P,Q)$ on $y^2 + y = x^3 + x + b$ curve over $\mathbb{F}_{2^m}$

Input P, Q
Output $\eta_T(P,Q)$
$P \leftarrow (x_P, y_P), Q = (x_Q, y_Q)$
$\theta \leftarrow x_P + 1$
$\sigma_1 \leftarrow \theta \cdot (x_P + x_Q + 1) + y_P + y_Q + 1 + (\theta + x_Q)u + v$
for $i = 1$ to $(m+1)/2$ **do**
  $\theta \leftarrow x_P, x_P \leftarrow \sqrt{x_P}, y_P \leftarrow \sqrt{y_P}$
  $\sigma_2 = \theta \cdot (x_P + x_Q) + y_P + y_Q + x_P + (\theta + x_Q)u + v$
  $\sigma_1 \leftarrow \sigma_1 \cdot \sigma_2$
  $x_Q \leftarrow x_Q^2$, $y_Q \leftarrow y_Q^2$
end for
return $\sigma_1^{(2^{2m}-1)(2^m - 2^{(m+1)/2+1})}$

Algorithm 2: Computation of $e(P,Q)$ with Tate Pairing

Input $Q \in E'(\mathbb{F}_{p^2}, P \in E(\mathbb{E}_p), \delta$
Output $e(P,Q)$
$T \leftarrow P, f \leftarrow 1$
$s \leftarrow \lfloor log_2(r-1) \rfloor$
for $i = 1$ to $(s-1)$ **do**
  $f \leftarrow f^2 \cdot l_T, T(Q)$
  $T \leftarrow T + P$
  if $s_i = 1$ **then**
    $f \leftarrow f \cdot l_T, P(Q)$
    $T \leftarrow T + P$
  end if
end for
$f \leftarrow f^{(p^2-1)}$
$f \leftarrow f^{34}$
$f \leftarrow f^p \cdot f^\delta$
return f

	Atmega128			MSP430			PXA271		
	mul	add	inv	mul	add	inv	mul	add	inv
Operation									
Assembly	7547	404	364291	4734	386	229724	843	155	49223
C code	22493	596	419812	11148	533	269768	1463	200	53318
Decrease	66 %	32 %	13 %	57 %	27 %	15 %	42 %	22 %	8 %

Table 4: Timing in clock cycle for modular arithmetics in $\mathbb{F}_p$ using 160-bit integer

Execution	$\|mul\|$	$\|add\|$	$\|inv\|$
Main loop	5730	15006	2
Final loop	571	2642	1

Table 5: Computational Cost for MNT $k = 4$

Let the extension field is $\mathbb{F}_{p^k}$. The Tate pairing computes as an element of this field. The function for the operation exponent, multiplication, addition and inversion in $\mathbb{F}^{\not\vdash}$ is to be constructed. The overall cost of Tate pairing is summarized in table-5. For different embedded processor, table-4 summarizes the overall results for the evaluation of Tate pairing.

The Ate pairing is implemented on Atmega128 and MSP430 processor [16]. The algorithm is given below. Performance of Ate pairing on Atmega128 and MSP430 are summerized in the following table.

7. Conclusion

In this article we have presented the pairing algorithms include Tate pairing and Ate pairing that compute $e(P, Q)$ for our proposed one-pass key establishment protocol. The algorithms are most suited to implement on wireless sensor networks. Also we have described the hardware architecture and micro pairing implementation issues on wireless sensor networks. We shows the evaluation of micro-pairings where pairings of full-size security parameters are feasible on

Algorithm 3: Computation of $e(P,Q)$ with Ate Pairing

Input $P \in E'(\mathbb{F}_{p^d}, Q \in E(\mathbb{E}_p)$,$t$ is the trace of Frobenius
Output $e(P,Q)$
$T \leftarrow P, f \leftarrow 1$
$s \leftarrow \lfloor log_2(t-1) \rfloor$
for $i = 1$ to $(s-1)$ **do**
  $f \leftarrow f^2 \cdot l_T, T(Q)$
  $T \leftarrow T + P$
  if $s_i = 1$ **then**
    $f \leftarrow f \cdot l_T, P(Q)$
    $T \leftarrow T + P$
  end if
end for
$f \leftarrow f^{(p^d-1)}$
$f \leftarrow \frac{f^{(p^d+1)}}{\phi_k(p)}$
$f \leftarrow \frac{f^{\phi_k(p)}}{r}$
return f

	Atmega128			MSP430	
Cycles	ROM	Stack	Cycles	ROM	Stack
132,373,604	71.9KB	2.5KB	96,829,440	47.0KB	3.0KB

Table 6: Performance of Ate pairing on Atmega128 and MSP430

various hardware platforms.

References

[1] A. Menzes, T. Okamoto, and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transactions on Information Theory, 39, pp. 1639–1646, 1993.

[2] R. Sakai, K. Ohgishi, and M. Kasahara, Cryptosystems based on pairing. Symposium on Cryptography and Information Security, Okinawa, Japan, 2000.

[3] M. R. Mishra, J.Kar and B.Majhi, One-Pass Authenticated Key Establishment Protocol on Bilinear Pairing for Wireless Sensor Networks" IEEE International Conference on Privacy and Security in Mobile Systems (PRISMS14), 2014.

[4] D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, 2004.

[5] V.S. Miller, Use of elliptic curves in cryptography, in: Proceedings of the Advances in Cryptology - Crypto'85, New York, USA, 1985, pp. 417-426.

[6] N. Koblitz, Elliptic curve cryptosystem, Mathematics of Computation 48 (1987), 203-209.

[7] N. Koblitz. *A course in Number Theory and Cryptography , 2nd edition* Springer-Verlag-1994

[8] A. Menezes, P. C Van Oorschot and S. A Vanstone, *Handbook of applied cryptography. CRC Press, 1997.*

[9] J.Kar, Authenticated Multiple-Key Establishment Protocol for Wireless Sensor Networks, "Case Studies in Secure Computing Achievements and Trends", CRC Press, Taylor and Francis (New York), Chapter-04, Pages 67-88, 2014.

[10] P. Motontgomery, Modular multiplication without division, Mathematics of Computation, 44, pp. 519-521, 1985.

[11] J.Kar, A Novel Construction of Certificateless Signcryption Scheme for Smart Card, "Case Studies in Secure Computing Achievements and Trends", CRC Press, Taylor and Francis (New York), Chapter-22, Pages 437-456, 2014.

[12] B. Doyle, S. Bell, A. F. Smeaton, K. Mccusker and N. O.Connor, Security considerations and key negotiation techniques for power constrained sensor networks, The Computer Journal, Oxford University Press, 49, pp. 443-453, 2006.

[13] J Kar, "Provably Secure Online/Off-line Identity-Based Signature Scheme for Wireless Sensor Network" International Journal of Network Security, Taiwan, Vol.16 (01), PP.26-36, Jan. 2014.

[14] L. B. Oliveira, R. Dahab, J. Lopez, F. Daguano and A. A. F.Loureiro, Identity-based encryption for sensor networks, in 5th IEEE International Conference on Pervasive Computing and Communications Workshops PERCOMW07, pp. 290-294, 2007.

[15] M. Scott, MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library, http://www.shamus, 2009.

[16] F. Hess, N. Smart and F. Vercauteern, The Eta pairing revisited, IEEE Transactions on Information Theory, 52 (2006). http://eprint.iacr.org/2006/110.